Mathematisch-
Naturwissenschaftliche
Bibliothek

13

L. HOLZER

ZAHLENTHEORIE

TEIL I

MATHEMATISCH-NATURWISSENSCHAFTLICHE
BIBLIOTHEK

13

ZAHLENTHEORIE

TEIL I

Von Professor Dr. LUDWIG HOLZER
Direktor des Mathematischen Instituts
an der Universität Rostock

B.G.TEUBNER VERLAGSGESELLSCHAFT · LEIPZIG
1 9 5 8

Liz.-Nr. 294/375/43/58

Printed in Germany

Satz und Druck: (III/18/154) B.G.Teubner, Leipzig C 1, Querstraße 17 · 388

VORWORT

Der vorliegende erste Teil des auf zwei Teile veranschlagten Buches Zahlentheorie ist so gedacht, daß er das Wichtigste aus der elementaren Zahlentheorie und der Theorie der Zahlkörper enthalten soll.

Die umfassenden Erweiterungen, die die moderne Algebra seit etwa dreißig Jahren erfahren hat und die einen durchaus sachgemäßen Aufbau dieser Disziplin erfordern, haben mir die Frage nahegelegt, ob nicht auch die verwandten Disziplinen der Mathematik weitgehend verallgemeinert und systematisiert werden können. Dementsprechend ist in diesem Buche die Zahlentheorie auf der modernen Algebra aufgebaut, aus der nur ganz einfache Sätze verwendet werden, und zwar die wichtigsten Sätze über Körper und Gruppen, Dinge, die man auch in der gegenwärtigen Zeit, wo die moderne Algebra immer mehr eine Schlüsselstellung einnimmt, nicht als allgemein bekannt voraussetzen kann, z. B. die Theorie der Galoisfelder werden entwickelt, doch geschieht dies nur so weit, als es unbedingt erforderlich ist.

Eben diese Theorie wurde dahin angewandt, daß das Fundamentaltheorem der elementaren Zahlentheorie, das quadratische Reziprozitätsgesetz, auf ganz neue Weise, fast ohne Rechnungen hergeleitet werden konnte, allerdings durch eine Folge von Schlüssen. Dieser Beweis ist meines Wissens noch nirgends so konsequent durchgeführt.

Die wahre Quelle dieses Gesetzes zu erschließen ist außerordentlich schwer. *Hecke* sah sie in seinen Theta-Reihen, *Hilbert* in tiefliegenden Sätzen des Kreisteilungskörpers. Ich kann nur sagen: Das Gesetz besteht, man kann es auf den verschiedensten Wegen zu erreichen trachten, aber alle Wege sind Umwege, ein direkter Weg ist kaum ersichtlich.

Der letzte Abschnitt umfaßt die Theorie der Zahlkörper in ihren Grundzügen. Es wurden nur Sätze berücksichtigt, die auf dem Idealbegriff beruhen und sich zwanglos ableiten lassen. Weitere Sätze, z. B. die über die Diskriminantenteiler, werden erst

im zweiten Teil erscheinen, da deren Ableitung ohne die Hilbertsche Theorie des Galoischen Körpers äußerst erzwungen zu sein scheint.
Beispiele zum Selbstrechnen wurden nur wenig angeführt, da neuerdings das Werk von *Winogradow*, Zahlentheorie, mit sehr vielen, allerdings schweren Beispielen in Übersetzung vorliegt.
Für die Mitarbeit bin ich meinem Assistenten, Herrn Dr. *Rühs*, meinem Oberassistenten, Herrn Dr. *Schröder*, sowie meinem Assistentenehepaar M. und I. *Bütow* zu Dank verpflichtet,

Rostock, im Frühjahr 1958

L. Holzer

INHALTSVERZEICHNIS

A. Grundbegriffe

B. Das quadratische Reziprozitätsgesetz

C. Theorie der algebraischen Körper

A. GRUNDBEGRIFFE

§ 1. Vorläufige Bemerkungen

Ganze Zahlen heißen *Primzahlen,* wenn sie nur durch ± 1, sich selbst und ihrem entgegengesetzten Wert teilbar und von ± 1 verschieden sind; ± 1 pflegen wir nicht zu den Primzahlen zu rechnen.

Primzahlen sind also z. B. 2, 3, 5, 31, 113, 6857, ..., auch -3, -7.

Wird nicht ausdrücklich das Gegenteil betont, so sollen die Primzahlen stets positiv angenommen werden.

Die Schreibweise $a \mid b$ bedeutet: *a ist Teiler von b* oder *a geht auf in b,* d. h., $b = ac$ mit ganzzahligem c; b heißt dann ein Vielfaches von a.

$a \nmid b$ (a teilt nicht b) heißt: a ist kein Teiler von b in diesem Sinne. Dies gilt auch für gebrochene a; es ist also z. B.

$$5 \mid 25, \quad -3 \mid 21, \quad \tfrac{1}{2} \mid 1, \quad \tfrac{2}{3} \mid \tfrac{8}{3}, \quad -\tfrac{1}{6} \mid \tfrac{1}{3}.$$

Die Zahl $a = 0$ wollen wir als Teiler ausschließen.

Sind a und b ganzzahlig und gilt $a + b \neq 0$, so ist $a + b \mid a^2 - b^2$.

Satz 1. *Ist* $a \mid b$, $b \mid c$, *so ist* $a \mid c$.

Beweis: Klar.

Satz 2. *Ist* $a \mid b$, $1 < a < b$, *so ist b keine Primzahl.*

Beweis: Klar.

Satz 3. *Eine natürliche Zahl kann nur endlich viele natürliche Teiler haben.*

Beweis: Jeder natürliche Teiler d erfüllt die Ungleichung $1 \leqq d \leqq n$.

Satz 4. *Zu zwei natürlichen Zahlen gibt es einen größten gemeinsamen Teiler D, auch größtes gemeinsames Maß genannt, abgekürzt g.g.T.*

Wir schreiben $D = (a, b) =$ g.g.T. von a, b und dehnen diese Bezeichnung auch auf mehrere Zahlen aus: $D = (a_1, a_2, \ldots, a_n) =$ g.g.T. von $a_1, a_2, \ldots, a_n$.

Der Beweis ergibt sich nicht ganz leicht.

So klar der Satz 4 ist, so ist durchaus nicht selbstverständlich, daß jeder gemeinsame Teiler d der Zahlen $a_1, a_2, \ldots, a_n$ die Beziehung $d \mid D$ erfüllt.

Um fortwährende Wiederholungen zu vermeiden, bedienen wir uns bei der Beweisführung der abkürzenden Bezeichnung $\Gamma(A, B, C)$; sie soll bedeuten: die diophantische Gleichung $Ax + By = C$ hat Lösungen, d. h., es gibt ganze Zahlen x, y mit $Ax + By = C$ oder, geometrisch gesprochen, die Gerade $Ax + By = C$ geht durch einen Gitterpunkt (Punkt mit ganzzahligen Koordinaten in der Ebene).

Hilfssatz. *Aus $\Gamma(A, B, C)$ und $\Gamma(A, B, C')$ folgt $\Gamma(A, B, Cu + C'v)$, wobei u, v beliebige ganze Zahlen sind.*

Beweis: Gilt mit Gitterpunkten $[\xi, \eta]$, $[\xi', \eta']$ der Reihe nach

$$A\xi + B\eta = C,$$
$$A\xi' + B\eta' = C',$$

so ergeben die Multiplikation der ersten Gleichung mit u, der zweiten mit v und ihre Addition

$$A(\xi u + \xi' v) + B(\eta u + \eta' v) = Cu + C'v,$$

und mit dem Gitterpunkt $[\xi u + \xi' v, \eta u + \eta' v]$ ist

$$\Gamma(A, B, Cu + C'v)$$

erfüllt.

Zur Berechnung des g.g.T. verwendet man das folgende Verfahren.

a, b seien zwei natürliche Zahlen. Mit ganzzahligem q und r_1 folgt

$$a = bq + r_1,$$

$0 \leqq r_1 < b$.

Es bleibt

$$a - bq = r_1$$

und daraus

$$\Gamma(a, b, r_1). \tag{1}$$

Nun können zwei Fälle eintreten:

1. Ist $r_1 = 0$, so sind wir fertig, und der g.g.T. ist b.
2. Ist $r_1 > 0$, so dividieren wir b durch r_1:

$$b = q_1 r_1 + r_2 \quad \text{mit} \quad 0 \leqq r_2 < r_1. \tag{2}$$

Wegen (1), (2) und der trivialen Beziehung $\Gamma(a, b, b)$ gilt nach dem Hilfssatz

$$\Gamma(a, b, r_2). \tag{3}$$

Dieses Verfahren setzen wir fort. r_i sei schon berechnet und damit

$$\Gamma(a, b, r_{i-1}),$$
$$\Gamma(a, b, r_i)$$

bewiesen. Haben wir dann

$$r_{i-1} = q_i r_i + r_{i+1}$$

mit $$0 \leqq r_{i+1} < r_i,$$

so ist auch $$\Gamma(a, b, r_{i+1}).$$

Da die eigentlich abnehmende Folge natürlicher Zahlen

$$a > b > r_1 > r_2 > \ldots$$

schließlich abbrechen muß, ist endlich

$$r_{n-1} = q_n r_n$$

und

$$\Gamma(a, b, r_n).$$

Also gibt es ganze Zahlen x, y, mit

$$ax + by = D, \tag{4}$$

wenn $r_n = D$ gesetzt wird.

Wir werden sehen, daß D die obenerwähnten Eigenschaften des g.g.T. hat.

Zunächst gilt wegen

$$D \mid r_{n-1}$$

und

$$r_{n-2} = q_{n-1} r_{n-1} + D$$

sofort

$$D \mid r_{n-2}.$$

Wegen
$$r_{n-3} = q_{n-2} r_{n-2} + r_{n-1}$$
gilt
$$D \mid r_{n-3}, \quad \text{usf.}$$

Wegen $D \mid r_1$, $D \mid b$ und (1) folgt
$$D \mid a.$$

D ist mithin ein gemeinsamer Teiler von a und b.
Nun sei d ein beliebiger gemeinsamer Teiler von a und b, und zwar — dies ist keine Einschränkung der Allgemeinheit — speziell $d > 0$. Mit a' und b' als ganzen Zahlen gilt dann
$$a = d a', \tag{5}$$
$$b = d b', \tag{6}$$
und durch Einsetzen von (5) und (6) in (4) ergibt sich
$$d(a' x + b' y) = D,$$
also
$$d \mid D. \tag{7}$$
(7) zeigt auch $d \leqq D$. Damit ist die Bezeichnung größter gemeinsamer Teiler gerechtfertigt.
Es gilt somit unter Berücksichtigung von (4)

Satz 5. *Den g.g.T. $D = (a, b)$ zweier natürlicher Zahlen findet man durch das obige Verfahren, jeder gemeinsame Teiler von a, b teilt D, und*
$$ax + by = D$$
ist ganzzahlig lösbar.

Die Zahlen $a_1 = \frac{a}{D}$, $b_1 = \frac{b}{D}$ sind also ganz. Sie können keinen gemeinsamen Teiler $X > 1$ haben, sonst wäre $DX \mid a$, $DX \mid b$ und DX ein gemeinsamer Teiler von a und b. Wegen $DX > D$ könnte dann D nicht größter gemeinsamer Teiler sein.
Zwei ganze Zahlen m, n mit $(m, n) = 1$ heißen *teilerfremd* oder *relativ prim*.
Damit kann die eben behandelte Tatsache so ausgesprochen werden:

Satz 6. *Die Division zweier ganzer Zahlen durch ihren g.g.T. gibt zwei relativ prime Zahlen.*

Wir kommen nun zu einem wichtigen

Satz 7. *Gilt $a \mid bc$ und ist $(a, b) = 1$, so ist $a \mid c$.*

Beweis: Mit ganzen Zahlen X, Y, für die $aX + bY = 1$ ist, gilt $a \mid acX + bcY = c$, wie behauptet.
Sind zwei Zahlen gegeben, eine Primzahl p und eine beliebige andere Zahl a, und gilt $p \mid a$, so ist $(a, p) = p$. Gilt $p \nmid a$, so ist $(a, p) = 1$.

Daraus ergeben sich die folgenden beiden Sätze:

Satz 8. *Ist von zwei Zahlen die eine eine Primzahl, die andere nicht durch sie teilbar, so sind die beiden relativ prim.*

Satz 9. *Ist $p \mid ab$, $p \nmid a$, so ist $p \mid b$, oder, eine Primzahl p geht in einem Produkt dann und nur dann auf, wenn sie in mindestens einem Faktor aufgeht.*
Der Satz 9 ist für alle weiteren Darlegungen außerordentlich wichtig.
Wir werfen noch einen Blick auf die diophantische Gleichung

$$ax + by = M \tag{8}$$

mit beliebigem (nicht notwendig positivem) ganzem M.
Leicht ist zu zeigen: Bei $D = (a, b) \mid M$ hat die Gleichung Lösungen. Denn löst $[k, l]$ die Gleichung (4), so löst das ganzzahlige Paar $\left[\frac{Mk}{D}, \frac{Ml}{D}\right]$ die gegebene Gleichung (8).
Ist nun $x = A$, $y = B$ eine Lösung von (8), so ergibt sich durch Subtraktion der Gleichung

$$aA + bB = M$$

von (8) mit den neuen Unbekannten $x' = x - A$, $y' = y - B$ für x', y' die Gleichung

$$ax' + by' = 0$$

oder mit $\frac{a}{D} = a_1$, $\frac{b}{D} = b_1$ (d. h. $(a_1, b_1) = 1$ nach Satz 6) die Gleichung

$$x' : y' = -b_1 : a_1,$$

deren Lösung offenbar $x' = -b_1 T$, $y' = a_1 T$ mit ganzem, sonst beliebigem T ist.
Mithin ist die Gesamtheit der Lösungen von (8)
Wir erhalten

$$x = A - b_1 T,\ y = B + a_1 T. \tag{9}$$

Satz 10. *Bei ganzzahligem a, b, M, $(a, b) \mid M$ hat $ax + by = M$ unendlich viele Lösungen in ganzen Zahlen.*

Nun sei $D \nmid M$. Dann kann (8) auch in der Form

$$a_1 x + b_1 y = \frac{M}{D} \tag{10}$$

geschrieben werden. Hier ist $\frac{M}{D}$ ein eigentlicher Bruch, keine ganze Zahl. $[x, y]$ mit ganzzahligen x und y kann offenbar die Gleichung nicht erfüllen. Also folgt

Satz 11. *Mit a, b, M ganz, M durch (a, b) nicht teilbar, hat die Gleichung $ax + by = M$ keine ganzzahligen Lösungen.*

Die Sätze 10 und 11 gelten auch, wenn a oder b oder beide negativ sind. Man braucht dann nur das Vorzeichen von x bzw. y zu wechseln.

Das in der Einleitung gegebene Verfahren zur Bestimmung des g.g.T. heißt *Euklidischer Algorithmus* oder Kettendivision. Wir fragen, wann es überhaupt auf Bereiche anwendbar ist. Dies ist dann der Fall, wenn man den Elementen des Bereiches natürliche Zahlen wie folgt zuordnen kann: Bei der Division kann man einen Rest angeben, so daß die ihm zugeordnete Zahl kleiner ist als die dem Divisor zugeordnete. Eine solche Zuordnung läßt sich z. B. bei der Division von Polynomen dadurch erreichen, daß man dem Polynom den Grad zuordnet.

Bei den später folgenden Erweiterungen des Bereiches der ganzen Zahlen läßt sich das Verfahren mitunter ebenfalls mit Vorteil anwenden. In unserem Buche kann auf diese Dinge nicht eingegangen werden.

Beispiele

1. Man bestimme (7 5 8 4 7 0 1, 2 1 3 0 2 5 7);
2. Man gebe durch Kettendivision eine Lösung von $23x + 8y = 1$.

§ 2. Das größte Ganze

Das *größte Ganze* einer reellen Zahl α sei durch die ganze Zahl x definiert, für die $x \leqq \alpha < x + 1$ gilt. Wir bezeichnen es mit $[\alpha]$, werden aber die eckige Klammer auch für andere Zwecke benutzen, wenn keine Mißverständnisse zu befürchten sind.

Beispiele

$[2] = 2$, $[\pi] = 3$, $[e] = 2$, $[e + \pi] = 5$, $[-\sqrt{3}] = -2$, $[-\pi] = -4$, $[\sqrt[3]{31} - \pi] = -1$.

In den nun folgenden Übungsbeispielen sollen die griechischen Buchstaben positive Zahlen, die lateinischen natürliche Zahlen bezeichnen.

Man beweise:

1. $[\alpha] + [\beta] \leqq [\alpha + \beta] \leqq [\alpha] + [\beta] + 1$.
2. $[\alpha]\,[\beta] \leqq [\alpha \cdot \beta] \leqq [\alpha]\,[\beta] + [\alpha] + [\beta]$.
3. Für $0 \leqq \alpha < 1$ gilt

$$\left[\frac{x+\alpha}{n}\right] = \left[\frac{x}{n}\right] \quad \left(\text{also } \left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]\right).$$

4. Es ist $[\sqrt{\alpha}] = [\sqrt{[\alpha]}]$.
5. $[\sqrt{n}]^2 \leqq n \leqq [\sqrt{n}]^2 + 2[\sqrt{n}]$.
6. $[\sqrt[3]{n}]^3 \leqq n \leqq [\sqrt[3]{n}]^3 + 3[\sqrt[3]{n}]^2 + 3[\sqrt[3]{n}]$.

7. Die Charakteristik (Kennziffer) des dekadischen Logarithmus ist das größte Ganze desselben (das gilt auch für einen negativen Logarithmus, also für einen Numerus < 1).

8. Mit n wächst die Zahl M der ganzen Zahlen N mit $[\log N] = n$ ins Unendliche; die Basis des Logarithmus ist beliebig, doch größer als eins.

§ 3. Lösung diophantischer Gleichungen in ganzen positiven Zahlen

Wir betrachten die beiden Gleichungen

$$ax + by = M, \tag{1}$$

$$ax - by = M \tag{2}$$

mit natürlichem a, b, M. Die Bedingung $(a, b) = 1$ ist keine Einschränkung der Allgemeinheit, da bei $(a, b) \mid M$ die Kürzung durch (a, b) möglich, bei $(a, b) \nmid M$ aber keine Lösung vorhanden ist. Mithin können vom Vorzeichen abgesehen die Größen a_1, b_1 der Formel (9) in § 1 gleich a, b gesetzt werden.

Besprechen wir zuerst (1). Es bleibt

$$x = A - bT,\ y = B + aT.$$

Wegen $x > 0$ muß $A - bT > 0$, also $T < \left[\frac{A}{b}\right]$ sein. $T > \left[-\frac{B}{a}\right]$ folgt ebenso aus $y > 0$. Da nur endlich viele ganze Zahlen T der Ungleichung $\left[-\frac{B}{a}\right] < T < \left[\frac{A}{b}\right]$ genügen, folgt

Satz 1. *Mit ganzzahligem positivem a, b, M, $(a, b) = 1$ hat $ax + by = M$ nur endlich viele (eventuell keine) Lösungen in ganzen positiven Zahlen. Oder: Auf der Geraden $ax + by = M$ liegen nur endlich viele Gitterpunkte (eventuell keine) im ersten Quadranten.*

Ganz anders verhält sich die Gleichung (2), aus der sich nach Formel (9) von § 1

$$x = A + bT, \quad y = B + aT$$

ergibt. Ist $T > \max\left\{\left[-\frac{A}{b}\right], \left[-\frac{B}{a}\right]\right\}$, so ist $x > 0$, $y > 0$, und es gilt

Satz 2. *$ax - by = M$ mit ganzzahligem, positivem a, b, M, $(a, b) = 1$ hat unendlich viele Lösungen in ganzen positiven Zahlen.*

Trivialerweise hat $ax + by = -M$ mit ganzem und positivem a, b, M keine Lösungen in positiven, also auch nicht in positiven ganzen Zahlen.

§ 4. Die Zerlegung der ganzen Zahlen

Primzahlen sind nicht in Faktoren zerlegbar.
Zwei Zerlegungen einer ganzen Zahl m fassen wir als nicht wesentlich verschieden auf, wenn in $m = abc \ldots = a'b'c' \ldots$ (beides bricht ab) die a', b', c', ... nur in der Reihenfolge und im Vorzeichen von den $a, b, c, \ldots$ verschieden sind. Alle Faktoren sollen absolut größer als eins sein.
Es gilt der Satz 9 in § 1, aus dem fast unmittelbar der Hauptsatz der Zerlegungstheorie folgt:

Satz 1. *Die Zerlegung ganzer Zahlen in Primzahlen ist im wesentlichen eindeutig.*

Beweis: In (alle Zahlen ganz > 0)

$$p_1 \ldots p_m = q_1 \ldots q_n = P$$

seien die p_i und q_j Primzahlen, und es gelte $p_i \leqq p_{i+1}$, $q_j \leqq q_{j+1}$.

Nach dem erwähnten Satze und $p_1 \mid P$ folgt $p_1 \mid q_j$ mit unbekanntem j, also $p_1 = q_j$. Man erhält: $p_2 \ldots p_m = q_1 \ldots q_{j-1} q_{j+1} \ldots q_n$. Die Fortsetzung des Verfahrens zeigt:

1. daß für $m = n$ die Primzahlen übereinstimmen,

2. daß für $m \neq n$, etwa $m > n$ schließlich eine sich selbst widersprechende Gleichung

$$p_a p_b \ldots p_k = 1$$

bleibt. Dieser Fall kann also nicht eintreten.

Die p_i heißen die *Primfaktoren* oder *Primteiler* von P. Faßt man gleiche zusammen, so erhält man die *kanonische Zerlegung*

$$P = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}.$$

In gleicher Weise kann ein *reduzierter Bruch*, d. h. eine Zahl $\frac{m}{n}$ mit $(m, n) = 1$ als

$$\frac{m}{n} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

eindeutig zerlegt werden, wobei die $\alpha_i > 0$ bei den Primteilern von m, die $\alpha_i < 0$ bei den Primteilern von n auftreten. Auch diese Zerlegung heiße kanonische Zerlegung.

Wir schreiben bei beliebigem rationalem a

$$p^\alpha \parallel a$$

(lies: p^α geht genau in a auf), wenn in der kanonischen Zerlegung von a die Potenz p^α erscheint.

Beispiele: $7^2 \parallel 147$, $2^7 \parallel 3456$, $5^3 \parallel 1000$, $2^3 \parallel \frac{8}{3}$.

$p^0 \parallel a = \frac{m}{n}$ heißt: p tritt weder in m noch in n als Faktor auf. In diesem Falle nennen wir a zu p prim, indem wir den ursprünglich nur für ganzzahlige Zahlenpaare definierten Begriff *relativ prim* auf den Fall ausdehnen, daß eine Zahl Primzahl, die andere ein Bruch ist.

Ist $p^m \parallel a$ mit $m \geqq 0$, so heißt a bezüglich p ganz.

Satz 2. *Summe und Produkt zweier bezüglich p ganzer Zahlen sind bezüglich p ganz.*

Beweis: Es sei

$$p^m \parallel a,\ p^n \parallel b,\ m \geqq 0,\ n \geqq 0.$$

Es wird

$$a = p^m a',$$
$$b = p^n b',$$

wobei im (eventuellen) Nenner von a' und b' die Primzahl p nicht aufgeht. Alle Zahlen sollen in reduzierter Form geschrieben sein, ganze Zahlen haben also den symbolischen Nenner eins.

Zuerst der Beweis für das Produkt: Offenbar folgt aus $p^0 \parallel a'$, $p^0 \parallel b'$ auch $p^0 \parallel a'b'$ (Zähler und Nenner von $a'b'$ sind Produkte von zu p primen Zahlen, also wieder zu p prim); es folgt wegen

$$ab = p^{m+n} a'b', \quad p^{m+n} \parallel ab,$$

daß ab nach p ganz ist. Die zweite Formel gilt offenbar auch, wenn m oder n oder beide Zahlen negativ sind. Bei der Summe treten Verwicklungen auf.

Es sei etwa $n > m$, was keine Einschränkung der Allgemeinheit ist, also $\max(m, n) = n$. Es bleibt

$$a + b = p^m (a' + p^{n-m} b').$$

Wir setzen $a' = \frac{M}{N}$, $b' = \frac{M'}{N'}$, mit ganzen Zahlen M, N, M', N' und $(M, p) = (N, p) = (M', p) = (N', p) = 1$. Leicht folgt

$$c = a' + p^{n-m} b' = \frac{MN' + p^{n-m} M'N}{NN'},$$

also $p^0 \parallel c$; denn aus $p \nmid N$, $p \nmid N'$ folgt $p \nmid NN'$. Aus $p \nmid M$, $p \nmid N'$ folgt $p \nmid MN'$.

Damit ist bewiesen: Der Zähler von c ist durch p nicht teilbar. Sofort folgt

$$a + b = p^m c,$$

wobei c zu p prim ist.

Ist $m = n$, so folgt wieder $(NN', p) = 1$. Ob und in welcher Potenz die Primzahl p in $MN' + NM'$ aufgeht, läßt sich nicht beurteilen. Es ist

$$a + b = p^r c',$$

wobei c' zu p prim und $r \geqq m = n$ ist.

Wir können etwas genauer sagen:

Satz 3. *Ist $p^m \parallel a$, $p^n \parallel b$, so ist $p^r \parallel a + b$ mit $r = \min(m, n)$ für $m \neq n$, aber $r \geqq m$ für $m = n$. Weiter gilt $p^{mn} \parallel ab$. Beides gilt auch, wenn m, n beide oder eine der Zahlen negativ ist.*

Der vorige Satz gilt auch für $m < 0$, $n < 0$, denn dann ist

$$p^{-m} \Big\| \frac{1}{a}, \qquad p^{-n} \Big\| \frac{1}{b}.$$

Nach dem bewiesenen Teil von Satz 3 ergibt sich also:

1. Für $m > n$ ist $-m < -n$, also wird $p^{-m} \Big\| \frac{1}{a} + \frac{1}{b}$. Nach dem bewiesenen Teilsatz ist weiter $p^{m+n} \| ab$, und mit nochmaliger Anwendung auf das Produkt

$$a + b = ab\left(\frac{1}{a} + \frac{1}{b}\right)$$

folgt $$p^n \| a + b.$$

2. Ist $m = n$, so ergibt derselbe Schluß

$$p^{r'} \Big\| \frac{1}{a} + \frac{1}{b} \text{ mit } r' \geqq -m = -n.$$

Multiplikation mit ab und Anwendung des Teilsatzes ergeben

$$p^{2m+r'} \| a + b,$$

mit $r = 2m + r' \geqq 2m - m = m$, und es folgt

$$p^r \| a + b \text{ mit } r \geqq m = n.$$

Ebenso gilt Teilsatz 3 beispielsweise auch für $m < 0$, $n \geqq 0$. Dann ist $m < n$, im reduzierten Nenner von $a + b$ kommt p^{-m} vor, das sich gegen den Nenner nicht wegheben kann.
Der Satz gilt also allgemein.

Beispiele: Berechne in folgenden Beispielen die Exponenten x

1. $7^x \| 686$.
2. $3^x \| 567$.
3. $7^x \| 7203$.
4. $3^x \Big\| \frac{486}{7}$
5. $2^x \| 12288$.
6. $5^x \| 3125$.
7. $2^x \Big\| \frac{7}{8}$
8. $3^x \Big\| \frac{123}{243}$

§ 5. Der Kongruenzbegriff

Im folgenden seien die Zahlen ganz. Wir schreiben

$$a \equiv b \bmod m,$$

wenn $b - a$ durch m teilbar ist. Wir lesen: „a kongruent b modulo m." m heißt der *Modul*.

Der so eingeführte Kongruenzbegriff ist ein spezieller Fall des in allen Teilen der Mathematik vorkommenden Äquivalenzbegriffes. Wir schreiben $A \sim B$, wenn A äquivalent zu B sein soll. Wir sprechen nur dann von einer Äquivalenz, wenn folgende drei Beziehungen erfüllt sind:

1. $A \sim A$, d. h., jedes Element ist zu sich selbst äquivalent (Reflexivität).

2. Aus $A \sim B$ folgt $B \sim A$ (Symmetrie).

3. Aus $A \sim B$, $B \sim C$ folgt $A \sim C$ (Transitivität).

Diese Begriffe sind voneinander unabhängig, worauf aber nicht näher eingegangen werden soll.

Beispiele für Äquivalenz sind: Gleichheit, Vorzeichengleichheit, Gleichheit des Absolutbetrags, geometrische Kongruenz, Inhaltsgleichheit ebener Figuren, Volumgleichheit räumlicher Körper, Parallelismus von Geraden und Ebenen, Ähnlichkeit.

Die vorhin definierte Kongruenz erfüllt die drei Eigenschaften der Äquivalenz. Um dies zu zeigen, bedenken wir, daß $a \equiv b \bmod m$ gleichbedeutend ist mit $m \mid b - a$.

1. Es ist $m \mid 0 = a - a$, also $a \equiv a \bmod m$ (Reflexivität).

2. Aus $m \mid b - a$ folgt $m \mid a - b$, oder aus $a \equiv b \bmod m$ folgt $b \equiv a \bmod m$ (Symmetrie).

3. $m \mid b - a$, $m \mid c - b$ hat $m \mid c - b + b - a = c - a$ zur Folge, oder aus $a \equiv b$, $b \equiv c \bmod m$ folgt $a \equiv c \bmod m$ (Transitivität).

Ist $a \equiv b \bmod m$, so heißt dies $m \mid b - a$. Ist ebenso $c \equiv d \bmod m$, oder $m \mid d - c$, so folgt mit beliebigen ganzen Zahlen X, Y $m \mid bX + dY - (aX + cY)$. Wir haben

Satz 1. *Aus $a \equiv b$, $c \equiv d$ mod m folgt $aX + cY \equiv bX + dY$ mod m mit beliebigen ganzen Zahlen X und Y.*

Wichtige Spezialfälle ergeben sich mit $X = Y = 1$; $X = 1$, $Y = -1$; X, Y beliebig, wenn die zweite Kongruenz $0 \equiv 0$ *mod m* heißt. Es folgt sofort

Satz 2a. *Man kann Kongruenzen miteinander addieren.*

Satz 2b. *Man kann Kongruenzen voneinander subtrahieren.*

Satz 3a. *Man kann eine Kongruenz (d. h. beide Seiten) mit einer beliebigen ganzen Zahl multiplizieren.*

Der letzte Satz lautet in Formeln: Aus $a \equiv b \bmod m$ folgt $aX \equiv bX \bmod m$ mit beliebigem ganzzahligem X. Er soll noch etwas genauer untersucht werden:

Ist $a \equiv b \bmod m$, also $m \mid b - a$, so gilt $mX \mid bX - aX$ oder $aX \equiv bX \bmod mX$.
Wir haben damit

Satz 3b. *Aus $a \equiv b \bmod m$ folgt $aX \equiv bX \bmod mX$ mit X als beliebiger ganzer Zahl.*

Satz 4. *Man kann Kongruenzen miteinander multiplizieren.*

Beweis: $a \equiv b$, $c \equiv d \bmod m$ hat zur Folge $ac \equiv bc$, $bc \equiv bd$ und wegen der Transitivität $ac \equiv bd \bmod m$.

Eine Kongruenz mod 0 wäre einfach Gleichheit. Eine Kongruenz mod 1 sagt gar nichts aus, denn mod 1 ist jede ganze Zahl jeder ganzen Zahl kongruent. Diese beiden Fälle schließen wir daher aus.
Einander kongruente Zahlen schließen wir in eine *Restklasse* zusammen. Nach den Sätzen 1, 2, 4 kann man mit Restklassen die gleichen Operationen wie mit Kongruenzen ausführen. Diese erfüllen die normalen Eigenschaften, also Kommutativität und Assoziativität bei der Addition, Kommutativität, Assoziativität und Distributivität bei der Multiplikation. Die Restklasse der Zahl 1 ist das Einselement bei der Multiplikation. Die Restklassen mod m bilden einen endlichen Ring; ihre Gesamtheit heißt *Restsystem*.
Dieser Restklassenring ist zugleich ein *Vollring*, d. h. ein Ring, bei dem die Division durch jeden Nichtnullteiler gestattet ist. Dies folgt aus

Satz 5. *Jeder endliche Ring ist ein Vollring.*

Beweis: Sind — was eintreten kann — keine Nichtnullteiler vorhanden, so ist der Satz richtig, wenn auch trivial. Wir wollen im folgenden mit $a, b, c, \ldots$ Ringelemente, speziell mit u einen Nichtnullteiler bezeichnen.

Multipliziere ich die Folge der Ringelemente $a = 0, b, c, \ldots$ mit einem Nichtnullteiler u, so entsteht eine Folge: $au = 0, bu, cu, \ldots$, in der keine zwei Elemente zusammenfallen, denn aus $tu = t'u$ folgt $(t - t')u = 0$ und, da u Nichtnullteiler ist, gilt $t = t'$.

Die zweite Folge enthält die gleiche endliche Zahl von Elementen wie die erste, es ist also jedes Ringelement k eindeutig in der Form tu darstellbar. Die Gleichung $tu = k$ ist eindeutig lösbar, die Division durch jeden Nichtnullteiler ist möglich und eindeutig.
Die letzte Eigenschaft: „Ist die Division durch einen Nichtnullteiler möglich, so ist sie eindeutig" gilt überhaupt, wie man sieht, für jeden Ring.

Der Restklassenring mod m ist also ein Vollring. Wir fragen: Welches sind die eventuellen Nullteiler des Ringes?
Wir beweisen

Satz 6. *Jedes Element einer durch a repräsentierten Restklasse mod m hat denselben g.g.T. $(a, m) = d$.*

Beweis: Es sei $a' \equiv a \bmod m$. Dann sei $(a', m) = d'$. Wegen $a' = a + mX$ teilt d auch die Zahl a', somit ist $d \mid d'$. Da ebensogut auch $d' \mid d$ gezeigt werden kann, so folgt $d = d'$.

Wir können also unterscheiden:

1. Restklassen, die zu m prim sind. Sie heißen *primo Restklassen*,
2. Restklassen, die mit m einen nur von der Restklasse abhängigen g.g.T. >1 haben.

Die Art 1. bildet gerade die Nichtnullteiler des Restklassenrings. Denn ist $(a, m) = 1$, so folgt aus $ab \equiv 0 \bmod m$, daß $b \equiv 0 \bmod m$ ist.

Die Art 2. bildet die Nullteiler, wenn man zu ihnen als uneigentlichen Nullteiler noch Null, d. h. die Restklasse der durch m teilbaren Zahlen rechnet.
Aus dem Satz, daß ein endlicher Ring Vollring ist, folgt

Satz 7. *Die Kongruenz $ax \equiv b \bmod m$ ist für $(a, m) = 1$ eindeutig mod m lösbar.*

Das ist der wichtige Satz über die Lösbarkeit der linearen Kongruenz. Er ist gleichbedeutend mit dem der Lösbarkeit der diophantischen Gleichung $ax + my = b$, also mit Satz 10 von § 1. Trotzdem wurde ein neuer Weg zum Beweis dieses Satzes gewählt, um auch ohne die Möglichkeit, den dort erläuterten Euklidischen Algorithmus zur Lösung der Kongruenz zu verwenden, einen dem Satz 7 analogen in anderen Moduln beweisen zu können, wobei allerdings wieder der Restklassenring endlich, also ein Vollring ist. Wir werden später davon Gebrauch machen.

Ist $m = p$ Primzahlmodul, so ist der Restklassenring P_p ein Körper, Primkörper der Charakteristik p genannt. Hier haben wir also nur eine Lösung mod p der Kongruenz $ax \equiv b \bmod p$, wenn $a \not\equiv 0 \bmod p$ ist.

Wir wollen nun eine weitere Definition beifügen. Ist a zu m prim, so bezeichnen wir als Restklasse der gebrochenen Zahl $\frac{b}{a}$ die von x, wenn $ax \equiv b \bmod m$ ist. Wir lehnen es dabei ausdrücklich ab, diese Definition auf $(a, m) > 1$ auszudehnen.

Diese Definition ist ein außerordentlich weitreichendes Hilfsmittel bei der tatsächlichen Lösung einer linearen Kongruenz $ax \equiv b \bmod m$, während der Beweis für die Lösbarkeit mit Hilfe des Vollringbegriffes ein reiner Existenzbeweis und die Lösung durch den Euklidischen Algorithmus meist viel umständlicher ist.

Das Wesentliche bei der Sache ist,

$$\frac{b}{a} \equiv \frac{b + mX}{a + mY}$$

zu setzen, so daß der Bruch sich möglichst kürzen läßt. Manchmal ist auch eine Erweiterung

$$\frac{b}{a} = \frac{bZ}{aZ},$$

wobei natürlich $(m, Z) = 1$ sein muß, vorteilhaft.

Wir wollen dies an einzelnen Beispielen erläutern:

1. $88x \equiv 1 \bmod 137$,

$$x \equiv \frac{1}{88} \equiv -\frac{136}{88} \equiv -\frac{17}{11} \equiv \frac{120}{11}$$

$$\equiv 11 - \frac{1}{11} \equiv 11 - \frac{1 + 274}{11} \equiv 11 - \frac{275}{11} \equiv -14$$

oder auch

$$x \equiv -\frac{1}{49} \equiv \frac{273}{49} \equiv \frac{39}{7} \equiv -\frac{98}{7} \equiv -14.$$

2. $31x \equiv 45 \bmod 239$,

$$x \equiv \frac{45}{31} \equiv \frac{45}{270} \equiv \frac{1}{6} \equiv \frac{240}{6} \equiv 40.$$

3. $33x \equiv 398 \bmod 691$,

$$x \equiv \frac{398}{33} \equiv \frac{398 + 691}{33} \equiv \frac{1089}{33} \equiv 33.$$

4. $23x \equiv 4 \bmod 28$,

$$x \equiv \frac{4}{23} \equiv -\frac{4}{5} \equiv \frac{80}{5} \equiv 16.$$

5. $55x \equiv 7 \bmod 71$,

$$x \equiv \frac{7}{55} \equiv -\frac{7}{16} \equiv \frac{64}{16} \equiv 4.$$

Im folgenden sei (für den Rest des Paragraphen) $m > 0$. Die Sätze gelten mit $|m|$ statt m auch für $m < 0$. Weiter führen wir das Zeichen $a \not\equiv b \bmod m$ (a inkongruent b) für $m \nmid b - a$ ein.

Wir können die Klassen eines Restsystems mod m auf verschiedene Weise repräsentieren.

Eine naheliegende Repräsentierung ist die durch die kleinsten nichtnegativen Reste

$$0, 1, 2, 3, \ldots, m-2, m-1.$$

Sie ist das Natürliche, wenn wir an die Division denken.

Eine andere Repräsentierung ist die durch die absolutkleinsten Reste. Ist m ungerade, also $m \equiv 1 \bmod 2$, so ist sie gegeben durch

$$0, \quad \pm 1, \quad \pm 2, \quad \ldots, \quad \pm\left(\left[\frac{m}{2}\right]-1\right), \qquad \pm\left[\frac{m}{2}\right].$$

Ist m hingegen gerade, $m \equiv 0 \bmod 2$, so nehmen wir sie so an:

$$0, \quad \pm 1, \quad \pm 2, \quad \ldots, \quad \pm\left(\frac{m}{2}-1\right), \qquad \frac{m}{2}.$$

Hier ist die letzte Normierung etwas willkürlich. Nach der Definition hätte ich für das letzte Element der Folge auch $-\frac{m}{2}$ schreiben können.

Unter den Resten ragen die Nichtnullteiler hervor, d. h. die Klassen von Zahlen a mit $(a, m) = 1$. Ihre Anzahl ist $\varphi(m)$, die wichtige Eulersche Funktion.

Wir definieren also auf Grund der Repräsentierung des Restsystems mod m durch die kleinsten positiven Reste:

Definition. *$\varphi(m)$ ist die Anzahl der zu m primen natürlichen Zahlen $\leqq m$, damit auch die Zahl der primen Restklassen mod m.*

Hiermit ist auch $\varphi(1) = 1$ definiert. Selbstverständlich kann für $m > 1$ das Zeichen $\leqq$ in der Definition durch $<$ ersetzt werden. Trivial ist $\varphi(p) = p - 1$, wenn p eine Primzahl ist, auch $\varphi(2p) = p - 1$, wenn p eine ungerade Primzahl ist. Wie man

sonst $\varphi(m)$ berechnet, werden wir im nächsten Paragraphen sehen. Im Gegensatz zum *reduzierten Restsystem* (der primen Restklassen) bildet der Restklassenring das *volle Restsystem* aus m Elementen. Wir haben z. B. mod 14 das volle Restsystem repräsentiert durch 0, 1, 2, ..., 12, 13.
Im Gegensatz dazu besteht das reduzierte Restsystem nur aus den sechs Restklassen 1, 3, 5, 9, 11, 13.
Mit den absolutkleinsten Resten repräsentiert sich das volle Restsystem mit $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, 7$. Hingegen ist das reduzierte Restsystem durch $\pm 1, \pm 3, \pm 5$ repräsentiert.

Satz 7 kann auch ausgesprochen werden:

Satz 8. *Die Multiplikation eines vollen Restsystems mit einem Rest des reduzierten Restsystems gibt wieder ein volles Restsystem.*

Daneben gilt auch

Satz 9. *Die Multiplikation eines reduzierten Restsystems mit einem Rest des reduzierten Restsystems gibt wieder ein reduziertes Restsystem.*

Der Beweis folgt einfach daraus, daß das Produkt zweier Nichtnullteiler in einem Ring wieder ein Nichtnullteiler ist.

Wir gehen nun an den Beweis des Fermatschen Satzes, meist „kleiner Fermat" genannt (der noch ungeklärte „große Fermat" wird in diesem Buche nicht betrachtet).

Satz 10. *Mit* $(a, m) = 1$ *ist* $a^{\varphi(m)} \equiv 1 \mod m$.

Beweis: Ist $b_1, \ldots, b_\varphi$ mit $\varphi = \varphi(m)$ ein reduziertes Restsystem, so ist die Gesamtheit der Zahlen $a b_j$ in unbekannter Reihenfolge der Gesamtheit der b_i kongruent, also wird

$$a^{\varphi(m)} b_1 \ldots b_\varphi \equiv b_1 \ldots b_\varphi \text{ und mit } B = b_1 \ldots b_\varphi,$$

kurz $$a^{\varphi(m)} B \equiv B \text{ oder } m \mid B(a^{\varphi(m)} - 1).$$

Wegen $(B, m) = 1$ bleibt daher $m \mid a^{\varphi(m)} - 1$, w. z. b. w.
Mit $m = p$ (positive Primzahl) haben wir den speziellen kleinen Fermat:

Satz 11. *Ist a nicht durch die Primzahl p teilbar, so ist* $a^{p-1} \equiv 1 \mod p$.

Multipliziere ich die letzte Kongruenz mit a, so erhalte ich

$$a^p \equiv a \bmod p,$$

und dies gilt offenbar auch für $a \equiv 0 \bmod p$.

Es folgt

Satz 12. *Für beliebiges ganzes a und eine Primzahl p ist $a^p \equiv a \bmod p$.*

Nun kommen wir zum *Satz von Wilson*, kurz „Wilson" genannt.

Satz 13. *Für Primzahlen p gilt $(p-1)! \equiv -1 \bmod p$.*

Bevor wir den Beweis dieses Satzes führen können, beweisen wir folgenden

Hilfssatz. *Für $p > 2$ hat die Kongruenz $x^2 \equiv 1 \bmod p$* (erstes Beispiel einer quadratischen Kongruenz) *die zueinander inkongruenten Lösungen $x \equiv 1$, $x \equiv -1$ und keine weiteren.*

Beweis des Hilfssatzes: Daß die genannten Zahlen Lösungen der Kongruenz sind, ist ohne weiteres klar. Daß es keine anderen gibt, folgt aus der Tatsache, daß im Körper P_p eine Gleichung nicht mehr Wurzeln, als ihr Grad beträgt, haben kann.

Will man diesen Satz aus der abstrakten Algebra nicht heranziehen, so kann man ganz einfach schließen: $(x+1)(x-1) \equiv 0 \bmod p$ ist nur möglich, wenn ein Faktor durch die Primzahl p teilbar ist (Satz 9 von § 1).

Beweis des Satzes von Wilson: Für $p = 2$ ist der Satz klar. Nun sei $p > 2$. Dann können wir die Zahlen $1, 2, \ldots, p-2$, $p-1$ wie folgt anordnen: Zuerst nehmen wir 1 und $p-1$, ihr Produkt ist kongruent -1. Dann stellen wir zusammen $2 = a_2$ und a_2' mit $a_2 a_2' \equiv 1 \bmod p$. Die nächste noch nicht entnommene Zahl in der Folge sei a_3, dazu geben wir a_3' mit $a_3 a_3' \equiv 1 \bmod p$. Es ist zu beachten, daß zu jedem a_j das zugehörige a_j' eindeutig gegeben und $\neq a_j$ ist. Denn $a_j' \equiv a_j$ gäbe $a_j^2 \equiv 1 \bmod p$, was unmöglich ist, da weder $a_j \equiv 1$ noch $a_j \equiv -1 \bmod p$ gilt. Weiter ist mit der Restklasse von a_j auch die Zahl a_j' gegeben, da wir hier die Klassen durch die kleinsten nichtnegativen Reste repräsentieren. Ist das durchgeführt, so gilt

$$(p-1)! \equiv 1 \cdot 2 \ldots (p-1) \equiv (-1)(a_2 a_2') \ldots (a_t a_t') \bmod p,$$

wo $t = \frac{p-3}{2}$ ist. Da die in Klammern zusammengefaßten Faktoren ein Produkt $\equiv 1 \bmod p$ geben, so bleibt

$$(p-1)! \equiv -1 \bmod p.$$

Wegen $(p-1)! = (p-2)!\,(p-1)$ kann der Wilsonsche Satz auch

$$(p-2)! \equiv 1 \bmod p$$

geschrieben werden. Dieser Satz ist auch für $p = 2$ richtig, wenn in üblicher Art $0! = 1$ definiert wird.
Der Wilsonsche Satz liefert ein notwendiges und hinreichendes Kriterium dafür, daß eine natürliche Zahl >1 Primzahl ist. Denn es gilt

Satz 14. *Für Nichtprimzahlen A (>1) gilt $(A-1)! \not\equiv -1 \bmod A$.*

Beweis: Wegen $A > 2$ ist $\frac{A}{2} < A - 1$. Es gibt eine Primzahl $q < A$ mit $q \mid A$, $q \leqq \frac{A}{2}$; es gilt also $\left(\left[\frac{A}{2}\right]\right)! \equiv 0 \bmod q$ und erst recht $(A-1)! \equiv 0 \bmod q$. Mithin ist $((A-1)!, A) > 1$ und $(A-1)! \equiv -1 \bmod A$ ist unmöglich.

Wir wollen die Besprechung der Kongruenz mit einigen leichten Sätzen abschließen.

Satz 15. *Ist $a \equiv b \bmod m$, $m \equiv 0 \bmod n$, so gilt $a \equiv b \bmod n$.*

Beweis: Folgt aus $n \mid m \mid b - a$.
Die folgende Schreibweise ist üblich:

$$a \equiv b \bmod m \equiv 0 \bmod n.$$

Wir werden sie gelegentlich verwenden.

Satz 16. *Ist $ac \equiv bc \bmod m$, $(c, m) = d$, $m = dn$, so folgt $a \equiv b \bmod n$.*

Beweis: Es gilt $dn \mid bc - ac$, wird $c = ed$ gesetzt, so ist $(e, n) = 1$ (Satz 6 von § 1), weiter folgt $dn \mid ed\,(b-a)$, $n \mid e\,(b-a)$, also (§ 1, Satz 7) $n \mid b - a$.
Ist insbesondere $(c, m) = 1$, so bleibt

Satz 17. *Ist $ac \equiv bc \bmod m$, $(c, m) = 1$, so ist $a \equiv b \bmod m$,* oder, *eine Kongruenz kann durch eine zum Modul teilerfremde Zahl gekürzt werden.*

Hierbei ist also wohl zu beachten, daß die Zahl, durch die gekürzt wird, zum Modul prim ist. Beispielsweise folgt nach dieser Regel aus der richtigen Kongruenz: $15 \equiv 225 \bmod 42$ nicht etwa $1 \equiv 15 \bmod 42$, was man sofort als unrichtig erkennt, sondern wegen $(15, 42) = 3$, $42 = 3 \cdot 14$ nur $1 \equiv 15 \bmod 14$.
Es sei noch bemerkt, daß in älteren Lehrbüchern der Zahlentheorie zwei Zahlen a, a' mit $aa' \equiv 1 \bmod m$ als socii oder assoziierte Zahlen bezeichnet werden. Es ist also a' die Restklasse

von $\frac{1}{a}$. Selbstverständlich ist die Definition nur für $(a, m) = 1$ sinnvoll. Die Beziehung zwischen a und a' ist symmetrisch, aber weder reflexiv noch transitiv.

Der kleine Fermat kann auch zur Lösung von

$$ax \equiv b \bmod m$$

mit $(a, m) = 1$ herangezogen werden. Denn sie folgt aus:

$$x \equiv b a^{\varphi(m)-1} \bmod m.$$

Für die Rechnung ist dies aber meist unpraktisch. Auch der Wilson kann bei Primzahlmoduln zur Berechnung der Wurzel einer linearen Kongruenz benutzt werden.

Reihenbeispiele:

1. $2x \equiv 17 \bmod 43$.
2. $17x \equiv 135 \bmod 223$.
3. $31x \equiv 28 \bmod 94$.
4. $50x \equiv 627 \bmod 1949$.
5. $17x \equiv 15 \bmod 16$.
6. $33x \equiv 4 \bmod 1093$.
7. $5x \equiv 6 \bmod 641$.
8. $101x \equiv 5 \bmod 223$.
9. $1009x \equiv 1 \bmod 225$.

§ 6. Simultane Kongruenzen

Es seien $a_1, a_2, \ldots, a_n$ paarweise prim, d. h. $(a_i, a_j) = 1$ für $i \neq j$. Dann kann die Aufgabe der gleichzeitigen Erfüllung des Systems

$$A_1 x \equiv B_1 \bmod a_1,\ A_2 x \equiv B_2 \bmod a_2, \ldots, A_n x \equiv B_n \bmod a_n \qquad (1)$$

erledigt werden, sofern stets $(A_i, a_i) = 1$ ist.

Es ergibt sich

$$x \equiv C_1 \bmod a_1,\ x \equiv C_2 \bmod a_2, \ldots, x \equiv C_n \bmod a_n. \qquad (2)$$

Mit $x = C_1 + a_1 y_1$ bleibt $C_1 + a_1 y_1 \equiv C_2 \bmod a_2$. Diese lineare Kongruenz ist wegen $(a_1, a_2) = 1$ eindeutig mod a_2 lösbar. Der aus ihr gefundene Wert

$$y_1 = D_1 + a_2 y_2$$

mit unbekanntem y_2 werde in die nächste Kongruenz eingesetzt

$$C_1 + a_1 D_1 + a_1 a_2 y_2 \equiv C_3 \bmod a_3. \qquad (3)$$

Wegen $(a_1 a_2, a_3) = 1$ ist (3) sicher lösbar und gibt

$$y_2 = D_2 + a_3 y_3 \quad \text{usf.}$$

Sind die Moduln nicht paarweise prim, so sind für die Existenz einer Lösung weitere Bedingungen erforderlich; auf diese Frage wollen wir aber nicht eingehen.

1. $x \equiv 4 \bmod 33$, $x \equiv 5 \bmod 17$, $x \equiv 1 \bmod 7$.

Mit $x = 4 + 33y$ bleibt $4 + 33y \equiv 5 \bmod 17$, $-y \equiv 1 \bmod 17$, $y = -1 + 17z$, also $x = 4 + (-1 + 17z) \cdot 33 = -29 + 561z$.
Daher muß sein

$$-29 + 561z \equiv 1 \bmod 7,\ z \equiv 30 \equiv 2 \bmod 7,\ z = 2 + 7u.$$

Endgültig folgt

$$x = -29 + 1122 + 3927u = 1093 + 3927u.$$

2. $x \equiv 10 \bmod 27$, $x \equiv -1 \bmod 73$, $x \equiv 4 \bmod 7$.
Man hat

$$x = -1 + 73y,\ -1 + 73y \equiv 10 \bmod 27,$$

$$8y \equiv -11 \equiv 16 \bmod 27,\ y \equiv 2 \bmod 27,\ y = 2 + 27z.$$

Also folgt

$$-1 + 73\,(2 + 27z) \equiv 4 \bmod 7,\ -1 + 3\,(2 - z) \equiv 4 \bmod 7,$$

$$3\,(2 - z) \equiv 5 \equiv 12 \bmod 7,\ 2 - z \equiv 4 \bmod 7,\ z = -2 \bmod 7.$$

Die letzte Kongruenz kann auch $z \equiv 5 \bmod 7$ geschrieben werden, sie gibt $z = 5 + 7u$. Man erhält

$$x = 145 + 1971z = 145 + 9855 + 13797u$$

oder

$$x \equiv 10000 \bmod 13797.$$

Rechenbeispiele

1. $x \equiv 2 \bmod 17$, $x \equiv 12 \bmod 29$, $x \equiv 9 \bmod 31$.
2. $x \equiv 1 \bmod 120$, $x \equiv 0 \bmod 37$.
3. $x \equiv 2 \bmod 3$, $x \equiv 5 \bmod 7$, $x \equiv 1 \bmod 11$.

§ 7. Die Eulersche Funktion $\varphi(n)$

Die bereits in § 5 definierte Funktion $\varphi(n)$ wurde dort nur für Primzahlen berechnet. Um die Berechnung im allgemeinen Falle durchzuführen, beweisen wir

Satz 1. *Ist* $(a, b) = 1$, *und durchläuft* x *das reduzierte Restsystem mod* a, *während gleichzeitig* $x \equiv 0$ *mod* b *ist, durchläuft weiter* y *das*

reduzierte Restsystem mod b, so durchläuft $ay + x$ das reduzierte Restsystem mod ab.

Beweis: Es muß gezeigt werden, daß I. zwei solche Ausdrücke $ay + x$ und $ay' + x'$ außer für $x = x'$, $y = y'$ niemals mod ab kongruent sind, II. auf diese Art wirklich jede Klasse des reduzierten Restsystems erfaßt wird, III. sich nur zu ab prime Zahlen ergeben.

I. Ist $ay + x \equiv ay' + x' \bmod ab$, so gibt diese Kongruenz, als solche mod a aufgefaßt, sofort $x \equiv x' \bmod a$, d. h. $x = x'$. Als Kongruenz mod b bleibt $ay \equiv ay' \bmod b$, die wir wegen $(a, b) = 1$ durch a kürzen können. Mithin ist $y \equiv y' \bmod b$ oder $y = y'$.

II. Ist c gegeben, so ergibt der Ansatz $ay + x \equiv c \bmod ab$, als solcher mod a aufgefaßt, die Kongruenz $x \equiv c \bmod a$ und damit einen bestimmten Wert $x = X$. Es bleibt $a \mid c - X$, etwa $c - X = aY_1$. Wir finden $ay \equiv aY_1 \bmod b$ und damit $y \equiv Y_1 \bmod b$, etwa $y = Y$. Hier ist $(X, a) = 1$ wegen $X \equiv c \bmod a$ und $(c, a) = 1$. Weiter ist $(c - X, b) = 1$ wegen $(c, b) = 1$ und $X \equiv 0 \bmod b$. Also folgt $(aY_1, b) = 1$, erst recht $(Y_1, b) = 1$ und auch $(Y, b) = 1$ wegen $Y \equiv Y_1 \bmod b$.

III. Es ist $(ay + x, b) = 1$ wegen $x \equiv 0 \bmod b$, $(ay + x, b) = (ay, b) = 1$. Weiter wird $(ay + x, a) = (x, a) = 1$. Damit ist alles bewiesen.

Satz 2. *Für $(a, b) = 1$ ist $\varphi(ab) = \varphi(a)\,\varphi(b)$.*

Beweis: In Satz 1 haben wir das reduzierte Restsystem mod ab von $\varphi(ab)$ Zahlen durch $\varphi(a)\,\varphi(b) \bmod ab$ inkongruente Zahlen dargestellt.

Wir berechnen zunächst $\varphi(p^a)$, wenn p eine Primzahl ist. Die zu p nicht primen natürlichen Zahlen $\leqq p^a$ sind im Ausdruck pX mit $0 < X \leqq p^{a-1}$ enthalten, also in der Anzahl p^{a-1}. Es ergibt sich

$$\varphi(p^a) = p^a - p^{a-1}$$

oder

$$\varphi(p^a) = p^a\left(1 - \frac{1}{p}\right).$$

Nach dem vorigen Satz haben wir sofort

Satz 3. *Ist die kanonische Zerlegung*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

so ist $$\varphi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

Beweis: Nach dem Satz 2 wird

$$\varphi(n) = \prod_{i=1}^{k}\varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k}p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

Zahlentheoretische Funktionen mit $f(mn) = f(m)f(n)$ für $(m, n)=1$ nennt man distributive Funktionen. Die φ-Funktion ist also eine solche. Von den distributiven zahlentheoretischen Funktionen soll der nächste Paragraph handeln.

§ 8. Zahlentheoretische Funktionen

Eine für alle ganzen Werte $t \geqq 0$ definierte Funktion $f(t)$ heißt zahlentheoretische Funktion. Der Wert für $t = 0$ ist oft gleichgültig.

Definition. *Eine zahlentheoretische Funktion $f(t)$ mit $f(mn) = f(m)f(n)$ für $(m, n) = 1$ heiße distributiv.*

Von der trivialen distributiven Funktion, die identisch Null ist, sehen wir ab. Eine andere distributive Funktion ist t^k, wobei k eine beliebige Zahl (auch negativ, gebrochen, irrational, eigentlich komplex) sein kann.
Ein anderes Beispiel wäre die Funktion, die mit $f(1) = 1$ und für $t > 1$, $t = \prod_{i=1}^{k} p_i^{a_i}$ mit $f(t) = \prod_{i=1}^{k} p_i^{a_i-1}$ erklärt ist.

Wir brauchen einen Satz über die Zerlegung.

Satz 1. *Ist $(m, n) = 1$, $d \mid mn$, so ist $d = d_1d_2$ mit $d_1 = (d, m)$, $d_2 = (d, n)$. Das ist zugleich die einzige Zerlegung $d = xy$ mit $x \mid m$, $y \mid n$. $(x, y > 0)$.*

Beweis: I. Es ist $(d_1, d_2) \mid (m, n) = 1$, also $(d_1, d_2) = 1$.
II. Mit ganzen Zahlen A, B, C, D, die $d_1 = dA + mB$ und $d_2 = dC + nD$ erfüllen, also $d_1 - dA = mB$, $d_2 - dC = nD$ folgt

$$(d_1 - dA)(d_2 - dC) = mnBD, \text{ d. h. } d \mid d_1d_2.$$

III. Nun setzen wir $d = xy$ mit $x \mid m$, $y \mid n$. Wir erhalten

$$d = xy \mid d_1d_2 \mid d.$$

Das Gleichheitszeichen kann also nur für $x = d_1$, $y = d_2$ eintreten. Über distributive Funktionen haben wir den

Satz 2. *Für eine distributive Funktion $f(t)$ gilt $f(1) = 1$.*

Beweis: Nach unserer Voraussetzung gibt es eine natürliche Zahl m mit $f(m) \neq 0$. Es ist $(m, 1) = 1$, weiter $f(m) = f(m \cdot 1) = f(m)\, f(1)$, $f(1) = 1$.

Wir geben nun einige Beispiele distributiver zahlentheoretischer Funktionen.

1. Die Anzahl $f_1(t)$ aller Teiler von t: Ist p eine Primzahl, so ist $f_1(p) = 2$, allgemein $f_1(p^k) = k+1$. Die Distributivität folgt aus Satz 1, weil für $(m, n) = 1$ die $f_1(m) f_1(n)$ Produkte $d_1 d_2$ mit $d_1 \mid m$, $d_2 \mid n$ alle Teiler von mn und jeden genau einmal durchlaufen.

Mit $n = \prod_{i=1}^{k} p_i^{a_i}$ (kanonische Zerlegung) bleibt

$$f_1(n) = \prod_{i=1}^{k} (a_i + 1).$$

2. Die Summe $f_2(t)$ aller Teiler von t: Die Distributivität folgt so:

$$f_2(mn) = \sum_{d \mid mn} d = \sum_{d_1 \mid m,\, d_2 \mid n} d_1 d_2 = \sum_{d_1 \mid m} d_1 \sum_{d_2 \mid n} d_2 = f_2(m)\, f_2(n).$$

3. Eine Zahl t mit der kanonischen Zerlegung $t = \prod_{i=1}^{k} p_i$, wobei alle Exponenten $a_i = 1$ sind, oder wobei $p \mid t$ (p Primzahl) $p \parallel t$ zur Folge hat, heißt *quadratfrei*.

1 pflegt auch zu den quadratfreien Zahlen gerechnet zu werden.

$f_3(t)$ sei die größte quadratfreie Zahl in t. Ist $t = \prod_{i=1}^{k} p_i^{a_i}$, so wird $f_3(t) = \prod_{i=1}^{k} p_i$. Die Distributivität ist klar.

4. $f_4(t) = u^A$ für $t = \prod_{i=1}^{A} p_i^{a_i}$. u ist dabei eine beliebige von t unabhängige Zahl. Offenbar ist $f_4(t)$ distributiv.

5. $f_5(t)$ sei das größte in t enthaltene Quadrat. Ist $t = a b^2$, a quadratfrei, so ist $f_5(t) = b^2$. Hier sowie beim folgenden Beispiel (6), das eine Verallgemeinerung von (5) ist, ist die Distributivität evident.

6. $f_6(t)$ sei die höchste in t enthaltene k-te Potenz (k natürliche Zahl >1). Bei der kanonischen Zerlegung

$$t = \prod_{i=1}^{A} p_i^{a_i k + b_i} \quad \text{mit} \quad 0 \leqq b_i < k$$

erhalten wir $$f_6(t) = \left(\prod_{i=1}^{A} p_i^{a_i}\right)^k.$$

7. $f_7(t)$ sei der von k-ten Potenzen freie Teil von t. Die vorige Zerlegung gibt $$f_7(t) = \prod_{i=1}^{A} p_i^{b_i}.$$

8. Überaus wichtig ist die zahlentheoretische Funktion $\mu(t)$. Es ist $\mu(1) = 1$, bei quadratfreien Zahlen $t = \prod_{i=1}^{A} p_i$ ist $\mu(t) = (-1)^A$. Bei nicht quadratfreiem t hingegen gilt $\mu(t) = 0$.

Der Beweis der Distributivität ist ganz einfach. Es sei $(m, n) = 1$. Ist mindestens eine der Zahlen m, n nicht quadratfrei, so ist sofort $0 = \mu(mn) = \mu(m)\,\mu(n)$.

Wir können also m und n als quadratfrei annehmen und haben die kanonischen Zerlegungen $m = \prod_{i=1}^{A} p_i$, $n = \prod_{j=1}^{B} q_j$, wobei jedes p_i von jedem q_j verschieden ist. Es wird

$$\mu(mn) = (-1)^{A+B} = (-1)^A\,(-1)^B = \mu(m)\,\mu(n).$$

9. Auch $\varphi(t)$, die im vorigen Paragraph genannte Eulersche Funktion, die Anzahl aller zu t primen natürlichen Zahlen $\leqq t$, ist distributiv, wie bereits dort gezeigt wurde.

Für $\varphi(t)$ gilt folgender

Satz 3. *Es ist* $\sum_{d|t} \varphi(d) = \sum_{d|t} \varphi\left(\frac{t}{d}\right) = t.$

Beweis: Für jedes $d \mid t$ gibt es $\varphi\left(\frac{t}{d}\right)$ natürliche Zahlen $x \leqq t$ mit $(x, t) = d$; denn sind $a, b, \ldots, g$ alle $\varphi\left(\frac{t}{d}\right)$ natürlichen Zahlen $y \leqq \frac{t}{d}$ mit $\left(y, \frac{t}{d}\right) = 1$, so ist $(yd, t) = d\left(y, \frac{t}{d}\right) = d$. Ein hd mit $\left(h, \frac{t}{d}\right) = l > 1$ gibt hingegen $(hd, t) = d\left(h, \frac{t}{d}\right) = dl$. Es hat aber jedes $x \leqq t$ einen Teiler d von t als g.g.T. mit t.

Satz 4. *Die Dirichletsumme* $f(t) = \sum_{d|t} g(d)$ *ist zugleich mit* $g(t)$ *distributiv.*

Beweis: Bei $(m, n) = 1$ wird $f(mn) = \sum_{d_1 \mid m} g(d_1) \sum_{d_2 \mid n} g(d_2) = f(m) f(n)$.

Satz 5. *Es ist* $\mu(1) = 1$, *aber* $\sum_{d \mid t} \mu(d) = 0$ *für* $t > 1$.

Beweis: Nach Satz 4 genügt der Beweis für Primzahlpotenzen. $t = p^\alpha$ gibt $\sum_{d \mid t} \mu(d) = \mu(1) + \mu(p) = 0$.

Satz 6. *Jede distributive zahlentheoretische Funktion* $f(t)$ *ist die Dirichletsumme der distributiven Funktion*

$$g(t) = \sum_{d \mid t} \mu\left(\frac{t}{d}\right) f(d) = \sum_{d \mid t} \mu(d) f\left(\frac{t}{d}\right).$$

Beweis:

I. Wir beweisen zunächst

$$\sum_{d \mid t} g(d) = \sum_{a \mid t} \sum_{\delta \mid d} \mu\left(\frac{d}{\delta}\right) f(\delta) = f(t).$$

Wir drehen die Reihenfolge der Summen um, nehmen δ als äußeren Summationsbuchstaben, diskutieren also zuerst die innere Summe $\sum_{d \equiv 0 \bmod \delta} \mu\left(\frac{d}{\delta}\right) f(\delta)$.

1a. Für $\delta = t$ bleibt nur $\mu(1) \cdot f(t) = f(t)$.

1b. Für $\delta < t$ bleibt als innere Summe

$$f(\delta) \sum_{\delta \mid d} \mu\left(\frac{d}{\delta}\right) = f(\delta) \sum_{k \mid \frac{t}{\delta}} \mu(k) = 0$$

wegen Satz 5 und $\frac{t}{\delta} > 1$.

II. Die Distributivität von $g(t)$ ergibt sich aus der für $(m, n) = 1$ gültigen Rechnung:

$$g(mn) = \sum_{d \mid mn} \mu\left(\frac{mn}{d}\right) f(d)$$

$$= \sum_{d_1 \mid m} \mu\left(\frac{m}{d_1}\right) f(d_1) \sum_{d_2 \mid n} \mu\left(\frac{n}{d_2}\right) f(d_2) = g(m)\, g(n).$$

Satz 7. *Die Beziehung* $f(t) = \sum_{t \mid d} g(d)$ *bestimmt* $g(t)$ *eindeutig. Ist insbesondere* $f(t)$ *distributiv, nicht die Nullfunktion, so ist* $g(1) = 1$ *und* $g(t)$ *distributiv.*

Beweis: Das Gleichungssystem:

$$\begin{aligned}
g(1) &= f(1),\\
g(1)+g(2) &= f(2),\\
g(1)+g(3) &= f(3),\\
g(1)+g(2)+g(4) &= f(4),\\
g(1)+g(5) &= f(5),\\
g(1)+g(2)+g(3)+g(6) &= f(6),\ \ldots
\end{aligned}$$

gestattet die rekursive Berechnung von $g(1)$, $g(2)$, $g(3)$, ...

Ist jedes $f(t)$ ganz, so auch jedes $g(t)$. Da die in Satz 6 genannte Funktion $g(t)$ im Falle eines nicht identisch verschwindenden distributiven $f(t)$ die Bedingung des Satzes 7 erfüllt, ist sie mit der hier genannten Funktion $g(t)$ identisch, also distributiv.

Im folgenden fragen wir uns, ob es bei einem Modul m Zahlen a mit $(a, m) = 1$ gibt, für die $a^x \equiv 1 \bmod m$ mit $0 < x < \varphi(m)$ gilt. Jedenfalls ist jeder Exponent y mit $a^y \equiv 1 \bmod m$ ein Vielfaches des kleinsten natürlichen Exponenten f mit $a^f \equiv 1$. Denn, wäre $(y, f) = f' < f$, $yY + fF = f'$, so wäre bereits $a^{f'} = (a^y)^Y (a^f)^F \equiv 1$. Näheres im nächsten Paragraphen.

§ 9. Primitive Wurzeln

Bei einem Primzahlmodul p ergibt sich für jedes a mit $(a, p) = 1$ nach dem kleinen Fermat $a^{p-1} \equiv 1 \bmod p$. Folglich gibt es einen kleinsten Exponenten f, so daß $a^f \equiv 1 \bmod p$ $(1 \leqq f \leqq p-1)$, aber $a^x \not\equiv 1$ für $1 \leqq x < f$ ist. Man sagt: a bzw. die Restklasse von a *gehört* $\bmod p$ zum Exponenten f.

Es gelten nun folgende Sätze:

Satz 1. *Jeder Exponent f, zu dem Zahlen $a \not\equiv 0 \bmod p$ gehören, ist ein Teiler von $p-1$.*

Beweis: Wir gehen nach dem Schlußabsatz des vorigen Paragraphen vor, da $p-1$ ein Spezialfall des dortigen y ist.

Satz 2. *Zu jedem Teiler f von $p-1$ gehören entweder keine oder $\varphi(f)$ Restklassen.*

Beweis: Ist $p - 1 \equiv 0 \bmod f$, so sind, wenn a zu f gehört, die f Restklassen von $1, a, a^2, \ldots, a^{f-1}$ voneinander verschieden. Denn wäre etwa $a^u \equiv a^v \bmod p$ mit $u < v \leqq f-1$, so wäre $a^{v-u} \equiv 1 \bmod p$, und $0 < v - u < f$. Aber nur dann, wenn in a^x die Beziehung $(x, f) = 1$ gilt, ist a^x eine zu f gehörige Restklasse.

Dies muß genau untersucht werden:

Ist $(x,f)=1$, so folgt aus $(a^x)^y \equiv 1 \bmod p$ oder $a^{xy} \equiv 1 \bmod p$, daß $f \mid xy$, also wegen $(f,x)=1$ weiter $f \mid y$ ist. Ist $(x,f)=f'$, wobei $f'>1$ ist, so ist $\frac{f}{f'}=f_1$ ganz, und es bleibt

$$\left(a^x\right)^{f_1} = a^{\frac{fx}{f'}} = \left(a^f\right)^{\frac{x}{f'}} \equiv 1 \bmod p,$$

wobei $\frac{x}{f'}$ ebenfalls ganz ist. Mithin gehört a^x zum Exponenten f_1 (oder einem Teiler von f_1), nicht zu f.

Die genannten f Potenzen von a sind zueinander inkongruente Lösungen von $x^f \equiv 1 \bmod p$, also alle, da der Grad dieser Kongruenz (Gleichung in P_p) gerade f ist. Daraus folgt, daß es dann $\varphi(f)$ zu f gehörende Restklassen gibt.

Alles zusammengefaßt ergibt sich der obige Satz.

Wir haben also für jedes $f \mid p-1$ gerade $c_f \cdot \varphi(f)$ Restklassen, wobei die Zahl c_f Null oder Eins sein kann. Insgesamt erhalten wir folgende Aufteilung der $(p-1)$ Restklassen des reduzierten Restsystems $\bmod p$ unter Anwendung des Satzes 3 von § 8

$$\sum_{f \mid p-1} \varphi(f) = p-1 = \sum_{f \mid p-1} c_f \varphi(f).$$

Die Gleichung zwischen der äußeren linken und der äußeren rechten Seite kann nur bei $c_f=1$ für alle f bestehen. Schreiben wir sie z. B. in der Form

$$\sum_{f \mid p-1} (1-c_f)\,\varphi(f) = 0,$$

so haben wir eine Gleichung, in der links eine Summe nichtnegativer Zahlen, rechts Null steht. Eine solche Gleichung kann nur bestehen, wenn alle Zahlen Null sind, für jedes f also

$$c_f = 1$$

ist. Wir haben eine Verschärfung des Satzes 2:

Satz 3. *Zu jedem Teiler f von $p-1$ gehören $\varphi(f)$ Restklassen. Insbesondere gilt dies für $p-1$ selbst. Es gibt also $\varphi(p-1)$ Restklassen, die zu $(p-1)$ gehören. Ist g eine Zahl einer solchen Restklasse, so heißt g eine primitive Wurzel mod p.*

Die aufeinanderfolgenden Potenzen von g, nämlich

$$g^0=1,\ g,\ g^2,\ g^3,\ \ldots,\ g^{p-2},$$

insgesamt $(p-1)$ Potenzen erfüllen das gesamte reduzierte Restsystem von p, nämlich die gesamten Restklassen mit Ausnahme der Nullklasse. Denn ist mit $0 \leqq a < b < p-1$ etwa

$$g^a \equiv g^b \bmod p,$$

so ist $g^{b-a} \equiv 1 \bmod p$ und g gehörte zum Exponenten $b-a < p-1$, oder zu einem Teiler von $b-a$. g gehört aber zu $p-1$. Wir haben also

Satz 4. *Zu jedem Primzahlmodul p gibt es $\varphi(p-1)$ primitive Wurzeln.*

Satz 5. *Jede Restklasse mod p wird durch eine Potenz einer gegebenen primitiven Wurzel mit Exponent zwischen Null und $p-2$ (beide inbegriffen) eindeutig festgelegt.*

Im übrigen ist der Exponent nur mod $(p-1)$ bestimmt.

Definition. *Bei gegebener Primitivwurzel g wird einer Restklasse a des reduzierten Restsystems mod p der Index a, geschrieben ind a mod $(p-1)$ zugeordnet, wenn $g^{\text{ind}\,a} \equiv a \bmod p$ ist.*

Wir folgern

Satz 6. *Der Index hat mod $(p-1)$ logarithmische Eigenschaft, d. h., es ist ind $(ab) \equiv$ ind $a +$ ind b mod $(p-1)$.*

Beweis: Es ist $ab \equiv g^{\text{ind}\,a} g^{\text{ind}\,b} \equiv g^{\text{ind}\,a + \text{ind}\,b} \bmod p$.

Wir sehen, daß sich genau wie beim logarithmischen Rechnen Rechenoperationen, wenn eine Indextafel vorliegt, sehr erleichtern lassen.

Zunächst ist die Kenntnis einer primitiven Wurzel mod p notwendig. Prinzipiell ist dies durch sehr umfangreiche Rechnungen immer möglich. Man probiert, ob 2, 3, ... primitive Wurzel ist, wobei man höchstens $p-2$ Versuche zu machen hat ($p-1$ kommt für $p > 3$ nicht in Frage). Das ist natürlich sehr umständlich. Man kennt Verfahren, mit deren Hilfe sich dies wenigstens einigermaßen abkürzen läßt. Im folgenden betrachten wir den Spezialfall $p = 31$, wobei wir annehmen, daß die primitive Wurzel $g = 17$ bekannt ist. Wir könnten auch z. B. von $g = 3$ ausgehen, was ebenfalls eine primitive Wurzel mod 31 ist. Bei 17 ist die Rechnung wegen $17^2 \equiv 10 \bmod 31$ besonders leicht.

Zunächst verfertigen wir auf diesem Wege eine Indexgegentafel „vom Index zur Zahl".

Tafel 1. Indexgegentafel mod 31

ind a	a	ind a	a	ind a	a	ind a	a	ind a	a	ind a	a
0	1	5	26	10	25	15	30	20	5	25	6
1	17	6	8	11	22	16	14	21	23	26	9
2	10	7	12	12	2	17	21	22	19	27	29
3	15	8	18	13	3	18	16	23	13	28	28
4	7	9	27	14	20	19	24	24	4	29	11

Es ist also z. B. $g^{16} \equiv 17^{16} \equiv 14 \bmod 31$.

Durch Umordnung erhält man die Indextafel selbst.

a	ind a	a	ind a	a	ind a	a	ind a	a	ind a	a	ind a
1	0	6	25	11	29	16	18	21	17	26	5
2	12	7	4	12	7	17	1	22	11	27	9
3	13	8	6	13	23	18	8	23	21	28	28
4	24	9	26	14	16	19	22	24	19	29	27
5	20	10	2	15	3	20	14	25	10	30	15

Nun geben wir einige Beispiele für die Anwendung der Indextafel.

1. Der kleinste positive Rest mod 31 von $A = 979 \cdot 1563$ ist zu berechnen. Wegen $979 \equiv 18$, $1563 \equiv 13$ wird $\operatorname{ind} A \equiv \operatorname{ind} 18 + \operatorname{ind} 13 \bmod 30$ also $\operatorname{ind} A \equiv 8 + 23 \equiv 1 \bmod 30$, $A \equiv 17 \bmod 31$.

2. Ist $22x \equiv 21 \bmod 31$ zu lösen, so bleibt $\operatorname{ind} x + \operatorname{ind} 22 \equiv \operatorname{ind} 21 \bmod 30$, $\operatorname{ind} x + 11 \equiv 17 \bmod 30$. Das gibt aber sofort $\operatorname{ind} x \equiv 6 \bmod 30$, $x \equiv 8 \bmod 31$.

3. Ist der kleinste positive Rest von $B = 1093^{6857} \bmod 31$ zu finden, so haben wir: $1093 \equiv 1000 \bmod 31$, $\operatorname{ind} 10 \equiv 2 \bmod 30$, $\operatorname{ind} 1000 \equiv 6 \bmod 30$; da $6857 \equiv 17 \bmod 30$ ist, so wird $\operatorname{ind} B \equiv 17 \cdot 6 \equiv 102 \equiv 12 \bmod 30$, $B \equiv 2 \bmod 31$.

4. Um den kleinsten positiven Rest von $C = 9^{9^9} \bmod 31$ zu finden, bedenken wir $9^3 \equiv 9 \bmod 30$, also durch nochmaliges Kubieren $9^9 \equiv 9^3 \equiv 9 \bmod 30$. Daher ist $\operatorname{ind} C \equiv 9 \operatorname{ind} 9 \equiv 9 \cdot 26 \equiv 234 \equiv 24 \bmod 30$, $C \equiv 4 \bmod 31$.

Nun soll die Frage erörtert werden, ob es auch zu anderen Moduln außer Primzahlmoduln primitive Wurzeln gibt.

Wir betrachten zuerst den Modul $2p$, p ungerade Primzahl. Es ist entweder $g\,(0 < g < p)$ oder $g + p$ ungerade, weiter ist $\varphi(2p) = \varphi(2)\,\varphi(p) = p - 1$. Ist nun g eine primitive Wurzel mod p, g_1 die ungerade der Zahlen g und $g + p$, dann ist g_1 offenbar eine primitive Wurzel mod p. Für $p = 2$, $2p = 4$ ist $g = 3$ eine primitive Wurzel, die einzige mod 4. Wir haben

Satz 7. *Für den Modul $2p$, wobei p eine Primzahl ist, gibt es $\varphi(\varphi(2p)) = \varphi(p-1)$ primitive Wurzeln.*

Es gibt keine primitiven Wurzeln mod 8. Denn bei einem zusammengesetzten Modul m müßte eine solche die Beziehung $g^x \not\equiv 1$ für $0 < x < \varphi(m)$ erfüllen. Es ist $\varphi(8) = 4$, aber $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1 \bmod 8$. Analoges gilt von höheren Potenzen von 2, wie man leicht sieht.

Nun sei p^m eine ungerade Primzahlpotenz. Wir brauchen zunächst

Satz 8. *Ist $(a, p) = 1$, p eine Primzahl und $a^p \equiv a \bmod p^2$, so ist $(a + p)^p \not\equiv a + p \bmod p^2$.*

Beweis: Es ist

$$(a + p)^p = a^p + \sum_{j>0} \binom{p}{j} a^{p-j} p^j,$$

wobei alle Glieder der Summe durch p^2 teilbar sind, also $(a + p)^p \equiv a^p \equiv a \bmod p^2$ und damit $(a + p)^p \not\equiv a + p \bmod p^2$.

Wir fragen uns nun, was unter einer primitiven Wurzel $g \bmod p^m$ zu verstehen ist. Es muß $g^x \not\equiv 1$ für $0 < x < \varphi(p^m) = p^{m-1}(p - 1)$ sein.

Wir beweisen zuerst

Satz 9. *Es gibt primitive Wurzeln $g \bmod p$, für die $g^{p-1} \not\equiv 1 \bmod p^2$ gilt.*

Beweis: Nach dem vorigen Satz kann man folgendermaßen schließen: Erfüllt eine primitive Wurzel g' die Kongruenz $x^{p-1} \equiv 1 \bmod p^2$, so wird diese Kongruenz durch die primitive Wurzel $g = g' + p$ nicht erfüllt.

Satz 10. *Ist p eine beliebige Primzahl, $(ab, p) = 1$, $k > 0$ und gilt $p^k \parallel a - b$, dann gilt auch $p^{k+1} \parallel a^p - b^p$ mit Ausnahme des Falles $p = 2$, $k = 1$, in welchem $2^3 \mid a^2 - b^2$ gilt, ohne daß sich über den genauen Exponenten x in $2^x \parallel a^2 - b^2$ etwas aussagen läßt.*

Beweis: Mit $a = b + Cp^k$, also C ganz, $C \not\equiv 0 \bmod p$ wird

$$a^p = b^p + p^{k+1} b^{p-1} C + \sum_{2 \leqq j \leqq p-1} \binom{p}{j} b^{p-j} p^{kj} C^j + C^p p^{kp}.$$

Heißt A das zweite, B das letzte Glied rechts, so ist $p^{k+1} \parallel A$, $p^{kp} \parallel B$; da außer in dem vorläufig ausgeschlossenen Falle $p = 2$, $k = 1$ stets $kp > k + 1$ ist, so ist $p^{k+1} \parallel A + B$ und auch, wenn die Glieder der Summe beigefügt werden, bleibt die Summe durch p^{k+1}, nicht durch p^{k+2} teilbar, da die Glieder der Summe alle durch p^{2k+1} teilbar sind.

Tafel 1. Indexgegentafel mod 31

ind a	a	ind a	a	ind a	a	ind a	a	ind a	a	ind a	a
0	1	5	26	10	25	15	30	20	5	25	6
1	17	6	8	11	22	16	14	21	23	26	9
2	10	7	12	12	2	17	21	22	19	27	29
3	15	8	18	13	3	18	16	23	13	28	28
4	7	9	27	14	20	19	24	24	4	29	11

Es ist also z. B. $g^{16} \equiv 17^{16} \equiv 14 \bmod 31$.

Durch Umordnung erhält man die Indextafel selbst.

a	ind a	a	ind a	a	ind a	a	ind a	a	ind a	a	ind a
1	0	6	25	11	29	16	18	21	17	26	5
2	12	7	4	12	7	17	1	22	11	27	9
3	13	8	6	13	23	18	8	23	21	28	28
4	24	9	26	14	16	19	22	24	19	29	27
5	20	10	2	15	3	20	14	25	10	30	15

Nun geben wir einige Beispiele für die Anwendung der Indextafel.

1. Der kleinste positive Rest mod 31 von $A = 979 \cdot 1563$ ist zu berechnen. Wegen $979 \equiv 18$, $1563 \equiv 13$ wird $\operatorname{ind} A \equiv \operatorname{ind} 18 + \operatorname{ind} 13 \bmod 30$ also $\operatorname{ind} A \equiv 8 + 23 \equiv 1 \bmod 30$, $A \equiv 17 \bmod 31$.

2. Ist $22x \equiv 21 \bmod 31$ zu lösen, so bleibt $\operatorname{ind} x + \operatorname{ind} 22 \equiv \operatorname{ind} 21 \bmod 30$, $\operatorname{ind} x + 11 \equiv 17 \bmod 30$. Das gibt aber sofort $\operatorname{ind} x \equiv 6 \bmod 30$, $x \equiv 8 \bmod 31$.

3. Ist der kleinste positive Rest von $B = 1093^{6857} \bmod 31$ zu finden, so haben wir: $1093 \equiv 1000 \bmod 31$, $\operatorname{ind} 10 \equiv 2 \bmod 30$, $\operatorname{ind} 1000 \equiv 6 \bmod 30$; da $6857 \equiv 17 \bmod 30$ ist, so wird $\operatorname{ind} B \equiv 17 \cdot 6 \equiv 102 \equiv 12 \bmod 30$, $B \equiv 2 \bmod 31$.

4. Um den kleinsten positiven Rest von $C = 9^{9^9} \bmod 31$ zu finden, bedenken wir $9^3 \equiv 9 \bmod 30$, also durch nochmaliges Kubieren $9^9 \equiv 9^3 \equiv 9 \bmod 30$. Daher ist $\operatorname{ind} C \equiv 9 \operatorname{ind} 9 \equiv 9 \cdot 26 \equiv 234 \equiv 24 \bmod 30$, $C \equiv 4 \bmod 31$.

Nun soll die Frage erörtert werden, ob es auch zu anderen Moduln außer Primzahlmoduln primitive Wurzeln gibt.

Wir betrachten zuerst den Modul $2p$, p ungerade Primzahl. Es ist entweder $g\,(0 < g < p)$ oder $g + p$ ungerade, weiter ist $\varphi(2p) = \varphi(2)\,\varphi(p) = p - 1$. Ist nun g eine primitive Wurzel mod p, g_1 die ungerade der Zahlen g und $g + p$, dann ist g_1 offenbar eine primitive Wurzel mod p. Für $p = 2$, $2p = 4$ ist $g = 3$ eine primitive Wurzel, die einzige mod 4. Wir haben

Satz 7. *Für den Modul $2p$, wobei p eine Primzahl ist, gibt es $\varphi(\varphi(2p)) = \varphi(p-1)$ primitive Wurzeln.*

Es gibt keine primitiven Wurzeln mod 8. Denn bei einem zusammengesetzten Modul m müßte eine solche die Beziehung $g^x \not\equiv 1$ für $0 < x < \varphi(m)$ erfüllen. Es ist $\varphi(8) = 4$, aber $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1 \bmod 8$. Analoges gilt von höheren Potenzen von 2, wie man leicht sieht.

Nun sei p^m eine ungerade Primzahlpotenz. Wir brauchen zunächst

Satz 8. *Ist $(a, p) = 1$, p eine Primzahl und $a^p \equiv a \bmod p^2$, so ist $(a+p)^p \not\equiv a + p \bmod p^2$.*

Beweis: Es ist

$$(a+p)^p = a^p + \sum_{j>0} \binom{p}{j} a^{p-j} p^j,$$

wobei alle Glieder der Summe durch p^2 teilbar sind, also $(a+p)^p \equiv a^p \equiv a \bmod p^2$ und damit $(a+p)^p \not\equiv a + p \bmod p^2$.

Wir fragen uns nun, was unter einer primitiven Wurzel $g \bmod p^m$ zu verstehen ist. Es muß $g^x \not\equiv 1$ für $0 < x < \varphi(p^m) = p^{m-1}(p-1)$ sein.

Wir beweisen zuerst

Satz 9. *Es gibt primitive Wurzeln $g \bmod p$, für die $g^{p-1} \not\equiv 1 \bmod p^2$ gilt.*

Beweis: Nach dem vorigen Satz kann man folgendermaßen schließen: Erfüllt eine primitive Wurzel g' die Kongruenz $x^{p-1} \equiv 1 \bmod p^2$, so wird diese Kongruenz durch die primitive Wurzel $g = g' + p$ nicht erfüllt.

Satz 10. *Ist p eine beliebige Primzahl, $(ab, p) = 1$, $k > 0$ und gilt $p^k \parallel a - b$, dann gilt auch $p^{k+1} \parallel a^p - b^p$ mit Ausnahme des Falles $p = 2$, $k = 1$, in welchem $2^3 \mid a^2 - b^2$ gilt, ohne daß sich über den genauen Exponenten x in $2^x \parallel a^2 - b^2$ etwas aussagen läßt.*

Beweis: Mit $a = b + Cp^k$, also C ganz, $C \not\equiv 0 \bmod p$ wird

$$a^p = b^p + p^{k+1} b^{p-1} C + \sum_{2 \leqq j \leqq p-1} \binom{p}{j} b^{p-j} p^{kj} C^j + C^p p^{kp}.$$

Heißt A das zweite, B das letzte Glied rechts, so ist $p^{k+1} \parallel A$, $p^{kp} \parallel B$; da außer in dem vorläufig ausgeschlossenen Falle $p = 2$, $k = 1$ stets $kp > k+1$ ist, so ist $p^{k+1} \parallel A + B$ und auch, wenn die Glieder der Summe beigefügt werden, bleibt die Summe durch p^{k+1}, nicht durch p^{k+2} teilbar, da die Glieder der Summe alle durch p^{2k+1} teilbar sind.

In dem ausgeschlossenen Falle $p = 2$, $k = 1$ wird die Summe leer, es gilt $A = 4A'$, $B = 4B'$ mit ungeradem A', B', also $A + B = 4(A' + B')$ mit geradem $A' + B'$, $A + B \equiv 0 \bmod 8$. Über den genauen Exponenten x in $2^x \parallel a^2 - b^2$ läßt sich nichts Allgemeines sagen: 1. Ist $a = 7$, $b = 5$, so ist $2^3 \parallel a^2 - b^2 = 24$. 2. Mit $a = 9$, $b = 7$ ist $2^5 \parallel a^2 - b^2 = 32$. 3. Mit $a = 1$, $b = -1$ ist $a^2 - b^2 = 0$, so daß man keinen Exponenten x mit $2^x \parallel a^2 - b^2 = D$ angeben kann. Man könnte $2^\infty \parallel D = 0$ schreiben, was nur bedeutet: Jede noch so hohe Potenz von 2 geht in $D = 0$ auf.

Satz 11. *Aus $p^k \parallel a^p - b^p$, $k > 0$ folgt zunächst $k > 1$. Weiter ergibt sich für ungerade Primzahlen p, daß $p^{k-1} \parallel a - b$ ist. Dabei ist $(ab, p) = 1$ vorausgesetzt.*

Beweis: Nach dem kleinen Fermat folgt zunächst $a \equiv b \bmod p$, nach dem vorigen Satz folgt aus $p^l \parallel a - b$, daß $l + 1 = k$ ist usw.

Satz 12. *Eine nach Satz 9 existierende primitive Wurzel $g \bmod p$ mit $g^{p-1} \not\equiv 1 \bmod p^2$ ist auch primitive Wurzel mod p^m, wobei $m > 1$ beliebig groß ist. Dabei ist p Primzahl > 2.*

Beweis: Zunächst sei $m = 2$. Aus $g^f \equiv 1 \bmod p^2$, wobei f der Exponent ist, zu dem $g \bmod p^2$ gehört, folgt zunächst $f \mid \varphi(p^2)$, genau wie beim Beweis des Satzes 2. Weiter ist $f \equiv 0 \bmod (p-1)$, wie man sofort sieht, wenn man die Kongruenz als solche mod p betrachtet und bedenkt, daß g primitive Wurzel mod p ist. Mithin gilt $p - 1 \mid f \mid \varphi(p^2) = p(p-1)$, wo aber $p - 1 < f$ ist, da $g^{p-1} \equiv 1 \bmod p^2$ nicht erfüllt ist. Es ist also $f = \varphi(p^2)$.

Ist der Satz schon für $m - 1$ bewiesen, so können wir die vollständige Induktion genau so durchführen. Bei f als Exponenten, zu dem $g \bmod p^m$ gehört, gilt $f \equiv 0 \bmod \varphi(p^{m-1}) = p^{m-2}(p-1)$; denn dies folgt, wenn wir $g^f \equiv 1 \bmod p^m$ als Kongruenz mod p^{m-1} auffassen. Nach Satz 10 folgt aber aus $p \parallel g^{p-1} - 1$ der Reihe nach $p^2 \parallel g^{p(p-1)} - 1$, $p^3 \parallel g^{p^2(p-1)} - 1, \ldots$, schließlich

$$p^m \parallel g^{p^{m-1}(p-1)} - 1 = g^{\varphi(p^m)} - 1 .$$

Damit folgt $p^{m-2}(p-1) \mid f \mid \varphi(p^m) = p^{m-1}(p-1)$, aber zugleich $p^{m-2}(p-1) < f$. Damit bleibt $f = \varphi(p^m)$, w. z. b. w.

Satz 13. *Ein Modul $m = a \cdot b$ mit $a \geqq 3$, ungeradem $b \geqq 3$ und $(a, b) = 1$, gestattet keine primitiven Wurzeln.*

Beweis: Bei beliebigem r mit $(r, m) = 1$ gilt $r^{\varphi(a)} \equiv 1 \bmod a$, $r^{\varphi(b)} \equiv 1 \bmod b$, also $r^v \equiv 1 \bmod ab$, wenn v das kleinste gemeinsame Vielfache von $\varphi(a)$ und $\varphi(b)$ ist. Da aber $\varphi(a) \equiv \varphi(b) \equiv 0 \bmod 2$ ist, gilt die Ungleichung $v \leqq \frac{\varphi(a)\,\varphi(b)}{2} = \frac{\varphi(ab)}{2}$. Es gibt mithin keine zu $\varphi(ab)$ gehörige Restklasse, w. z. b. w.

§ 10. Allgemeine lineare Kongruenzen

Wir nehmen an, es sei mit ganzem a, b, m eine Kongruenz

$$ax \equiv b \bmod m \tag{1}$$

mit $(m, a) = d > 1$

gegeben.

Jedenfalls muß $d \mid b$ sein, sonst hat die Kongruenz keine Lösung. Wir wollen also $b \equiv 0 \bmod d$ annehmen.

Dann ist aber (1) mit der folgenden Kongruenz gleichbedeutend, wenn wir zur Abkürzung

$$\frac{a}{d} = a_1, \qquad \frac{b}{d} = b_1, \qquad \frac{m}{d} = c$$

setzen, also a_1, b_1, c ganz sind und $(a_1, c) = 1$ ist:

$$a_1 x \equiv b_1 \bmod c. \tag{2}$$

Diese hat also stets mod c eine und nur eine Lösung, etwa $x \equiv A \bmod c$.

Die folgenden d zueinander mod m inkongruenten Zahlen

$$A,\ A + c,\ A + 2c,\ \ldots,\ A + (d-1)c \tag{3}$$

erfüllen (2), und damit auch (1), also hat (1) d inkongruente Lösungen mod m und offenbar keine weiteren, da nur diese Restklassen mod m der Zahl A nach c kongruent sind.

Wir haben also folgenden

Satz 1. *Eine Kongruenz*

$$ax \equiv b \bmod m$$

mit ganzzahligem a, b, m, $a \neq 0$, $(a, m) = d > 1$ ist für $b \not\equiv 0$ mod d unlösbar. Bei $b \equiv 0$ mod d löse man mit den Abkürzungen $\frac{a}{d} = a_1$, $\frac{b}{d} = b_1$, $\frac{m}{d} = c$ die Kongruenz $a_1 x \equiv b_1 \bmod c$, etwa durch $x \equiv A$ und hat die d mod m inkongruenten Lösungen $A + uc$ mit $0 \leqq u < d$.

Beispiele: Man löse

1. $3x \equiv 15 \bmod 21$.
2. $7x \equiv 42 \bmod 91$.
3. $2x \equiv 6 \bmod 26$.
4. $5x \equiv 5 \bmod 10$.
5. $25x \equiv 75 \bmod 100$.
6. $221x \equiv 85 \bmod 340$.

Bemerkung zu 6: Es ist $221 = 13 \cdot 17$.

§ 11. Binomische Kongruenzen

Wir definieren eine binomische Kongruenz mit der Unbekannten x, gegebenen ganzzahligen A und m und einer natürlichen Zahl $n > 1$ wie folgt

$$x^n \equiv A \bmod m. \tag{1}$$

Satz 1. *Die Lösung einer binomischen Kongruenz läßt sich auf die Auflösung nach den Primzahlpotenzfaktoren des Moduls und die Lösung eines Simultansystems linearer Kongruenzen zurückführen.*

Beweis: Es sei $f(x) = x^n - A$. Wir können die gegebene Kongruenz in die r Kongruenzen $f(x) \equiv 0 \bmod p_1^{a_1}, \ldots, \bmod p_r^{a_r}$ zergliedern, wenn $m = \prod_{i=1}^{r} p_i^{a_i}$ die kanonische Zerlegung von m ist. Hat eine dieser Kongruenzen keine Lösung, dann hat auch (1) keine. Haben alle diese Kongruenzen Lösungen, und zwar die erste m_1, die zweite $m_2, \ldots$, die letzte m_r, so haben wir $M = \prod_{i=1}^{r} m_i$ Simultankongruenzen für x mit paarweise primen Moduln und demnach $M \bmod m$ inkongruente Lösungen.

Bei der Beweisführung ist der spezielle Charakter von $f(x)$ als linke Seite einer auf Null reduzierten binomischen Kongruenz überhaupt nicht angewandt worden. Wir können den allgemeineren Satz aussprechen:

Satz 2. *Die Lösung einer Kongruenz n-ten Grades*

$$f(x) = a_0 x^n + \cdots + a_n \equiv 0 \bmod m,$$

in der mindestens ein Koeffizient durch m nicht teilbar ist, läßt sich auf die Lösung von Kongruenzen nach Primzahlpotenzmoduln und eines Systems linearer Kongruenzen zurückführen.

Im folgenden werde bei (1) immer $(A, m) = 1$ vorausgesetzt. Ist dann die Kongruenz lösbar, so spricht man von A als einem *n-ten*

Potenzrest mod m; ist sie unlösbar, so sagt man: A ist *n-ter Potenznichtrest* mod m.
Im Falle $n = 2$ spricht man von *quadratischen Resten* und *quadratischen* Nichtresten. Das Wort quadratisch wird im folgenden bei diesen Begriffen überall weggelassen, wo es aus dem Zusammenhang hervorgeht.
Es ist z. B. 2 quadratischer Rest mod 7, weil $3^2 \equiv 2 \bmod 7$ ist, dagegen -1 quadratischer Nichtrest mod 4, da jedes ungerade Quadrat durch 4 dividiert den Rest 1 läßt.
Für $n = 3$ haben wir kubische Reste bzw. Nichtreste. Es ist z. B. 2 ein kubischer Rest mod 31 wegen $4^3 \equiv 2 \bmod 31$.
Nochmals sei betont, daß wir für $(A, m) > 1$ weder von n-ten Potenzresten, noch von n-ten Potenznichtresten sprechen. Z. B. 44 ist nicht quadratischer Rest mod 100, obwohl $12^2 \equiv 44 \bmod 100$ gilt.

Satz 3. *Sind r und s prim zueinander, dann ist A mit $(A, m) = 1$ genau dann rs-ter Potenzrest mod m, wenn es sowohl r-ter als auch s-ter Potenzrest ist.*

Beweis:
I. $B^{rs} \equiv A \bmod m$ hat $(B^s)^r \equiv A$ und $(B^r)^s \equiv A$ zur Folge.
II. Ist $C^r \equiv A$, $D^s \equiv A \bmod m$ und sind x, y ganze Zahlen mit $rx + sy = 1$, so ist

$$C^{rsy} D^{rsx} \equiv A \bmod m,$$

also

$$(C^y D^x)^{rs} \equiv A \bmod m.$$

Wir können uns auf l^n-te Potenzreste beschränken, wobei l eine Primzahl ist. Zur Abkürzung sei $h = l^n$ gesetzt.
Wir haben also zu untersuchen:

$$x^h \equiv A \bmod p^r, \tag{2}$$

wobei $p \nmid A$ eine Primzahl ist.
Es sei $p \neq l$, $p > 2$. Mit einer primitiven Wurzel $g \bmod p^r$, wobei der Index mod $\varphi(p^r)$ zu nehmen ist, haben wir sofort aus (2)

$$l^n \operatorname{ind} x \equiv \operatorname{ind} A \bmod \varphi(p^r) = p^{r-1}(p-1). \tag{3}$$

Ist nun $l \nmid p - 1$, so hat (3) genau eine Wurzel mod $\varphi(p^r)$, also (2) genau eine Wurzel mod p^r. Ist $l^z (z \leqq n) = (l^n, p-1)$, so muß $\operatorname{ind} A \equiv 0 \bmod l^z$ sein; dann hat (3) und damit (2) genau l^z Lösungen; sonst keine. Für $z = 0$ ist also genau eine Lösung da.

Der Fall $p = 2$ entzieht sich dieser Untersuchungsmethode: Zunächst muß in diesem Falle A ungerade sein. $x^h \equiv 1 \bmod 2$ ist trivial lösbar. $x^h \equiv A \bmod 2^{r-1}$ sei schon gelöst; die einzige Lösung sei $x \equiv X \bmod 2^{r-1}$. Dann gibt der Ansatz $x = X + y \cdot 2^{r-1}$ durch Einsetzen in die Kongruenz, wenn $X^h - A = C \cdot 2^{r-1}$ ist,

$$hX^{h-1} y \cdot 2^{r-1} \equiv C \cdot 2^{r-1} \bmod 2^r,$$

das heißt

$$hX^{h-1} y \equiv C \bmod 2,$$

und da hX^{h-1} ungerade ist, einfach

$$y \equiv C \bmod 2.$$

Damit ist dieser Fall ebenfalls erledigt, indem rekursiv gezeigt ist, daß eine und nur eine Lösung existiert. Er ordnet sich dem Falle $(l^h, p-1) = 1$ unter. Es bleibt

Satz 4. *Sind l, p voneinander verschiedene Primzahlen, so hat die Kongruenz $x^h \equiv A \bmod p^r$ mit $(A, p) = 1$, $h = l^n$ im Falle $(l^n, p-1) = 1$ eine und nur eine Lösung, dagegen für $(l^n, p-1) = l^z$ mit $z \geqq 1$ entweder l^z Lösungen oder keine.*

Damit ist der Fall $p \neq l$ weitgehend erledigt; wir wenden uns dem Fall $p = l$ zu. Immer sei $(A, l) = 1$. Wir setzen zuerst $n = 1$, also $h = l$.

Satz 5. *$x^l \equiv A \bmod l$ hat nur die Lösung $x \equiv A \bmod l$.*

Der Beweis folgt sofort aus dem kleinen Fermat.

Satz 6. *Mit $l > 2$ hat $x^l \equiv A \bmod l^m$ genau für $A^{l-1} \equiv 1 \bmod l^2$ Lösungen, und zwar dann l inkongruente ($m \geqq 2$).*

Beweis:

I. Daß die Bedingung notwendig ist, ist klar. Denn aus der Lösbarkeit von $x^l \equiv A \bmod l^m$ folgt die Lösbarkeit $\bmod l^2$ und daraus

$$A^{l-1} \equiv x^{l(l-1)} \equiv x^{\varphi(l^2)} \equiv 1 \bmod l^2.$$

II. Ist g eine primitive Wurzel $\bmod l^2$, also nach Satz 12 von § 9 auch primitive Wurzel nach jeder noch so hohen Potenz von l, so gilt folgendes:

Wir wollen mit $\operatorname{ind}_i C$ den Index einer Zahl C mit $(C, l) = 1$ bezeichnen, wenn g als primitive Wurzel $\bmod l^i$ gilt. Dabei ist $i \geqq 2$ und $\operatorname{ind}_i C \equiv \operatorname{ind}_2 C \bmod l\,(l-1) = \varphi(l^2)$. Es sei $X = \operatorname{ind}_i C$, $Y = \operatorname{ind}_2 C$. Aus $g^X \equiv C \bmod l^i$, also auch $g^X \equiv C \bmod l^2$, weiter

$g^Y \equiv C \bmod l^2$ folgt $X \equiv Y \bmod l\,(l-1) = \varphi(l^2)$. Ist nun $A^{l-1} \equiv 1 \bmod l^2$, also $\operatorname{ind}_2 A \equiv 0 \bmod l$, so ist auch $\operatorname{ind}_m A \equiv 0 \bmod l$. Die Kongruenz $x^l \equiv A \bmod l^m$ geht über in $l \operatorname{ind} x \equiv \operatorname{ind}_m A \bmod l^{m-1}\,(l-1) = \varphi(l^m)$. Wegen $(\varphi(l^m), l) = l \mid \operatorname{ind}_m A$ hat diese lineare Kongruenz l Lösungen.
Wir untersuchen jetzt die quadratischen Reste nach Zweierpotenzen.

Satz 7. *$A \equiv 1 \bmod 4$ ist notwendig und hinreichend, damit A quadratischer Rest von 4 ist, $x^2 \equiv A \bmod 4$ hat dann zwei Lösungen.*

Der Beweis ist trivial.

Satz 8. *$A \equiv 1 \bmod 8$ ist notwendig und hinreichend, damit A quadratischer Rest mod 2^T mit $T \geqq 3$ ist, $x^2 \equiv A \bmod 2$ hat dann vier Lösungen.*
Beweis: $x^2 \equiv 1 \bmod 8$ hat die vier Lösungen $x \equiv 1, 3, 5, 7 \bmod 8$, $x^2 \equiv A \bmod 8$ mit A (ungerade!) $\not\equiv 1 \bmod 8$ hat keine Lösung.
Der Satz sei für $T-1$ bewiesen, wobei $T \geqq 4$ angenommen werden kann. Von einer Lösung $B^2 \equiv A \bmod 2^{T-1}$ ausgehend setzen wir $x = B + y \cdot 2^{T-2}$ und erhalten durch Einsetzen in $x^2 \equiv A \bmod 2^T$ die Kongruenz

$$B^2 - A + By \cdot 2^{T-1} + U \equiv 0 \bmod 2^T \tag{4}$$

mit der Abkürzung

$$U = y^2 \cdot 2^{2T-4}.$$

Nun ist aber $2T - 4 \geqq T$, also $U \equiv 0 \bmod 2^T$. Damit wird die Kongruenz (4), wenn noch $B^2 - A = V \cdot 2^{T-1}$ (mit ganzzahligem V) gesetzt wird

$$V \cdot 2^{T-1} + By \cdot 2^{T-1} \equiv 0 \bmod 2^T \tag{5}$$

oder

$$V + By \equiv 0 \bmod 2. \tag{6}$$

Damit ist, da B ungerade ist, die Größe y berechenbar.
Es ist noch zu zeigen, daß es genau 4 Lösungen gibt. Das sei für $T(\geqq 3)$ bewiesen und soll für $T+1$ gezeigt werden.
Es sei N eine Lösung von $x^2 \equiv A \bmod 2^{T+1}$.
Wir gehen von $M^2 \equiv N^2 \equiv A \bmod 2^{T-1}$ aus. Es ist keine Einschränkung der Allgemeinheit, $M + N \equiv 2 \bmod 4$, also $2 \parallel M + N$ anzunehmen. Denn $M + N$, $M - N$ können nicht beide durch 4 teilbar sein, da sonst M und N gerade wären. Ist $M + N \equiv 0 \bmod 4$, so ersetze man N durch $-N$. Es folgt $M - N \equiv 0 \bmod 2^T$.

Also muß entweder $M \equiv N \bmod 2^{T+1}$ oder $M \equiv N + 2^T \bmod 2^{T+1}$ sein. Diese zweite Zahl erfüllt auch $x^2 \equiv A \bmod 2^{T+1}$. Die vier Lösungen sind also $\pm N$, $\pm N + 2^T$.

Satz 9. *Ist l eine Primzahl > 2, A nicht durch l teilbar, $n > 1$, $h = l^n$, so ist mit $C = min\,(n, r-1)$ zur Lösbarkeit von $x^h \equiv A \bmod l^r$ $(r > 1)$ notwendig und hinreichend, daß A ein l^C-ter Potenzrest mod l^{C+1} ist.*

Beweis: Ist g eine primitive Wurzel mod l^r, so gibt die Kongruenz die folgende

$$l^n \operatorname{ind} x \equiv \operatorname{ind} A \bmod l^{r-1}(l-1) = m \tag{7}$$

(abkürzende Bezeichnung).
Sofort sehen wir $(l^n, m) = l^C$. Genau dann, wenn (7) lösbar ist, gilt $\operatorname{ind} A \equiv 0 \bmod l^C$, d. h. A ist ein l^C-ter Potenzrest mod l^{C+1} (7) und die gegebene Kongruenz haben dann l^C Lösungen.
Den Fall $l = 2$ wollen wir in diesem Buche nicht erörtern.
Rückschauend können wir für eine ungerade Primzahl p den Satz aussprechen:

Satz 10. *Die binomische Kongruenz*

$$x^m - A \equiv 0 \bmod p$$

mit $(A, p) = 1$ hat für $(m, p-1) = 1$ genau eine Wurzel. Ist $(m, p-1) = d > 1$, so hat sie nur für $\operatorname{ind} A \equiv 0 \bmod d$ Wurzeln, und zwar dann genau d Wurzeln.

Beispiel: $x^3 \equiv 2 \bmod 31$ gibt mit der Indextafel $3 \operatorname{ind} x \equiv 12 \bmod 30$, damit $\operatorname{ind} x \equiv 4 \bmod 10$, $\operatorname{ind} x \equiv 4, 14, 24 \bmod 30$, $x \equiv 7, 20, 4 \bmod 31$.

Bemerkung: Wie man sieht, ist die Bedingung $\operatorname{ind} A \equiv 0$ von der Wahl der primitiven Wurzel unabhängig.

Satz 11. *Für jede ungerade Primzahl p gibt es genau $\frac{p-1}{2}$ quadratische Reste und Nichtreste.*

Beweis: Es muß $\operatorname{ind} A \equiv 0 \bmod 2$ sein, damit A ein Rest ist, $\operatorname{ind} A \equiv 1 \bmod 2$ gibt die Nichtreste.

Satz 12. *Sei p eine ungerade Primzahl, so ist das Produkt zweier (quadratischer) Reste oder Nichtreste ein Rest, das Produkt eines Restes und eines Nichtrestes ein Nichtrest.*

Beweis: Es seien im folgenden r, r_1, r_2 Reste; n, n_1, n_2 Nichtreste.

Es ist $\operatorname{ind} r_1 + \operatorname{ind} r_2 \equiv 0$, $\operatorname{ind} n_1 + \operatorname{ind} n_2 \equiv 0$, $\operatorname{ind} n + \operatorname{ind} r \equiv 1$, alles mod 2.

Satz 13. *Es ist* $g^{\frac{p-1}{2}} \equiv -1 \bmod p$, *wenn* g *eine primitive Wurzel ist.*

Beweis: Es ist mit $h = g^{\frac{p-1}{2}}$ sofort $h^2 \equiv 1 \bmod p$. Aber es ist $h \equiv 1 \bmod p$ ausgeschlossen, da sonst g keine primitive Wurzel wäre; also bleibt $h \equiv -1 \bmod p$.

In Satz 13 kann auch $\operatorname{ind}(-1) = \operatorname{ind}(p-1) = \frac{p-1}{2}$ geschrieben werden. Dieser Index ist also von der Wahl der primitiven Wurzel unabhängig.

Satz 14. *Für jeden Rest* r *ist* $r^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Beweis: Es ist

$\operatorname{ind} r \equiv a \bmod (p-1)$ mit $2 \mid a$, daraus $\frac{p-1}{2} \operatorname{ind} a \equiv 0 \bmod (p-1)$.

Satz 15. *Für jeden Nichtrest* n *ist* $n^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Beweis: Es ist $\operatorname{ind} n \equiv b \bmod (p-1)$ mit ungeradem b. Der weitere Schluß ist völlig analog.

Definition. *Wir bezeichnen für zu* p *(ungerade Primzahl) prime* a *die positive Einheit mit* $\left(\frac{a}{p}\right)$, *wenn* a *quadratischer Rest nach* p *ist, dagegen mit dem gleichen Symbol die negative Einheit, wenn* a *quadratischer Nichtrest nach* p *ist.*

Das ist das *Legendresche Symbol.* Es ist ausdrücklich nicht definiert für $p = 2$ und auch nicht für zu p nicht prime a.
Dagegen definieren wir es ohne weiteres für gebrochene Zahlen $\frac{a}{b}$, wenn a und b beide zu p prim sind. Es ist dann

$$\left(\frac{\frac{a}{b}}{p}\right) = \left(\frac{a}{p}\right) : \left(\frac{b}{p}\right),$$

oder, da Multiplikation und Division mit ± 1 auf dasselbe herausläuft:

$$\left(\frac{\frac{a}{b}}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Dies fällt, wie wir gleich sehen werden, damit zusammen, daß

$$\left(\frac{\frac{a}{b}}{p}\right) = \left(\frac{c}{p}\right)$$

ist, wenn $\frac{a}{b} \equiv c \bmod p$ ist.

Im folgenden werde bei Legendreschen Symbolen angenommen, daß sie definiert sind, d. h. der symbolische Zähler zum symbolischen Nenner (Primzahl) prim ist. p sei im folgenden eine ungerade Primzahl.

Satz 16. *Es ist* $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$, *wenn* $m \equiv n \bmod p$ *ist.*

Der Beweis folgt aus der Definition.

Satz 17. *Es ist* $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$.

Beweis: Zunächst folgt aus $(m, p) = (n, p) = 1$ auch $(mn, p) = 1$, es ist also dieses Legendresche Symbol definiert. Der weitere Beweis folgt aus Satz 12.

Satz 18. *Es ist* $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^m$, *wenn m ganz (positiv, negativ, auch Null) ist.*

Der Beweis folgt aus Satz 17.

Satz 19. *Es ist* $\left(\frac{a^2}{p}\right) = 1$.

Der Beweis ergibt sich aus der Definition oder Satz 18.

Satz 20. *Es ist* $\left(\frac{ab^2}{p}\right) = \left(\frac{\frac{a}{c^2}}{p}\right) = \left(\frac{a}{p}\right)$, *wenn* a, b, c *zu* p *prim sind.*

Der Beweis folgt aus Satz 17 und 19.

Satz 21. *Es gilt* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Der Beweis ergibt sich aus Satz 14 und 15.
Nun folgt der wichtige

Satz 22 (erster Ergänzungssatz zum quadratischen Reziprozitätsgesetz). *Es ist*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

oder, -1 *ist quadratischer Rest aller Primzahlen der Form* $4n+1$, *quadratischer Nichtrest aller Primzahlen der Form* $4n+3$.

Beweis: Nach Satz 21 ist

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p,$$

also wegen $p > 2$ auch gleich seinem absolutkleinsten Rest.

Satz 23. $x^2 \equiv n \bmod p^k$ *mit* $(n, p) = 1$ *hat entweder zwei Lösungen oder keine.*

Beweis: Keine Lösung ist sicher da für $\left(\frac{n}{p}\right) = -1$. Denn dann hat schon $x^2 \equiv n \bmod p$ keine Lösung. Ist $\left(\frac{n}{p}\right) = +1$, so ist mit g als primitiver Wurzel mod p die Beziehung $\operatorname{ind}_1 n \equiv 0 \bmod 2$ erfüllt. (Es werden die Beziehungen im Beweise von Satz 6 verwendet, wobei p an die Stelle von l tritt.) Dort ist gezeigt (mit den entsprechend geänderten Bezeichnungen), daß $\operatorname{ind}_k A \equiv \operatorname{ind}_2 A \bmod \varphi(p^2)$ ist. Es gilt aber auch $\operatorname{ind}_k n \equiv \operatorname{ind}_1 n \bmod (p-1)$, was genau wie dort bewiesen wird:

$g^X \equiv n \bmod p^k$, $g^Y \equiv n \bmod p$ gilt mit $X = \operatorname{ind}_k n$, $Y = \operatorname{ind}_1 n$, also $X \equiv Y \bmod (p-1)$. Also gilt bei $\left(\frac{n}{p}\right) = 1$, daß $\operatorname{ind}_k n \equiv \operatorname{ind}_1 n \bmod (p-1)$, mithin wegen $\operatorname{ind}_1 n \equiv 0 \bmod 2$ auch $\operatorname{ind}_k n \equiv 0 \bmod 2$ ist. Somit ist n auch quadratischer Rest mod p^k. Daher

Satz 24. *Ist* $\left(\frac{n}{p}\right) = 1$, *so ist* n *quadratischer Rest nach jeder noch so hohen Potenz von* p, *und* $x^2 \equiv n \bmod p^k$ *hat zwei inkongruente Lösungen.*

Man kann aus einer Lösung von $x^2 \equiv n \bmod p$ durch den Ansatz $x = s + py$, wenn s Kongruenzlösung ist, eine Lösung der Kongruenz mod p^2 rekursiv gewinnen, aus dieser dann durch analogen Ansatz eine Lösung der Kongruenz mod p^3 usf.

Beispiele: Es ist $3^2 \equiv 2 \bmod 7$. Setzen wir $x = 3 + 7y$ in $x^2 \equiv 2 \bmod 7^2$ ein, so bleibt nach Weglassung des durch 7^2 teilbaren Gliedes die Kongruenz

$$\begin{aligned} 9 + 42y &\equiv 2 \bmod 7^2, \\ 42y &\equiv -7 \bmod 7^2, \\ 6y &\equiv -1 \bmod 7, \\ -y &\equiv -1 \bmod 7, \\ y &\equiv 1 \bmod 7. \end{aligned}$$

Mithin wird $x \equiv 3 + 7 \equiv 10 \bmod 49$ eine Lösung von $x^2 \equiv 2 \bmod (7^2 \equiv 49)$. Wollen wir noch $x^2 \equiv 2 \bmod 7^3 = 343$ lösen, so gilt $x = 10 + 49y$, daher

$$\begin{aligned} 100 + 980y &\equiv 2 \bmod 7^3, \\ 980y &\equiv -98 \bmod 7^3, \\ 10y &\equiv -1 \bmod 7, \\ 10y &\equiv 20 \bmod 7, \\ y &\equiv 2 \bmod 7. \end{aligned}$$

Es löst also $x \equiv 108 \bmod 343$ die Kongruenz $x^2 \equiv 2 \bmod 343$. Die zweite Wurzel der Kongruenz ist $x \equiv -108 \equiv 235 \bmod 343$.

Bei $p \equiv 1 \bmod 4$ gestattet der Satz von *Wilson* die effektive Angabe einer Wurzel von $x^2 \equiv -1 \bmod p$, nämlich $x \equiv \left(\frac{p-1}{2}\right)!$ Der Nachweis ist ganz kurz

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \prod_{j=1}^{\frac{p-1}{2}} j \prod_{j=1}^{\frac{p-1}{2}} (p-j)\,(-1)^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1, \bmod p$$

das letzte nach dem Satz von *Wilson*.

Satz 25. *Ist* $p \equiv 3$ *mod* 4, $\left(\frac{a}{p}\right) = 1$, *so löst* $x \equiv a^{\frac{p+1}{4}}$ *die Kongruenz* $x^2 \equiv a \bmod p$.

Beweis: Nach Satz 14 ist $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, also

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p-1}{2}}\, a \equiv a \bmod p\,.$$

Beispiel: $p = 23$, $3^3 \equiv 4$, $3^6 \equiv 16$, $3^9 \equiv 64 \equiv -5$, $3^{11} \equiv -45 \equiv 1 \bmod 23$, also $\left(\frac{3}{23}\right) = 1$, $x^2 \equiv 3 \bmod 23$ hat also die Lösung $x \equiv 3^6 \equiv 16$. Die zweite Lösung ist $x \equiv -16 \equiv 7$.

Aufgaben:

1. Aus $13^2 \equiv 6 \bmod 163$ (Primzahl) gewinne man eine Lösung von $x^2 \equiv 6 \bmod 163^2$.

2. Aus den beinahe selbstverständlichen Lösungen von $x^2 \equiv 2 \bmod 7$, $\bmod 23$ berechne man alle Lösungen von $x^2 \equiv 2 \bmod 161 = 7.23$.

§ 12. Das Eingreifen des Schubfachschlusses

Der Schubfachschluß beruht auf dem fast selbstverständlichen

Satz 1. *Sind $M > N$ Gegenstände auf N Fächer verteilt, so ist mindestens ein Fach mit zwei Gegenständen da.*

Beweis: Befände sich in jedem Fach höchstens ein Gegenstand, so wäre $M \leqq N$, also $N \geqq M > N$, d. h. $N > N$.
Fast unmittelbar ersieht man die Verschärfung:

Satz 2. *Ist $M = qN + r$, M, N, q natürliche Zahlen, $0 \leqq r < N$, und sind M Gegenstände in N Fächer zu verteilen, so sind für $r = 0$ mindestens in einem Fache q Gegenstände vorhanden, für $r > 0$ sogar mindestens $q+1$ Gegenstände.*
Nur aus dem Grunde, daß der Schubfachschluß außer in der Zahlentheorie nie verwendet wird, ist er für den Anfänger schwierig. Wir wenden uns nun einem wichtigen Satz zu:

Satz 3. *Gegeben eine Primzahl $p > 2$.* (Für $p = 2$ gilt der Satz auch, sagt aber nichts aus.) *Weiter seien α, β positive Zahlen mit $\alpha\beta = 1$ und min $(\alpha\sqrt{p}, \beta\sqrt{p}) > 1$. Dann kann jede durch x repräsentierte Restklasse mod p durch einen Quotienten ganzer Zahlen $\frac{a}{b}$ mit $0 \leqq |a| < \alpha\sqrt{p}$, $0 < b < \beta\sqrt{p}$ gegeben werden.*

Beweis: Es sei zunächst $(p, x) = 1$, ferner $A = [\alpha\sqrt{p}]$, $B = [\beta\sqrt{p}]$. Wir setzen $u = 0, 1, \ldots, B$; $v = 0, 1, \ldots, A$ in den Ausdruck $ux + v$ ein. Das sind insgesamt $(A+1)(B+1)$ Zahlen. Es ist $(A+1)(B+1) > \alpha\beta p = p$. Mithin gibt es unter diesen Zahlen mindestens zwei, die mod p kongruent sind.
Es folgt eine Kongruenz

$$u'x + v' \equiv u''x + v'', \tag{1}$$

ohne daß das Paar $[u', v']$ mit $[u'', v'']$ zusammenfällt.
$v = p$ ist unmöglich. Denn es folgte $\alpha \geqq \sqrt{p}$, $\beta \leqq \frac{1}{\sqrt{p}}$ im Widerspruch zu min $(\alpha\sqrt{p}, \beta\sqrt{p}) > 1$. Daher ist $v', v'' < p$. $v' \equiv v''$ mod p ist also nur für $v' = v''$ möglich. Nun sei $u'x + v' = u''x + v''$.
Wir nehmen an, $v' = v''$. Dann bleibt $u'x = u''x$. Nun ist $(p, x) = 1$, also x sicher nicht Null. Aus $v' = v''$ folgt $u' = u''$.
Also gilt (1) für zwei Paare $[u', v']$, $[u'', v'']$, wo v', v'' und u', u'' voneinander verschieden sind. Für u', u'' können wir dieselben

Schlüsse wie oben für v', v'' durchführen, es werden u', u'' beide kleiner als p, positiv, vielleicht eines Null, dann aber nur eines, voneinander verschieden und daher auch einander mod p inkongruent. Es ist $|v' - v''| < p$, $|u' - u''| < p$ und daher die zweite Zahl zu p prim. Hier haben wir die Voraussetzung: p ist Primzahl angewandt. Wir erhalten

$$x \equiv \pm \frac{v' - v''}{|u' - u''|} \bmod p .$$

Mit $\pm (v' - v'') = a$, $|u' - u''| = b$ haben wir die Behauptung. Der Fall $x \equiv 0 \bmod p$ erledigt sich sofort mit $a = 0$, $b = 1$. Ein Spezialfall ist

Satz 4. *Jede zu einer Primzahl p prime Restklasse mod p gestattet eine Darstellung $\frac{a}{b}$ mit $0 < |a| < \sqrt{p}$, $0 < b < \sqrt{p}$.*

Die Voraussetzung, daß p Primzahl ist, ist nicht überflüssig. Andernfalls braucht der Satz nicht einmal für die Restklassen des reduzierten Restsystems eines Moduls T zu gelten. Z. B. für $T = 8$ ist die Restklasse 3 als Quotient zweier zu 8 primer Restklassen, deren absolut kleinste Reste $< \sqrt{8}$ sind, nicht darstellbar; denn dann hätten wir nur die Restklassen ± 1 zur Verfügung und erhielten nur 1; $-1 \equiv 7$. Sei $T = 42$. Zu T prime Restklassen, deren absolutkleinste Reste $< \sqrt{T}$ sind, sind nur durch ± 1, ± 5 gegeben. Wegen $\frac{1}{5} \equiv 17$ haben wir dann nur die sechs Restklassen 1, 5, 17, 25, 37, 41. Es ist also z. B. 11, 13 in dieser Form nicht darstellbar.

Satz 5. *Sei die natürliche Zahl m zur Primzahl $p > 2$ prim, $\left(\frac{-m}{p}\right) = 1$, $m < p^2$. Dann gibt es durch p teilbare Zahlen $< 2p\sqrt{m}$, die durch die quadratische Form $x^2 + my^2$ darstellbar sind.*

Beweis:

I. Mit $|x| = \alpha\sqrt{p}$, $|y| = \frac{\sqrt{p}}{\alpha}$ wird

$$x^2 + my^2 = p\left(\alpha^2 + \frac{m}{\alpha^2}\right),$$

und dies hat mit $\alpha = \sqrt[4]{m}$ den Kleinstwert $2p\sqrt{m}$.

II. Ist $\qquad |x| \leqq \alpha\sqrt{p}, \quad |y| \leqq \frac{\sqrt{p}}{\alpha},$

wobei $\alpha = \sqrt[4]{m}$ sein und mindestens ein Ungleichheitszeichen gelten soll, so ist $x^2 + my^2 < 2p\sqrt{m}$.

III. Gegeben die Kongruenz

$$U^2 + m \equiv 0 \bmod p.$$

Mit derselben Abkürzung α ist dann $\frac{\sqrt{p}}{\alpha} > 1$. Denn es ist $m < p^2$ angenommen, also

$$\frac{p^2}{m} > 1, \quad \frac{\sqrt[4]{p^2}}{\sqrt[4]{m}} > 1, \quad \text{d.h.} \quad \frac{\sqrt{p}}{\alpha} > 1.$$

Nach Satz 3 können wir also

$$U \equiv \frac{x}{y} \bmod p$$

ansetzen mit $|x| < \alpha\sqrt{p}$, $|y| < \frac{\sqrt{p}}{\alpha}$. Es folgt $x^2 + my^2 \equiv 0 \bmod p$ und zugleich $x^2 + my^2 < 2p\sqrt{m}$.

Satz 6. *Jede Primzahl der Form $4n+1$ ist Summe zweier Quadrate ganzer Zahlen.*

Beweis: Wegen $\left(\frac{-1}{p}\right) = 1$ (erster Ergänzungssatz zum quadratischen Reziprozitätsgesetz) gibt es nach Satz 5 eine Zahl $A = x^2 + y^2 \equiv 0 \bmod p$ mit $0 < A < 2p$. Es folgt $A = p$.

Satz 7. *Jede Primzahl p, nach der -2 quadratischer Rest ist, gestattet eine Darstellung in der Form $x^2 + 2y^2$.*

Beweis: Nach Satz 5 gibt es ein A mit $A = x^2 + 2y^2 \equiv 0 \bmod p$, $0 < A < 2p\sqrt{2}$. Nur $A = p$ oder $A = 2p$ ist möglich. Im zweiten Falle ist x gerade $= 2x'$, aus

$$x^2 + 2y^2 = 4x'^2 + 2y^2 = 2p \text{ folgt } y^2 + 2x'^2 = p.$$

Satz 8. *Die Zahl -2 ist Nichtrest aller Primzahlen p der Form $8n+5$, $8n+7$.*

Beweis: Wäre -2 Rest, so wäre $p = A^2 + 2B^2$ mit ungeradem A. Nun folgt aus $A^2 \equiv 1$, $2B^2 \equiv 0$, $2 \bmod 8$, daß $p \equiv 1, 3 \bmod 8$ ist.

Satz 9. *Die Zahl 2 ist quadratischer Rest aller Primzahlen p der Form $8n+1$, $8n+7$ und Nichtrest aller Primzahlen der Form $8n+5$.*

Beweis:

I. Ist $p \equiv 5 \bmod 8$, so gibt der erste Ergänzungssatz $\left(\frac{-1}{p}\right) = 1$, und der Satz 8 hat $\left(\frac{-2}{p}\right) = -1$ zur Folge.

Es gilt daher

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right) = -1.$$

II. Ist $p \equiv 7 \bmod 8$, so folgt genau entsprechend, da jetzt $\left(\frac{-1}{p}\right) = -1$ ist:

$$\left(\frac{2}{p}\right) = 1.$$

III. Nun erledigen wir $p \equiv 1 \bmod 8$. Ist g eine primitive Wurzel $\bmod p$, $A = g^{\frac{p-1}{8}}$, so ist $A^4 = g^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Wir haben

$$A^4 + 1 \equiv 0 \bmod p$$

$$(A^2+1)^2 - 2A^2 \equiv 0 \bmod p,$$

hieraus $\left(\frac{2A^2}{p}\right) = 1$, also $\left(\frac{2}{p}\right) = 1$.

Der Beweisgang liefert noch

Satz 10. *Die Zahl* -1 *ist biquadratischer Rest aller Primzahlen der Form* $8n+1$.

Satz 11. *Ist 2 quadratischer Rest einer Primzahl* p, *so gibt es eine Darstellung* $x^2 - 2y^2 = -p$ *mit* $0 < |x| < \sqrt{p}$, $0 < |y| < \sqrt{p}$.

Beweis: Eine Lösung U der Kongruenz $X^2 \equiv 2 \bmod p$ kann als $\frac{x}{y}$ mit $0 < |x| < \sqrt{p}$, $0 < |y| < \sqrt{p}$ dargestellt werden. Es ist dann $A = x^2 - 2y^2 \equiv 0 \bmod p$ und offenbar $-2p < A < p$, also $A = 0$ oder $A = -p$. Aber $A = 0$ ist ausgeschlossen, da sonst $\sqrt{2}$ rational wäre. Es gilt also $A = -p$.

Satz 12. *Die Zahl 2 ist Nichtrest aller Primzahlen der Form* $8n+3$, $8n+5$.

Beweis: Nach Satz 11 gilt für eine Primzahl p mit $\left(\frac{2}{p}\right) = 1$, daß $-p = x^2 - 2y^2$ mit ganzem x, y ist; hier ist offenbar x ungerade, also $x^2 \equiv 1 \bmod 8$. Weiter ist $2y^2 \equiv 2,\ 0 \bmod 8$. Es bleibt $-p \equiv -1,\ 1$; $p \equiv 1,\ 7 \bmod 8$. Also ist $p \equiv 3,\ 5 \bmod 8$ ausgeschlossen.

Die Sätze 9, 12 geben zusammengenommen den überaus wichtigen

Satz 13. (zweiter Ergänzungssatz zum quadratischen Reziprozitätsgesetz). *Die Zahl 2 ist quadratischer Rest aller Primzahlen der Form* $8n+1$, $8n+7$, *quadratischer Nichtrest aller Primzahlen der Form* $8n+3$, $8n+5$.
Der zweite Ergänzungssatz kann auch

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

geschrieben werden.

Beweis: Aus $a \equiv b \bmod 8$ folgt $a^2 \equiv b^2 \bmod 16$ (§ 9, Satz 10), also aus $\left(\frac{2}{p}\right) = 1$, $p \equiv \pm 1 \bmod 8$ folgt $p^2 - 1 \equiv 0 \bmod 16$, $\frac{p^2-1}{8} \equiv 0 \bmod 2$. Ebenso aus $\left(\frac{2}{p}\right) = -1$, $p \equiv \pm 3 \bmod 8$ folgt $p^2 \equiv 9 \bmod 16$, $p^2 - 1 \equiv 8 \bmod 16$, $\frac{p^2-1}{8} \equiv 1 \bmod 2$.

Satz 14. *Ist* $p \equiv 1, 7$ *mod* 8, *so gibt es ganzzahlige Lösungen von* $x^2 - 2y^2 = -p$ *mit* $0 < |x| < \sqrt{p}$, $0 < |y| < \sqrt{p}$.

Beweis: Er folgt aus dem zweiten Ergänzungssatz und Satz 11.
Im folgenden sollen *eigentliche Darstellungen* einer Zahl, d. h. solche durch $x^2 + my^2$ mit $(x, y) = 1$ untersucht werden. Es soll also

$$x^2 + my^2 = A$$

mit $(x, y) = 1$ gelten. Dabei sei m eine quadratfreie natürliche Zahl. Ferner sei $(A, m) = 1$.
Darstellungen mit $(x, y) > 1$ heißen *uneigentliche Darstellungen* Sie sind nur bei nicht quadratfreien Zahlen möglich. Solche werden also jetzt nicht berücksichtigt.
Für $m > 1$ wollen wir einstweilen die Darstellung durch $[x, y]$ und $[x, -y]$ voneinander verschieden auffassen, dabei aber $x > 0$ annehmen, bei $m = 1$ hingegen wollen wir die Darstellungen $A = x^2 + y^2$ und $A = y^2 + x^2$ als voneinander verschieden annehmen, aber $x > 0$, $y > 0$ festhalten.
Ist A eine ungerade Primzahl ($A = 2$ interessiert nicht), so gibt es nur zwei Darstellungen. Denn $x^2 + my^2 = r^2 + ms^2 = A$ mit $0 < r < x$, also $0 < y < s$ hätte $\frac{x}{y} \equiv \pm \frac{r}{s} \bmod A$, daher $\varphi = xs \mp yr \equiv 0 \bmod A$ zur Folge. Es ist aber

$$(xr \pm mys)^2 + m\,(xs \mp yr)^2 = A^2$$

mit beiden Vorzeichen richtig, also für $m > 1$ wäre $|\varphi| < A$, d.h. $\varphi = 0$, $\frac{x}{y} = \frac{r}{s}$, $x = r, y = s$, das ist ein Widerspruch. Für $m = 1$ ist auch $|\varphi| = A$ möglich, dann ist $xr - ys = 0$; $x = s$, $y = r$. Ebenso sieht man, daß einer Wurzel U der Kongruenz $X^2 + m \equiv 0 \bmod A$, wenn überhaupt eine, dann nur eine Darstellung $U \equiv \frac{x}{y} \bmod A$, $x^2 + my^2 = A$ entspricht, auch wenn A keine Primzahl ist.
Einer bestimmten Darstellung entspricht dann von den entgegengesetzt gleichen Wurzelpaaren $\frac{x}{y}, -\frac{x}{y}$ der Kongruenz $X^2 + m \equiv 0 \bmod A$ nur eines bzw. bei $m = 1$ von den Wurzelpaaren $\frac{x}{y}, \frac{y}{x}$, die auch hier $\frac{x}{y} \equiv -\frac{y}{x}$ erfüllen, nur eines.
Grundlegend für das weitere ist die Gleichung

$$(x + y\sqrt{-m})(x' + y'\sqrt{-m}) = (xx' - myy') + \sqrt{-m}\,(x'y + xy'). \quad (2)$$

Weitere Voraussetzungen seien $(A, m) = 1$ und A ungerade.
Wir setzen

$$\alpha = x + y\sqrt{-m}, \quad \beta = x' + y'\sqrt{-m}.$$

Mit $N(\xi) = A^2 + mB^2$ bezeichnet man die *Norm* einer Zahl $\xi = A + B\sqrt{-m}$ des Zahlrings der Größen $a + b\sqrt{-m}$ mit ganzzahligen a und b. Für $\gamma = \alpha\beta$ ergibt mit den Bezeichnungen $N(\alpha) = A$, $N(\beta) = B$ die Relation

$$N(\gamma) = N(\alpha\beta) = N(\alpha)\,N(\beta)$$

eine Darstellung von AB in der Form

$$X^2 + mY^2 \quad \text{mit} \quad X = xx' - myy', \; Y = x'y + y'x.$$

Wir nennen $A = x^2 + my^2$ die durch α vermittelte Darstellung.

Satz 15. *Sind die durch α, β vermittelten Darstellungen eigentlich und $N(\alpha)$, $N(\beta)$ prim zueinander, dann ist auch die durch $\alpha\beta$ vermittelte Darstellung eigentlich. Hier kann auch $m < 0$ sein.*

Beweis: Wir nehmen an, die Primzahl p erfülle $p \mid xx' - myy'$, $x'y + xy'$. Sofort folgt

$$xx' - myy' \equiv 0 \bmod p,$$
$$x'y + y'x \equiv 0 \bmod p.$$

Diese beiden Gleichungen mögen als lineare homogene Gleichungen für die Restklassen von x', y' im Körper P_p der Charakteristik p aufgefaßt werden. Bei Nichtverschwinden der Determinante können sie nur so bestehen, daß $x' \equiv y' \equiv 0 \bmod p$ ist. Aber dies ist ausgeschlossen, da wir ausdrücklich eigentliche Darstellungen voraussetzen. Es folgt, daß die Determinante in P_p verschwinden muß, d. h.

$$\begin{vmatrix} x & -my \\ y & x \end{vmatrix} \equiv 0 \bmod p$$

sein muß. Folglich bleibt

$$A = N(\alpha) \equiv 0 \bmod p.$$

Da aber ebensogut

$$B = N(\beta) \equiv 0 \bmod p$$

bewiesen werden könnte, wären wir mit der Voraussetzung $(A, B) = 1$ in Widerspruch.

Satz 16. *Die Voraussetzungen seien die des vorigen Satzes. Den durch $\alpha\beta$ und $\alpha\bar{\beta}$, wobei $\bar{\beta}$ die konjugierte Zahl zu β ist, vermittelten Darstellungen entsprechen verschiedene Wurzeln von $X^2 \equiv -m \bmod AB$, die auch nicht Restklassen entgegengesetzt gleicher Zahlen sind.*

Beweis: Es wird

$$\alpha\beta = xx' - m\,yy' + \sqrt{-m}\,(xy' + yx'),$$
$$\alpha\bar{\beta} = xx' + m\,yy' + \sqrt{-m}\,(-xy' + yx').$$

Aus der Annahme

$$\frac{xx' - myy'}{xy' + yx'} \equiv \frac{xx' + myy'}{-xy' + yx'} \bmod AB \tag{3}$$

folgt

$$\begin{vmatrix} xx' - m\,yy' & xx' + m\,yy' \\ xy' + yx' & -xy' + yx' \end{vmatrix} \equiv 0 \bmod AB$$

und durch Addition der ersten Spalte zur zweiten

$$\begin{vmatrix} xx' - m\,yy' & 2\,xx' \\ xy' + yx' & 2\,yx' \end{vmatrix} \equiv 0 \bmod AB,$$

daraus wegen $(2, AB) = 1$

$$\begin{vmatrix} xx' - m\,yy' & xx' \\ xy' + yx' & yx' \end{vmatrix} \equiv 0 \bmod AB,$$

durch Subtraktion der zweiten Spalte von der ersten

$$\begin{vmatrix} -my y' & xx' \\ y'x & yx' \end{vmatrix} \equiv 0 \bmod AB$$

oder

$$-x'y'(x^2+my^2) \equiv 0 \bmod AB,$$

d. h.

$$x'y' \equiv 0 \bmod B. \tag{4}$$

Das kann nicht sein, da x', y' beide zu B teilerfremd sind.
Eine Primzahl $p \mid xx'+myy'$, A würde geben

$$xx' \equiv -myy' \bmod p,$$

$$x^2 \equiv -my^2 \bmod p,$$

dabei kann p in x nicht aufgehen, da es sonst auch in my^2 aufginge, also, da m quadratfrei ist, auch in y in Widerspruch zur eigentlichen Darstellung. Ebenso führt $p \mid y$ auf einen Widerspruch. Es wäre also

$$\frac{x'}{x} \equiv \frac{y'}{y} \bmod p.$$

Auch x' und y' müssen aus analogem Grunde ($x'^2+my'^2$ ist eine eigentliche Darstellung) zu p prim sein. Es folgt $x \equiv tx'$, $y \equiv ty' \bmod p$ mit $(p,t)=1$, und $p \mid xx'+myy'$ würde

$$t(x'^2+my'^2) \equiv 0 \bmod p,$$

also $B \equiv 0 \bmod p$ im Widerspruch zu $(A,B)=1$ zur Folge haben.
Ebenso ist auch

$$\begin{vmatrix} xx'-myy' & -xx'-myy' \\ xy'+yx' & -xy'+yx' \end{vmatrix} \equiv 0 \bmod AB$$

ausgeschlossen.

Leicht ist zu zeigen, daß Kombinationen von Darstellungen $t^2+mu^2=A$, $t'^2+mu'^2=B$, wobei die Zahlenpaare

$$[t(>0), \pm u]$$

einerseits,

$$[x(>0), \pm y]$$

andererseits voneinander verschieden sind, nicht zu einer der beiden in Formel (4) angeführten Wurzeln der Kongruenz $U^2+m \equiv 0 \bmod AB$ und damit auch zu keiner der durch

$\alpha\beta$, $\alpha\bar{\beta}$, $\bar{\alpha}\beta$, $\bar{\alpha}\bar{\beta}$ vermittelten Abbildungen führen kann. Wäre dies mit $\alpha\ \beta$ der Fall, so hätten wir analog zu (4) eine Kongruenz

$$\begin{vmatrix} tt' - muu' & xx' - myy' \\ tu' + ut' & xy' + yx' \end{vmatrix} \equiv 0 \bmod AB. \tag{5}$$

Wir überlegen: Es ist $(u, A) = (y, A) = 1$, da sonst die Darstellung nicht eigentlich wäre. Wir fassen (5) als Kongruenz $\bmod A$ auf, dividieren durch uy und setzen $\frac{t}{u} = R$, $\frac{x}{y} = S$. Dann ist $R^2 \equiv S^2 \equiv -m \bmod A$. Die Division führen wir so aus, daß wir die erste Spalte durch u, die zweite durch y dividieren, überdies in der ersten Spalte die Zahl $-m$ durch den $\bmod A$ kongruenten Wert R^2, in der zweiten ebenso durch S^2 ersetzen. Dann bleibt

$$\begin{vmatrix} Rt' + R^2u' & Sx' + S^2y' \\ t' + Ru' & x' + Sy' \end{vmatrix} \equiv 0 \bmod A.$$

Das ergibt sofort

$$(t' + Ru')\,(x' + Sy') \begin{vmatrix} R & S \\ 1 & 1 \end{vmatrix} \equiv 0 \bmod A$$

oder

$$(t' + Ru')\,(x' + Sy')\,(R - S) \equiv 0 \bmod A.$$

Multiplikation mit uy gibt

$$(t'u + u't)\,(x'y + xy')\,(R - S) \equiv 0 \bmod A.$$

Es möge die Primzahl p in $t'u + u't$ und A aufgehen. Wegen

$$(tt' - muu')^2 + m\,(t'u + u't)^2 = AB$$

wäre diese Darstellung nicht eigentlich im Widerspruch zu Satz 15.

Also bleibt $(t'u + u't, A) = 1$, in derselben Art $(x'y + xy', A) = 1$. Somit ist $\frac{t}{u} \equiv \frac{x}{y} \bmod A$. Die noch verbleibende Möglichkeit

$$\begin{vmatrix} tt' - muu' & -xx' + myy' \\ t'u + u't & xy' + yx' \end{vmatrix} \equiv 0 \bmod AB$$

führt ebenso auf $\frac{t}{u} \equiv -\frac{x}{y} \bmod A$.

Satz 17. *Mit $A = p^k$, $B = p$, wobei p eine durch $x^2 + my^2$ darstellbare Primzahl ist, gibt die Formel (2) rekursiv genau zwei eigentliche Darstellungen von p^{k+1}, die den beiden Wurzeln der Kongruenz $U^2 + m \equiv 0 \bmod p^{k+1}$ entsprechen.*

Beweis: Sei $k = 1$, $\alpha = x + y\sqrt{-m}$, $\bar{\alpha} = x - y\sqrt{-m}$, dann liefert offenbar $\alpha\bar{\alpha}$ nur eine triviale, jedenfalls uneigentliche Darstellung von p^2, es ist ja $\alpha\bar{\alpha} = x^2 + my^2 = p$. Diese Zahl $\alpha\bar{\alpha}$ vermittelt nur die selbstverständliche Darstellung $p^2 = p^2 + m \cdot 0^2$. α^2 hingegen vermittelt eine eigentliche Darstellung

$$N(a^2) = (x^2 - my^2)^2 + m(2xy)^2 = p^2.$$

Die Darstellung ist eigentlich wegen $2mxy \not\equiv 0 \bmod p$. Umkehrung des Vorzeichens von y gibt die der Wurzel der entgegengesetzten Restklasse entsprechende Darstellung. (Analog Vertauschung der x, y für die $m = 1$ entsprechenden Werte.)
Ist der Satz für p^k bewiesen, so sei angenommen

$$x'^2 + my'^2 = p^k,\ x' + y'\sqrt{-m} = \beta.$$

Es folgt aus (3), daß genau eine der Größen $xy' + yx'$, $-xy' + yx'$, der beiden Koeffizienten von $\sqrt{-m}$ in $\alpha\beta$ und $\alpha\bar{\beta}$ durch p teilbar sein muß. Entweder gilt $\frac{x}{y} \equiv \frac{x'}{y'}$ oder $\frac{x}{y} \equiv -\frac{x'}{y'} \bmod p$, da es nur zwei Wurzeln der Kongruenz $U^2 + m \equiv 0 \bmod p$ gibt, weiter $\frac{x'}{y'}$ als Wurzel der Kongruenz $U^2 + m \equiv 0 \bmod p^k$ auch eine solche $\bmod p$ ist. Eine der beiden sich ergebenden Darstellungen kann daher als uneigentlich übergangen werden. Es bleiben nur zwei den Wurzeln der Kongruenz $\bmod p^k$ entsprechende Darstellungen.
Aus Satz 16 und 17 folgt

Satz 18. *Ein zu m primes ungerades Potenzprodukt (kanonische Zerlegung)*

$$\prod_{i=1}^{k} p_i^{a_i},$$

in dem sämtliche Primfaktoren durch $x^2 + my^2$ ($m > 1$, quadratfrei) darstellbar sind, gestattet genau 2^k eigentliche Darstellungen durch diese Form, wenn dieselben durch $[x, y]$, $[x, -y]$ als verschieden gerechnet werden ($x > 0$), also 2^{k-1} eigentliche Darstellungen mit $x > 0$, $y > 0$.

Satz 19. *Ein ungerades Potenzprodukt*

$$\prod_{i=1}^{k} p_i^{a_i},$$

in dem sämtliche Primfaktoren durch x^2+y^2 darstellbar sind, gestattet genau 2^k eigentliche Darstellungen $(x, y > 0)$, wenn $[x, y]$, $[y, x]$ als verschieden gerechnet werden, also 2^{k-1} eigentliche Darstellungen mit $0 < x < y$.

Aus Satz 18 und 19, sowie dem ersten und zweiten Ergänzungssatz folgen die Sätze:

Satz 20. *Eine Zahl der Form $4n+1$ ist dann und nur dann Primzahl, wenn sie sich im wesentlichen eindeutig als Summe zweier teilerfremder Quadrate darstellen läßt.*

Im wesentlichen eindeutig heißt: Zwei Darstellungen durch dieselben Summanden in verschiedener Reihenfolge werden als gleich betrachtet.

Satz 21. *Eine Zahl der Form $8n+1$ oder $8n+3$ ist dann und nur dann Primzahl, wenn sie sich eindeutig in der Form x^2+2y^2 mit x, y als zueinander teilerfremden natürlichen Zahlen darstellen läßt.*

Wir gehen zu einem umfassenden Satze über.

Satz 22. *Ist $-m$ quadratischer Rest einer ungeraden Primzahl p, so ist diese für $m = 3, 7$ durch x^2+my^2 darstellbar. Ist bei sonst gleichen Voraussetzungen p von der Form $4n+1$, so gilt dies auch für $m = 5, 13, 37$. Werden nur Darstellungen mit positivem x und y gezählt, so ist die Darstellung eindeutig.*

Beweis: Nach Satz 5 gibt es durch p teilbare, durch x^2+my^2 darstellbare Zahlen $< 2p\sqrt{m}$.

Ist $m=3$, so haben wir $0 < A = x^2+3y^2 < 4p$. $x^2+3y^2 = 2p$ ist ausgeschlossen, denn dann müßten x, y ungerade sein und es folgte $0 \equiv 2 \bmod 4$. Dagegen hat $x^2+3y^2 = 3p$ zur Folge, daß x durch 3 teilbar ist, $x = 3x'$, woraus $y^2+3x'^2 = p$ folgt.

Für $m=7$ haben wir $0 < A = x^2+7y^2 < 6p$. Setzen wir $A = kp$ $(1 \leqq k \leqq 5)$, so scheiden gerade Werte k aus, da man bei x, y gerade, also $k=4$ durch 4 kürzen könnte, hingegen bei ungeradem x und y $0 \equiv 2, 4 \bmod 8$ hätte. Somit bleibt nur $k=3$ und $k=5$ zu betrachten. $A = 5p$ würde $\left(\frac{-7}{5}\right) = 1 = \left(\frac{2}{5}\right)$ im Widerspruch zum zweiten Ergänzungssatz geben. Nur der Wert

$k = 3$ ist noch zu erledigen. Aus $x^2 + 7y^2 \equiv x^2 + y^2 \equiv 0 \bmod 3$ folgte $\left(\frac{-1}{3}\right) = 1$ im Widerspruch zum ersten Ergänzungssatz.

Es bleibt $m = 5, 13, 37$, wobei noch $p \equiv 1 \bmod 4$ vorausgesetzt wird. Wir wollen, da die Beweise einander sehr ähneln, nur den schwersten Fall $m = 37$ untersuchen. Satz 5 gibt die Existenz eines $A \equiv 0 \bmod p$, $A = x^2 + 37y^2$ mit $A < 2p\sqrt{37}$, also $A \leqq 12p$.

Wir setzen wieder $A = kp$. Durch 3 und 5 teilbare Werte von k sind unmöglich, da -37 Nichtrest mod 3,5 ist. Es bleibt also außer $k = 1$ nur $k = 2, 4, 7, 8, 11$. $k = 2, 4$ fallen wieder aus, wenn wir die Gleichung $x^2 + 37y^2 = kp$ als Kongruenz mod 8 auffassen. Da -37 auch Nichtrest mod 7, 11 ist, fällt auch diese Möglichkeit aus. Es bleibt $k = 8$; da dann $x = 2x'$, $y = 2y'$ gerade sein müßten, so kämen wir doch auf $k = 2$.

Nun gehen wir auf die Möglichkeit der eigentlichen Darstellung einer durch 2, nicht durch 4 teilbaren Zahl durch $x^2 + my^2$ über, wobei m ungerade ist. Also betrachten wir $x^2 + my^2 = 2A$, dabei sei A ungerade.

Ist wieder $\alpha = x + y\sqrt{-m}$, $\beta = x' + y'\sqrt{-m}$, $x'^2 + my'^2 = B$, so vermitteln die Zahlen $\alpha\beta$, $\alpha\bar{\beta}$ zwei Darstellungen von $2AB$ durch die Form $x^2 + my^2$. Den Darstellungen $x^2 + my^2 = 2A$, $x^2 + m(-y)^2 = 2A$, wobei die Zahl x wieder als positiv normiert werde, mögen der Reihe nach die Wurzeln der Kongruenz $U^2 + m \equiv 0 \bmod A$, nämlich $U \equiv \frac{y}{x}$, $U \equiv -\frac{y}{x}$ entsprechen.

Bei der Darstellung von B sei die Zuordnung wie früher. Es entsprechen den vier durch $\alpha\beta$, $\alpha\bar{\beta}$, $\bar{\alpha}\beta$, $\bar{\alpha}\bar{\beta}$ vermittelten Darstellungen von $2AB$ vier verschiedene Wurzeln der Kongruenz $U^2 + m \equiv 0 \bmod AB$.

Satz 16 nebst Beweis kann hier fast wörtlich übertragen werden. Auch die weiteren Schlüsse gelten völlig analog.

Ähnlich kann bei eigentlichen Darstellungen $x^2 + my^2 = 2A$, $x'^2 + my'^2 = 2B$ vorgegangen werden. Da hier $m \equiv 1 \bmod 4$ ist, so sind x, y ungerade, die durch $\alpha\beta$ in die Darstellung von $4AB$ durch $X^2 + mY^2$ eintretenden Zahlenwerte $X = xx' - myy'$, $Y = xy' + yx'$ sind beide gerade, und es resultiert eine eigentliche Darstellung von AB.

Wir können analog zu Satz 22 den folgenden aussprechen:

Satz 22a. *Ist p eine Primzahl der Form $4n+3$, von der eine der Zahlen $-m$, $m=5, 13, 37$ quadratischer Rest ist, so ist $2p$ durch x^2+my^2 $(x>0,\ y>0)$ eindeutig darstellbar.*

Die Anwendung der früheren Sätze gibt dann den folgenden

Satz 23. *Es sei $-m$ Rest von N, und*

$$N=\prod_{i,j=1}^{r,s} p_i^{a_i} q_j^{b_j}$$

kanonisch zerlegt, so daß alle $p_i \equiv 1 \bmod 4$, alle $q_j \equiv 3 \bmod 4$ sind. Ist dann Σb_j gerade (also z. B. Null), so ist N auf genau 2^{k-1} Arten durch x^2+my^2 eigentlich darstellbar; ist Σb_j ungerade, so ist N nicht durch diese Form eigentlich darstellbar, aber $2N$ und zwar wieder auf 2^{k-1} Arten. Dabei ist $m=5, 13, 37$.

Die vorhergehenden Sätze lassen sich zu dem folgenden zusammenfassen:

Satz 24. *Ist eine Zahl N durch die Form x^2+my^2 mit $(x,y)=1$, $x>0$, $y>0$ genau auf eine Art eigentlich darstellbar, wobei $m=1, 2, 3, 7$ ist, so ist N Primzahl. Ist N durch diese Form auf mehr als eine Art eigentlich darstellbar, so ist N keine Primzahl. Ist $N \equiv 1 \bmod 4$, so gilt dasselbe, wenn $m=5, 13, 37$ ist. Bei $N \equiv 3 \bmod 4$ hingegen gilt dasselbe mit $2N$ statt N.*

Auch in Satz 24 ist $-m$ als Rest von N vorausgesetzt, falls N Primzahl ist.

Beispiele:

1. Es ist $1481 = 1444 + 37 = 38^2 + 37 \cdot 1^2$. Es wird gefragt, ob $1481 = N$ Primzahl ist. Eine Darstellung durch die Form x^2+37y^2 kommt offenbar nur für $y < \left[\sqrt{\frac{N}{37}}\right] = 6$ in Frage. Wir haben also nur $N - 37y^2$ für $1 < y \leqq 6$ zu bilden und erhalten der Reihe nach 1333, 1148, 889, 556, 149. Das sind keine Quadrate. Mithin ist 1481 Primzahl.

2. Soll $N = 1081$ auf Primzahlcharakter mit der Form x^2+5y^2 untersucht werden, so erwäge man: $N \equiv 1 \bmod 4$. Wir untersuchen also N. Der Ansatz $N = x^2+5y^2$ gibt

$$y < \left[\sqrt{\frac{N}{5}}\right] = [\sqrt{216}] = 14.$$

Es kann nicht $y \equiv 2 \bmod 4$ sein, denn wegen $N \equiv 1 \bmod 8$ folgte dann $x^2 \equiv 5 \bmod 8$, was unmöglich ist.

Nun betrachten wir die Gleichung als Kongruenz mod 3, also $x^2 - y^2 \equiv 1 \bmod 3$. Hier folgt sofort $x^2 \not\equiv 2 \bmod 3$, also $-y^2 \not\equiv -1 \bmod 3$, $y^2 \not\equiv 1 \bmod 3$, also $y \not\equiv 1,2 \bmod 3$. Es muß also $y \equiv 0 \bmod 3$ sein, so daß für y nur die drei Werte 3, 9, 12 bleiben. Von ihnen werden die Zahlen $N - 5y^2$

für $y = 9$, 12 Quadrate, nämlich $N = 26^2 + 5.9^2$, $N = 19^2 + 5.12^2$. Also ist N keine Primzahl, da es zwei Darstellungen durch $x^2 + 5y^2$ gibt. Es ist $N = 23 \cdot 47$.

Wir werden später sehen, wie sich dieses Verfahren weiter ausbauen läßt, nur wollen wir jetzt schon die Bezeichnung anführen: Verfahren der *Exkludenten*. Es muß noch bemerkt werden, daß aus dem Bisherigen nicht hervorgeht, ob das Fehlen jeder Darstellung dazu ausreichend ist, daß N keine Primzahl ist. Nur in den Fällen $m = 1$, 2 ist dies erledigt. In den anderen Fällen müßte erst gezeigt werden, ob N unter die Zahlen fällt, für die $-m$ quadratischer Rest ist, wenn sie Primzahlen sind, mit anderen Worten, es muß eine Bedingung für N gegeben werden, die aussagt, daß $U^2 + m \equiv 0 \bmod N$ lösbar ist, wenn N Primzahl ist. Dies kann erst später untersucht werden. Wir kommen nochmals auf die Frage zurück (vgl. S. 78).

Die tatsächliche Lösung einer Kongruenz $x^2 \equiv a \bmod p$ ohne Indextafel, selbstverständlich wenn $\left(\frac{a}{p}\right) = 1$ ist (p Primzahl), erfordert für größere p oft ziemlich mühselige Versuche. Auch dies werde erst später durchgeführt (S. 89). Hier wollen wir nur kurz sehen, wie der Satz 14 die Lösung der Kongruenz $x^2 \equiv 2 \bmod p$ oft sehr erleichtert. Selbstverständlich muß nach dem zweiten Ergänzungssatz die Primzahl $p \equiv 1,7 \bmod 8$ sein.

In $x^2 - 2y^2 = -p$ mit $0 < |x| < \sqrt{p}$, $0 < |y| < \sqrt{p}$ gilt genauer $\sqrt{\frac{p}{2}} < y < \sqrt{p}$, so daß die Zahl der möglichen Werte von y sich sehr herabsetzt. Denn erstens können x, y positiv angenommen werden, zweitens muß $-2y^2 < -p$, $2y^2 > p$, $y > \sqrt{\frac{p}{2}}$ sein, da $x^2 > 0$ ist.

Es sei vorgelegt $x^2 \equiv 2 \bmod 239$ (Primzahl).

Da $p = 239 \equiv 7 \bmod 8$ ist, gibt es Lösungen. Es muß

$$\sqrt{\frac{p}{2}} < y < \sqrt{p},$$

also $11 \leqq y \leqq 15$ sein. In $x^2 - 2y^2 = -p$ muß x ungerade sein, also $x^2 \equiv 1 \bmod 8$. Die Gleichung wird als Kongruenz $1 - 2y^2 \equiv 1$

mod 8, $2y^2 \equiv 0 \bmod 8$, $y \equiv 0 \bmod 2$. Es bleiben nur die Werte $y = 12, 14$. Setzt man $y = 12$, so bleibt $x = 7$, also $7^2 - 2.12^2 = -239$. Der Wert $x \equiv \frac{7}{12} \equiv \frac{140}{240} \equiv 140$ löst $x^2 \equiv 2 \bmod 239$. Die andere Wurzel der Kongruenz ist $x \equiv -140 \equiv 99$.

§ 13. Einiges über Kongruenzen beliebiger Grade

Nach Satz 2 von § 11 können wir uns bei Besprechung einer allgemeinen Kongruenz n-ten Grades

$$f(x) = a_n x^n + \cdots + a_0 \equiv 0 \bmod m$$

auf den Fall $m = p^k$ = Primzahlpotenz beschränken. Wir behandeln nur den Fall $(a_n, p) = 1$.

Die Tatsache, daß P_p, der Restklassenring mod p, ein Körper ist, gibt sofort

Satz 1. *Eine Kongruenz n-ten Grades $f(x) \equiv 0$ mod p hat höchstens n Wurzeln.*

Für die folgenden Betrachtungen wollen wir annehmen, daß $f(x)$, das wir jetzt lieber nach steigenden Potenzen

$$f(x) = \sum_j a_j x^j$$

in Form einer endlichen Reihe ansetzen wollen, eine Wurzel $a \bmod p$ habe, also $f(a) \equiv 0 \bmod p$ sei.

Wir brauchen einen Hilfssatz

Hilfssatz 1. *Mit $f(x)$ ist auch $\frac{f^{(r)}(x)}{r!}$ ein ganzzahliges Polynom, wobei r eine beliebige natürliche Zahl ist.*

Beweis: Es wird

$$\frac{f^{(r)}(x)}{r!} = \sum \frac{a_j j(j-1)\dots(j-r+1)\, x^{j-r}}{r!}$$

$$= \sum a_j \frac{j!}{r!\,(j-r)!}\, x^{j-r} = \sum a_j \binom{j}{r} x^{j-r}.$$

Dabei ist $\binom{j}{r} = 0$, wenn $j < r$ ist.

Weiter gilt

Hilfssatz 2. *Für x, z ganz und k als natürlicher Zahl gilt:*

$$f(x + p^k z) \equiv f(x) + p^k f'(x)\, z \bmod p^{k+1}.$$

Der Beweis folgt sofort aus der abbrechenden Taylor-Reihe:

$$f(x + h) = f(x) + hf'(x) + h^2 \frac{f''(x)}{2!} + \cdots.$$

Wir gehen nun mit vollständiger Induktion vor: Für den Exponenten k sei eine Wurzel b von $f(x) \equiv 0 \bmod p^k$ gefunden, die $b \equiv a \bmod p$ erfüllt. Wir nehmen in die Voraussetzung die Bedingung $f'(a) \not\equiv 0 \bmod p$ auf, d. h., daß die Restklasse von a in $\mathbf{P}_p$ keine Doppelwurzel von $f(x)$ ist.

Ausgehend von

$$f(b) \equiv 0 \bmod p^k$$

setzen wir in die Kongruenz

$$f(x) \equiv 0 \bmod p^{k+1}$$

den Wert

$$x \equiv b + p^k z \bmod p^{k+1}$$

ein. Nach unseren Hilfssätzen folgt aber weiter

$$f(b) + p^k f'(b)\, z \equiv 0 \bmod p^{k+1}.$$

Wegen

$$f'(b) \equiv f'(a) \bmod p,$$

also

$$p^k f'(b) \equiv p^k f'(a) \bmod p^{k+1},$$

kann dies auch

$$f(b) + p^k f'(a)\, z \equiv 0 \bmod p^{k+1}$$

geschrieben werden.

Es ist $f(b) = A p^k$ mit A ganz. Setzt man dies ein, so erhält man (nach Kürzung durch p^k)

$$A + f'(a)\, z \equiv 0 \bmod p.$$

Diese lineare Kongruenz ist aber wegen $f'(a) \not\equiv 0 \bmod p$ auflösbar.

Da die Induktionsvoraussetzung für $k = 1$ selbstverständlich ist, so gilt

Satz 2. *Hat $f(x) \equiv 0 \bmod p$ (Primzahl) eine einfache Wurzel a, so hat diese Kongruenz Lösungen nach jeder noch so hohen Potenz von p, und zwar Lösungen, die $\equiv a \bmod p$, sind.*

Wir wollen den Satz ergänzen durch den folgenden

Satz 3. *Durch* $f(a) \equiv 0 \bmod p$, $f'(a) \not\equiv 0 \bmod p$, $b \equiv a \bmod p$, $f(b) \equiv 0 \bmod p^k$ *ist die Zahl* $b \bmod p^k$ *eindeutig bestimmt.*

Beweis: Für $k=1$ ist der Satz klar. Er sei für k bewiesen. Wir zeigen ihn dann für $k+1$.

Sei also $f(u) \equiv f(v) \equiv 0 \bmod p^{k+1}$, $u \equiv v \equiv a \bmod p$. Nach der Induktionsvoraussetzung ist $u \equiv v \bmod p^k$, also $v = u + p^k t$ mit ganzzahligem t. Einsetzen in $f(v) \equiv f(u) \equiv 0 \bmod p^{k+1}$ gibt $tp^k f'(a) \equiv 0 \bmod p^{k+1}$, $tf'(a) \equiv 0 \bmod p$. Da $f'(a)$ durch p nicht teilbar ist, bleibt $t \equiv 0 \bmod p$.

Beispiel: $x^3 - x - 1 \equiv 0$ hat als Lösung mod 7: $x \equiv -2$ (einzige Lösung). Es soll eine Lösung mod $7^2 = 49$ hergeleitet werden.
Wir setzen $x = -2 + 7y$ und haben wegen $f(x) = x^3 - x - 1$, $f'(x) = 3x^2 - 1$, $f(-2) = -7$, $f'(-2) = 11 \equiv 4 \bmod 7$ die Kongruenz $-7 + 4.7y \equiv 0 \bmod 7^2$, $y \equiv \frac{1}{4} \equiv 2 \bmod 7$, somit $x \equiv 12 \bmod 49$.

§ 14. Schlußbemerkungen

In Ringen (es werden hier nur kommutative Ringe betrachtet), versteht man unter einem *Ideal* $(a, b, c, \ldots)$ einen endlichen *Modul*[1]) aller $ax + by + cz + \cdots$, wobei $x, y, z, \ldots$ Ringelemente sind.

Ist der Ring Teilintegritätsbereich eines Körpers, so nennt man ein solches Ideal *ganzes Ideal*. Wir führen dann auch *gebrochene Ideale* ein, wobei also $(a, b, c, \ldots)$ zum Körper gehören, aber in $ax + by + cz + \cdots$ alle $x, y, z, \ldots$ zum betrachteten Teilintegritätsbereich gehören.

Ein *eingliedriges Ideal* (a) heißt *Hauptideal*. Es besteht also aus allen Größen ax, wobei x ein beliebiges *Ringelement* ist.

Unser Fundamentalsatz (Satz 5 von § 1) lautet nunmehr:

Satz 1. *Jedes ganze Ideal im Bereiche der ganzen rationalen Zahlen ist Hauptideal.*

Ein endlicher Modul $\left[\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\right]$ mit ganzzahligen a_i und natürlichen b_j ist, wenn $B = \prod b_j$, $\frac{B}{b_j} = C_j$ gesetzt wird mit

$$\frac{1}{B}[a_1 C_1, \ldots, a_n C_n],$$

[1]) Ein Modul ist dadurch definiert, daß mit a und b auch $a-b$, also $a-a=0$, $0-a=-a$, $a-(-a)=2a$ usw. im Modul enthalten sind.

d.h. mit den $\frac{1}{B}$-fachen der ganzen Zahlen $a_1C_1x_1 + \cdots + a_nC_nx_n$, wobei die $x_1, x_2, \ldots, x_n$ ganz sind, gleichbedeutend. Diese letzten Zahlen a_iC_i bestimmen einen Modul; er ist ein eingliedriges Ideal. Sofort folgt

Satz 2. *Jeder endliche Modul im Bereiche der rationalen Zahlen ist ein eingliedriger Modul.*

Satz 3. *Jedes ganze oder gebrochene Ideal im Bereich der ganzen Zahlen ist Hauptideal.*

Schreiben wir den g.g.T. (a, b) an. Man könnte ihn $(a) + (b)$ schreiben, wie dies manchmal geschieht. Er ist, als Ideal betrachtet, der Modul aller Zahlen $aX + bY$, wobei X, Y ganze rationale Zahlen sind.

Dem Leser wird es vielleicht auffallen, daß ich in diesem Teil des § 14 auch ganz rational statt ganz sage. Das soll auf spätere Kapitel vorbereiten, in denen wir den Begriff der ganzen Zahl erweitern.

Aus dieser Auffassung des g.g.T. als Ideal $aX + bY$ folgen sofort die Sätze

Satz 4. $((a, b), c) = (a, (b, c))$.

Satz 5. $(a, b)\, c = (ac, bc)$.

Wir setzen noch den trivialen Satz

Satz 6. $(a, b) = (b, a)$

dazu.

In der vorhin vorgeschlagenen Schreibweise werden die drei Sätze außerordentlich übersichtlich:

Satz 4. $((a) + (b)) + (c) = (a) + ((b) + (c))$.

Satz 5. $((a) + (b))\, c = (ac) + (bc)$.

Satz 6. $(a) + (b) = (b) + (a)$.

Hier ist also eine Addition von Idealen definiert, die nach Satz 6 kommutativ, nach Satz 4 assoziativ, nach Satz 5 gegenüber der Multiplikation mit einer Zahl distributiv ist.

Satz 4 gestattet den g.g.T. von n Zahlen $a_1, \ldots, a_n$ einfach als $(a_1, \ldots, a_n)$ zu schreiben.

Für manche zahlentheoretische Betrachtungen ist folgender Satz wichtig

Satz 7. *Für gegebene ganze Zahlen $x_1, \ldots, x_n$ mit $d = (x_1, \ldots, x_n)$ gibt es ganzzahlige n-reihige Determinanten Δ mit dem ersten Spaltenvektor $x_1, \ldots, x_n$, deren Wert gleich d ist.*

Beweis: Für $n = 2$ ist nichts zu zeigen. Denn nach Satz 5 von § 1 gibt es ganze Zahlen X, Y mit $x_1 X - x_2 Y = d$, also

$$\begin{vmatrix} x_1 & Y \\ x_2 & X \end{vmatrix} = d .$$

Wir nehmen an, der Satz sei für $n-1$ bewiesen. Im allgemeinen Falle können wir annehmen, daß mindestens ein $x_j \neq 0$ ist. (Verschwinden alle x_j so ist nichts zu zeigen.) Sind x_1, x_2 allein von Null verschieden, so ist nichts zu beweisen. Es seien also x_1, x_2, x_3 von Null verschieden, weiter $(x_3, \ldots, x_n) = d'$, es gibt daher ganze Zahlen A_j mit $d' = A_3 x_3 + \cdots + A_n x_n$. Sofort folgt $(x_1, x_2, d') = d$. Wir setzen $x_1 = d g_1$, $x_2 = d g_2$, $d' = dk$. Es gilt $(g_1, g_2, k) = 1$. Nun führen wir die Zahl r ein, das Produkt aller Primfaktoren von g_1, die in g_2 nicht vorkommen. Wir können nun die Menge der Primfaktoren von g_1 in zwei einander ausschließende Teilmengen zerlegen:

1. Alle Primfaktoren von g_1, die in rk aufgehen. Diese können nicht in g_2 aufgehen. Gilt $p \mid r$, so $g_2 \not\equiv 0 \bmod p$ nach der Definition von r. Gilt $p \mid k$, so $g_2 \not\equiv 0 \bmod p$, da sonst $1 = (g_1, g_2, k) \equiv 0 \bmod p$ wäre. (Mit anderen Worten: Jeder in k aufgehende Primfaktor von g_1 geht auch in r auf.)

2. Alle Primfaktoren von g_1, die in g_2 aufgehen.
Wir bilden nun $s = g_2 + rk$. Nach dem Gesagten ist $(s, g_1) = 1$, es gibt Zahlen A, B mit

$$g_1 A - sB = 1,$$

d. h.

$$A x_1 - sdB = d.$$

Wir haben

$$sd = x_2 + rd' = x_2 + r(A_3 x_3 + \cdots + A_n x_n).$$

Die Determinante

$$\Delta = \begin{vmatrix} x_1 & B & 0 & 0 & \dots & 0 \\ sd & A & -A_3 r & -A_4 r & \dots & -A_n r \\ x_3 & 0 & 1 & 0 & \dots & 0 \\ x_4 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \cdot & \cdot & \cdot & & \cdot \\ x_n & 0 & 0 & 0 & \dots & 1 \end{vmatrix}$$

bleibt bei der Addition der $(A_i r)$-fachen i-ten Zeile $(i \geqq 3)$ zur zweiten ihrem Werte nach ungeändert. Wir erhalten

$$\Delta = \begin{vmatrix} x_1 & B & 0 & 0 & \dots & 0 \\ x_2 & A & 0 & 0 & \dots & 0 \\ x_3 & 0 & 1 & 0 & \dots & 0 \\ x_4 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \cdot & \cdot & \cdot & & \cdot \\ x_n & 0 & 0 & 0 & \dots & 1 \end{vmatrix} = d,$$

womit der Satz bewiesen ist.

Wir haben gesehen, daß eine Kongruenz

$$x^m \equiv a \bmod p,$$

(p Primzahl, $(a, p) = 1$) mit

$$y^d \equiv a \bmod p,$$

wobei $d = (m, p-1)$ ist, gleichbedeutend ist.

Es hat also insbesondere bei $(m, p-1) = 1$ keinen Sinn, von m-ten Potenzresten zu sprechen; z. B. hat ein dritter Potenzrest (kubischer Rest) mod 5, ein fünfter Potenzrest mod 13, ein siebenter Potenzrest mod 31 keinen Sinn. Ebenso ist ein quadratischer Rest mod p, wenn p die Form $4n+3$ hat, zugleich biquadratischer Rest. Biquadratische Reste (vierte Potenzreste) haben also nur für Primzahlen $p \equiv 1 \bmod 4$ Bedeutung.

Satz 8. *Sind p, q zwei verschiedene Primzahlen, so ist*

$$p^{q-1} + q^{p-1} \equiv 1 \bmod pq.$$

Beweis: Heißt die linke Seite A, so gilt

$$p \mid A-1, \; q \mid A-1, \quad \text{also wegen} \quad (p, q) = 1 \quad \text{folgt} \quad pq \mid A-1.$$

Der Satz läßt sich unter Anwendung des allgemeinen kleinen Fermat ohne weiteres auf beliebige ganze Zahlen m, n mit $(m, n) = 1$ ausdehnen.

Satz 9. *Sind m, n teilerfremde ganze Zahlen, so ist*

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn.$$

Im Beweis von Satz 8 wurde mitbewiesen

Satz 10. *Aus $a \equiv b \bmod m$ und $\bmod n$ mit $(m, n) = 1$ folgt $a \equiv b \bmod mn$.*

Hieraus ergibt sich sofort

Satz 11. *Ist v das kleinste gemeinsame Vielfache von $\varphi(c_1), \ldots, \varphi(c_t)$, wobei $c_1, \ldots, c_t$ paarweise prim zueinander sind, so ist mit*

$$C = \prod_{j=1}^{t} c_j, \quad (a, C) = 1$$

die Kongruenz

$$a^v \equiv 1 \bmod C$$

erfüllt.

Wir wollen am Ende des ersten Teils die vier letzten Stellen von

$$a = 9^{9^{9^9}}$$

berechnen. Sei $b = 9^9$, $c = 9^b$, also $a = 9^c$.

Wir setzen $c_1 = 5^4$, $c_2 = 2^4$. Es ist daher der kleinste positive Rest von c mod 1000 zu berechnen; denn $\varphi(c_1) = 500$, $\varphi(c_2) = 8$. Wegen $\varphi(5^3) = 100$, $\varphi(2^3) = 4$ genügt der kleinste Rest von b mod 100.

Wegen $9^4 \equiv 61$, $9^5 \equiv 49 \bmod 100$ ist

$$\begin{array}{r} b \equiv 49 \cdot 61 \\ \hline 49 \\ \ldots 4 \\ \hline 89 \end{array}$$

also $b \equiv 89 \bmod 100$. Man beachte: es sind nur die letzten beiden Stellen bei der Multiplikation auszuführen.

Es ist

$$c \equiv 9^{89} \equiv 9^{-11} \bmod 1000.$$

Wir haben wegen $9^5 \equiv 49 \bmod 1000$:

$$9^{-11} \equiv (49 \cdot 441)^{-1}.$$

Es ist

$$\begin{array}{r} 49 \cdot 441 \\ .96 \\ ..6 \\ \hline ..609 \end{array}$$

Wir bekommen $c \equiv \frac{1}{609} \bmod 1000$. Das ist aber schnell umzurechnen:

$$c \equiv \frac{1}{609} \equiv \frac{1001}{609} \equiv \frac{143}{87} = \frac{1143}{87} \equiv \frac{381}{29}$$

$$\equiv 13 + \frac{4}{29} = 13 + \frac{4 \cdot 69}{2001} \equiv 13 + 4 \cdot 69 \equiv 289.$$

Nun bleibt noch zu rechnen

$$a \equiv 9^{289} \bmod 10\,000.$$

Es ist $9^2 \equiv 1 \bmod 16$.

Weiter ist

$$3^{\varphi(625)} \equiv 3^{500} \equiv 1 \bmod 625,$$

also

$$\begin{array}{r} 9^{250} \equiv 1 \bmod 625, \\ 9^{250} \equiv 1 \bmod 16 \\ \hline 9^{250} \equiv 1 \bmod 10000. \end{array}$$

Wir haben $9^{289} \equiv 9^{39}$. Nun rechnen wir

$$9^9 = 9^5 \cdot 9^4 \equiv \begin{array}{r} 9049 \cdot 6561 \\ ..294 \\ ...45 \\ ....4 \\ \hline ....0489 \end{array}$$

$$9^{18} \equiv \begin{array}{r} 489 \cdot 489 \\ \hline 4401 \\ .912 \\ ..56 \\ \hline ..9121 \end{array}$$

$$9^{19} \equiv \quad 2089,$$

$$9^{38} \equiv \quad 2089 \cdot 2089$$

$$\begin{array}{r} .\,8801 \\ ..\,712 \\ ...\,8 \\ \hline ...\,3921, \end{array}$$

schließlich $a \equiv 5289 \bmod 10\,000$.

B. DAS QUADRATISCHE REZIPROZITÄTSGESETZ

§ 15. Ein Blick auf die Galoisfelder

Adjungiert man im Polynombereich $\mathsf{P}_p[x]$ über dem Primkörper P_p der Charakteristik p symbolisch die Wurzel α eines irreduziblen Polynoms n-ten Grades

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \tag{1}$$

so ist der neue Bereich ein Ring mit den p^n Elementen

$$\gamma = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

wobei $c_0, c_1, c_2, \ldots, c_{n-1}$ die Elemente von P_p durchlaufen. Er heißt *Galoisfeld* $GF(p^n)$.

Als endlicher Ring ist das Galoisfeld ein Vollring. Es ist zugleich ein Körper. Wir können uns dies einfach überlegen.

Eine Gleichung im Galoisfeld

$$f_1(\alpha) f_2(\alpha) = f_0(\alpha),$$

wobei die f_j Polynome höchstens vom Grade $n-1$ mit Koeffizienten aus P_p sind, ist gleichwertig mit einer Gleichung in $\mathsf{P} = \mathsf{P}_0$

$$f_1(x) f_2(x) = f_0(x) + q(x) f(x), \tag{2}$$

oder, wenn man will, einer Gleichung in $\mathsf{P}_0[x]$, wobei P_0 der Primkörper der Charakteristik Null, d. h. der Körper der rationalen Zahlen ist

$$f_1(x) f_2(x) = f_0(x) + q(x) f(x) + pF(x).$$

($F(x)$ ist ein Polynom mit mod p ganzen Koeffizienten.)

Nun folgte aus $f_0(\alpha) = 0$ (die Null ist in P_p oder — was auf dasselbe hinauskommt — im Galoisfeld gemeint), daß in $\mathsf{P}_p[x]$ sich die Gleichung (2) zu

$$f_1(x) f_2(x) = q(x) f(x) \tag{3}$$

vereinfacht. Nun ist sehr wesentlich, daß $f(x)$ irreduzibel ist. Mithin muß entweder $f_1(x)$ oder $f_2(x)$ durch $f(x)$ teilbar sein,

d. h. im Galoisfeld $GF(p^n)$ eine der Zahlen $f_1(\alpha)$, $f_2(\alpha)$ Null sein. Also gilt

Satz 1. *Das Galoisfeld $GF(p^n)$ ist ein Körper von p^n Elementen.*

Da die von Null verschiedenen Elemente eines Körpers eine Gruppe bilden, in diesem Falle aber diese Gruppe endlich und ihre Ordnung p^n-1 ist, folgt sofort

Satz 2. *Für ein beliebiges in $GF(p^n)$ liegendes Element $\varrho \neq 0$ ist*

$$\varrho^{p^n-1} = 1 .$$

Multiplikation mit ϱ gibt

$$\varrho^{p^n} = \varrho , \tag{4}$$

und dies gilt offenbar auch, wenn ϱ das Nullelement ist. Wir haben also

Satz 3. *Die p^n-te Potenz jedes Elements des Galoisfelds ist das Element selbst.*

Dies kann auch so ausgesprochen werden:

Satz 4. *Jedes Element des Galoisfelds ist Wurzel des Polynoms*

$$F(x) = x^{p^n} - x .$$

Erhebt man (1) zur p-ten Potenz:

$$f^p(x) = x^{np} + a_1{}^p x^{(n-1)p} + \cdots + a_n{}^p ,$$

so sieht man sofort wegen $a_j{}^p = a_j$ (kleiner Fermat)

$$f^p(x) = f(x^p) . \tag{5}$$

Wegen $f(\alpha) = 0$ ist auch $f(\alpha^p) = 0$, also α^p eine von α verschiedene Wurzel von $f(x) = 0$. Fortsetzung dieses Schlusses ergibt, daß der Reihe nach

$$\alpha , \ \alpha^p , \ \alpha^{p^2} , \ \ldots , \ \alpha^{p^{n-1}} \tag{6}$$

Wurzeln des Polynoms (1) sind. Die in (6) angeführten Größen sind alle voneinander verschieden. Dies folgt so: Wir nehmen an, es sei

$$\alpha^{p^a} = \alpha^{p^b} \tag{7}$$

mit $0 \leqq a < b < n$ erfüllt. Setzen wir die linke Seite der Gleichung gleich β, weiter $b - a = c$, also $0 < c < n$, so folgt aus (7)

$$\beta = \beta^{p^c} . \tag{8}$$

Zugleich ist $f(\beta) = 0$. Es folgt weiter, da man das Galoisfeld auch durch $\mathsf{P}_p(\beta)$ erzeugt denken kann, daß seine Elemente auch durch

$$\gamma = k_0 + k_1\beta + \cdots + k_{n-1}\beta^{n-1}$$

gegeben gedacht werden können. Die k_j liegen in P_p.
Wegen

$$k_j^p = k_j$$

(kleiner Fermat) und (8) folgt

$$\gamma^{p^c} = \gamma \tag{9}$$

für jedes Element des Galoisfelds $GF(p^n)$.
Es müßte also die Gleichung

$$x^{p^c} - x = 0$$

alle Elemente des Galoisfeldes zur Wurzel haben, also mehr als ihr Grad angibt, was in einem Körper unmöglich ist. Es folgt

Satz 5. *Entsteht durch Adjunktion der Wurzel α eines in P_p irreduziblen Polynoms ein Galoisfeld $GF(p^n)$, so sind sämtliche Wurzeln durch*

gegeben.

$$\alpha,\ \alpha^p,\ \alpha^{p^2},\ \ldots,\ \alpha^{p^{n-1}} \tag{10}$$

Jedes irreduzible Polynom n-ten Grades $g(x)$ mit Koeffizienten aus P_p ist Teiler von $F(x) = x^{p^n} - x$. Adjungiert man zu P_p symbolisch eine Wurzel β von $g(x)$, so entsteht ebenfalls ein Galoisfeld mit p^n Elementen. Nun sind aber durch die p^n Elemente des vorhin konstruierten Körpers alle Wurzeln von $F(x)$ erschöpft. β liegt also auch in diesem Galoisfeld. Wir können von jetzt ab statt von einem Galoisfeld $GF(p^n)$ von dem Galoisfeld $GF(p^n)$ sprechen. Im Sinne der abstrakten Körpertheorie ist also das Galoisfeld eindeutig bestimmt.
Eine Gleichung (die Koeffizienten der Polynome f_j liegen im Körper P_p)

$$f_1(\alpha) f_2(\alpha) + f_3(\alpha) + f_4(\alpha) = f_5(\alpha)$$

im Galoisfeld geht bei Ersetzung von α durch α^p in

$$f_1(\alpha^p) f_2(\alpha^p) + f_3(\alpha^p) + f_4(\alpha^p) = f_5(\alpha^p)$$

über. Es ist also $s = (\alpha/\alpha^p)$ (Ersetzungen von α durch α^p) ein Automorphismus in $GF(p^n)$. Hierbei geht jedes Element δ in δ^p über. Denn ist

$$\delta = d_0 + d_1\alpha + \cdots + d_{n-1}\alpha^{n-1},$$

wobei die Koeffizienten d_j in P_p liegen, so ist wegen $d_j^p = d_j$ (kleiner Fermat)

$$\delta^p = d_0 + d_1\alpha^p + \cdots + d_{n-1}\alpha^{(n-1)p}.$$

Wir bekommen die n Automorphismen

$$s = (\alpha/\alpha^p),\ s^2 = (\alpha/\alpha^{p^2}), \ldots, s^{n-1} = (\alpha/\alpha^{p^{n-1}}),$$

$s^n = (\alpha/\alpha^{p^n}) = (\alpha/\alpha) = 1$ (identischer Automorphismus). Weitere Automorphismen gibt es nicht.

Dieses ergibt sich wie folgt: Jeder Automorphismus muß P_p unverändert lassen. Denn P_p hat keine Automorphismen außer dem identischen. Dies ergibt sich ganz einfach. Denn da der Automorphismus das Einselement, das ich in diesem Paragraphen kurz mit 1 bezeichne, unverändert lassen muß, weiter, wenn t der Automorphismus ist, der als symbolische Potenz bezeichnet werde, stets

$$(a+b)^t = a^t + b^t,\ (ab)^t = a^t b^t$$

gilt, so ist für ein beliebiges Element m (Restklasse von m in P_p)

$$m = 1+1+\cdots+1\ (m - \text{mal}),$$

daher

$$m^t = 1+1+\cdots+1 = m.$$

Es muß also t die definierende Gleichung $f(x) = 0$ unverändert lassen. Daher muß α^t eine Wurzel von $f(x)$, etwa

$$\alpha^t = \alpha^{p^j}$$

mit $0 \leqq j < n$ sein (wenn wir den identischen Automorphismus mitrechnen). Das sollte aber eben gezeigt werden. Wir haben

Satz 6. *Die Automorphismen von $GF(p^n)$ sind*

$$1,\ s = (\alpha \mid \alpha^p),\ s^2 = (\alpha \mid \alpha^{p^2}),\ s^3 = (\alpha \mid \alpha^{p^3}), \ldots, s^{n-1} = (\alpha \mid \alpha^{p^{n-1}}).$$

Hierbei ist 1 der identische Automorphismus. Diese n Automorphismen bilden eine zyklische Gruppe. Weitere gibt es nicht. Die Elemente a aus P_p sind durch $a^s = a^p = a$ ausgezeichnet.

Wir nehmen an, es seien über P_p zwei Galoisfelder $\Lambda = GF(p^a)$, $\Lambda' = GF(p^b)$ aufgebaut, mit $1 \leqq a < b$, weiter gelte $\mathsf{P}_p \leqq \Lambda < \Lambda'$. Hierzu ist notwendig und hinreichend $b \equiv 0 \bmod a$. Das reicht jedenfalls aus. Denn die Elemente von Λ sind die Wurzeln von $F_1(x) = x^{p^a} - x$, die von Λ' die Wurzeln von $F_2(x) = x^{p^b} - x$

und für $b \equiv 0 \bmod a$ gilt $F_1(x) \mid F_2(x)$ (dies ist schon richtig, wenn wir beide Polynome nur über P_0 betrachten). Es ist auch notwendig. Denn ist α ein erzeugendes Element von Λ über P_p, also $\Lambda = \mathsf{P}_p(\alpha)$, so ist

$$\alpha^{p^a-1} = 1, \tag{11}$$

und dies gilt für keine niedrigere Potenz von α. Ist nun $b \not\equiv 0 \bmod a$, so ist

$$p^b - 1 \not\equiv 0 \bmod (p^a - 1).$$

Denn ist $b = ax + y$ mit $0 < y < a$, so wird

$$p^b - 1 = p^{ax+y} - 1 = (p^a)^x \cdot p^y - 1$$

$$= p^y \{(p^a)^x - 1\} + p^y - 1 \equiv p^y - 1 \bmod (p^a - 1).$$

Also gilt für $d = (p^b - 1, p^a - 1)$ die Ungleichung $d < p^a - 1$. Wäre nun

$$\alpha^{p^b-1} = 1, \tag{12}$$

so folgte mit ganzen Zahlen X, Y, die

$$(p^a - 1)\, X + (p^b - 1)\, Y = d$$

erfüllen, durch Erhebung von (11) zur Potenz X, von (12) zur Potenz Y zur Multiplikation

$$\alpha^d = 1,$$

im Widerspruch dazu, daß die durch (11) gegebene Potenz die kleinste von α mit positivem Exponenten ist, die gleich dem Einselement wird.

Nun sei also $\mathsf{P}_p \subseteqq \Lambda < \Lambda'$.

Satz 7. *Ist ϱ ein Element von Λ', dann liegt mit ϱ^p auch ϱ in Λ.*

Beweis: Es entsteht ϱ^p aus ϱ durch den Automorphismus s in Λ'. Dieser läßt die Elemente von P_p, also die definierende Gleichung unverändert.

Sofort folgt

Satz 8. *Ist ϱ ein Element von Λ', dann liegt mit ϱ^{p^c} auch ϱ in Λ.*

Wir brauchen später noch

Satz 9. *Ist $(x - \varrho)^A = \sum g_j x^j$ ein Polynom in $\Lambda[x]$, und liegt ϱ in Λ', so liegt ϱ bereits in Λ.*

Beweis: Zunächst sei $A \not\equiv 0 \bmod p$. Dann ist der Koeffizient von x^{A-1} in dem Polynom gleich

$$\underset{A-1}{g} = -A\varrho.$$

Da dieser Koeffizient in Λ liegt, so liegt ϱ in Λ.
Vor Übergang zum Falle $p \mid A$ einige Bemerkungen: Es wird in jedem Körper der Charakteristik p

$$(x+a)^p = x^p + a^p,$$

$$(x+a)^{p^2} = x^{p^2} + a^{p^2}, \ldots$$

Demnach wird für $p > 2$

$$(x-a)^{p^m} = x^{p^m} - a^{p^m}.$$

Dies kann aber auch für $p = 2$ angesetzt werden, da in Körpern der Charakteristik 2 Addition und Subtraktion auf dasselbe hinauskommt.
Wir haben etwa $p^T \| A$, $A = p^T A'$, wobei A' zur Charakteristik p prim ist.
Es gilt mit $x^{p^T} = y$, $\varrho^{p^T} = \varrho'$:

$$(x-\varrho)^A = \left\{(x-\varrho)^{p^T}\right\}^{A'} = (y-\varrho')^{A'}.$$

Nach dem bereits Bewiesenen liegt ϱ' in Λ, nach Satz 8 auch ϱ.

Wir haben nur diejenigen Sätze aus der Theorie der Galoisfelder hier besprochen, die für unsere weiteren Darlegungen noch gebraucht werden. Für ein tieferes Eindringen sei der Leser auf ein Lehrbuch der modernen Algebra verwiesen.

§ 16. Bestimmung der Anzahl der Lösungspaare einer Kongruenz

Satz 1. *Ist p eine ungerade Primzahl, sind die Zahlen A, B, C ganz und zu p prim, so gibt es ganze Zahlen x, y mit $Ax^2 - By^2 - C \equiv 0 \bmod p$.*

Beweis: Mit $x = 0, 1, \ldots, \frac{p-1}{2}$; $y = 0, 1, \ldots, \frac{p-1}{2}$ durchläuft Ax^2 genau $\frac{p+1}{2}$ inkongruente Werte, nämlich Null und die A-fachen quadratischen Reste, $By^2 + C$ ebenfalls $\frac{p+1}{2}$ inkongruente

Werte. Es muß ein Wertepaar $[x, y]$ mit $Ax^2 \equiv By^2 + C \bmod p$ existieren, da es sonst $(p+1)$ Reste $\bmod p$ gäbe (Schubfachschluß).
Zunächst brauchen wir den Satz für $A = t$, $B = -1$, $C = k$ ($k \not\equiv 0 \bmod p$), können also die Existenz von Lösungen von

$$x^2 + y^2 - k \equiv 0 \bmod p \tag{1}$$

voraussetzen.

Wir gehen aus von einem Lösungspaar $[m, n]$; ohne Einschränkung der Allgemeinheit können wir $n \not\equiv 0 \bmod p$ annehmen, da wegen $k \not\equiv 0 \bmod p$ nicht beide Zahlen m, n durch p teilbar sind. Dann haben wir zwei Lösungspaare $[m, n]$, $[m, -n]$, die im folgenden nicht weiter betrachtet werden, auf die wir aber im Schlußergebnis zurückkommen müssen.
Wir haben

$$x^2 + y^2 \equiv m^2 + n^2 \bmod p$$

oder $$(x + m)(x - m) \equiv (n + y)(n - y) \bmod p,$$

wobei die rechte Seite jedenfalls durch p nicht teilbar ist. Daher gilt

$$x + m \equiv A(n + y) \bmod p,$$

$$x - m \equiv \frac{1}{A}(n - y) \bmod p,$$

oder

$$x - Ay \equiv An - m \bmod p,$$

$$x + \frac{y}{A} \equiv \frac{n}{A} + m \bmod p. \tag{2}$$

Wir bekommen also alle weiteren Lösungen, wenn wir A, soweit dies möglich ist, aus den von der Nullklasse verschiedenen Restklassen $\bmod p$ (den von Null verschiedenen Elementen des Körpers P_p) wählen.
Nun sind zwei Fälle zu unterscheiden:
Zunächst sei $p \equiv 1 \bmod 4$.
Dann sind wegen

$$\begin{vmatrix} 1 & -A \\ 1 & \frac{1}{A} \end{vmatrix} \equiv \frac{A^2+1}{A} \bmod p$$

unter den Restklassen die beiden $x \equiv A_1$, A_2 mit $A_1^2 \equiv A_2^2 \equiv -1$ ($A_2 \equiv -A_1$) auszuschließen. Es bleiben $p - 3$ mögliche Werte von A, also mit Einschluß der beiden zurückgestellten Wertepaare $(p - 1)$ Lösungen von (1).

Bei $p \equiv 3 \bmod 4$ gelten ähnliche Überlegungen, nur daß die Zahlen A_1, A_2 wegen $\left(\frac{-1}{p}\right) = -1$ nicht existieren; es bleiben $(p+1)$ Lösungen von (1).

Ganz anders ist es in dem bisher ausgeschlossenen Fall $k \equiv 0 \bmod p$.

Für $p \equiv 3 \bmod 4$ erledigt er sich sofort: Wegen $\left(\frac{-1}{p}\right) = -1$ existiert dann (bis auf kongruente) nur das lösende Wertepaar $[0, 0]$. Ist p von der Form $4X+1$, so haben wir, wenn A_1, A_2 die vorige Bedeutung haben, die $(2p-1)$ inkongruenten Wertepaare $[A_1 t, t]$, $[A_2 t, t]$, $[0, 0]$, wobei t das reduzierte Restsystem mod p durchläuft.

Zusammengefaßt ergibt sich

Satz 2. *Für $k \not\equiv 0 \bmod p$ hat $x^2 + y^2 \equiv k \bmod p$ genau $(p-1)$ inkongruente Lösungen, wenn $p \equiv 1 \bmod 4$ ist, hingegen $(p+1)$ inkongruente Lösungen für $p \equiv 3 \bmod 4$. Ist k durch p teilbar, so ist für $p \equiv 1 \bmod 4$ die Anzahl der Lösungen $(2p-1)$, für ein p der Form $4X+3$ hingegen 1.*

Man kann Satz 2 noch etwas anders aussprechen:

Satz 3. *Ist p eine ungerade Primzahl, so hat $x^2 + y^2 \equiv k \bmod p$ für durch p nicht teilbare k Lösungen in der Anzahl $p - \left(\frac{-1}{p}\right)$, für $p \mid k$ hingegen in der Anzahl $pt\,(p-1)\left(\frac{-1}{p}\right)$.*

§ 17. Die Darstellung der ganzen Zahlen als Summe von vier Quadraten

Satz 1 von § 16 gibt sofort

Satz 1. *Ist p eine ungerade Primzahl, so gibt es ganzzahlige Werte x, y, z, die nicht alle durch p teilbar sind, so daß $x^2 + y^2 + z^2 \equiv 0 \bmod p$ ist.*

Beweis: Im erwähnten Satz sei $A=1$, $B=C=-1$. Dann gilt der Satz für $z=1$, was sicher nicht durch p teilbar ist.

Satz 2. *Ist p eine ungerade Primzahl, so existieren ganze Zahlen x, y, z, u mit $x^2 + y^2 + z^2 + u^2 \equiv 0 \bmod p$, ohne daß alle diese vier Zahlen durch p teilbar sind.*

Werte. Es muß ein Wertepaar $[x, y]$ mit $Ax^2 \equiv By^2 + C \bmod p$ existieren, da es sonst $(p+1)$ Reste $\bmod p$ gäbe (Schubfachschluß).
Zunächst brauchen wir den Satz für $A = t$, $B = -1$, $C = k$ ($k \not\equiv 0 \bmod p$), können also die Existenz von Lösungen von

$$x^2 + y^2 - k \equiv 0 \bmod p \tag{1}$$

voraussetzen.

Wir gehen aus von einem Lösungspaar $[m, n]$; ohne Einschränkung der Allgemeinheit können wir $n \not\equiv 0 \bmod p$ annehmen, da wegen $k \not\equiv 0 \bmod p$ nicht beide Zahlen m, n durch p teilbar sind. Dann haben wir zwei Lösungspaare $[m, n]$, $[m, -n]$, die im folgenden nicht weiter betrachtet werden, auf die wir aber im Schlußergebnis zurückkommen müssen.
Wir haben

$$x^2 + y^2 \equiv m^2 + n^2 \bmod p$$

oder $$(x+m)(x-m) \equiv (n+y)(n-y) \bmod p,$$

wobei die rechte Seite jedenfalls durch p nicht teilbar ist. Daher gilt

$$x + m \equiv A(n+y) \bmod p,$$

$$x - m \equiv \frac{1}{A}(n-y) \bmod p,$$

oder

$$x - Ay \equiv An - m \bmod p,$$

$$x + \frac{y}{A} \equiv \frac{n}{A} + m \bmod p. \tag{2}$$

Wir bekommen also alle weiteren Lösungen, wenn wir A, soweit dies möglich ist, aus den von der Nullklasse verschiedenen Restklassen $\bmod p$ (den von Null verschiedenen Elementen des Körpers P_p) wählen.
Nun sind zwei Fälle zu unterscheiden:
Zunächst sei $p \equiv 1 \bmod 4$.
Dann sind wegen

$$\begin{vmatrix} 1 & -A \\ 1 & \frac{1}{A} \end{vmatrix} \equiv \frac{A^2+1}{A} \bmod p$$

unter den Restklassen die beiden $x \equiv A_1$, A_2 mit $A_1^2 \equiv A_2^2 \equiv -1$ ($A_2 \equiv -A_1$) auszuschließen. Es bleiben $p-3$ mögliche Werte von A, also mit Einschluß der beiden zurückgestellten Wertepaare $(p-1)$ Lösungen von (1).

Bei $p \equiv 3 \bmod 4$ gelten ähnliche Überlegungen, nur daß die Zahlen A_1, A_2 wegen $\left(\frac{-1}{p}\right) = -1$ nicht existieren; es bleiben $(p+1)$ Lösungen von (1).

Ganz anders ist es in dem bisher ausgeschlossenen Fall $k \equiv 0 \bmod p$.

Für $p \equiv 3 \bmod 4$ erledigt er sich sofort: Wegen $\left(\frac{-1}{p}\right) = -1$ existiert dann (bis auf kongruente) nur das lösende Wertepaar $[0, 0]$. Ist p von der Form $4X+1$, so haben wir, wenn A_1, A_2 die vorige Bedeutung haben, die $(2p-1)$ inkongruenten Wertepaare $[A_1 t, t]$, $[A_2 t, t]$, $[0, 0]$, wobei t das reduzierte Restsystem mod p durchläuft.

Zusammengefaßt ergibt sich

Satz 2. *Für $k \not\equiv 0 \bmod p$ hat $x^2 + y^2 \equiv k \bmod p$ genau $(p-1)$ inkongruente Lösungen, wenn $p \equiv 1 \bmod 4$ ist, hingegen $(p+1)$ inkongruente Lösungen für $p \equiv 3 \bmod 4$. Ist k durch p teilbar, so ist für $p \equiv 1 \bmod 4$ die Anzahl der Lösungen $(2p-1)$, für ein p der Form $4X+3$ hingegen 1.*

Man kann Satz 2 noch etwas anders aussprechen:

Satz 3. *Ist p eine ungerade Primzahl, so hat $x^2 + y^2 \equiv k \bmod p$ für durch p nicht teilbare k Lösungen in der Anzahl $p - \left(\frac{-1}{p}\right)$, für $p \mid k$ hingegen in der Anzahl $p\,t\,(p-1)\left(\frac{-1}{p}\right)$.*

§ 17. Die Darstellung der ganzen Zahlen als Summe von vier Quadraten

Satz 1 von § 16 gibt sofort

Satz 1. *Ist p eine ungerade Primzahl, so gibt es ganzzahlige Werte x, y, z, die nicht alle durch p teilbar sind, so daß $x^2 + y^2 + z^2 \equiv 0 \bmod p$ ist.*

Beweis: Im erwähnten Satz sei $A=1$, $B=C=-1$. Dann gilt der Satz für $z=1$, was sicher nicht durch p teilbar ist.

Satz 2. *Ist p eine ungerade Primzahl, so existieren ganze Zahlen x, y, z, u mit $x^2 + y^2 + z^2 + u^2 \equiv 0 \bmod p$, ohne daß alle diese vier Zahlen durch p teilbar sind.*

Beweis: In der Kongruenz des vorigen Satzes füge man $u = 0$ bei.

Satz 3. *Jede Primzahl p ist als Summe von vier Quadraten darstellbar.*

Beweis

I. Es ist $2 = 1^2 + 1^2 + 0^2 + 0^2$.

II. Wir können daher $p > 2$ annehmen. Der vorige Satz gibt

$$x^2 + y^2 + z^2 + u^2 = pm.$$

Nun ersetzen wir x, y, z, u durch die Absolutbeträge ihrer absolutkleinsten Reste mod p, sie seien $x', \ldots, u'$. Wir haben

$$x'^2 + y'^2 + z'^2 + u'^2 = pm'$$

mit $m' < p$. Wir schreiben wieder

$$x^2 + y^2 + z^2 + u^2 = pm \tag{1}$$

mit $m < p$, daher $(p, m) = 1$.

Ist $m = 1$, so sind wir fertig. Bei $m = 2$ sind entweder alle vier Zahlen ungerade oder zwei gerade. Die Allgemeinheit wird durch die Annahme $x \equiv y$, $z \equiv u \bmod 2$ nicht verletzt. Dann haben wir

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+u}{2}\right)^2 + \left(\frac{z-u}{2}\right)^2 = p\,.$$

Also können wir $m \geqq 3$ annehmen. Der Fall $x \equiv y \equiv z \equiv u \equiv \frac{m}{2} \bmod m$, wobei m gerade ist, erledigt sich sehr schnell; denn dann ist $pm \equiv 0 \bmod \frac{m^2}{4}$, $2pm \equiv 0 \bmod \frac{m^2}{2}$, $2p \equiv 0 \bmod \frac{m}{2}$. Wegen $(p, m) = 1$ bleibt $2 \equiv 0 \bmod \frac{m}{2}$, also $m = 4$; es sind x, y, z, u gerade, so daß man (1) durch 4 kürzen könnte.

Es sei also $m \geqq 3$, $\min(|A|, |B|, |C|, |D|) < \frac{m}{2}$, wobei A, B, C, D die absolutkleinsten Reste von $x, y, z, u \bmod m$ sind. Es folgt eine Gleichung

$$A^2 + B^2 + C^2 + D^2 = mn \tag{2}$$

mit $n < m$. Dabei gilt

$$x \equiv A,\ y \equiv B,\ z \equiv C,\ u \equiv D \bmod m. \tag{3}$$

Für vier komplexe Zahlen $\alpha, \beta, \gamma, \delta$ (der Querstrich kennzeichnet die konjugiertkomplexe Zahl) gilt nach dem Multiplikationstheorem der Determinanten

$$\begin{vmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{vmatrix} \cdot \begin{vmatrix} \delta & -\bar{\gamma} \\ \gamma & \bar{\delta} \end{vmatrix} = \begin{vmatrix} \xi & -\bar{\eta} \\ \eta & \bar{\xi} \end{vmatrix} \tag{4}$$

mit $$\xi = \alpha\delta - \beta\gamma,\ \eta = \bar{\alpha}\gamma + \bar{\beta}\delta.$$

Bei den Formeln dieses Absatzes seien alle mit lateinischen Buchstaben bezeichneten Größen reell. Mit $\alpha = x + yi$, $\beta = z + ui$, $\gamma = A + Bi$, $\delta = C + Di$, $\xi = M + Ni$, $\eta = P + Qi$ folgt aus (4)

$$(x^2 + y^2 + z^2 + u^2)\,(A^2 + B^2 + C^2 + D^2) = M^2 + N^2 + P^2 + Q^2. \tag{5}$$

Wir erhalten

Satz 4. *Das Produkt zweier als Summe von vier Quadraten darstellbarer Zahlen ist wieder als Summe von vier Quadraten darstellbar.*

Nach (3) können wir $\gamma = \alpha + m\sigma$, $\delta = \beta + m\tau$ setzen. Dabei gehören $\alpha, \beta, \gamma, \delta, \sigma, \tau$ dem Ring der Zahlen $U + iV$ mit ganzem rationalem U, V an. Wir erhalten

$$\xi = \alpha\delta - \beta\gamma = \alpha\beta + m\alpha\tau - (\alpha\beta + m\beta\sigma) = m\Gamma,$$

weiter unter Beachtung von (1)

$$\eta = \bar{\alpha}\gamma + \bar{\beta}\delta = \alpha\bar{\alpha} + m\bar{\alpha}\sigma + \beta\bar{\beta} + m\bar{\beta}\tau = m\Delta,$$

wobei Γ, Δ Zahlen dieses Rings sind. Nunmehr setzen wir $\Gamma = r + si$, $\Delta = h + ki$ mit r, s, h, k ganz rational. Die Multiplikation der Gleichungen (1) und (2) gibt

$$m^2 (r^2 + s^2 + h^2 + k^2) = p\,m^2 n$$

oder

$$r^2 + s^2 + h^2 + k^2 = pn.$$

Ist n noch nicht Eins (oder 2), so kann man dieses Verfahren fortsetzen. Schließlich bleibt

$$G^2 + H^2 + K^2 + L^2 = p.$$

Satz 5. *Jede natürliche Zahl ist als Summe von vier Quadraten darstellbar.*

Beweis: Er folgt aus Satz 3 und 4.

§ 18. Gaußsche Summen

Im folgenden seien p, q zwei ungerade voneinander verschiedene (positive) Primzahlen. Entweder in P_q oder einem entsprechenden Erweiterungskörper liegt eine primitive p-te Einheitswurzel α. Grundlegend für das folgende ist der Ausdruck

$$T_p = \sum_{m=0}^{p-1} \alpha^{m^2}.$$

bzw. das Quadrat dieses Ausdrucks.
T_p heißt Gaußsche Summe (über P_q); am Ende des Paragraphen widmen wir auch einige Worte der Gaußschen Summe T_p über P_0, wenn unter α speziell die primitive p-te Einheitswurzel

$$\alpha = e^{\frac{2\pi i}{p}} \tag{1}$$

verstanden wird. Dabei wird sich herausstellen, daß T_p bis auf ein Vorzeichen sehr leicht zu finden ist. Die (überaus wichtige!) Frage nach dem Vorzeichen ist aber außerordentlich schwer zu beantworten. Wir wollen sie auf den zweiten Band verschieben.
Gegeben sei also T_p über P_q. Es wird

$$T_p^2 = \sum_{m,n=0}^{p-1} \alpha^{m^2+n^2}. \tag{2}$$

Sei zunächst $p \equiv 1 \bmod 4$. Dann enthält nach § 16, Satz 2 (oder 3) die Summe genau $(p-1)$ Glieder gleich α^k mit $1 \leqq k < p$, aber $2p-1$ Glieder gleich $\alpha^0 = 1$ (Einselement in P_q). Mithin ist

$$T_p^2 = (p-1)\sum_{k=1}^{p-1} \alpha^k + 2p - 1 = (p-1)\sum_{k=0}^{p-1} \alpha^k + p = p. \tag{3}$$

Ist hingegen $p \equiv 3 \bmod 4$, so enthält die Summe $(p+1)$ Glieder gleich α^k mit $1 \leqq k < p$. Nur ein Glied mit Eins (Einselement in P_q) ist vorhanden. Daher wird jetzt

$$T_p^2 = (p+1)\sum_{k=1}^{p-1} \alpha^k + 1 = (p+1)\sum_{k=0}^{p-1} \alpha^k - p = -p. \tag{4}$$

Die Formeln (3) und (4) lassen sich in

$$T_p^2 = (-1)^{\frac{p-1}{2}} p \tag{5}$$

zusammenfassen.

Selbstverständlich gelten die Entwicklungen genau so, wenn statt P_2 der Körper P_0 oder der Körper aller reellen oder aller komplexen Zahlen eintritt. Dann gilt die Formel (5) auch hier, somit

$$T_p = \pm \sqrt{(-1)^{\frac{p-1}{2}} p}\,, \tag{6}$$

wobei wir die Quadratwurzel ausnahmsweise auch bei negativem Radikanden normieren: $\sqrt{-A^2} = +Ai$ $(A > 0)$. Bis auf das Vorzeichen ist also die Formel (6) sehr leicht zu erhalten. Der Beweis für den (richtigen!) Satz, daß bei Normierung der p-ten Einheitswurzel nach Formel (1) in (6) das positive Vorzeichen gilt, ist sehr schwer zu erbringen.

§ 19. Das quadratische Reziprozitätsgesetz

Wir sind nun sehr nahe daran, das bisher nur angeführte, noch nicht ausgesprochene quadratische Reziprozitätsgesetz zu beweisen.

Wir gehen aus von § 18, Formel (5).

1. Sei $\left(\frac{q}{p}\right) = 1$. Dann gilt

$$T_p = \sum_{m=0}^{p-1} \alpha^{m^2} = \sum_{m=0}^{p-1} \alpha^{q\,m^2} = \left(\sum_{m=0}^{p-1} \alpha^{m^2}\right)^q, \qquad T_p^{q-1} = 1\,,$$

also liegt T_p in P_q, es ist

$$\left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = 1\,. \tag{1}$$

2. Sei $\left(\frac{q}{p}\right) = -1$. Mit

$$T_p' = \sum_{m=0}^{p-1} \alpha^{q\,m^2}$$

ist zunächst $T_p + T_p' = 0$, da in der Summe jede Potenz von α von der nullten bis zur $(p-1)$-ten (beides inkl.) genau zweimal vorkommt; aber es ist $T_p = T_p'$ ausgeschlossen, sonst wäre $2\,T_p = 0$, also, da die Charakteristik von P_q von 2 verschieden

ist, $T_p = 0$. Es ist $T_p' = T_p{}^q$, aber $T_p{}^{q-1} \neq 1$, T_p liegt nicht im Primkörper P_q (sondern im Galoisfeld $GF(q^2)$), und daher ist

$$\left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = -1. \tag{2}$$

Die Formeln (1) und (2) können in

$$\left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = \left(\frac{q}{p}\right) \tag{3}$$

zusammengefaßt werden. Sofort bleibt $\left(\text{wegen } \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}\right)$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{4}$$

Die Formel (4) *ist das quadratische Reziprozitätsgesetz.* Sie kann auch so ausgesprochen werden:

Satz 1. *Sind p, q ungerade voneinander verschiedene Primzahlen, davon mindestens eine der Form $4X+1$, so sind sie entweder gegenseitige quadratische Reste oder quadratische Nichtreste. Gilt aber $p \equiv q \equiv 3 \bmod 4$, so ist p Rest von q, wenn q Nichtrest von p ist, und p Nichtrest von q, wenn q Rest von p ist.*

§ 20. Das verallgemeinerte Reziprozitätsgesetz

Wir führen hier zunächst für ungerade Werte des Arguments $A, B, \ldots$ die Funktionen $Q(A) \equiv \frac{A-1}{2} \bmod 2$ und $Q'(A) \equiv \frac{A^2-1}{8} \bmod 2$ ein. Wir beweisen

Satz 1. *Für ungerade Werte des Arguments haben $Q(A)$, $Q'(A)$ mod 2 die logarithmische Eigenschaft*

$$Q(AB) \equiv Q(A) + Q(B) \bmod 2,$$
$$Q'(AB) \equiv Q'(A) + Q'(B) \bmod 2.$$

Beweis: Multiplikation der Kongruenzen

$$A \equiv 1 + 2Q(A),\ B \equiv 1 + 2Q(B) \bmod 4$$

gibt $AB \equiv 1 + 2\{Q(A) + Q(B)\} \bmod 4$, w. z. b. w.

Ebenso folgt aus

$$A^2 \equiv 1 + 8Q'(A),\ B^2 \equiv 1 + 8Q'(B) \bmod 16,$$
$$\text{daß } A^2B^2 \equiv 1 + 8\{Q'(A) + Q'(B)\} \bmod 16$$

(sogar mod 64) ist. Daher gilt

$$\frac{A^2B^2-1}{8} \equiv \frac{A^2-1}{8} + \frac{B^2-1}{8} \bmod 2, \quad \text{w. z. b. w.}$$

Wir definieren nunmehr das Jacobi-Symbol als Verallgemeinerung des Legendre-Symbols. Haben wir für ein positives ungerades n die kanonische Zerlegung

$$n = \prod_{i=1}^{k} p_i^{a_i},$$

so definieren wir für zu n prime m das Symbol wie folgt

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{k} \left(\frac{m}{p_i}\right)^{a_i}.$$

Weiter werde für negatives ungerades n und zu n primes m einfach

$$\left(\frac{m}{-n}\right) = \left(\frac{m}{n}\right)$$

gesetzt.

Sofort folgt

Satz 2. *Ist m quadratischer Rest von n, wobei n ungerade ist, so ist* $\left(\frac{m}{n}\right) = 1$.

Satz 3. *Ist bei gleichen Bedingungen* $\left(\frac{m}{n}\right) = -1$, *so ist m quadratischer Nichtrest von n.*

Darüber hinaus darf nichts geschlossen werden. Beispielsweise ist 2 quadratischer Nichtrest von 9, obwohl $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = 1$ ist. Nun gilt das *verallgemeinerte Reziprozitätsgesetz*:

Satz 4. *Sind m, n ungerade, teilerfremd, und mindestens eine der Zahlen positiv, so ist*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Beweis:

I. Sei m und $n > 0$. Dann erhalten wir, wenn $m = \Pi p_i$, $n = \Pi q_j$ ist, wobei die p_i und q_j auch teilweise wiederholt vorkommen können, und jedes p_i von jedem q_j verschieden ist:

$$X = \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \Pi\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$$

und nach dem R.G. (von jetzt an Abkürzung für Reziprozitätsgesetz!)

$$X = (-1)^{\sum A_{ij}}$$

mit

$$\sum A_{ij} = \sum Q(p_i)\, Q(q_j) \equiv Q(m)\, Q(n) \equiv \frac{m-1}{2}\frac{n-1}{2} \bmod 2.$$

II. Sei eine der Zahlen m, n negativ. Ohne Einschränkung der Allgemeinheit sei $m > 0$. Dann ist $n < 0$. Mit $n' = -n = |n|$ gilt

$$\left(\frac{m}{n'}\right)\left(\frac{n'}{m}\right) = (-1)^{\frac{n'-1}{2}\frac{m-1}{2}}.$$

Es folgt

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \left(\frac{m}{n'}\right)\left(\frac{n'}{m}\right)\left(\frac{-1}{m}\right)$$
$$= (-1)^{\frac{n'-1}{2}\frac{m-1}{2}+\frac{m-1}{2}} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Hierbei wurde Gebrauch gemacht von dem folgenden

Satz 5 (verallgemeinerter erster Ergänzungssatz). *Für ungerades n ist*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{|n|-1}{2}}.$$

Beweis: Sei $n > 0$, $n = \Pi q_j$. Es ist

$$\left(\frac{-1}{n}\right) = (-1)^{\sum B_j}$$

mit $B_j = Q(q_j)$, also $\sum B_j \equiv Q(n) \bmod 2$.

Für $n < 0$ folgt nun auch der Satz aus $\left(\frac{-1}{n}\right) = \left(\frac{-1}{|n|}\right)$.

Satz 6 (verallgemeinerter zweiter Ergänzungssatz). *Für ungerades n ist*

$$\left(\frac{2}{n}\right) = (-1)^{Q'(n)}.$$

Beweis: Zunächst ist $Q'(-n) = Q'(n)$, es genügt also der Beweis für $n > 0$.
Mit der gleichen Annahme wird

$$\left(\frac{2}{n}\right) = (-1)^{\Sigma Q'(q_j)}$$

und

$$\Sigma Q'(q_j) \equiv Q'(n) \equiv \frac{n^2-1}{8} \bmod 2\,.$$

Ich bemerke ausdrücklich: Sind m, n beide negativ, so ist das Reziprozitätsgesetz unrichtig.

Beispiel: -3, -7 sind beide $\equiv 1 \bmod 4$, es ist

$$\left(\frac{-3}{-7}\right) = \left(\frac{4}{7}\right) = 1\,,$$

aber

$$\left(\frac{-7}{-3}\right) = \left(\frac{-1}{3}\right) = -1\,.$$

Nun können wir Satz 24 von § 12 erst richtig fassen:

Satz 7. *Gegeben sei eine ungerade Zahl N mit $\left(\frac{-m}{N}\right) = 1$ für $m = 5$, 13, 37. Ist $N \equiv 1$ mod 4 und N auf keine oder auf mehr als eine Art durch $x^2 + my^2$ eigentlich oder uneigentlich darstellbar, so ist N keine Primzahl. Ist genau eine, und zwar eigentliche Darstellung möglich, so ist N Primzahl. Genau dasselbe gilt für $2N$ statt N, wenn unter sonst gleichen Bedingungen $N \equiv 3$ mod 4 ist (selbstverständlich sei $N > 1$). Hier wie im Satz 8 ist $x > 0$, $y > 0$).*

Die Anwendung des R.G. gestattet eine etwas andere Fassung des Satzes. Ist $N \equiv 1 \bmod 4$, so ist

$$\left(\frac{-m}{N}\right) = \left(\frac{N}{-m}\right) = \left(\frac{N}{m}\right).$$

Ist aber $N \equiv 3 \bmod 4$, so ist

$$\left(\frac{-m}{N}\right) = -\left(\frac{N}{-m}\right) = -\left(\frac{N}{m}\right),$$

da jetzt $-m \equiv N \equiv 3 \bmod 4$ gilt. Wir erhalten den Satz in folgender Gestalt:

Satz 8. *Ist N quadratischer Rest mod $m = 5$, 13, 37, $N \equiv 1$ mod 4, so ist N genau dann Primzahl, wenn es auf genau eine Art durch $x^2 + my^2$ eigentlich darstellbar ist. Ist $N \equiv 3$ mod 4 quadratischer*

Nichtrest mod 5, 13, 37, *so ist* N *genau dann Primzahl, wenn* $2N$ *auf genau eine Art durch* $x^2 + my^2$ *eigentlich darstellbar ist.*

Es soll z. B. 481 untersucht werden. Es ist $481 \equiv 1 \bmod 4$, $\left(\frac{481}{5}\right) = 1$. Also fragen wir nach der Zahl der Darstellungen durch $x^2 + 5y^2$. Es muß $y \leqq \left[\sqrt{\frac{481}{5}}\right] = 9$ sein. Wir setzen $x^2 + 5y^2 = 481$ an. Als Kongruenz mod 3 wird dies $x^2 - y^2 \equiv 1 \bmod 3$. Da $x^2 \not\equiv 2 \bmod 3$ ist, so ist $y^2 \not\equiv 1 \bmod 3$ und $y \equiv 0 \bmod 3$. Es bleibt nur $y = 3, 6, 9$ zu versuchen, worauf $481 - 5y^2$ kein Quadrat wird. (Man könnte auch auf $y = 6$ verzichten, ebenso auf $y = 3, 9$, da $N = 481 \equiv 1 \bmod 8$ wird und $N - 5y^2$ nur für $y \equiv 0 \bmod 4$ ein Quadrat werden kann.) Es gibt keine Darstellung. N ist keine Primzahl. Es ist $N = 13 \cdot 37$.

§ 21. Das Kronecker-Symbol

In anderer Verallgemeinerung des Legendre-Symbols definieren wir nunmehr ein *Kronecker-Symbol* nur für im folgenden genau definierte (positive oder negative) Zähler d, die wir Diskriminanten nennen, und positive Nenner. Der Grund für die Bezeichnung folgt viel später.

Die Diskriminanten d können sein: 1. Zahlen $d \equiv 1 \bmod 4$, die quadratfrei und keine Quadrate sind. 2. Zahlen $-4d_1$, wobei d_1 unter die Zahlen der 1. Kategorie fällt oder Eins ist. 3. Zahlen $\pm 8d_1$; d_1 wie unter 2. Bei 2. 3. ist auch $d_1 = 1$ möglich.

Nun ist $\left(\frac{d}{p}\right)$ für jede Primzahl p definiert, auch für $d \equiv 0 \bmod p$ und $p = 2$. Wir setzen $\left(\frac{d}{p}\right) = 0$ für $d \equiv 0 \bmod p$, weiter für $d \equiv 1 \bmod 4$, $\left(\frac{d}{2}\right) = \left(\frac{2}{d}\right)$ (Jacobi-Symbol), also $\left(\frac{d}{2}\right) = 1$ für $d \equiv 1 \bmod 8$, $\left(\frac{d}{2}\right) = -1$ für $d \equiv 5 \bmod 8$. Für ungerade Primzahlen p hingegen fällt das Kronecker-Symbol mit dem Legendre-Symbol zusammen.

Wir setzen noch $\left(\frac{d}{1}\right) = 1$.

Ist nun $n = \Pi p_j$, wobei die Primzahlen p_j nicht voneinander verschieden zu sein brauchen, so ist

$$\left(\frac{d}{n}\right) = \Pi\left(\frac{d}{p_j}\right).$$

Immer dann, wenn das Kronecker-Symbol und das Jacobi-Symbol zugleich definiert sind, haben sie denselben Wert.

Als Beispiel nehmen wir $d = 21$ und $d = -40$ und berechnen $\left(\frac{d}{n}\right)$ für $1 \leqq n \leqq 10$.

Es wird $\left(\frac{21}{1}\right) = 1$, $\left(\frac{21}{2}\right) = -1$, weil $21 \equiv 5 \bmod 8$ ist, $\left(\frac{21}{3}\right) = 0$, $\left(\frac{21}{4}\right) = 1$, $\left(\frac{21}{5}\right) = 1$, $\left(\frac{21}{6}\right) = 0$, $\left(\frac{21}{7}\right) = 0$, $\left(\frac{21}{8}\right) = -1$, $\left(\frac{21}{9}\right) = 0$, $\left(\frac{21}{10}\right) = -1$.

Ebenso ist $\left(\frac{-40}{1}\right) = 1$, $\left(\frac{-40}{2}\right) = 0$, $\left(\frac{-40}{3}\right) = -1$, $\left(\frac{-40}{4}\right) = \left(\frac{-40}{5}\right) = \left(\frac{-40}{6}\right) = 0$, $\left(\frac{-40}{7}\right) = \left(\frac{2}{7}\right) = 1$, $\left(\frac{-40}{8}\right) = 0$, $\left(\frac{-40}{9}\right) = 1$, $\left(\frac{-40}{10}\right) = 0$.

Triviale Sätze über das Kronecker-Symbol sind

Satz 1. *Es ist* $\left(\frac{d}{n}\right) = 0$, *wenn* $(d, n) > 1$ *ist.*

Satz 2. *Es ist* $\left(\frac{d}{n^2}\right) = 1$, *wenn* $(d, n) = 1$. *Sonst* $\left(\frac{d}{n^2}\right) = 0$.

Satz 3. *Es ist* $\left(\frac{d}{a^2 b}\right) = \left(\frac{d}{b}\right)$, *wenn* $(d, a) = 1$ *ist.*

Bei Satz 3 darf die Bedingung $(d, a) = 1$ nicht wegfallen, sonst braucht der Satz nicht zu gelten: Es ist $\left(\frac{-40}{75}\right) = 0$, aber

$$\left(\frac{-40}{3}\right) = -1.$$

Satz 4. *Ist d ungerade, n gerade, so ist mit* $2^a \parallel n$, $n = 2^a n'$ *für gerades a die Beziehung* $\left(\frac{d}{n}\right) = \left(\frac{d}{n'}\right)$, *für ungerades a hingegen* $\left(\frac{d}{n}\right) = \left(\frac{2}{d}\right)\left(\frac{d}{n'}\right)$ *erfüllt.*

Satz 5. *Es ist* $\left(\frac{d}{mn}\right) = \left(\frac{d}{m}\right)\left(\frac{d}{n}\right)$.

Schon etwas schwerer ist der Nachweis des folgenden Satzes, bei dem die Diskriminante d das Produkt zweier Diskriminanten d_1, d_2 ist.

Satz 6. $\left(\frac{d}{n}\right) = \left(\frac{d_1}{n}\right)\left(\frac{d_2}{n}\right)$ *für* $d = d_1 d_2$.

Satz 6 ist für $(d, n) > 1$ klar.
Denn dann ist auch $\max\{(d_1, n), (d_2, n)\} > 1$, und es steht einfach „Null ist Null" da. — Sei jetzt $(d, n) = 1$. Der Satz ist auch klar, wenn n ungerade, zugleich $(d, n) = 1$ ist. Denn dann stehen Jacobi-Symbole da. Für $2^a \parallel n$ mit geradem a steht, wenn $n = 2^a n'$ gesetzt wird, einfach da: $\left(\frac{d}{n'}\right) = \left(\frac{d_1}{n'}\right)\left(\frac{d_2}{n'}\right)$, was wieder auf bekannte Formeln beim Jacobi-Symbol hinausläuft. Nur der Fall eines ungeraden a bietet einige Schwierigkeiten:

$$\left(\frac{d}{n}\right) = \left(\frac{2}{d}\right)\left(\frac{d}{n'}\right) = \left(\frac{2}{d_1}\right)\left(\frac{2}{d_2}\right)\left(\frac{d_1}{n'}\right)\left(\frac{d_2}{n'}\right)$$
$$= \left(\frac{2}{d_1}\right)^a \left(\frac{d_1}{n'}\right)\left(\frac{2}{d_2}\right)^a \left(\frac{d_2}{n'}\right) = \left(\frac{d_1}{n}\right)\left(\frac{d_2}{n}\right).$$

Bemerkt sei, daß das Produkt $d_1 d_2$ zweier teilerfremder Diskriminanten d_1, d_2 wieder eine Diskriminante ist. Umgekehrt läßt sich jede Diskriminante in das Produkt zweier Diskriminanten zerlegen mit Ausnahme von $-4, \pm 8, (-1)^{\frac{l-1}{2}} l$, wobei im letzten Fall l eine ungerade Primzahl ist.
Die beiden Teiler d_1, d_2 mit $d_1 d_2 = d$, wobei d, d_1, d_2 Diskriminanten sind, sind zueinander prim.
Beispiele für die Diskriminantenzerlegung:
$21 = (-3) \cdot (-7)$, $105 = (-7) \cdot (-15) = (-7) \cdot (-3) \cdot 5$, $-20 = (-4) \cdot 5$, $40 = (-8) \cdot 5$, $-168 = (-8) \cdot 21 = (-8) \cdot (-3) \cdot (-7)$.
Sehr wesentlich ist der folgende

Satz 7. *Das Kroneckersymbol* $\left(\frac{d}{n}\right)$ *hängt von der Restklasse von* n *mod* d *ab, oder aus* $n \equiv n' \bmod d$ *folgt* $\left(\frac{d}{n}\right) = \left(\frac{d}{n'}\right)$.

Beweis: Für $(d, n) > 1$ ist des Satz klar, denn dann steht „Null ist Null" da, weil auch $(d, n') = (d, n) > 1$ ist. Sei jetzt $(d, n) = 1$. Für ungerade d steht wegen des R.G. da: $\left(\frac{n}{d}\right) = \left(\frac{n'}{d}\right)$, was für

$n \equiv n' \bmod d$ gilt. Bei $d = -4, \pm 8$ folgt dasselbe aus den Ergänzungssätzen. Bei geradem d, $|d| > 8$ ist $d = \pm 2 d_2$ mit d_2 als ungerader Diskriminante. Der Satz folgt dann aus Satz 6.

Als sehr wichtig wird sich erweisen

Satz 8. *Sind d_1, d_2 zwei zueinander prime Diskriminanten, ($d = d_1 d_2$ ist dann von selbst eine Diskriminante), ist weiter $\varepsilon = 1$, wenn mindestens eine der Zahlen d_1, $d_2 > 0$ ist, hingegen $\varepsilon = -1$, wenn beide Zahlen d_1, d_2 negativ sind, so ist*

$$\left(\frac{d_1}{|d_2|}\right)\left(\frac{d_2}{|d_1|}\right) = \varepsilon\,.$$

Beweis: Wir können ohne Einschränkung der Allgemeinheit, da von den zueinander teilerfremden Diskriminanten nur eine gerade sein kann, d_2 als ungerade, also $d_2 \equiv 1 \bmod 4$ annehmen. Weiter sehen wir gleich, daß die Behauptung des Satzes mit der folgenden

$$\varepsilon = \left(\frac{\operatorname{sgn} d_1}{|d_2|}\right)$$

zusammenfällt.

Denn ist $d_1 > 0$, so ist $\varepsilon = 1$ entsprechend der Behauptung. Ist $d_1 < 0$, $d_2 > 0$, so ist

$$\varepsilon = \left(\frac{-1}{d_2}\right), \tag{1}$$

also nach dem ersten Ergänzungssatz $\varepsilon = +1$, da $d_2 \equiv 1 \bmod 4$. Gleichung (1) gilt auch für $d_1 < 0$, $d_2 < 0$; aber dann folgt $\varepsilon = -1$, da $|d_2| \equiv 3 \bmod 4$ wird (verallgemeinerter erster Ergänzungssatz).

Daher unterscheiden wir drei Fälle:

1. d_1 ungerade. Dann ist $\left(\frac{d_2}{|d_1|}\right)$ ein ganz gewöhnliches Jacobi-Symbol, also nach dem R.G. gleich $\left(\frac{|d_1|}{d_2}\right)$, da $d_2 \equiv 1 \bmod 4$, weiter $|d_1| > 0$ ist. Mithin bleibt

$$\varepsilon = \left(\frac{d_1}{|d_2|}\right)\left(\frac{|d_1|}{|d_2|}\right) = \left(\frac{\operatorname{sgn} d_1}{|d_2|}\right).$$

2. $d_1 = -4 d_1'$. Dann ist zunächst $\left(\frac{d_2}{|d_1|}\right) = \left(\frac{d_2}{|d_1'|}\right)$, letzteres ist wieder ein Jacobi-Symbol, also wie vorher $= \left(\frac{|d_1'|}{d_2}\right)$. Wir erhalten

$$\varepsilon = \left(\frac{d_1}{|d_2|}\right)\left(\frac{|d_1'|}{d_2}\right) = \left(\frac{-1}{|d_2|}\right)\left(\frac{d_1'}{|d_2|}\right)\left(\frac{|d_1'|}{|d_2|}\right)$$
$$= \left(\frac{-1}{|d_2|}\right)\left(\frac{\operatorname{sgn} d_1'}{|d_2|}\right) = \left(\frac{\operatorname{sgn} d_1}{|d_2|}\right).$$

3. $d_1 = \pm 8 d_1'$. Es wird

$$\left(\frac{d_1}{|d_2|}\right) = \left(\frac{\pm 2}{|d_2|}\right)\left(\frac{d_1'}{|d_2|}\right),$$
$$\left(\frac{d_2}{|d_1|}\right) = \left(\frac{2}{|d_2|}\right)\left(\frac{d_2}{|d_1'|}\right),$$

also

$$\left(\frac{d_1}{|d_2|}\right)\left(\frac{d_2}{|d_1|}\right) = \left(\frac{\pm 1}{|d_2|}\right)\left(\frac{\operatorname{sgn} d_1'}{|d_2|}\right) = \left(\frac{\operatorname{sgn} d_1}{|d_2|}\right).$$

Satz 9. *Es gilt für* $(d_1, d_2) = 1$, $d = d_1 d_2$ *die Beziehung* $(m, n > 0)$

$$\left(\frac{d}{m|d_1| + n|d_2|}\right) = \varepsilon \left(\frac{d_1}{n}\right)\left(\frac{d_2}{m}\right), \tag{2}$$

wobei ε *die Bedeutung des Satzes 8 hat.*

Beweis: Heißt A die linke Seite von (2), so ist nach Satz 6 und 7 mit $X = m|d_1| + n|d_2|$

$$A = \left(\frac{d_1}{X}\right)\left(\frac{d_2}{X}\right) = \left(\frac{d_1}{n|d_2|}\right)\left(\frac{d_2}{m|d_1|}\right)$$
$$= \left(\frac{d_1}{|d_2|}\right)\left(\frac{d_2}{|d_1|}\right)\left(\frac{d_1}{n}\right)\left(\frac{d_2}{m}\right) = \varepsilon \left(\frac{d_1}{n}\right)\left(\frac{d_2}{m}\right) \text{ w. z. b. w.}$$

Wir gehen nun zum Polynom $|d|$-ten Grades

$$F(x) = \sum_{j=1}^{|d|}\left(\frac{d}{j}\right) x^j \tag{3}$$

über.
Trivial ist

$$F(0) = 0.$$

Satz 10. $F(1) = 0$.

Beweis: Es ist etwa $Y = F(1) = \sum_{j=1}^{|d|}\left(\frac{d}{j}\right)$. Mit einem beliebigen k, welches $\left(\frac{d}{k}\right) = -1$ erfüllt, damit auch $(d, k) = 1$, wird

$$-Y = \sum_{j=1}^{|d|}\left(\frac{d}{jk}\right).$$

Da nach Satz 7 das Symbol $\left(\frac{d}{j}\right)$ nur von der Restklasse von j mod d abhängt, und wegen $(k, d) = 1$ mit j auch jk ein volles Restsystem mod d durchläuft, so ist die rechte Seite wieder Y. Es gilt $Y = -Y$, $Y = 0$.

Satz 11. *Sind F_1, F_2 die bei einer Zerlegung $d = d_1 d_2$ einer Diskriminante in das Produkt zweier auftretenden, F entsprechenden Funktionen, so ist für jede (nicht notwendig primitive) $|d|$-te Einheitswurzel $\alpha = e^{\frac{2\pi i j}{|d|}}$ die Beziehung*

$$F(\alpha) = \varepsilon F_1(\alpha^{|d_2|}) F_2(\alpha^{|d_1|}) \tag{4}$$

erfüllt. Dabei hat ε die Bedeutung von Satz 8.

Beweis: Zunächst gilt $(d_1, d_2) = 1$. Anders ist eine solche Zerlegung $d = d_1 d_2$ unmöglich, wenn beide Faktoren Diskriminanten sind.

Mit

$$1 \leqq m \leqq |d_2|, \; 1 \leqq n \leqq |d_1|,$$

erfüllt der Ausdruck $X = m|d_1| + n|d_2|$ genau einmal das volle Restsystem mod $d = d_1 d_2$. Denn erstens gibt $a|d_1| + b|d_2| \equiv a'|d_1| + b'|d_2| \bmod d$ durch Auffassung als Kongruenz mod d_2 sofort $a|d_1| \equiv a'|d_1| \bmod d_2$. Hieraus folgt wegen $(d_1, d_2) = 1$ die weitere Kongruenz $a \equiv a' \bmod d_2$, also $a = a'$, ebenso $b = b'$, und man erhält also jede Restklasse nur einmal.

Ferner gibt $m|d_1| + n|d_2| \equiv A \bmod d$ als Kongruenz mod d_2 eindeutig den Wert von m (zunächst mod d_2, dann aber eindeutig wegen $0 < m \leqq |d_2|$); ebenso erhält man den Wert von n eindeutig.

Mithin bleibt mit der Abkürzung $X = m|d_1| + n|d_2|$:

$$\begin{aligned} F(\alpha) &= \sum \left(\frac{d}{m|d_1| + n|d_2|}\right) \alpha^X \\ &= \varepsilon \sum_{n=1}^{|d_1|} \left(\frac{d_1}{n}\right) \alpha^{n|d_2|} \sum_{m=1}^{|d_2|} \left(\frac{d_2}{m}\right) \alpha^{m|d_1|} = \varepsilon F_1(\alpha^{|d_2|}) F_2(\alpha^{|d_1|}). \end{aligned}$$

Satz 12. *Ist $\alpha = \zeta^j$ mit $\zeta = e^{\frac{2\pi i}{|d|}}$ als $|d|$-ter Einheitswurzel, so ist*

$$F(\alpha) = \left(\frac{d}{j}\right) F(\zeta).$$

Beweis: Vorweggenommen ist der Fall $j = |d|$ durch Satz 10, da $\left(\frac{d}{|d|}\right) = 0$ ist.

I. Es sei $(j, d) > 1$, d ungerade. Dann kann mit $\pm (j, d) = d' \equiv 1 \bmod 4$, also mit d als Diskriminante, $d = d' d''$ gesetzt werden, wobei auch d'' Diskriminante ist. $(j, d) > 1$ gelte auch bei II, III. Wir erhalten

$$F(\alpha) = \sum_{k=1}^{|d''|} \left(\frac{d}{k}\right) \alpha^k + \sum_{k=|d''|+1}^{2|d''|} \left(\frac{d}{k}\right) \alpha^k + \sum_{k=2|d''|+1}^{3|d''|} \left(\frac{d}{k}\right) \alpha^k + \cdots + \sum_{k=(|d'|-1)|d''|+1}^{|d|} \left(\frac{d}{k}\right) \alpha^k,$$

oder

$$F(\alpha) = \sum_{k=1}^{|d''|} \alpha^k \sum_{t=0}^{|d'|-1} \left(\frac{d}{k + t|d''|}\right).$$

Nun wird aber

$$\left(\frac{d}{k + t|d''|}\right) = \left(\frac{d'}{k + t|d''|}\right)\left(\frac{d''}{k + t|d''|}\right) = \left(\frac{d''}{k}\right)\left(\frac{d'}{k + t|d''|}\right).$$

Damit erhält man die übersichtliche Formel

$$F(\alpha) = \sum_{k=1}^{|d''|} \left(\frac{d''}{k}\right) S_k \alpha^k,$$

wobei die innere Summe gleich

$$S_k = \left(\frac{d'}{k}\right) + \left(\frac{d'}{k + |d''|}\right) + \cdots + \left(\frac{d'}{k + (|d'| - 1)|d''|}\right),$$

d. h. der über ein volles Restsystem $u \bmod d'$ erstreckten Summe der $\left(\frac{d'}{u}\right)$ wird. Nach Satz 7 und 10 ist also $S_k = 0$, somit $F(\alpha) = 0 = \left(\frac{d}{j}\right) F(\zeta)$.

II. Für die Diskriminanten -4, 8, -8, kommt, da $\zeta^j = 1$ durch Satz10 erledigt ist, bei der ersten nur $j = 2$, $\zeta^2 = -1$, bei den beiden anderen nur $j = 2, 4, 6$, $\zeta^2 = i$, $\zeta^4 = -1$, $\zeta^6 = -i$ in Frage. Da F ein Polynom mit reellen Koeffizienten ist, braucht, wenn $F(i) = 0$ bewiesen ist, $F(-i)$ als dazu konjugiert, daher ebenfalls Null, nicht für sich gerechnet zu werden.

a) $d = -4, j = 2$ gibt

$$F(-1) = -\left\{\left(\frac{-4}{1}\right) + \left(\frac{-4}{3}\right)\right\} = -(1-1) = 0.$$

b) $d = +8, j = 2$ gibt $F(i) = i\left\{\left(\frac{2}{1}\right) - \left(\frac{2}{3}\right) + \left(\frac{2}{5}\right) - \left(\frac{2}{7}\right)\right\}$
$= i(1+1-1-1) = 0$. Weiter wird

$$F(-1) = -\left\{\left(\frac{2}{1}\right) + \left(\frac{2}{3}\right) + \left(\frac{2}{5}\right) + \left(\frac{2}{7}\right)\right\} = -(1-1-1+1) = 0.$$

c) $d = -8, j = 2$ gibt $F(i) = i\left\{\left(\frac{-2}{1}\right) - \left(\frac{-2}{3}\right) + \left(\frac{-2}{5}\right) - \left(\frac{-2}{7}\right)\right\}$
$= i\,(1-1-1+1) = 0.$

Auch $F(-1) = -\left\{\left(\frac{-2}{1}\right) + \left(\frac{-2}{3}\right) + \left(\frac{-2}{5}\right) + \left(\frac{-2}{7}\right)\right\}$
$= -(1+1-1-1) = 0.$

III. Ist $d = d_1 d_2$ mit $d_1 = -4, 8, -8$, hingegen d_2 ungerade, so hat j mit mindestens einer der Zahlen d_1 oder d_2 einen größten gemeinsamen Teiler >1. In (4) ist also mit $\zeta^{j|d_2|} = \alpha_1$, $\zeta^{j|d_1|} = \alpha_2$ mindestens eine der Zahlen α_s keine primitive $|d_s|$-te Einheitswurzel ($s = 1, 2$). Es folgt $F_s(\alpha_s) = 0$, $F(\zeta^j) = 0$.
Damit ist für $(j, d) > 1$ der Satz 12 bewiesen.

IV. Nun sei $(j, d) = 1$. Sofort erhalten wir aus der Gleichung

$$F(\zeta^j) = \sum_{k=1}^{|d|} \frac{d}{k} \zeta^{jk},$$

daß $$\left(\frac{d}{j}\right) F(\zeta^j) = \sum_{k=1}^{|d|} \left(\frac{d}{jk}\right) \zeta^{jk} = \sum_{t=1}^{|d|} \left(\frac{d}{t}\right) \zeta^t = F(\zeta)$$

wird, das letzte, weil mit k wegen $(j, d) = 1$ auch $k \cdot j$ ein volles Restsystem mod d durchläuft. Also ist

$$F(\zeta^j) = \left(\frac{d}{j}\right) F(\zeta)$$

in jedem Falle.

§ 22. Die Methode der Exkludenten

Ist $\left(\frac{m}{p}\right) = 1$, so erfordert die Lösung von $x^2 \equiv m \bmod p$ bei einigermaßen großem p, wenn keine Indextafel gegeben ist,

sehr viel Rechnung und dasselbe fordert auch etwa § 11, Satz 25. Schreiben wir die Kongruenz

$$x^2 = m + py, \tag{1}$$

so fallen bei Betrachtung von (1) mod q alle Werte y aus, die aus einem Wert $m + py$, der kein Quadrat sein kann, folgen. Wenn q Primzahl ist, nehmen wir also in die Tabelle alle quadratischen Nichtreste auf, bei einer Nichtprimzahl q können auch weitere Restklassen aufgenommen werden, z. B. bei $q = 9$ die Zahlen 3, 6.

Wir erhalten folgende Tabelle der Exkludenten:

$q = 3$: 2	$q = 8$: 2, 3, 5, 6, 7
$q = 4$: 2, 3	$q = 9$: 3, 6
$q = 5$: 2, 3	$q = 11$: 2, 6, 7, 8, 10
$q = 7$: 3, 5, 6	$q = 13$: 2, 5, 6, 7, 8, 11

Einige Beispiele

1. Aus einer Primzahltabelle ersehen wir, daß $p = 8737$ Primzahl ist. Es soll die Kongruenz $x^2 \equiv -1 \bmod p$ gelöst werden.
Es ist p als Summe zweier Quadrate darstellbar: $p = A^2 + B^2$. Sei B ungerade, also $B^2 \equiv 1 \bmod 8$. Da $p \equiv 1 \bmod 8$ ist, folgt $A^2 \equiv 0 \bmod 8$, $A \equiv 0 \bmod 4$.
Wegen $A \leqq [\sqrt{p}] = 93$ kommen für A die Werte 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92 in Frage.
Mit dem Exkludenten 3 bleibt $1 \equiv A^2 + B^2$, $B^2 \not\equiv 2$, also $A^2 \not\equiv \bmod 3$, was nichts liefert.

Der Exkludent 5 gibt $2 \equiv A^2 + B^2$, $B^2 \not\equiv 2$, 3 gibt $A^2 \not\equiv 0$, 4; also $A \not\equiv 0$, 2, 3 mod 5. Es fallen 8, 12, 20, 28, 32, 40, 48, 52, 60, 68, 72, 80, 92 aus.

Geblieben sind nur 4, 16, 24, 36, 44, 56, 64, 76, 84.

Der Exkludent 7 gibt $1 \equiv A^2 + B^2$; $B^2 \not\equiv 3$, 5, 6 hat $A^2 \not\equiv 5$, 3, 2 zur Folge. Davon liefert nur $A^2 \not\equiv 2 \bmod 7$ etwas, da 3 und 5 quadratische Nichtreste mod 7 sind. Es fällt aus: $A \equiv 3$, 4 mod 7, also $A = 4$, 24.
Nun sind nur noch 16, 36, 44, 56, 64, 76, 84 als mögliche Werte von A da.
Der Exkludent 11 gibt $3 \equiv A^2 + B^2$. $B^2 \not\equiv 2$, 6, 7, 8, 10 mod 11 gibt $A^2 \not\equiv 1$, 8, 7, 6, 4 mod 11, davon sind nur die Zahlen 1, 4 quadratische Reste mod 11, es fallen die Werte $A \equiv 1$, 2, 9, 10 mod 11 aus, also die Zahlen 56, 64, 76. Somit hat sich die Menge der zu untersuchenden Zahlen A auf 16, 36, 44, 84 reduziert. Von ihnen liefert nur $A = 84$ einen rationalen Wert von B, nämlich $B = 41$.
Also ist $p = 84^2 + 41^2$.
Es löst

$$x \equiv \frac{41}{84} \equiv -\frac{8696}{84} \equiv -\frac{2174}{21} \equiv -\frac{10911}{21} \equiv -\frac{3637}{7} \equiv -520 + \frac{3}{7}$$

die Kongruenz $x^2+1 \equiv 0 \bmod p$. Wegen $p = 7 \cdot 1248 + 1$ wird weiter

$$-\frac{3}{7} \equiv \frac{3744}{-1} \equiv -3744.$$

Es ist also $x \equiv -4264$ Kongruenzwurzel. Die zweite Wurzel der Kongruenz ist $x \equiv 4264$.

2. $x^2 \equiv 41 \bmod 83$.

Nach dem R.G. ist $\left(\frac{41}{83}\right) = \left(\frac{83}{41}\right) = \left(\frac{1}{41}\right) = 1$.

Mit $x^2 = 41 + 83y$ kann man erstens x im Intervall (0,83), zweitens als ungerade, also $x^2 \equiv 1 \bmod 8$ annehmen. Auch y ist in diesem Intervall, es folgt $8 \mid y$.

Der Exkludent 3 liefert $x^2 \equiv 2 - y$. Wegen $x^2 \not\equiv -1 \bmod 3$ folgt $y \not\equiv 0 \bmod 3$. Es bleiben nur die Restklassen von 8, 16 mod 24.

Der Exkludent 5 gibt $2,3 \not\equiv 1 + 3y$, $1,2 \not\equiv 3y$, $y \not\equiv 2,4 \bmod 5$. Es bleiben nur als mögliche Zahlen $y = 8, 16, 40, 56, 80$.

Der Exkludent 7 hat zur Folge:

$3, 5, 6 \not\equiv -1 - y \bmod 7$, $y \not\equiv -4, -6, -7 \bmod 7$, $y \not\equiv 0, 1, 3 \bmod 7$.

Es bleibt nur $y = 16, 40$.
Mit $y = 16$ bleibt $x^2 = 1369 = 37^2$. Die zu lösende Kongruenz hat also die Wurzel $x \equiv 37$ und die zweite Wurzel $x \equiv -37 \equiv 46$.

§ 23. Der biquadratische Restcharakter von 2

Wir brauchen nur Primzahlen $p \equiv 1 \bmod 8$ zu betrachten. Bei Primzahlen $p \equiv 3, 5 \bmod 8$ ist 2 quadratischer Nichtrest, damit auch biquadratischer Nichtrest, bei Primzahlen $p \equiv 7 \bmod 8$ ist 2 quadratischer Rest, damit auch biquadratischer Rest, da nach einem Primzahlmodul $p \equiv 3 \bmod 4$ quadratischer und biquadratischer Rest zusammenfällt. Im folgenden sei somit $p \equiv 1 \bmod 8$.

Satz 1. *Gibt es eine Darstellung $p = x^2 + y^2$ mit $8 \mid y$, so ist 2 biquadratischer Rest mod p; bei $y \equiv 4 \bmod 8$ ist dagegen 2 biquadratischer Nichtrest.*

Satz 2. *Ist in $p = m^2 + 8n^2$ sowohl $p \equiv 9 \bmod 16$ als auch n ungerade oder sowohl $p \equiv 1 \bmod 16$ als auch n gerade, so ist 2*

biquadratischer Rest mod p. Ist hingegen $p \equiv 9 \mod 16$ und n gerade, oder $p \equiv 1 \mod 16$ und n ungerade, so ist 2 biquadratischer Nichtrest.

Die Sätze wollen wir auf einmal beweisen. Es sei

$$p = x^2 + y^2 = r^2 + 2s^2 \text{ mit } 4 \mid y,\ 2 \mid s.$$

Dann ist zunächst

$$\left(\frac{p}{r}\right) = \left(\frac{2}{r}\right), \qquad \text{d. h.} \qquad \left(\frac{r}{p}\right) = \left(\frac{2}{r}\right),$$

das letzte nach dem R.G. Weiter wollen wir annehmen $2^n \parallel s$, $s = 2^n s'$, es wird $\left(\frac{p}{s'}\right) = 1$, also nach dem R.G. $\left(\frac{s'}{p}\right) = 1$, auch $\left(\frac{s}{p}\right) = 1$. Aus der Voraussetzung folgt, daß $t \equiv \frac{r}{s}$ eine Lösung von $t^2 \equiv -2 \mod p$ ist; es ist also auch $\left(\frac{t}{p}\right) = \left(\frac{2}{r}\right)$. Sofort folgt

$$\left(\frac{t}{p}\right) = 1 \text{ für } r \equiv \pm 1 \mod 8. \tag{1}$$

$$\left(\frac{t}{p}\right) = -1 \text{ für } r \equiv \pm 3 \mod 8. \tag{2}$$

Gilt (1), so ist -2 und wegen des Satzes 9, § 12 auch $+2$ biquadratischer Rest; bei (2) sind hingegen -2 und $+2$ biquadratische Nichtreste.

Gilt (1), so ist $r^2 \equiv 1 \mod 16$, d. h. für $p \equiv 9 \mod 16$ folgt dann $2 \parallel s$, also $s = 2n$ mit ungeradem n, bei $p \equiv 1 \mod 16$ ist dagegen $4 \mid s$, also $s = 2n$ mit geradem n. Gilt (2), so ist hingegen $r^2 \equiv 9 \mod 16$; für $p \equiv 9 \mod 16$ ist dann $4 \mid s$, für $p \equiv 1 \mod 16$ aber $2 \parallel s$. Damit ist Satz 2 in allen Teilen bewiesen.

Nun ist

$$x^2 - 2s^2 = (r + y)(r - y).$$

Aus der Gleichung ersieht man unmittelbar, daß 2 quadratischer Rest der beiden Faktoren rechts ist. Sofort folgt

$$\left(\frac{2}{r+y}\right) = \left(\frac{2}{r-y}\right) = 1,$$

also $r + y$ und $r - y$ sind beide von der Form $8X \pm 1$.

Ist dann $r \equiv \pm 1 \bmod 8$, so $y \equiv 0 \bmod 8$, wenn aber $r \equiv \pm 3 \bmod 8$ ist, so ist $y \equiv 4 \bmod 8$. Es bleibt

$$\left(\frac{t}{p}\right) = (-1)^{\frac{y}{4}}.$$

Damit ist auch Satz 1 in allen Teilen bewiesen.

Den Beweis verdanke ich Herrn A. Aigner (Graz).

§ 24. Einiges über kubische Kongruenzen

Gegeben sei eine Kongruenz

$$f(x) = x^3 + ax^2 + bx + c \equiv 0 \bmod p.$$

Wir wollen p als Primzahl > 3 annehmen. Genau dann, wenn $f(x)$ in P_p eine Wurzel hat, ist $f(x)$ in $\mathsf{P}_p[x]$ reduzibel. Es können dann entweder alle Wurzeln in P_p liegen, dann zerfällt $f(x)$ in das Produkt dreier Linearfaktoren, oder es liegt genau eine Wurzel in P_p, dann zerfällt $f(x)$ in das Produkt eines linearen und eines quadratischen Faktors.

Da $p > 3$ angenommen wurde, so können wir durch die Substitution $x = y - \frac{a}{3}$ das quadratische Glied wegschaffen und erhalten eine Kongruenz

$$f_1(y) \equiv y^3 + Ay + B \equiv 0 \bmod p.$$

Wegen $p > 3$ können wir die Cardanische Formel (die in den Körpern der Charakteristik 2 und 3 nicht gilt) anwenden, und sehen, daß sich die Diskriminante der kubischen Gleichung nach derselben Formel wie bei einer Gleichung in P_0 oder im Körper der komplexen Zahlen mit

$$d = -4A^3 - 27B^2$$

berechnet.

Es möge $d \not\equiv 0$ in $\mathsf{P}p$ sein, so daß die drei Wurzeln voneinander also verschieden sind.

1. Die Gleichung sei irreduzibel. Dann liegen die drei Wurzeln, die wir nach § 15, Formel (10) mit

$$\alpha,\ \alpha^p,\ \alpha^{p^2}$$

ansetzen, in $GF(p^3)$. Das Differenzprodukt

$$\delta(\alpha) = (\alpha - \alpha^p)\,(\alpha^p - \alpha^{p^2})\,(\alpha^{p^2} - \alpha)$$

bleibt beim Automorphismus (α/α^p) unverändert, liegt also in P_p. Es ist $\delta^2(\alpha) = d$ in P_p oder $\left(\frac{d}{p}\right) = 1$.

2. Die Gleichung habe drei Wurzeln in P_p, etwa U, V, W. Es wird

$$d = \{(U-V)\,(V-W)\,(W-U)\}^2$$

und trivialerweise $\left(\frac{d}{p}\right) = 1$.

3. Die Gleichung habe genau eine Wurzel U in P_p. Es ist $f(x) = (x-U)\,f_1(x)$, wobei $f_1(x)$ ein in P_p irreduzibles quadratisches Polynom ist. Die Wurzeln β, γ von $f_1(x)$ liegen dann im Galoisfeld $GF(p^2)$.

Es ist $(U-\beta)\,(U-\gamma) = f_1(U)$ Element von P_p, doch $\beta - \gamma$ liegt nicht in P_p, wohl aber $(\beta-\gamma)^2 \cdot d$ ist also kein Quadrat eines Elements von P_p, auf die Kongruenz übertragen, heißt dies: d ist quadratischer Nichtrest von p, es ist $\left(\frac{d}{p}\right) = -1$.

Wir haben den folgenden *Satz von Skolem*:

Satz 1. *Eine Kongruenz*

$$f(x) = x^3 + ax^2 + bx + c \equiv 0 \bmod p$$

nach einem Primzahlmodul $p > 3$ hat, wenn d die Diskriminante von $f(x)$ und $\left(\frac{d}{p}\right) = -1$ ist, genau eine Wurzel. Ist $\left(\frac{d}{p}\right) = 1$, so hat sie entweder drei oder keine Wurzel.

Durch die Voraussetzungsformulierung fällt der ausgeschlossene Fall $d \equiv 0 \bmod p$ von selbst aus.

Beispiele

1. $x^3 + 4x - 5 \equiv 0 \bmod 11$ hat die Diskriminante

$$d = -256 - 675 \equiv -3 - 4 \equiv -7 \equiv 4 \bmod 11,$$

es ist $\left(\frac{4}{11}\right)=1$. Da die Kongruenz offenbar die Wurzel $x_1 \equiv 1$ hat, muß sie drei Wurzeln haben. Es ergibt sich $x_2 \equiv 2$, $x_3 \equiv -3$.

2. Gegeben $f(x) = x^3 - x - 2 \equiv 0 \bmod 7$. Es ist

$$d = 4 - 108 \equiv -104 \equiv 1 \bmod 7,$$

also $\left(\frac{d}{7}\right)=1$. Die Kongruenz $f(x) \equiv 0$ hat also entweder keine oder drei Wurzeln. Da $x \equiv 0, \pm 1$ offenbar sofort ausscheidet, ist mit $f(2) \equiv 4$, $f(3) \equiv 1$ gezeigt, daß keine Wurzel vorhanden ist, da nur zwei nicht untersuchte Restklassen übrig bleiben.

3. Wir untersuchen $g(x) = x^3 - x - 3 \equiv 0 \bmod 7$. Es ist $g(x) = f(x) - 1$, wobei $f(x)$ dem vorigen Beispiel entnommen ist. Sofort ersieht man $g(3) \equiv 0$. Hier wird $d = 4 - 243 = -239 \equiv -1 \bmod 7$, also $\left(\frac{d}{7}\right) = -1$. Daher ist $x \equiv 3$ die einzige Wurzel.

4. $x^3 - 1 \equiv 0 \bmod p$ hat die Diskriminante -27. Wir ersehen, daß die Kongruenz für $\left(\frac{-3}{p}\right)=1$ drei Wurzeln, für $\left(\frac{-3}{p}\right)=-1$ eine Wurzel hat. Da aus bekannten Sätzen folgt, daß das erste für $p \equiv 1 \bmod 3$, das zweite für $p \equiv -1 \bmod 3$ gilt, so haben wir: -3 ist Rest aller Primzahlen $6X+1$, Nichtrest aller Primzahlen $6X-1$. Dies bestätigt sich durch das $R.G.$ $\left(\frac{-3}{p}\right)=\left(\frac{p}{-3}\right)=\left(\frac{p}{3}\right)$, weil $p>0$, $-3 \equiv 1 \bmod 4$ ist.

Man beachte wohl, daß die Diskriminante in diesem Paragraphen nichts mit der Diskriminante in § 21 zu tun hat.

C. THEORIE DER ALGEBRAISCHEN KÖRPER

§ 25. Begriff der ganzen algebraischen Zahl

Definition. *Ein Polynom in x heißt normiert, wenn sein höchster Koeffizient, d. h. der Koeffizient der höchsten Potenz gleich Eins ist.*

Definition. *Die Wurzeln eines in P irreduziblen normierten Polynoms mit ganzen rationalen Koeffizienten*

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

heißen ganze algebraische Zahlen.

Man kann nun entweder nach der Methode der modernen Algebra zu P, dem Zahlkörper der rationalen Zahlen, der auch der Primkörper der Charakteristik Null ist, eine Wurzel α des Polynoms $f(x)$ symbolisch adjungieren. Oder man kann nach dem sog. Fundamentalsatz der Algebra unter α eine wirkliche reelle oder komplexe Zahl verstehen, die Wurzel von $f(x)$ ist. In der Zahlentheorie ist der letzte Weg unausweichlich, denn mit der bloßen symbolischen Adjunktion kommt man hier nicht sehr weit.

Es sei also $\alpha^{(1)} = \alpha$ eine Wurzel von $f(x) = 0$. Dann sind etwa $\alpha^{(2)}, \ldots, \alpha^{(n)}$ die anderen Wurzeln. Man kann den abstrakten Körper $k = \mathsf{P}(\alpha)$ durch die n Körper $\mathsf{P}(\alpha^{(1)}), \ldots, \mathsf{P}(\alpha^{(n)})$ wirklich im Bereiche des Körpers aller komplexen Zahlen darstellen. n sei im weitern stets der Körpergrad. Ein solcher Körper heißt *Zahlkörper*.

Nun können verschiedene Verhältnisse eintreten, es können die Körper $\mathsf{P}(\alpha^{(j)})$ ganz oder teilweise zusammenfallen. Wenn alle Körper $\mathsf{P}(\alpha^{(j)})$ zusammenfallen, so spricht man von einem Galoischen Körper. Die dafür häufig gebrauchte Bezeichnung „normaler Körper" wollen wir lieber vermeiden, da sie neuerdings auch in einem anderen Sinn verwendet wird. Ein Beispiel für einen Galoischen Körper ist der quadratische Zahlkörper $k = \mathsf{P}(\sqrt{m})$. Hier ist $\sqrt{m}$ die Quadratwurzel aus einer quadratfreien rationalen Zahl. Die Zahlen des Zahlkörpers sind von der

Form $\gamma^{(1)} = a + b\sqrt{m}$ mit ganz rationalem a, b. Die Zahl $\gamma^{(2)} = a - b\sqrt{m}$ liegt ebenfalls im Körper, ist aber für $b \neq 0$ von $\gamma^{(1)}$ verschieden. Ist $b = 0$, so kann die $\gamma = a$ nicht zur Definition des Körpers dienen. Denn für $\mathsf{P}(a) = \mathsf{P}$ kämen wir nicht über den Körper der rationalen Zahlen hinaus.

Es sei α eine erzeugende Zahl des Körpers $k = \mathsf{P}(\alpha)$. Dann kann es unter Umständen in k auch nicht rationale Zahlen β geben, so daß $k_1 = \mathsf{P}(\beta)$ noch nicht k ist, sondern $\mathsf{P} < k_1 < k$ gilt. α heißt hingegen erzeugendes oder primitives Element von k über P.

Wir unterscheiden unter den n Körpern $\mathsf{P}(a^{(j)})$ etwa r_1 reelle und r_2 Paare konjugiertkomplexer Körper, so daß $r_1 + 2r_2 = n$ ist. Wir definieren hier gleich die wichtige Zahl r. Es sei $r = r_1 + r_2 - 1$. Im reellquadratischen Körper, also bei positivem m in $\mathsf{P}(\sqrt{m})$ ist dann $r_1 = 2$, $r_2 = 0$, $r = 1$, hingegen wird im imaginärquadratischen Körper $(m < 0)$ $r_1 = 0$, $r_2 = 1$, $r = 0$.

Eine ganze algebraische Zahl ist natürlich auch Wurzel anderer normierter rationalzahliger Polynome als des irreduziblen normierten, von dem sie Wurzel ist. So ist z. B. $\alpha = \frac{1+\sqrt{5}}{2}$ eine ganze algebraische Zahl, Wurzel des normierten irreduziblen ganzzahligen Polynoms $f(x) = x^2 - x - 1$, aber auch Wurzel des normierten rationalzahligen nicht ganzzahligen Polynoms

$$g(x) = x^3 - \frac{x^2}{2} - \frac{3x}{2} - \frac{1}{2} = f(x)\left(x + \frac{1}{2}\right).$$

Damit eine algebraische Zahl ganz ist, genügt es, wie wir bald sehen werden, daß sie Wurzel eines normierten ganzzahligen Polynoms ist; das Polynom braucht nicht irreduzibel zu sein. Um darüber ins klare zu kommen, brauchen wir einen Satz über den Inhalt von Polynomen:

Satz 1. *Es seien* $f(x) = \Sigma a_j x^j$ *und* $g(x) = \Sigma b_k x^k$ *ganzzahlige Polynome (nur endlich viele* a_j *und* b_k *verschieden von Null); ferner mögen die größten gemeinsamen Teiler* $(a_0, a_1, a_2, \ldots) = I(f)$ *bzw.* $(b_0, b_1, b_2, \ldots) = I(g)$ *die Inhalte von* f *bzw.* g *heißen. Dann gilt*

$$I(fg) = I(f)\, I(g),$$

mit anderen Worten: Der Inhalt des Produktes zweier ganzzahliger Polynome ist gleich dem Produkt der Inhalte.

Beweis: Sei $fg = h$, dann ist $h(x) = \sum c_l x^l$ mit

$$c_l = \sum_{j+k=l} a_j b_k .$$

Wir gehen von einer rationalen Primzahl p aus, für die $p^A \parallel I(f)$, $^B \parallel I(g)$ gilt. Wir nehmen an, es seien $a_0, \ldots, a_{s-1}$ durch p^{A+1} teilbar, hingegen gelte $p^A \parallel a_s$. Ebenso seien $b_0, \ldots, b_{t-1}$ durch p^{B+1} teilbar, dagegen sei $p^B \parallel b_t$.

Jedenfalls gilt $p^{A+B} \mid c_l$ für jedes l.

Wir brauchen den Koeffizienten c_{s+t}. Man erhält

$$c_{s+t} = a_s b_t + a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \cdots + a_{s+t} b_0 + a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \cdots + a_0 b_{s+t} .$$

Ein Ausdruck $a_{s+j} b_{t-j}$ ist durch p^{A+B+1} teilbar, da a_{s+j} durch p^A, b_{t-j} durch p^{B+1} teilbar ist. Ebenso zeigen wir, daß $a_{s-j} b_{t+j}$ durch p^{A+B+1} teilbar ist; mithin gilt wegen $p^{A+B} \parallel a_s\, b_t$

$$p^{A+B} \parallel I(fg), \quad \text{w. z. b. w.}$$

Satz 2. *Zerfällt ein ganzzahliges Polynom $h(x)$ in das Produkt zweier rationalzahliger Polynome $f(x)$, $g(x)$, dann auch in das Produkt zweier ganzzahliger Polynome $F(x)$, $G(x)$.*

Beweis: Wir können $I(h) = 1$ annehmen. Denn gilt der Satz in diesem Falle, dann auch nach Multiplikation von h mit einer ganzen rationalen Zahl.

Es seien M und N bzw. die Inhalte der Zählerpolynome, wenn die gemeinsamen Nenner P, Q hergestellt werden. Es wird also

$$f(x) = \frac{M r(x)}{P}, \qquad g(x) = \frac{N r(x)}{Q}$$

mit $r(x)$, $s(x)$ als ganzzahligen Polynomen des Inhaltes eins. Wir können von vornherein P, Q als natürliche Zahlen annehmen. Dasselbe gilt von M, N der Definition nach. Die sich ergebende Gleichung

$$\frac{M r(x)}{P} \cdot \frac{N s(x)}{Q} = h(x)$$

multiplizieren wir mit PQ, und erhalten

$$MN r(x)\, s(x) = h(x)\, PQ.$$

Gleichsetzen der Inhalte gibt

$$MN = PQ,$$

daher

$$r(x)\, s(x) = h(x), \quad \text{w. z. b. w.}$$

Fast unmittelbar folgt

Satz 3. *Zerfällt ein normiertes ganzzahliges Polynom in das Produkt normierter rationalzahliger Faktoren, so sind diese ganzzahlig.*

Beweis: Da das Polynom normiert ist, hat es den Inhalt Eins. Es muß, da es zerfällt, in das Produkt zweier ganzzahliger Faktoren zerfallen; diese können normiert genommen werden. Zerfällt es in mehr als zwei Faktoren, so wenden wir auf einen der bisherigen zwei Faktoren denselben Schluß an.
Es folgt

Satz 4. *Die normierten irreduziblen Faktoren eines ganzzahligen normierten Polynoms sind ganzzahlig.*

Nun sind wir am Ziele:

Satz 5. *Ist die algebraische Zahl α Wurzel eines normierten ganzzahligen Polynoms, so ist sie ganz.*

Beweis: α ist dann Wurzel eines der normierten irreduziblen Faktoren, die ganzzahlig sind.

Beispielsweise ist $\cos\frac{2\pi}{35} + i \sin\frac{2\pi}{35}$ eine ganze algebraische Zahl als Wurzel des normierten, ganzzahligen Polynoms $x^{35} - 1$, obwohl dieses Polynom reduzibel ist.

Wir übernehmen einen Satz aus der klassischen Algebra. Ist $f(x) = (x - x_1) \ldots (x - x_n)$ ein Polynom, also $x_1, \ldots, x_n$ seine Wurzeln, so ist $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$. Dabei sind die Koeffizienten

$$\begin{aligned}
a_1 &= -(x_1 + x_2 + \cdots + x_n),\\
a_2 &= x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n,\\
a_3 &= -(x_1x_2x_3 + \cdots + x_1x_2x_n + x_1x_3x_4 + \cdots + x_{n-2}x_{n-1}x_n),\\
&\cdots\\
a_n &= (-1)^n x_1x_2 \ldots x_n
\end{aligned}$$

die elementarsymmetrischen Funktionen der Wurzeln, und es gilt

Satz 6. *Jedes symmetrische ganzzahlige Polynom $S(x_1, \ldots, x_n)$ der Wurzeln läßt sich als ganzzahliges Polynom der elementarsymmetrischen Funktionen darstellen.*

Nunmehr sei α Wurzel des normierten ganzzahligen, irreduziblen Polynoms $f(x)$, etwa $\alpha = \alpha^{(1)}$, die Zahlen $\alpha^{(2)}, \ldots, \alpha^{(n)}$ heißen die *konjugierten* von α. Ein symmetrisches Polynom

$$S(\alpha^{(1)}, \ldots, \alpha^{(n)})$$

mit ganzzahligen Koeffizienten ist also eine ganze rationale Zahl. Wir erhalten nun sehr schnell folgende Sätze:

Satz 7. *Das Produkt einer ganzen algebraischen Zahl mit einer ganzen rationalen Zahl ist ganz algebraisch.*

Beweis: α genüge $f(x) = 0$, $A\alpha$ genügt $f\left(\frac{x}{A}\right) = 0$, d.h. mit $f(x) = a_0 + a_1 x + \cdots + x^n$ genügt die Zahl $A\alpha$ der Gleichung

$$a_0 A^n + a_1 A^{n-1} x + \cdots + x^n = 0.$$

Satz 8. *Summe, Differenz und Produkt zweier ganzer algebraischer Zahlen sind ganz algebraisch.*

Beweis: Zunächst kann nach Satz 7 der Fall der Differenz unter den der Summe einbegriffen werden.

Seien die $\alpha^{(i)}$ zu $\alpha = \alpha^{(1)}$, die $\beta^{(j)}$ zu $\beta = \beta^{(1)}$ konjugiert. Das normierte Polynom

$$P(x) = \prod_{i,j} (x - \alpha^{(i)} - \beta^{(j)})$$

hat zum Koeffizienten von $(-1)^t x^t$ Summen der Art

$$\sum \prod \alpha^{(i)^{e_i}} \prod \beta^{(j)^{g_j}}.$$

Greifen wir ein $U = \prod \alpha^{(i)^{e_i}}$ heraus, dann ist der Koeffizient ein symmetrisches ganzzahliges Polynom in den $\beta^{(j)}$, also eine ganze rationale Zahl; da Analoges für U gilt, sind alle Koeffizienten von $P(x)$ ganz rational. Damit ist $\alpha + \beta$ als ganz algebraisch nachgewiesen.

In derselben Art ergibt sich durch Betrachtung des Polynoms

$$Q(x) = \prod_{i,j} (x - \alpha^{(i)} \beta^{(j)}),$$

daß $\alpha\beta$ ganz algebraisch ist.

Noch darüber hinausgehend ist

Satz 9. *Ist α Wurzel eines normierten Polynoms*

$$f(x) = \beta + \gamma x + \cdots + \varkappa x^{N-1} + x^N,$$

dessen Koeffizienten ganze algebraische Zahlen sind, so ist α ganz algebraisch.

Beweis: Wir bezeichnen die konjugierten Zahlen zu $\beta, \gamma, \ldots, \varkappa$ der Reihe nach wie folgt:

$$\begin{aligned}
&\beta^{(1)} = \beta = \lambda^{(1)}, \ \beta^{(2)} = \lambda^{(2)}, \ \ldots, \ \beta^{(b_1)} = \lambda^{(b)}.\\
&\gamma^{(1)} = \gamma = \lambda^{(b+1)}, \ \ldots, \ \gamma^{(b_2)} = \lambda^{(c)},\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\varkappa^{(1)} = \varkappa = \lambda^{(s+1)}, \ \ldots, \ \varkappa^{(b_t)} = \lambda^{(u)}.
\end{aligned}$$

(Es möge das normierte irreduzible ganzzahlige Polynom mit der Wurzel β vom Grade b_1, dasjenige mit der Wurzel γ vom Grade $b_2, \ldots,$ schließlich dasjenige mit der Wurzel $\varkappa$ vom Grade b_t sein. Weiter sollen die Abkürzungen gelten: $b_1 = b$, $b_1 + b_2 = c$, $\ldots$, $b_1 + b_2 + \cdots + b_t = u$).

Dann ist α Wurzel des normierten ganzzahligen Polynoms $R(x)$, nämlich des über alle $u!$ Permutationen erstreckten Produkts

$$R(x) = \prod_{i_1, i_2, \ldots, i_u} (\lambda^{(i_1)} + \lambda^{(i_2)} x + \cdots + \lambda^{(i_n)} x^{n-1} + x^n).$$

Nun noch ein sehr einfacher, aber äußerst wichtiger Satz:

Satz 10. *Ist eine ganze algebraische Zahl rational, so ist sie ganz rational.*

Beweis: $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ mit ganzen rationalen a_j habe eine rationale Wurzel c, also $f(x)$ den Faktor $x - c$. Nach Satz 3 muß $x - c$ ein ganzzahliges Polynom, also c eine ganze Zahl sein.

Satz 8 kann auch so ausgesprochen werden:

Satz 11. *Die ganzen algebraischen Zahlen bilden einen Ring, genauer einen Integritätsbereich.*

Beweis: Aus $\alpha\beta = 0$ (α, β ganz algebraisch) folgt $\alpha = 0$ oder $\beta = 0$. Der nach Satz 8 von den ganzen algebraischen Zahlen gebildete Ring ist daher ein Integritätsbereich.

Beispiele

1. Soll untersucht werden, ob

$$\alpha = \frac{-1+\sqrt{5}}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4}$$

ganz algebraisch ist, so bilden wir die Gleichung mit den Wurzeln $\alpha, \bar{\alpha}$, wobei $\bar{\alpha}$ die konjugiertkomplexe Zahl zu α ist. Fast augenblicklich folgt

$$\alpha + \bar{\alpha} = \frac{-1+\sqrt{5}}{2}.$$

Leicht berechnet man auch $\alpha\bar{\alpha} = \frac{6-2\sqrt{5}}{16} + \frac{10+2\sqrt{5}}{16} = 1$.

Mithin erfüllt α die Gleichung

$$x^2 + \frac{1-\sqrt{5}}{2}x + 1 = 0$$

mit ganzen algebraischen Zahlen als Koeffizienten. Die Gleichung in $\mathsf{P}[x]$, der α genügt, findet sich als

$$f(x) = \left(x^2 + \frac{x}{2} + 1\right)^2 - \left(\frac{\sqrt{5}x}{2}\right)^2$$

oder ausgeführt

$$x^4 + x^3 + x^2 + x + 1 = 0.$$

Mithin genügt α auch der reduziblen Gleichung $x^5 - 1 = 0$, es ist α eine primitive fünfte Einheitswurzel. Werden die Quadratwurzeln als positiv angenommen, so ist $\alpha = \cos 72° + i \sin 72°$.

2. Wir untersuchen, ob

$$\beta = \frac{\sqrt{6}+\sqrt{2}}{2}$$

algebraisch ganz ist. Wir bilden die Gleichung mit den Wurzeln β und $\beta_1 = \frac{\sqrt{6}-\sqrt{2}}{2}$. Es wird $\beta + \beta_1 = \sqrt{6}$, $\beta\beta_1 = 1$. Mithin genügt β der Gleichung

$$x^2 - x\sqrt{6} + 1 = 0$$

mit ganzen algebraischen Zahlen als Koeffizienten. β und β_1 sind also ganz algebraisch.

3. Gegeben $\gamma = \frac{1+\sqrt{3}}{2}$. γ und $\gamma_1 = \frac{1-\sqrt{3}}{2}$ sind Wurzeln des normierten rationalzahligen nicht ganzzahligen irreduziblen Polynoms $f(x) = x^2 - x - \frac{1}{2}$. Es ist somit γ nicht ganz.

Nochmals sei darauf hingewiesen: Ist ein ganzzahliges normiertes Polynom $f(x)$ oder auch nur ein normiertes Polynom $f(x)$ mit ganzen algebraischen Zahlen als Koeffizienten gefunden, dessen Wurzel eine Zahl ϑ ist, so ist ϑ ganz algebraisch. Ist hingegen das normierte Polynom nicht ganzzahlig, so darf daraus nicht ohne weiteres geschlossen werden, daß ϑ nicht ganz algebraisch ist, es muß hierzu erst nachgewiesen werden, daß das Polynom irreduzibel ist.

Beispiele zum Selbstrechnen

Man untersuche, ob folgende Zahlen ganz algebraisch sind:

1. $\dfrac{\sqrt{6}+\sqrt{-2}}{2}$.
2. $\dfrac{\sqrt{3}+\sqrt{5}}{2}$.
3. $\dfrac{1+\sqrt{-7}}{2}$.
4. $\dfrac{1+\sqrt{-13}}{2}$.

§ 26. Lineare Unabhängigkeit

Ist ϑ, das wir im folgenden als ganz voraussetzen wollen, erzeugendes Element von k über P, was gewöhnlich abgekürzt k/P geschrieben wird, also $k = \mathsf{P}(\vartheta)$, so sind die Zahlen des algebraischen Zahlkörpers gegeben durch

$$\alpha = a_1 + a_2\vartheta + \cdots + a_n\vartheta^{n-1}. \tag{1}$$

Hierbei ist $f(\vartheta) = 0$, $f(x)$ irreduzibel vom Grade n, die a_j rational.

Höhere Potenzen von ϑ sind nicht notwendig, denn, da $f(\vartheta) = 0$ ist, kann ϑ^n durch die niedrigeren Potenzen von ϑ ausgedrückt werden, ebenso ϑ^{n+1} usw.

Satz 1. *Die durch* (1) *gegebene Darstellung einer Zahl ist eindeutig.*

Beweis: Würde außer (1) auch $\alpha = b_1 + \cdots + b_n\vartheta^{n-1}$ gelten, so folgte $(a_1 - b_1) + \cdots + (a_n - b_n)\vartheta^{n-1} = 0$. Hätte nun das Polynom $g(x) = (a_1 - b_1) + \cdots + (a_n - b_n)x^{n-1}$ einen Grad $\geqq 0$, so müßte es, da $g(x)$ mit dem irreduziblen Polynom $f(x)$ eine Wurzel gemein hat, durch $f(x)$ teilbar sein. Dies ist aber unmöglich, denn der Grad ist kleiner als der Grad n von $f(x)$. Dieser

Widerspruch kann nur dadurch behoben werden, daß $g(x)$ überhaupt keinen Grad hat, somit das Nullpolynom und

$$a_1 = b_1, \ldots, a_n = b_n$$

ist.

Satz 2. *Sind in* (1) *die* a_j *ganz (rational), so ist* α *ganz algebraisch.*

Beweis: Er folgt aus Satz 9 in § 25.

Es braucht aber (1) noch nicht alle ganzen algebraischen Zahlen des Körpers zu liefern, z. B. liegt in $k = \mathsf{P}(\sqrt{5})$ die Zahl $\frac{1+\sqrt{5}}{2}$, die mit $\vartheta = \sqrt{5}$ nicht unter die Gestalt (1) mit ganzen a_j fällt.

Es ist $(1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1})$ eine Basis des Körpers k über P, da alle Zahlen des Körpers durch (1) gegeben werden.

Wir wollen in diesem Buche sagen „Basis aller Körperzahlen", da der Ausdruck Körperbasis einem spezielleren Begriff in der Zahlentheorie vorbehalten ist, zu dem wir im nächsten Paragraphen kommen.

Definition I. *t Zahlen des Körpers* $\gamma_1, \ldots, \gamma_t$ *heißen linear unabhängig, wenn eine Relation*

$$c_1\gamma_1 + \cdots + c_t\gamma_t = 0 \tag{2}$$

mit rationalen c_j *nur beim Verschwinden sämtlicher* c_j *möglich ist.*

Gleichwertig ist

Definition II. *t Zahlen eines Körpers* $\gamma_1, \ldots, \gamma_t$ *heißen linear unabhängig, wenn eine Relation*

$$C_1\gamma_1 + \cdots + C_t\gamma_t = 0 \tag{3}$$

mit ganzen rationalen C_j *nur bei Verschwinden aller* C_j *möglich ist.*

Die Erfüllung der Bedingung der Definition I hat offenbar die der Bedingung von II zur Folge. Aber auch das Umgekehrte gilt. Denn ist die Bedingung von II erfüllt, eine Beziehung (2) gegeben, und $c_j = \frac{C_j}{B}$, wobei die C_j und $B > 0$ ganzzahlig sind, so folgt (3), daher sind alle $C_j = 0$ und auch alle $c_j = 0$.

Satz 3. *Es gibt n linear unabhängige Größen im Körper k.*

Beweis: Nach Satz 1 sind z. B. die Größen $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$ linear unabhängig.

Sind $\gamma_1, \ldots, \gamma_t$ nicht linear unabhängig, so heißen sie linear abhängig.

Satz 4. *$(n+1)$ Körperzahlen $\gamma_1, \ldots, \gamma_{n+1}$ sind stets linear abhängig.*

Beweis: Es sei

$$\gamma_j = \sum_{k=1}^{n} c_{kj} \vartheta^{k-1}.$$

Wir wollen die Existenz von Größen x_j mit $\sum_{j=1}^{n+1} \gamma_j x_j = 0$ nachweisen, wobei die x_j rational sind und nicht sämtlich verschwinden. Der Ansatz gibt

$$\sum_{j,k} x_j c_{kj} \vartheta^{k-1} = 0,$$

also wegen der Irreduzibilität von $f(x)$

$$\sum_{j} x_j c_{kj} = 0$$

für $k = 1, 2, 3, \ldots, n$. Ausführlich geschrieben wird dies

$$\begin{aligned} c_{11} x_1 + \cdots + c_{1,n+1} x_{n+1} &= 0, \\ &\cdots \\ c_{n1} x_1 + \cdots + c_{n,n+1} x_{n+1} &= 0. \end{aligned}$$

Das sind n homogene lineare Gleichungen mit den $(n+1)$ Unbekannten $x_1, \ldots, x_{n+1}$ und Koeffizienten aus P. Da mehr Unbekannte als Gleichungen gegeben sind, gibt es nichttriviale Lösungen $[x_1, \ldots, x_{n+1}]$ in P.
Ein weiterer trivialer Satz:

Satz 5. *Ist unter den γ_j die Null, so sind $\gamma_1, \ldots, \gamma_t$ stets linear abhängig.*

Beweis: Die Annahme $\gamma_1 = 0$ verletzt nicht die Allgemeinheit. Mit $C_1 = 1$, $C_2 = \cdots = C_t = 0$ ist $\sum_j C_j \cdot \gamma_j = 0$.
Die quadrierte Determinante

$$\Delta(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \alpha_1^{(2)} & \ldots & \alpha_n^{(2)} \\ \vdots & \cdots & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{vmatrix}^2$$

heißt *Diskriminante der n Zahlen* $\alpha_1, \ldots, \alpha_n$. Sind $k^{(1)}, \ldots, k^{(n)}$ die n konjugierten Körper, so ist $\alpha^{(1)}$ die abstrakte Zahl α, ver-

wirklicht im Körper $k^{(1)}; \ldots; \alpha^{(n)}$ ebenso die Zahl α, verwirklicht im letzten Körper $k^{(n)}$. Die Quadratwurzel aus Δ, also den Ausdruck für Δ ohne den Exponenten 2 der Determinante bezeichnen wir mit Q (nur im folgenden).

Satz 6. *Sind $\gamma_1, \ldots, \gamma_n$ linear abhängig, so verschwindet ihre Diskriminante.*

Beweis: Gilt $x_1\gamma_1 + \cdots + x_n\gamma_n = 0$ mit rationalen, nicht durchweg verschwindenden x_i, so gibt die Verwirklichung dieser Beziehung in den n Körpern

$$x_1\gamma_1^{(1)} + \cdots + x_n\gamma_n^{(1)} = 0,$$

$$x_1\gamma_1^{(n)} + \cdots + x_n\gamma_n^{(n)} = 0.$$

Wir haben n homogene lineare Gleichungen in $x_1, \ldots, x_n$. Aber diese Größen sind nicht alle Null. Daher verschwindet die Determinante des Systems, es ist $Q = 0$, also $\Delta(\gamma_1, \ldots, \gamma_n) = Q^2 = 0$.

Definition. *Unter der Spur $S(\alpha)$ einer Zahl verstehen wir die Summe der Konjugierten*: $S(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)} = \sum_{i=1}^{n} \alpha^{(i)}$. *Die Spur ist daher eine rationale Zahl. Ist α ganz, so ist die Spur ganz rational.*

Satz 7. *Sind die Zahlen x, y beliebig rational, so ist $S(x\alpha + y\beta) = xS(\alpha) + yS(\beta)$.*

Beweis: Es wird

$$S(x\alpha + y\beta) = \sum_{i=1}^{n} \{x\alpha^{(i)} + y\beta^{(i)}\}$$

$$= x\sum_{i=1}^{n} \alpha^{(i)} + y\sum_{i=1}^{n} \beta^{(i)} = xS(\alpha) + yS(\beta).$$

Insbesondere ist der Spezialfall wichtig:

Satz 8. $S(\alpha + \beta) = S(\alpha) + S(\beta)$.

Nun beweisen wir

Satz 9. *Die Diskriminante $\Delta(\alpha_1, \ldots, \alpha_n)$ ist eine rationale Zahl. Sind $\alpha_1, \ldots, \alpha_n$ ganz, so ist sie eine ganze rationale Zahl.*

Beweis: Mit dem Vektor $\alpha_j = [\alpha_j^{(1)}, \ldots, \alpha_j^{(n)}]$ läßt sich

$$Q = \begin{vmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{vmatrix} = |\alpha_1, \alpha_2, \ldots, \alpha_n|$$

schreiben. Es wird

$$\alpha_j \alpha_k = \sum_{i=1}^{n} \alpha_j^{(i)} \alpha_k^{(i)} = S(\alpha_j \alpha_k).$$

Nach dem Multiplikationssatz der Determinanten ist

$$\Delta(\alpha_1, \ldots, \alpha_n) = Q^2 = \begin{vmatrix} \alpha_1^2 & \ldots & \alpha_1 \alpha_n \\ \cdot & & \cdot \\ \alpha_n \alpha_1 & \ldots & \alpha_n^2 \end{vmatrix} = \begin{vmatrix} S(\alpha_1^2) & \ldots & S(\alpha_1 \alpha_n) \\ & & \\ S(\alpha_n \alpha_1) & \ldots & S(\alpha_n^2) \end{vmatrix},$$

also eine, nebenbei bemerkt, symmetrische Determinante mit rationalen Elementen. Damit ist $\Delta(\alpha_1, \ldots, \alpha_n)$ als rational erwiesen. Sind alle α_j ganz, so alle $\alpha_j \alpha_k$; es werden alle Spuren $S(\alpha_j \cdot \alpha_k)$ ganz rational, die Diskriminante ist eine ganze rationale Zahl.

Definition. *Die Diskriminante* $\triangle(1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1})$, *wobei* ϑ *eine Zahl von* k *ist, heißt Diskriminante von* ϑ *und werde kurz mit* $\Delta(\vartheta)$ *bezeichnet.*

Sofort folgt

Satz 10. *Die Diskriminante einer erzeugenden Körperzahl* ϑ *ist eine rationale von Null verschiedene Zahl. Ist* ϑ *ganz, so ist* $\Delta(\vartheta)$ *ganz rational von einem Absolutbetrag* $\geqq 1$.

Bemerkung: Wir werden bald den Satz dahin verschärfen, daß der Absolutbetrag der Diskriminante einer erzeugenden ganzen Körperzahl ϑ die Beziehung $|\Delta(\vartheta)| > 1$ erfüllt.

Satz 11. *n Körperzahlen*

$$\gamma_j = \sum_{i=1}^{n} c_{ij} \vartheta^{i-1} \quad (j = 1, \ldots, n)$$

mit rationalem c_{ij} *sind genau dann linear unabhängig, wenn die Determinante* $|c_{ij}| \neq 0$ *ist.*

Beweis:

I. Ist $\sum_{j=1}^{n} x_j \gamma_j = 0$ erfüllt mit rationalen nicht durchweg verschwindenden x_j, so folgt sofort

$$\sum_{i,j} c_{ij} x_j \vartheta^{i-1} = 0 .$$

Wegen der Irreduzibilität der erzeugenden Gleichung n-ten Grades für ϑ haben wir also $\sum_{j=1}^{n} c_{ij} \cdot x_j = 0$; das sind n homogene Gleichungen für die nicht durchweg verschwindenden Größen x_j. Demnach ist die Determinante $|c_{ij}| = 0$.

II. Aus $|c_{ij}| = 0$ (Determinante Null), folgt sofort, daß das Gleichungssystem

$$\sum_{j=1}^{n} c_{ij} x_j = 0$$

$(1 \leqq i \leqq n)$ nichttriviale rationale ganzzahlige Lösungen hat. Es bleibt

$$\sum_{j=1}^{n} \gamma_j x_j = 0 ,$$

womit Satz 11 völlig bewiesen ist.

Wir betrachten nun weiter die Diskriminante

$$\Delta(\vartheta) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \vartheta^{(1)} & \vartheta^{(2)} & \dots & \vartheta^{(n)} \\ \vartheta^{(1)^2} & \vartheta^{(2)^2} & \dots & \vartheta^{(n)^2} \\ . & . & \dots & . \\ \vartheta^{(1)^{n-1}} & \vartheta^{(2)^{n-1}} & \dots & \vartheta^{(n)^{n-1}} \end{vmatrix}^2 .$$

Nach einem bekannten Determinantensatz ist daher

$$\Delta(\vartheta) = \prod_{u>v} (\vartheta^{(u)} - \vartheta^{(v)})^2 ,$$

also genau dann von Null verschieden, wenn ϑ eine erzeugende Körperzahl ist.

Um über das Vorzeichen von $\Delta(\vartheta)$ etwas zu ermitteln, ordnen wir die n Körper, wie folgt, an: Wir nennen $k^{(1)}, \dots, k^{(n)}$ die *konjugierten Körper* Zuerst sollen die r_1 reellen Körper kommen

$$k^{(1)}, \dots, k^{(r_1)},$$

sodann nehmen wir von jedem der konjugiert komplexen Paare einen Körper

$$k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}.$$

Nun folgen die restlichen Körper, und zwar so, daß für

$$r_1 < j \leqq r_1 + r_2$$

stets

$$k^{(r_2+j)} = \overline{k^{(j)}}$$

folgt, wobei der Strich den Übergang zum Konjugiertkomplexen bedeutet.

Nun bestimmen wir das Vorzeichen von $\Delta(\vartheta)$. Dies hängt offenbar nur davon ab, wieviel Paare konjugiertkomplexer eigentlich komplexer Zahlen unter den $\vartheta^{(j)}$ vorkommen, wobei von der speziellen Bedeutung der $\vartheta^{(j)}$ als konjugierter Zahlen zu ϑ abgesehen wird. Natürlich sind die $\vartheta^{(j)}$ als paarweise verschieden anzunehmen. Wir benennen um: es seien $\xi_1, \ldots, \xi_{r_1}$ die reellen, dagegen $\eta_1, \bar{\eta}_1, \ldots, \eta_{r_2} = \tau, \bar{\eta}_{r_2} = \bar{\tau}$ die konjugierten Paare unter den $\vartheta^{(j)}$.

Wir behaupten: $\operatorname{sgn} \Delta(\vartheta) = (-1)^{r_2}$.

Für $r_2 = 0$ ist der Satz selbstverständlich, da $\Delta(\vartheta)$ das Quadrat einer reellen Zahl $\neq 0$ ist. Er sei für $r_2 - 1$ bewiesen; es komme $\tau, \bar{\tau}$ hinzu. Die Diskriminante der $r_1 + 2r_2 - 2$ Größen

$$\xi_1, \ldots, \bar{\eta}_{r_2-1}$$

bezeichnen wir mit $\Delta_1(\vartheta)$. Nach der Induktionsvoraussetzung ist $\operatorname{sgn} \Delta_1(\vartheta) = (-1)^{r_2-1}$.

Weder die Quadrate der Produkte

$$(\xi_j - \tau)(\xi_j - \bar{\tau})$$

noch die der Produkte

$$(\eta_j - \tau)(\eta_j - \bar{\tau})(\bar{\eta}_j - \tau)(\bar{\eta}_j - \bar{\tau})$$

ändern das Vorzeichen. (Die Produkte selbst sind schon > 0). Aber $\tau - \bar{\tau}$ ist rein imaginär, $(\tau - \bar{\tau})^2 < 0$ und

$$\operatorname{sgn} \Delta(\vartheta) = -\operatorname{sgn} \Delta_1(\vartheta) = (-1)^{r_2}.$$

Somit ergibt sich

Satz 12. *Das Vorzeichen von $\Delta(\vartheta)$, wobei ϑ eine erzeugende Körperzahl ist, ist $(-1)^{r_2}$.*

Die beim Beweis verwendete Körperanordnung wollen wir kurz Anordnung (A) nennen und oft verwenden. Wir behalten uns

allerdings das Recht vor, von ihr, wenn es zweckmäßig ist, abzuweichen.

Satz 13. *Sind (wie bei Satz 11) n Körperzahlen*

$$\gamma_j = \sum_{i=1}^{n} c_{ij} \vartheta^{i-1} \quad (j = 1, \ldots, n)$$

mit der Matrix $\mathfrak{C} = (c_{ij})$ *gegeben, so ist*

$$\Delta(\gamma_1, \ldots, \gamma_n) = |\mathfrak{C}|^2 \Delta(\vartheta).$$

Beweis: Wir bezeichnen mit $\{\gamma_j^{(t)}\}$ den Spaltenvektor mit dem Element $\gamma_j^{(t)}$ in der j-ten Zeile. Bezeichnet $\mathfrak{g}_t$ den Spaltenvektor der Zahlen $1, \vartheta^{(t)}, \ldots, \vartheta^{(t)n-1}$, so wird $\{\gamma_j^{(t)}\} = \mathfrak{C}\mathfrak{g}_t$. Die Matrix der Determinante, die die Quadratwurzel aus der Determinante $\Delta(\gamma_1, \ldots, \gamma_n)$ ist, wird

$$(\mathfrak{C}\mathfrak{g}_1, \ldots, \mathfrak{C}\mathfrak{g}_n) = \mathfrak{C}(\mathfrak{g}_1, \ldots, \mathfrak{g}_n).$$

Sofort folgt

$$\Delta(\gamma_1, \ldots, \gamma_n) = |\mathfrak{C}|^2 |\mathfrak{g}_1, \ldots, \mathfrak{g}_n|^2.$$

Es ist aber $|\mathfrak{g}_1, \ldots, \mathfrak{g}_n|^2 = \Delta(\vartheta)$.

Satz 14. (Verschärfung von Satz 6). *Notwendig und hinreichend für die lineare Abhängigkeit von* $\gamma_1, \ldots, \gamma_n$ *ist das Verschwinden der Diskriminante* $\Delta(\gamma_1, \ldots, \gamma_n)$.

Beweis: Satz 6 sagt aus, daß das Verschwinden notwendig ist. Nach Satz 13 folgt bei Verschwinden der Diskriminante, daß $|\mathfrak{C}| = 0$ ist, daraus nach Satz 11 die lineare Abhängigkeit.

Satz 15. *Für linear unabhängige* $\gamma_1, \ldots, \gamma_n$ *ist* $\operatorname{sgn} \Delta(\gamma_1, \ldots, \gamma_n) = (-1)^{r_2}$.

Beweis: Er folgt aus Satz 12 und 13.

Durch das Vorzeichen der Diskriminante von ϑ, das nach Satz 15 mit dem aller Diskriminanten linear unabhängiger Zahlen zusammenfällt, wird also bei kleinen Werten von n die Größe r_2 bestimmt:

Ist $n = 2$, also der Körper quadratisch, $\Delta(\vartheta) > 0$, so ist $r_2 = 0$, da dann r_2 gerade ist und nicht 2 sein kann; es muß $r_1 = 2$ sein, der Körper ist reellquadratisch. Ist bei sonst gleichen Umständen $\Delta(\vartheta)$ negativ, so ist $r_2 = 1$, $r_1 = 0$, die konjugierten Körper sind konjugiertkomplex im Sinne der Analysis.

Ist $n = 3$, $\Delta(\vartheta) > 0$, so ist wieder $r_2 = 0$, $r_1 = 3$; alle drei Körper sind reell. Ist jetzt $\Delta(\vartheta)$ negativ, so ist $r_1 = 1$, $r_2 = 1$, und es ist ein Körper reell, zwei Körper sind konjugiertkomplex.

Bei $n = 4$, $\Delta(\vartheta) < 0$ folgt $r_2 = 1$, $r_1 = 2$. Wir haben zwei reelle Körper und ein konjugiertkomplexes Körperpaar. Hingegen kann bei positiver Diskriminante keine eindeutige Entscheidung getroffen werden, es kann $r_2 = 0$, $r_1 = 4$ oder aber $r_2 = 2$, $r_1 = 0$ sein.

§ 27. Die Hauptgleichung

Es sei $k = \mathsf{P}(\vartheta)$, ϑ eine erzeugende Körperzahl, α eine andere nicht notwendig erzeugende Zahl des Körpers. ϑ ist Wurzel des Polynoms $f(x)$, das irreduzibel und vom Grade n sei. Es möge mit rationalem a_{1j}

$$\alpha = a_{11} + a_{12}\vartheta + \cdots + a_{1n}\vartheta^{n-1} \tag{1; 1}$$

sein, wir finden

$$\alpha\vartheta = a_{21} + a_{22}\vartheta + \cdots + a_{2n}\vartheta^{n-1}, \tag{1; 2}$$

$$\cdots$$

$$\alpha\vartheta^{n-1} = a_{n1} + a_{n2}\vartheta + \cdots + a_{nn}\vartheta^{n-1}. \tag{1; n}$$

Wir bezeichnen mit $\mathfrak{A}$ die Matrix (a_{ij}). Dann kann das Gleichungssystem (1; 1), (1; 2), . . . , (1; n) kurz als

$$(\mathfrak{A} - \alpha\,\mathfrak{E})\,\mathfrak{g} = \mathfrak{o} \tag{2}$$

geschrieben werden. Dabei ist $\mathfrak{E}$ die Einheitsmatrix, $\mathfrak{o}$ der Nullvektor, endlich

$$\mathfrak{g} = \begin{pmatrix} 1 \\ \vartheta \\ \vdots \\ \vartheta^{n-1} \end{pmatrix}.$$

Da (2) für den vom Nullvektor verschiedenen Vektor $\mathfrak{g}$ ein homogenes System von n Gleichungen mit n Unbekannten darstellt, so muß die Determinante Null sein. Wir wollen die mit $(-1)^n$

multiplizierte Null sein lassen, also schreiben

$$(-1)^n \,|\mathfrak{A} - \alpha\,\mathfrak{E}| = 0, \tag{3}$$

oder ausführlich geschrieben

$$(-1)^n \begin{vmatrix} a_{11}-\alpha & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\alpha & \dots & a_{2n} \\ \cdot & \cdot & \dots & \\ a_{n1} & a_{n2} & \dots & a_{nn}-\alpha \end{vmatrix} = 0. \tag{4}$$

(3) *bzw.* (4) *gibt die Hauptgleichung für* α. Die Lehrbücher der Determinantenrechnung geben einfache Regeln, die die Berechnung der linken Seite $g(\alpha)$ von (3) und (4) wenigstens für kleine Werte von n ermöglichen. Wird somit

$$g(x) = (-1)^n \,|\mathfrak{A} - x\,\mathfrak{E}|$$

gesetzt, so ist z. B. bei $n = 3$

$$g(x) = x^3 - x^2\,S(\mathfrak{A}) + x\,C(\mathfrak{A}) - |\mathfrak{A}|. \tag{5}$$

Hierbei ist $S(\mathfrak{A})$ die sog. Spur der Matrix, die Summe der Hauptdiagonalglieder. $C(\mathfrak{A})$ ist die Summe der zweireihigen Hauptdiagonalunterdeterminanten. In (3) und (4) ist der Vorfaktor beigesetzt, damit $g(x)$ normiert sei.
Es gilt nun über die Hauptgleichung der wichtige

Satz 1. *Die linke Seite der Hauptgleichung ist entweder irreduzibel oder reine Potenz eines normierten irreduziblen Polynoms.*

Beweis: Ist $g(x)$ nicht irreduzibel, so sei $h(x)$ ein normierter irreduzibler Faktor. Die Gleichung (1; 1) werde kurz $\alpha = T(\vartheta)$ geschrieben.
Wir betrachten speziell den Wert $\alpha = \alpha^{(1)}$. Dies ist keine Einschränkung der Allgemeinheit, die Anordnung (A) wollen wir ausdrücklich hier nicht machen. Es ist also $\alpha^{(1)} = T(\vartheta^{(1)})$, $h(x)$ sei der normierte irreduzible Faktor, von dem $\alpha^{(1)}$ Wurzel ist. Es kann $h(x)$ mehr als einmal in $g(x)$ aufgehen, sei $h^q(x) \parallel g(x)$, also $g(x) = h^q(x)\,u(x)$, wobei $u(x)$ nicht mehr durch $h(x)$ teilbar ist. Wir nehmen an, der Grad von $u(x)$ sei positiv. Dann muß etwa ein $\alpha^{(j)} \neq \alpha^{(1)}$ Wurzel von $u(x)$ sein. Wir setzen $u\{T(x)\} = U(x)$. Die Gleichung $u(\alpha^{(j)}) = 0$ hat $U(\vartheta^{(j)}) = 0$ zur Folge, also hat U mit dem irreduziblen Polynom f eine Wurzel gemein, also alle, es ist $U(\vartheta^{(1)}) = 0$, d. h. $u(\alpha^{(1)}) = 0$. Es hat $u(x)$ mit

dem irreduziblen Polynom $h(x)$ eine Wurzel gemein, damit alle. Es wäre also doch $u(x)$ durch $h(x)$ teilbar. Dieser Widerspruch kann nur dadurch behoben werden, daß $u(x)$ den Grad Null hat, also eine Konstante ist, die Eins sein muß, weil $g(x)$, $h(x)$ normiert sind.

Auf jeden Fall ist $\mathsf{P}(\alpha) \leqq \mathsf{P}(\vartheta) = k$.

Ist nun $g(x)$ irreduzibel, so ist $\mathsf{P}(\alpha)$ ebenfalls vom Grade n, also $k = \mathsf{P}(\alpha)$, α ein erzeugendes Element.

Ist $g(x)$ reduzibel, und zwar

$$g(x) = h^q(x),$$

so gilt: Der Grad von h möge t sein, es folgt $n = qt$, also $n \equiv 0 \bmod q$. Als irreduzibles Polynom hat h keine mehrfachen Wurzeln, seine t Wurzeln sind paarweise verschiedene konjugierte Zahlen, etwa

$$\alpha^{(1)}, \alpha^{(q+1)}, \ldots, \alpha^{((t-1)q+1)}.$$

Es ist $\alpha^{(1)}$ eine q-fache Wurzel von g, durch eventuelle Umnumerierung ergibt sich

$$\alpha^{(1)} = \alpha^{(2)} = \cdots = \alpha^{(q)},$$

$$\alpha^{(q+1)} = \alpha^{(q+2)} = \cdots = \alpha^{(2q)},$$

$$\cdots$$

$$\alpha^{((t-1)q+1)} = \alpha^{((q-1)t+2)} = \cdots = \alpha^{(tq)}.$$

Wir haben

Satz 2. *Ist α einfache Wurzel der Hauptgleichung, so ist α erzeugende Körperzahl, $k = \mathsf{P}(\alpha)$. Ist α eine q-fache Wurzel der Hauptgleichung, so ist der Körpergrad n ein Vielfaches von q, $n = qt$, und $k' = \mathsf{P}(\alpha)$ ist vom Grade t bezüglich P, also ein echter (mit k nicht zusammenfallender) Teilkörper zwischen P und k, wobei k ausgeschlossen ist. Es fallen dann in k je q Konjugierte von α zusammen.*

Beispiel für die Hauptgleichung: Man sieht leicht, daß

$$f(x) = x^3 - x^2 - 2x - 8$$

irreduzibel ist, also durch $f(\vartheta) = 0$ ein kubischer Körper $k = \mathsf{P}(\vartheta)$ definiert wird. Wir setzen $\alpha = \frac{\vartheta^2 - \vartheta}{2}$. Man hat sofort die Rechenregel $\vartheta^3 = \vartheta^2 + 2\vartheta + 8$, daher

$$\alpha\vartheta = \tfrac{1}{2}(\vartheta^2 + 2\vartheta + 8 - \vartheta^2) = \vartheta + 4, \; \alpha\vartheta^2 = \vartheta^2 + 4\vartheta.$$

Diese drei Gleichungen geben geordnet

$$-\alpha - \tfrac{1}{2}\vartheta + \tfrac{1}{2}\vartheta^2 = 0,$$
$$4 + \vartheta(1-\alpha) = 0,$$
$$4\vartheta + \vartheta^2(1-\alpha) = 0.$$

Nun ergibt sich sofort die Hauptgleichung

$$-\begin{vmatrix} -\alpha & -\frac{1}{2} & \frac{1}{2} \\ 4 & 1-\alpha & 0 \\ 0 & 4 & 1-\alpha \end{vmatrix} = 0.$$

Die Matrix $\mathfrak{A}$, auf die es bei Formel (5) ankommt, ist daher

$$\mathfrak{A} = \begin{pmatrix} 0 & -\frac{1}{2} & \frac{1}{2} \\ 4 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix}.$$

Man hat sofort mit den dortigen Bezeichnungen

$$S(\mathfrak{A}) = 2,\ C(\mathfrak{A}) = \begin{vmatrix} 0 & -\frac{1}{2} \\ 4 & 1 \end{vmatrix} + \begin{vmatrix} 0 & \frac{1}{2} \\ 0 & 1 \end{vmatrix} + \begin{vmatrix} 1 & 0 \\ 4 & 1 \end{vmatrix} = 2 + 1 = 3,$$

$$|\mathfrak{A}| = -4\begin{vmatrix} -\frac{1}{2} & \frac{1}{2} \\ 4 & 1 \end{vmatrix} = 10.$$

Wir erhalten

$$g(\alpha) = \alpha^3 - 2\alpha^2 + 3\alpha - 10 = 0.$$

Wir sehen, α ist eine ganze algebraische Zahl.
Bei der Hauptgleichung haben wir

$$g(x) = \prod_{i=1}^{n}(x - \alpha^{(i)}),$$

also

$$g(x) = x^n - x^{n-1}\sum_{i=1}^{n}\alpha^{(i)} + \cdots + (-1)^n \alpha^{(1)}\alpha^{(2)}\ldots\alpha^{(n)}.$$

Sofort folgt $S(\alpha) = S(\mathfrak{A})$ oder

Satz 3. *Die Spur der bei der Hauptgleichung auftretenden Matrix ist gleich der Spur der Zahl.*

Weiter wird

$$|\mathfrak{A}| = \alpha^{(1)}\ldots\alpha^{(n)} = \prod_{j=1}^{n}\alpha^{(j)}.$$

Diese Zahl heißt *Norm* von α, sie ist rational. Wir schreiben sie $N(\alpha)$ oder auch symbolisch α^{N}. Letztere Schreibweise rechtfertigt sich durch den folgenden sehr schnell abzuleitenden

Satz 4. *Die Norm eines Produktes ist gleich dem Produkt der Normen. In Formeln:* $N(\alpha\beta) = N(\alpha)\,N(\beta)$ *oder* $(\alpha\beta)^{\mathsf{N}} = \alpha^{\mathsf{N}}\beta^{\mathsf{N}}$.

Beweis: $(\alpha\beta)^{\mathsf{N}} = \prod_{j=1}^{n} \alpha^{(j)}\beta^{(j)} = \prod_{j=1}^{n}\alpha^{(j)} \prod_{j=1}^{n}\beta^{(j)} = \alpha^{\mathsf{N}}\beta^{\mathsf{N}}$.

Aufgabe: Bestimme die Hauptgleichung für $\alpha = \frac{1-\vartheta+\vartheta^2}{3}$, wobei $\vartheta = \sqrt[3]{17}$ ist.

§ 28. Körperbasis und Körperdiskriminante

Der Absolutbetrag einer Diskriminante $\Delta(\alpha_1, \ldots, \alpha_n)$, wobei die α_j ganz und linear unabhängig sind, ist eine natürliche Zahl. Mithin gibt es Systeme $\omega_1, \ldots, \omega_n$ ganzer algebraischer Zahlen der Diskriminante d, wobei $|d|$ der Minimalbetrag von $|\Delta|$ ist. Man nennt $\omega_1, \ldots, \omega_n$ eine *Körperbasis*, d die *Körperdiskriminante*. d ist also bei geradem r_2 nach § 26, Satz 15 positiv, bei ungeradem r_2 negativ.
Der Name Körperbasis rechtfertigt sich mit

Satz 1. *Durch den Modul* $[\omega_1, \ldots, \omega_n]$, *also durch die Gesamtheit*

$$\alpha = x_1\omega_1 + \cdots + x_n\omega_n, \tag{1}$$

wobei die x_j *ganz rational sind, wird jede ganze Zahl des Körpers geliefert.*

Beweis: Satz 8 von § 25 zeigt, daß (1) nur ganze Zahlen liefert. Gezeigt werde nun, daß, wenn mindestens ein x_j, ohne Einschränkung der Allgemeinheit x_1 gebrochen ist, α nicht ganz ist. Hierzu genügt es zu beweisen: $\beta = \alpha - [x_1]\,\omega_1$, also

$$\beta = x_1'\,\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

ist nicht ganz. Es ist $0 < x_1' < 1$. Wir bilden die Diskriminante $\Delta(\beta, \omega_2, \ldots, \omega_n) = \Delta_1$.

Wir haben

$$\Delta_1 = \begin{vmatrix} x_1'\omega_1^{(1)} + x_2\omega_2^{(1)} + \cdots + x_n\omega_n^{(1)} & \omega_2^{(1)} & & \omega_n^{(1)} \\ \cdot & \cdot & & \cdot \\ x_1'\omega_1^{(n)} + x_2\omega_2^{(n)} + \cdots + x_n\omega_n^{(n)} & \omega_2^{(n)} & & \omega_n^{(n)} \end{vmatrix}^2.$$

Subtraktion der mit x_2 multiplizierten zweiten, der mit x_3 multiplizierten dritten, ..., der mit x_n multiplizierten n-ten Spalte von der ersten gibt

$$\Delta_1 = x_1'^2 \begin{vmatrix} \omega_1^{(1)} & \cdots & \omega_n^{(1)} \\ \cdot & & \cdot \\ \omega_1^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2 = x_1'^2 d,$$

also wegen $0 < x_1'^2 < 1$:

$$|\Delta_1| < |d|.$$

Es kann also β nicht ganz sein.

Satz 2. *Mit dem Vektor*

$$\mathfrak{t} = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

und $\mathfrak{A}$ *als rationalganzzahliger Matrix, wobei* $|\mathfrak{A}| = \pm 1$ *ist, gibt* $\mathfrak{A}\mathfrak{t}$ *eine weitere Basis.*

Beweis: Ist

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \mathfrak{a},$$

so bezeichnen wir mit $\Delta(\mathfrak{a})$ die Diskriminante $\Delta(\alpha_1, \ldots, \alpha_n)$. Weiter sei

$$\mathfrak{t}_j = \begin{pmatrix} \omega_1^{(j)} \\ \vdots \\ \omega_n^{(j)} \end{pmatrix}.$$

Wir haben

$$\Delta(\mathfrak{A}\mathfrak{t}) = |\mathfrak{A}\mathfrak{t}_1, \mathfrak{A}\mathfrak{t}_2, \ldots, \mathfrak{A}\mathfrak{t}_n|^2 = |\mathfrak{A}|^2 |\mathfrak{t}_1, \ldots, \mathfrak{t}_n|^2 = |\mathfrak{t}_1, \ldots, \mathfrak{t}_n|^2 = d,$$

somit

$$|\Delta(\mathfrak{A}\mathfrak{t})| = |d|.$$

Zugleich sehen wir, daß mit

$$\alpha_1 = a_{11}\omega_1 + \cdots + a_{1n}\omega_n,$$
$$\cdots$$
$$\alpha_n = a_{n1}\omega_1 + \cdots + a_{nn}\omega_n,$$

$(a_{ij}) = \mathfrak{A}$ sich $\Delta(\mathfrak{a}) = |\mathfrak{A}|^2 d$ ergibt. Wir erhalten

Satz 3. *Die Diskriminante von n linear unabhängigen ganzen Körperzahlen ist gleich der Körperdiskriminante mal dem Quadrat einer natürlichen Zahl.*

Wichtig ist der Spezialfall der Diskriminante

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \Delta(\alpha)$$

= Diskriminante der Zahl α. Hier gilt

Satz 4. *Die Diskriminante einer ganzen erzeugenden Körperzahl ist gleich der Körperdiskriminante multipliziert mit dem Quadrat einer natürlichen Zahl.*

Klar ist folgender

Satz 5. *Der Absolutbetrag der Körperdiskriminante ist* $\geqq 1$.

Wir werden ihn bald dahin verschärfen, daß der genannte Absolutbetrag >1 ist.
Aus Satz 3, 4 folgt

Satz 6. *Lassen sich n linear unabhängige Körperzahlen angeben, deren Diskriminante quadratfrei ist, so ist diese die Körperdiskriminante und die Zahlen geben eine Körperbasis.*

Beispiel: Ist $m \equiv 1 \bmod 4$, m ganz, quadratfrei, kein Quadrat, so ist $\alpha = \frac{1+\sqrt{m}}{2}$ eine ganze algebraische Zahl in $k = \mathsf{P}(\sqrt{m})$. Die Diskriminante $\Delta(\alpha)$ wird

$$\begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m.$$ Mithin ist $[1, \alpha]$ eine Basis.

In derselben Art ist zunächst, wenn ϑ eine Wurzel von

$$f(x) = x^3 - x^2 - 2x - 8$$

wird, die Diskriminante $\Delta(\vartheta)$ zu berechnen. Ist s_j die j-te Potenzsumme von ϑ, also $s_j = S(\vartheta^j)$, so ist diese sehr schnell nach folgender Ableitung zu bestimmen:

Seien die x_ν die Wurzeln von

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n.$$

Differentiation von

$$\log f(x) = \sum_{\nu=1}^{n} \log(x - x_\nu)$$

gibt

$$\frac{f'(x)}{f(x)} = \sum_{\nu=1}^{n} \frac{1}{x - x_\nu}.$$

Wir multiplizieren mit x, setzen $x = \frac{1}{t}$ und erhalten

$$\frac{n + a_{n-1}(n-1)t + a_{n-2}(n-2)t^2 + \cdots + a_1 t^{n-1}}{1 + a_{n-1}t + a_{n-2}t^2 + \cdots + a_0 t^n} = \sum \frac{1}{1 - t x_\nu} = \sum_{\nu,\varrho} t^\varrho x_\nu^\varrho = \sum_{\varrho} s_\varrho t^\varrho .$$

Die Koeffizienten s_ϱ erhalten wir durch Division der angeschriebenen Polynome in t, wobei wir nur deren Koeffizienten anzuschreiben brauchen (man beachte, daß hier nur s_0 bis s_4 zu berechnen sind):

$$\begin{array}{rrrrl}
(3, & -2, & -2 &) : & \underline{(1, -1, -2, -8)} \\
-(3 & -3 & -6 & -24) & 3,\ 1,\ 5,\ 31,\ 49,\ \cdots \\
 & + & + & + & \\
\hline
 & 1 & 4 & 24 & \\
 & 1 & -1 & -2 & -8 \\
 & - & + & + & + \\
\hline
 & & 5 & 26 & 8\cdots \\
 & & 5 & -5 & -10\cdots \\
 & & - & + & + \\
\hline
 & & & 31 & 18\cdots \\
 & & & 31 & -31\cdots \\
 & & & - & + \\
\hline
 & & & & 49\cdots
\end{array}$$

Man erhält $s_0 = 3$, $s_1 = 1$, $s_2 = 5$, $s_3 = 31$, $s_4 = 49, \cdots$, daher

$$\Delta(\vartheta) = \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = \begin{vmatrix} 3 & 1 & 5 \\ 1 & 5 & 31 \\ 5 & 31 & 49 \end{vmatrix} = 3\begin{vmatrix} 5 & 31 \\ 31 & 49 \end{vmatrix} - \begin{vmatrix} 1 & 31 \\ 5 & 49 \end{vmatrix} + 5\begin{vmatrix} 1 & 5 \\ 5 & 31 \end{vmatrix},$$

$$= 3 \cdot (-716) + 106 + 30 = -2012 = -4 \cdot 503,$$

wobei 503 eine Primzahl ist. Es sind nur die Möglichkeiten $d = -4 \cdot 503$ und $d = -503$ vorhanden.

Im vorangegangenen Paragraphen sahen wir, daß $\alpha = \frac{-\vartheta + \vartheta^2}{2}$ eine ganze Zahl ist. Mit der Abkürzung $\mathfrak{g}_j = \begin{pmatrix} \vartheta^{(1)^j} \\ \vartheta^{(2)^j} \\ \vartheta^{(3)^j} \end{pmatrix}$ erhalten wir

$$\Delta(1, \vartheta, \alpha) = \left|\mathfrak{g}_0, \mathfrak{g}_1, \frac{-\mathfrak{g}_1 + \mathfrak{g}_2}{2}\right|^2 = \frac{1}{4}|\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2|^2 = \frac{1}{4}\Delta(\vartheta) = -503.$$

Mithin ist $d = -503$ und $[1, \vartheta, \alpha]$ eine Körperbasis.

§ 29. Die kanonische Basis

Es sei ϑ eine erzeugende ganze Körperzahl. Wir trachten eine Basis $[\omega_1, \ldots, \omega_n]$ zu gewinnen, so daß alle ganzen Zahlen des Moduls $c_1 + c_2\vartheta + \cdots + c_j\vartheta^{j-1}$, wobei die c_j rational sind und $j \leqq n$ ist, sich durch $x_1\omega_1 + \cdots + x_n\omega_n$ ergeben. Die x_j sollen also ganz rational sein.

1. Es sollen alle ganzen Zahlen des Moduls der c_1 durch $X\omega_1$ dargestellt werden. Offenbar genügt die Wahl $\omega_1 = 1$.

2. Alle ganzen Zahlen des Moduls $c_1 + c_2\vartheta$ sollen durch $x\omega_1 + y\omega_2$ mit ganzen rationalen x, y dargestellt werden.

Wir setzen an

$$\omega_2 = \frac{m_1 + m\vartheta}{N}$$

mit ganzem rationalem m_1, m, N. (sgn m = sgn N, dies gilt auch weiter.)

In $\vartheta = A\omega_1 + B\omega_2$ muß A, B ganz rational ausfallen.

Das gibt

$$\vartheta = A + B\frac{m_1 + m\vartheta}{N}.$$

Gleichsetzung des Koeffizienten von ϑ rechts und links gibt

$$1 = \frac{Bm}{N}$$

oder

$$N = Bm,$$

also

$$m \mid N.$$

Gleichsetzung der Koeffizienten von eins gibt

$$0 = A + \frac{Bm_1}{N} = A + \frac{m_1}{m},$$

oder da A ganz ist:

$$m \mid m_1.$$

Mit $\frac{m_1}{m} = a_{21}$, $\frac{N}{m} = b_2$ ist die Teilbasis

$$1, \quad \frac{a_{21} + \vartheta}{b_2}$$

sichergestellt. Zugleich folgt, wenn $b_1 = 1$ definiert wird: $b_1 \mid b_2$.

3. Nun gehen wir zur Gewinnung von ω_3. Es sollen m_1, m, N neue Bedeutung haben. Dann setzen wir an

$$\omega_3 = \frac{m_1 + m_2\vartheta + m\vartheta^2}{N}.$$

Es ist $\vartheta\omega_2 = \frac{a_{21}\vartheta + \vartheta^2}{b_2}$ ganz. Also gibt es eine Darstellung

$$\frac{a_{21}\vartheta + \vartheta^2}{b_2} = U + V\frac{a_{21} + \vartheta}{b_2} + W\frac{m_1 + m_2\vartheta + m\vartheta^2}{N}.$$

Nun gibt Gleichsetzung der Koeffizienten von ϑ^2

$$\frac{1}{b_2} = \frac{Wm}{N}, \quad Wmb_2 = N, \quad \text{also} \quad m \mid N, \quad b_2 \Big| \frac{N}{m} = b_3.$$

Gleichsetzung der Koeffizienten von ϑ gibt

$$\frac{a_{21}}{b_2} = \frac{V}{b_2} + \frac{m_2}{mb_2}, \qquad (a_{21} - V)m = m_2,$$

daher

$$m \mid m_2.$$

Endlich ergibt Vergleich der Koeffizienten von Eins

$$0 = U + \frac{Va_{21}}{b_2} + \frac{m_1}{mb_2}, \quad m_1 = -m(Ub_2 + Va_{21}),$$

also

$$m \mid m_1.$$

Mit $\frac{m_1}{m} = a_{31}$, $\frac{m_2}{m} = a_{32}$ erhalten wir

$$\omega_3 = \frac{a_{31} + a_{32}\vartheta + \vartheta^2}{b_3}.$$

Zugleich sehen wir

$$1 = b_1 \,|\, b_2 \,|\, b_3.$$

Wir gehen nun von folgender Induktionsvoraussetzung aus: Es sei schon

$$\omega_1 = 1, \quad \omega_2 = \frac{a_{21} + \vartheta}{b_2},$$

$$\omega_3 = \frac{a_{31} + a_{32}\vartheta + \vartheta^2}{b_3}, \quad \ldots, \quad \omega_j = \frac{a_{j1} + a_{j2}\vartheta + \cdots + a_{j,j-1}\vartheta^{j-2} + \vartheta^{j-1}}{b_j}$$

mit $1 = b_1 \,|\, b_2 \,|\, b_3 \ldots |\, b_{j-1} \,|\, b_j$ nachgewiesen. Nun setzen wir mit neuen $m_1, m_2, \ldots, m_j, m$ und einem neuen Nenner N an:

$$\omega_{j+1} = \frac{m_1 + m_2\vartheta + \cdots + m_j\vartheta^{j-1} + m\vartheta^j}{N}.$$

Wir führen für den Augenblick neue Bezeichnungen ein.

1. Für $k \leqq j$ soll $A_{kl} = a_{kl}$ sein, wenn $l < k$ ist, hingegen $A_{kk} = 1$, $A_{kl} = 0$ für $l > k$. Weiter sei $B_k = b_k$, $A_{k0} = 0$.

2. Für $k = j+1$ hingegen sei
$A_{j+1,l} = m_l$ für $l \leqq j$, $A_{j+1,j+1} = m$, weiter $A_{j+1,l} = 0$ für $l > j+1$, $B_{j+1} = N$.

Dann gilt für $1 \leqq k \leqq j+1$

$$\omega_k = \sum_l \frac{A_{kl}\vartheta^{l-1}}{B_k}.$$

Nun muß aber

$$\omega_j\vartheta = \sum_{k \leqq j+1} X_k \omega_k$$

mit ganzen rationalen X_k sein. Das gibt

$$\sum_{t \leqq j} \frac{A_{jt}\vartheta^t}{B_j} = \sum_{k,l} \frac{X_k A_{kl}\vartheta^{l-1}}{B_k} = \sum_l \vartheta^{l-1} \sum_k \frac{X_k A_{kl}}{B_k}.$$

Wir vergleichen rechts und links den Koeffizienten von ϑ^j, setzen also rechts $l = j+1$, links $t = j$. Wir erhalten

$$\frac{1}{B_j} = \frac{X_{j+1} A_{j+1,j+1}}{B_{j+1}},$$

somit

$$\frac{1}{b_j} = \frac{X_{j+1} m}{N},$$

also

$$N = X_{j+1} m b_j,$$

daher

$$m b_j \mid N, \quad b_j \Big| \frac{N}{m} = b_{j+1}.$$

Nun betrachten wir einen beliebigen Exponenten $s < j$. Links setzen wir $t = s$, rechts $l = s+1$. Es ist $s \geqq 0$. Wir erhalten

$$\frac{A_{j\,s}}{B_j} = \sum_{k \geqq j} \frac{X_k A_{k,\,s+1}}{B_k} + A,$$

wobei A eine abkürzende Bezeichnung für

$$A = \frac{X_{j+1} m_{s+1}}{B_{j+1}} = \frac{m_{s+1}}{m b_j}$$

ist. Einführung der früheren Bezeichnungen und Multiplikation mit $m b_j$ gibt

$$a_{j\,s} m = m \sum_{k \geqq j} X_k a_{k,\,s+1} \frac{b_j}{b_k} + m_{s+1}.$$

Auf Grund der Induktionsvoraussetzung gilt

$$b_j \equiv 0 \bmod b_k$$

für $k \leqq j$. Mithin wird

$$m \mid m_{s+1},$$

gültig für $s = 0, 1, 2, \ldots, j-2, j-1$.

Mit

$$\frac{m_1}{m} = a_{j+1,\,1}, \quad \ldots, \quad \frac{m_j}{m} = a_{j+1,\,j}$$

bleibt

$$\omega_{j+1} = \frac{a_{j+1,\,1} + a_{j+1,\,2}\vartheta + \cdots + a_{j+1,\,j}\vartheta^{j-1} + \vartheta^j}{b_{j+1}}.$$

Damit ist durch vollständige Induktion der Beweis erbracht zum folgenden wichtigen Satz über die Körperbasis.

Satz 1. *Ist ϑ eine erzeugende ganze Körperzahl, so gibt es eine Körperbasis*

$$\omega_1 = 1, \quad \omega_2 = \frac{a_{21} + \vartheta}{b_2}, \quad \omega_3 = \frac{a_{31} + a_{32}\vartheta + \vartheta^2}{b_3}, \quad \ldots,$$

$$\omega_j = \frac{a_{j1} + a_{j2}\vartheta + \cdots + a_{j,\,j-1}\vartheta^{j-2} + \vartheta^{j-1}}{b_j}, \quad \ldots,$$

$$\omega_n = \frac{a_{n1} + a_{n2}\vartheta + \cdots + a_{n,\,n-1}\vartheta^{n-2} + \vartheta^{n-1}}{b_n},$$

wobei alle a_{jk} und b_j ganz sind und

$$1 = b_1 \mid b_2 \mid b_3 \mid \ldots \mid b_{n-2} \mid b_{n-1} \mid b_n$$

ist. Eine solche Basis heiße kanonische Basis.

Bemerkungen:

1. Sei etwa $a_{jk}' = a_{jk} + b_j V_{jk}$ mit a_{ik}' als absolutkleinstem Rest von a_{jk} mod b_j. Ersetzen wir in der Basis die Zahl ω_j durch die folgende

$$\omega_j - V_{jk}\vartheta^{k-1},$$

so ist im neuen ω_j der Koeffizient von ϑ^{k-1} im Intervall $\left(-\frac{b_j}{2}, +\frac{b_j}{2}\right)$ enthalten. Da dies mit jedem Koeffizienten geschehen kann, können wir in der kanonischen Basis für alle $k < j$

$$-\frac{b_j}{2} < a_{jk} \leqq \frac{b_j}{2}$$

annehmen. Ist etwa $b_1 = b_2 = \cdots = b_t = 1$, so fängt daher die Basis mit $1, \vartheta, \vartheta^2, \ldots, \vartheta^{t-1}$ an. In dieser Art kann die kanonische Basis normiert werden. Es ist aber wohl zu beachten, daß sie dann noch nicht eindeutig gegeben ist, da sie noch von der erzeugenden Körperzahl ϑ abhängt.

2. Ist

$$\mathfrak{h}_j = \begin{pmatrix} 1 \\ \vartheta^{(j)} \\ \vartheta^{(j)^2} \\ \vdots \\ \vartheta^{(j)^{n-1}} \end{pmatrix}, \qquad \mathfrak{M} = \begin{pmatrix} \frac{1}{b_1} & 0 & 0 \\ \frac{a_{21}}{b_2} & \frac{1}{b_2} & 0 \\ \cdot & \cdot & \cdot \\ \frac{a_{n1}}{b_n} & \frac{a_{n2}}{b_n} & \frac{1}{b_n} \end{pmatrix},$$

so wird

$$\mathfrak{T} = \begin{pmatrix} \omega_1^{(1)} & \ldots & \omega_n^{(1)} \\ \cdot & & \cdot \\ \omega_1^{(n)} & \ldots & \omega_n^{(n)} \end{pmatrix} = (\mathfrak{M}\mathfrak{h}_1, \mathfrak{M}\mathfrak{h}_2, \ldots, \mathfrak{M}\mathfrak{h}_n) = \mathfrak{M}\mathfrak{H}$$

mit $\mathfrak{H} = (\mathfrak{h}_1, \ldots, \mathfrak{h}_n)$, $|\mathfrak{H}|^2 = \Delta(\vartheta)$. Die Bildung der Determinanten mit nachfolgendem Quadrieren gibt

$$d = |\mathfrak{M}|^2 \Delta(\vartheta).$$

Nun ist aber $|\mathfrak{M}|^2 = \frac{1}{b_2^2 b_3^2 \ldots b_n^2}$, da $b_1 = 1$ ist. Also folgt, da d ganz ist

$$b_2^2 b_3^2 \ldots b_n^2 \mid \Delta(\vartheta).$$

Weiter folgt wegen $b_j \mid b_{j+1}$ sofort

$$b_2^{2n-2} \mid \Delta(\vartheta), \quad b_3^{2n-4} \left| \frac{\Delta(\vartheta)}{b_2^2}, \quad b_4^{2n-6} \right| \frac{\Delta(\vartheta)}{b_2^2 b_3^2}, \quad \ldots, \quad b_n^2 \left| \frac{\Delta(\vartheta)}{b_2^2 b_3^2 \ldots b_{n-1}^2} \right.$$

Hierdurch wird die Anzahl der Möglichkeiten der b_j sehr eingeschränkt.

Als erste Anwendung bestimmen wir eine Körperbasis und die Körperdiskriminante im quadratischen Zahlenkörper $k = \mathsf{P}(\sqrt{m})$, wobei m eine ganze rationale quadratfreie Zahl, die kein Quadrat ist, bedeutet. Es ist somit $m = -1$ oder $|m| > 1$. Sei also $\vartheta = \sqrt{m}$. Da $\Delta(\sqrt{m}) = 4m$ und m quadratfrei ist, kommt für b_2 nur 2 in Frage. Wegen $\left(\frac{\sqrt{m}}{2}\right)^{\mathsf{N}} = -\frac{m}{4}$, was keine ganze Zahl ist, kommt für die normierte kanonische Basis nur $b_2 = 1$, $\omega_2 = \vartheta$ oder $b_2 = 2$, $\omega_2 = \frac{1+\vartheta}{2}$ in Frage. Wir betrachten den letzten Fall: Es wird $S(\omega_2) = 1$, $\omega_2^{\mathsf{N}} = \frac{1-m}{4}$. Die letzte Zahl ist genau für $m \equiv 1 \bmod 4$ ganz. Damit ist alles erledigt. Es bleibt

Satz 2. *Im quadratischen Zahlkörper* $\mathsf{P}(\sqrt{m})$, *wobei* m *eine ganze rationale quadratfreie Zahl, kein Quadrat ist, gilt*

I. *Ist* $m \equiv 2, 3 \bmod 4$, *so ist* $1, \sqrt{m}$ *eine Basis, die Diskriminante* $d = 4m$.

II. *Ist* $m \equiv 1 \bmod 4$, *so ist* $1, \frac{1+\sqrt{m}}{2}$ *eine Basis, die Diskriminante* $d = m$.

Für $m = -1$, $k = \mathsf{P}(i)$ ist $d = -4$, $|d| > 1$. Sonst ist $|d| \geqq |m| > 1$. Wir haben

Satz 3. *Der Absolutbetrag der Diskriminante eines quadratischen Zahlkörpers ist größer als eins.*

Wir bemerken noch, daß die in § 21 (Kronecker-Symbol) erwähnten Diskriminanten gerade die Diskriminanten quadratischer Körper sind.

ϑ sei Wurzel der Gleichung $\vartheta^3 - 7\vartheta - 14 = 0$. Man findet $\Delta(\vartheta) = 4 \cdot 7^3 - 27 \cdot 14^2 = 4 \cdot 7^2 (7 - 3^3) = -2^4 \cdot 7^2 \cdot 5$. Wegen

$$b_2^4 \mid \Delta(\vartheta)$$

kommt nur $b_2 = 2$ in Frage. Aber $\frac{\vartheta}{2}$ ist keine ganze Zahl, wie man sofort aus $\left(\frac{\vartheta}{2}\right)^{\mathsf{N}} = \frac{14}{8} = \frac{7}{4}$ ersieht, auch $\gamma = \frac{1+\vartheta}{2}$ nicht, da $S(\gamma) = \frac{3}{2}$ ist. (Man bedenke $S(\vartheta) = 0$.) Es ist somit $\omega_1 = 1$, $\omega_2 = \vartheta$ in der kanonischen Basis. Um ω_3 zu berechnen, bedenken

wir $b_3^2 \mid \Delta(\vartheta)$; es kommen also $p=2$ und $p=7$ als Primteiler von b_3 in Frage. Wir untersuchen zunächst, wann eine Zahl $\sigma=\frac{L+M\vartheta+\vartheta^2}{p}$ mit $p=2,7$ ganz ist. Wir haben $\vartheta^3=7\vartheta+14$ und daraus leicht

$$\sigma=\frac{L}{p}+\frac{M}{p}\vartheta+\frac{1}{p}\vartheta^2,$$

$$\sigma\vartheta=\frac{14}{p}+\left(\frac{L}{p}+\frac{7}{p}\right)\vartheta+\frac{M}{p}\vartheta^2,$$

$$\sigma\vartheta^2=\frac{14M}{p}+\left(\frac{14}{p}+\frac{7M}{p}\right)\vartheta+\left(\frac{L}{p}+\frac{7}{p}\right)\vartheta^2.$$

Es wird also die normierte Hauptgleichung

$$-\begin{vmatrix} \frac{L}{p}-\sigma & \frac{M}{p} & \frac{1}{p} \\ \frac{14}{p} & \frac{L}{p}+\frac{7}{p}-\sigma & \frac{M}{p} \\ \frac{14M}{p} & \frac{14}{p}+\frac{7M}{p} & \frac{L}{p}+\frac{7}{p}-\sigma \end{vmatrix}=0,$$

kurz $-|\mathfrak{A}-\sigma\mathfrak{E}|=0$. Nun wenden wir § 27, Satz 3 an: Die Spur der Matrix $S(\mathfrak{A})=\frac{3L}{p}+\frac{14}{p}$ ist die Spur von σ. Da $\frac{14}{p}$ ganz ist, muß $\frac{3L}{p}$ ganz sein, da aber $p=2,7$ ist, ist dies nur für $L\equiv 0 \bmod p$ möglich und L kann Null gesetzt werden. Die so vereinfachte Hauptgleichung

$$-\begin{vmatrix} -\sigma & \frac{M}{p} & \frac{1}{p} \\ \frac{14}{p} & \frac{7}{p}-\sigma & \frac{M}{p} \\ \frac{14M}{p} & \frac{14}{p}+\frac{7M}{p} & \frac{7}{p}-\sigma \end{vmatrix}=0$$

erhält daher die linke Seite

$$f(\sigma)=\sigma^3-\frac{14}{p}\sigma^2+\frac{49-42M-7M^2}{p^2}\sigma-\frac{14}{p^3}(M^3-7M+14).$$

Dieses Polynom muß ganzzahlig sein.
Nun sieht man sofort, daß $p=7$ ausgeschlossen ist, da

$$49-42M-7M^2\equiv 0 \bmod 7^2$$

$M \equiv 0 \bmod 7$ ergibt, was wegen $\left(\frac{\vartheta^2}{7}\right)^N = \frac{4}{7}$ nicht möglich ist. $M=1$, $p=2$, jedoch liefert

$$f(\sigma) = \sigma^3 - 7\sigma^2 + 21\sigma - 35.$$

Also ist $\sigma = \frac{-\vartheta + \vartheta^2}{2}$ ganz.

Bedenkt man, daß wegen $S\left(\frac{\sigma}{2}\right) = \frac{7}{2}$ die Zahl $\frac{\sigma}{2}$ nicht ganz ist, so sehen wir, daß $\omega_1 = 1$, $\omega_2 = \vartheta$, $\omega_3 = \frac{-\vartheta + \vartheta^2}{2}$ eine Basis von k ist.

Wir betrachten die *rein kubischen Zahlkörper* $k = \mathsf{P}(\sqrt[3]{f^2 g})$. Es seien f, g quadratfreie zueinander prime ganze Zahlen, etwa $\alpha = \sqrt[3]{f^2 g}$, natürlich mit $\max(|f|, |g|) > 1$, da sonst k mit P zusammenfiele. Es sind mit $\varrho = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ zu α, das wir beispielsweise als reell annehmen, die Zahlen

$$\alpha^{(2)} = \alpha\varrho, \quad \alpha^{(3)} = \alpha\varrho^2$$

konjugiert.

Wegen $|1-\varrho| = |1-\varrho^2| = |\varrho - \varrho^2| = \sqrt{3}$, $r_2 = 1$,

also $\Delta(\alpha) < 0$ wird $\Delta(\alpha) = -27 f^4 g^2$. Alle Kubikwurzeln seien reell. Wir fragen, ob $\gamma = \frac{L+\alpha}{p}$ ganz werden kann, wobei L ganz rational, p eine Primzahl ist. Wegen $S(\gamma) = \frac{3L}{p}$ gilt für $p > 3$, auch für $p = 2$, daß $L \equiv 0 \bmod p$ sein muß, also weggelassen werden kann. Setzen wir $\gamma = \frac{\alpha}{p}$, so wird $\gamma^N = \frac{f^2 g}{p^3}$, was nie ganz ist, da weder f noch g einen Primfaktor in einer Potenz mit Exponenten >1 enthalten, überdies $(f, g) = 1$ ist.

Daher braucht nur $p = 3$ untersucht zu werden. Sei

$$F(x) = x^3 - f^2 g = (x-\alpha)(x-\alpha\varrho)(x-\alpha\varrho^2).$$

Sofort folgt

$$3x^2 = (x-\alpha)(x-\alpha\varrho) + (x-\alpha)(x-\alpha\varrho^2) + (x-\alpha\varrho)(x-\alpha\varrho^2).$$

Ersetzt man x durch $-\frac{x}{y}$, multipliziert mit y^2 und setzt

$$x + \alpha y = \tau, \quad x + \alpha\varrho y = \tau^{(2)}, \quad x + \alpha\varrho^2 y = \tau^{(3)}, \tag{1a}$$

so bleibt

$$3x^2 = \tau\tau^{(2)} + \tau\tau^{(3)} + \tau^{(2)}\tau^{(3)}. \tag{1}$$

Sei $\gamma = \frac{L+\alpha}{3}$, dann wird nach (1) die elementarsymmetrische Funktion $\sum_{i<j} \gamma^{(i)}\gamma^{(j)}$ gleich $\frac{L^2}{3}$, also für $L \not\equiv 0 \bmod 3$ nicht ganz. Teilbasis der kanonischen Basis wird also $\omega_1 = 1$, $\omega_2 = \alpha$.
Wir betrachten den Ausdruck

$$\frac{L + M\alpha + \alpha^2}{N}$$

und fragen, ob dieser ganz ist. Hier sehen wir sofort, daß $\beta = \sqrt[3]{fg^2}$, das in diesem Körper liegt, ganz ist. Wir müssen also in N die Zahl f aufnehmen, wenn wir ω_3 berechnen wollen. Damit ein Ausdruck mit ganzzahligen L, M, z

$$\tau = \frac{L + M\alpha + \alpha^2}{zf}$$

ganz ist, muß $L \equiv M \equiv 0 \bmod f$ sein, denn es muß $\delta = z\tau - \beta$ ganz sein; es ist aber $\delta = \frac{L + M\alpha}{f}$. Wir brauchen also nur Ausdrücke

$$\tau = \frac{A + B\alpha + C\beta}{z}$$

zu betrachten. Wir setzen zunächst $z = p$ (Primzahl). Mit den Multiplikationsregeln $\alpha^2 = f\beta$, $\alpha\beta = fg$, $\beta^2 = g\alpha$ ergibt sich

$$\tau = \frac{A}{p} + \frac{B}{p}\alpha + \frac{C}{p}\beta,$$

$$\tau\alpha = \frac{Cfg}{p} + \frac{A}{p}\alpha + \frac{Bf}{p}\beta,$$

$$\tau\beta = \frac{Bfg}{p} + \frac{Cg}{p}\alpha + \frac{A}{p}\beta$$

oder die Hauptgleichung

$$-\begin{vmatrix} \frac{A}{p} - \tau & \frac{B}{p} & \frac{C}{p} \\ \frac{Cfg}{p} & \frac{A}{p} - \tau & \frac{Bf}{p} \\ \frac{Bfg}{p} & \frac{Cg}{p} & \frac{A}{p} - \tau \end{vmatrix} = 0. \tag{2}$$

Die Spur der Matrix wird $\frac{3A}{p}$. Ist $p \neq 3$, so folgt $A \equiv 0 \bmod p$ und A kann wegbleiben. Aber Weglassen von A schließt sich überhaupt aus, auch für $p = 3$. Denn dann wird

$$\tau = \sqrt[3]{fg}\,\frac{B\sqrt[3]{f} + C\sqrt[3]{g}}{p}$$

$$\tau^{(2)} = \sqrt[3]{fg}\,\frac{B\sqrt[3]{f}\varrho + C\sqrt[3]{g}\varrho^2}{p},$$

$$\tau^{(3)} = \sqrt[3]{fg}\,\frac{B\sqrt[3]{f}\varrho^2 + C\sqrt[3]{g}\varrho}{p},$$

also

$$\tau^N = fg\,\frac{B^3 f + C^3 g}{p^3}.$$

Da nur Primzahlen $p \mid \Delta(\vartheta) = -27 f^4 g^2$ in Frage kommen, sei etwa $p \mid f$ also $p \parallel f$. Dann ist $g \not\equiv 0 \bmod p$, und der Zähler könnte nur bei $C \equiv 0 \bmod p$ durch p teilbar sein. Aber dann könnte C weggelassen werden, es bliebe $B^3 f^2 g \equiv 0 \bmod p^3$, also wegen $p \parallel f$, $g \not\equiv 0 \bmod p$ die Kongruenz $B \equiv 0 \bmod p$.
$p \mid g$ wird ebenso behandelt (f und g treten völlig symmetrisch auf). Der noch mögliche Fall $p = 3$, $(fg, 3) = 1$ gibt

$$S = \frac{1}{9}\sum_{i<j}(B\alpha^{(i)} + C\beta^{(i)})(B\alpha^{(j)} + C\beta^{(j)}) = \frac{\sqrt[3]{f^2 g^2}}{9}\sum_{i<j}(\xi^{(i)}\xi^{(j)})$$

mit

$$\xi = B\sqrt[3]{f} + C\sqrt[3]{g},\quad \xi^{(2)} = B\varrho\sqrt[3]{f} + C\varrho^2\sqrt[3]{g},\quad \xi^{(3)} = B\varrho^2\sqrt[3]{f} + C\varrho\sqrt[3]{g}.$$

Da S rational ist, muß $f^{\frac{2}{3}}$ und $g^{\frac{2}{3}}$ in der Summe herausfallen und wir erhalten

$$-S = \frac{fgBC}{3}.$$

Wegen $(fg, 3) = (BC, 3) = 1$ ist S keine ganze Zahl.
Es sei weiter $p = 3$. Die linke Seite der Hauptgleichung (2), nämlich

$$h(\tau) = \tau^3 - A\tau^2 + \frac{A^2 - BCfg}{3}\tau - \frac{A^3 + B^3 f^2 g + C^3 f g^2 - 3ABCfg}{27} \qquad (3)$$

muß ein ganzzahliges Polynom in τ sein. Da wir B, C auf ihre absolutkleinsten Reste mod 3 reduzieren können, während wir dies bei A nicht tun, so haben wir $|B| = |C| = 1$. Denn $3 \mid BC$

ist unmöglich. Bei eventueller Ersetzung von ω_3 durch $-\omega_3$ ist direkt $C=1$. Es ist $B=\pm 1$, daher $B^3=B$. Wir erhalten den einfacheren Ausdruck:

$$h(\tau)=\tau^3-A\tau^2+\frac{A^2-Bfg}{3}\tau-\frac{A^3+Bf^2g+fg^2-3ABfg}{27}. \tag{4}$$

Es müssen also die Kongruenzen

$$A^2-Bfg\equiv 0 \bmod 3, \tag{5}$$

$$A^3+Bf^2g+fg^2-3ABfg\equiv 0 \bmod 27 \tag{6}$$

gelten.

Aus (5) läßt sich eine Folgerung ziehen: Sei von jetzt ab $m=f^2g$, also $k=\mathsf{P}(\sqrt[3]{m})$. Ist nun m durch 3 teilbar, so ist eine Kongruenz (5) ausgeschlossen und eine Basis wird $1, \alpha, \beta$; die Körperdiskriminante wird dann $d=-27f^2g^2$. Von jetzt an sei $(fg, 3)=1$.

Wir betrachten nun (6) als Kongruenz mod 3. Da nach (5)

$$Bfg\equiv 1 \bmod 3$$

wird, bleibt einfach

$$A+f+f\equiv 0 \bmod 3,\ A\equiv f \bmod 3.$$

Da wir A mod 3 beliebig annehmen können, so wählen wir $A=f$. Die Kongruenz (6) wird dann

$$f^3-2Bf^2g+fg^2\equiv 0 \bmod 27,$$

also wegen $(3, f)=1$.

$$f^2-2Bfg+g^2\equiv 0 \bmod 27. \tag{7}$$

Mit $B=1$ ist (7) die Kongruenz

$$(f-g)^2\equiv 0 \bmod 27.$$

Dazu ist notwendig und hinreichend

$$f\equiv g \bmod 9.$$

Es ist $f^3\equiv\pm 1 \bmod 9$, also $f^2g\equiv\pm 1 \bmod 9$, daher

$$m\equiv\pm 1 \bmod 9.$$

Dies genügt auch.

Genau so ergibt sich mit $B=-1$ wieder $m\equiv\pm 1 \bmod 9$ und $f\equiv -g \bmod 9$. Wegen $3^3 \| \Delta(\vartheta)$ geht 3^2 als Nenner von τ nicht.

Wir haben

Satz 3. *Ist m eine kubenfreie Zahl $m = f^2 g$, wobei $(f, g) = 1$, $|m| > 1$, so ist für $m \equiv \pm 1 \bmod 9$ das Zahlentripel*

$$1, \quad \alpha, \quad \frac{f + \alpha + \beta}{3}$$

für $f \equiv g \bmod 9$ eine Basis von $\mathbf{P}(\sqrt[3]{m})$. Hierbei ist $\alpha = \sqrt[3]{f^2 g}$, $\beta = \sqrt[3]{f g^2}$. Ist $f \equiv -g \bmod 9$, so ist dagegen

$$1, \quad \alpha, \quad \frac{f - \alpha + \beta}{3}$$

eine Basis. Für alle anderen solchen m ist $1, \alpha, \beta$ eine Körperbasis.

Bemerkung: Wegen $f^3 \equiv \pm 1$ und $f^2 g \equiv \pm 1 \bmod 9$ muß bei den beiden Voraussetzungen $f \equiv \varepsilon g \bmod 9$ mit $\varepsilon = \pm 1$ sein.

§ 30. Einige Teilbarkeitssätze

Bei algebraischen Zahlen gilt genauso wie bei rationalen die Definition: $\alpha \mid \beta$ (lies: α teilt β) heißt: $\frac{\beta}{\alpha}$ ist ganz.

Nach Satz 9 von § 25 ist dieser Begriff transitiv: $\mid \beta, \beta \mid \gamma$ hat $\alpha \mid \gamma$ zur Folge.

Satz 1. *Ist $\alpha_0, \ldots, \alpha_r$ ganz, β Wurzel von $f(x) = \alpha_r x^r + \cdots + \alpha_0$, so ist $\alpha_r \beta$ ganz.*

Beweis: $\alpha_r \neq 0$ werde vorausgesetzt. Sonst ist der Satz richtig, wenn auch trivial. Die Richtigkeit folgt daraus, daß $\alpha_r \beta$ Wurzel des normierten ganzzahligen Polynoms

$$g(y) = y^r + \alpha_{r-1} y^{r-1} + \alpha_{r-2} \alpha_r y^{r-2} + \cdots + \alpha_0 \alpha_r^{r-1} \quad \text{ist.}$$

Satz 2. *Bei den Voraussetzungen des Satzes 1 hat das Polynom $\frac{f(x)}{x - \beta}$ lauter ganzzahlige Koeffizienten.*

Beweis: Für $r = 1$ ist der Satz richtig:

$$f(x) = \alpha_1 x + \alpha_0 = \alpha_1 (x - \beta), \qquad \frac{f(x)}{x - \beta} = \alpha_1.$$

Der Satz gelte für alle Polynome eines Grades $< r$. Mit

$$\varphi(x) = f(x) - \alpha_r x^{r-1} (x - \beta)$$

entsteht $\frac{\varphi(x)}{x-\beta}$ aus einem Polynom eines Grades kleiner als $< r$, ist also ganzzahlig, somit auch

$$\frac{f(x)}{x-\beta} = \frac{\varphi(x)}{x-\beta} + \alpha_r x^{r-1}.$$

Satz 3 (mit denselben Voraussetzungen). *Es mögen* $\beta = \beta_1$, $\beta_2, \ldots, \beta_R$ *Wurzeln von* $f(x)$ *sein, eventuell auch mehrfache, aber jede höchstens in der betreffenden Vielfachheit, dann ist* $\alpha_r \beta_1 \ldots \beta_R$ *ganz.*

Beweis: Das Polynom

$$\frac{f(x)}{\prod_{j=R+1}^{r}(x-\beta_j)} = \alpha_r (x-\beta_1) \ldots (x-\beta_R),$$

wobei $\beta_{R+1}, \ldots, \beta_r$ die übrigen Wurzeln sind, hat lauter ganzzahlige Koeffizienten. Mithin ist auch das Absolutglied

$$(-1)^R \alpha_r \beta_1 \ldots \beta_R$$

ganz.

Satz 4. *Ist* $\alpha \mid \beta_1, \ldots, \beta_m$ *und* $\lambda_1, \ldots, \lambda_m$ *ganz, so ist*

$$\alpha \mid \sum_{j=1}^{m} \beta_j \lambda_j.$$

Beweis: Klar.

Sehr wichtig ist der folgende

Satz 5. *Es seien in*

$$g(x) = \xi_t x^t + \cdots + \xi_0,$$
$$h(x) = \eta_u x^u + \cdots + \eta_0$$

die ξ_i, η_j *ganz, weiter*

$$F(x) = g(x)\, h(x) = \alpha_v x^v + \cdots + \alpha_0,$$

also $v = t + u$; *ferner gelte für die ganze Zahl* $\gamma \mid \alpha_k$ *für jedes* k $(0 \leqq k \leqq v)$. *Dann gilt* $\gamma \mid \xi_i \eta_j$ *für jedes Paar* $[i, j]$.

Beweis: Ist $tu = 0$, so ist der Satz trivial, aber richtig. Sei daher $tu > 0$. Es sei

$$g(x) = \xi_t \prod_{i=1}^{t}(x-\varrho_i), \qquad h(x) = \eta_u \prod_{j=1}^{u}(x-\sigma_j).$$

Die Funktion

$$\frac{F(x)}{\gamma} = \frac{\xi_t \eta_u}{\gamma}(x-\varrho_1) \ldots (x-\sigma_u)$$

hat nach Voraussetzung lauter ganzzahlige Koeffizienten. Nach Satz 3 ist also jedes Produkt

$$\frac{\xi_t \eta_u}{\gamma} \varrho' \varrho'' \dots \sigma' \sigma'' \dots,$$

wobei die $\varrho^{(a)}$ irgendwelche ϱ_i, die $\sigma^{(b)}$ irgendwelche σ_j sind, ganzzahlig.

Nun ist aber nach den Fundamentalsätzen über symmetrische Funktionen

$$\xi_i = \pm \xi_t \sum \varrho' \varrho'' \dots,$$
$$\eta_j = \pm \eta_u \sum \sigma' \sigma'' \dots,$$

also $$\frac{\xi_i \eta_j}{\gamma} = \sum \left(\pm \frac{\xi_t \eta_u}{\gamma} \varrho' \varrho'' \dots \sigma' \sigma'' \dots\right)$$

ganz als Summe ganzer Zahlen.

Dieser von *E. Steinitz* herrührende Beweis des Satzes 5 ist sehr schön und einfach. Der Satz wird in der nun folgenden Idealtheorie wichtig sein.

§ 31. Begriff der Einheiten

Definition. *Eine ganze Zahl ε ist dann und nur dann eine Einheit, wenn die reziproke Zahl ε^{-1} ganz ist.*

Das normierte ganzzahlige irreduzible Polynom $f(x)$, von dem ε Wurzel ist, laute $f(x) = a_0 + a_1 x + \dots + x^n$.

Die Zahl ε^{-1} ist hingegen Wurzel von

$$h(x) = 1 + a_{n-1} x + \dots + a_0 x^n.$$

Normiert wird dieses Polynom

$$g(x) = \frac{1}{a_0} + \frac{a_{n-1}}{a_0} x + \dots + x^n.$$

Da $g(x)$ wieder ganzzahlig sein muß, so ist $a_0 = \pm 1$, und dies genügt auch. Sofort folgt

Satz 1. *Die Norm ε^{N} einer Einheit ε ist ± 1.*

Auch folgt weiter

Satz 2. *Hat eine ganze algebraische Zahl die Norm ± 1, so ist sie eine Einheit.*

Hieraus folgt aber

Satz 3. *Das Produkt zweier Einheiten, ebenso der Quotient zweier Einheiten ist eine Einheit.*

Dieser Satz 3 kann auch, wie folgt, ausgesprochen werden:

Satz 4. *Die Einheiten bilden bezüglich der Multiplikation eine Gruppe.*

Es ist oft nicht möglich, das irreduzible Polynom, dem eine Einheit genügt, anzugeben. Aber es gilt der folgende

Satz 5. *Genügt eine algebraische Zahl α einer normierten ganzzahligen Gleichung*

$$\pm 1 + a_1 x + \cdots + x^m = 0,$$

so ist sie eine Einheit.

Beweis: Zunächst ist α ganz. $\frac{1}{\alpha}$ genügt der normierten ganzzahligen Gleichung

$$\pm(1 + a_{m-1}x + \cdots + a_1 x^{m-1} \pm x^m) = 0,$$

ist also auch ganz.

Satz 5 kann noch allgemeiner ausgesprochen werden:

Satz 6. *Genügt eine algebraische Zahl α einer normierten Gleichung*

$$\eta + \beta x + \cdots + \varkappa x^{m-1} + x^m = 0,$$

wobei η eine Einheit, weiter $\beta, \ldots, \varkappa$ ganz algebraisch sind, so ist α eine Einheit (nach § 25, Satz 9 ist α ganz).

Beweis: α^{-1} genügt der normierten Gleichung mit ganzen algebraischen Zahlen als Koeffizienten

$$\eta^{-1} + \varkappa\eta^{-1}x + \cdots + \beta\eta^{-1}x^{m-1} + x^m = 0,$$

ist also auch ganz.

Definition. *Zwei algebraische Zahlen α, β heißen assoziiert, wenn $\beta = \alpha\varepsilon$ ist (ε Einheit).*

Diese Definition erfüllt die drei Eigenschaften der Äquivalenz:

1. Reflexivität: α ist zu α assoziiert, denn $\alpha = \alpha \cdot 1$.

2. Symmetrie: aus α zu β assoziiert, folgt β zu α assoziiert. Denn $\beta = \alpha\varepsilon$ hat $\alpha = \beta\varepsilon^{-1}$ zur Folge.

3. Transitivität: Ist β zu α assoziiert, γ zu β assoziiert, so ist γ zu α assoziiert; denn es ist $\beta = \alpha\varepsilon$, $\gamma = \beta\eta$ mit ε, η als Einheiten, mithin $\gamma = \alpha(\varepsilon\eta)$, und $\varepsilon\eta$ ist auch Einheit.

§ 32. Der Idealbegriff, Primideale

Wie im Körper der rationalen Zahlen gibt es in allen anderen algebraischen Zahlkörpern ganze Zahlen, die sich nicht als Produkt ganzer Zahlen, abgesehen von Einheiten, desselben Körpers darstellen lassen. Wir nennen sie unzerlegbare Zahlen. Sie haben nicht die Bedeutung der Primzahlen des rationalen Zahlkörpers, denn in vielen Fällen läßt sich eine ganze Zahl eines solchen Körpers nicht eindeutig als Produkt unzerlegbarer Zahlen darstellen.

Beispiel: Nehmen wir als verhältnismäßig einfachen Körper $k = \mathsf{P}(\sqrt{-23})$. Die Einheiten sind nur ± 1; denn aus der Annahme $\varepsilon^{\mathsf{N}} = +1$ folgt, da sich die ganzen Zahlen des Körpers aus der Basis

$$1, \quad \frac{1+\sqrt{-23}}{2}$$

als $\frac{x+y\sqrt{-23}}{2}$, $x \equiv y \bmod 2$, dabei x, y ganz rational ergeben, die Gleichung

$$x^2 + 23y^2 = 4,$$

die offenbar nur die ganzzahligen Lösungen $[2, 0]$, $[-2, 0]$ hat. $\varepsilon^{\mathsf{N}} = -1$ ist ganz ausgeschlossen, da die Norm einer von Null verschiedenen Zahl des Körpers als Produkt zweier konjugiert komplexen Zahlen positiv ist.

Wir haben die Zerlegungen

$$6 = 2 \cdot 3, \quad 6 = \frac{1+\sqrt{-23}}{2}\,\frac{1-\sqrt{-23}}{2} = \beta\bar{\beta}.$$

Die Zahlen 2, 3 sind offenbar unzerlegbar. Denn wäre

$$\alpha = \frac{x+y\sqrt{-23}}{2} \mid 2,$$

wobei angenommen wird, daß $x \equiv y \bmod 2$, x, y ganz und ein eigentlicher (von 1 und 2 verschiedener) Teiler vorliegt, so müßte

$$1 < \alpha^{\mathsf{N}} < 4 = 2^{\mathsf{N}},$$

aber zugleich

$$\alpha^{\mathsf{N}} \mid 4$$

sein, d. h. $\alpha^{\mathsf{N}} = 2$.

Dies gibt die Gleichung $x^2 + 23y^2 = 8$ mit ganzzahligem x und y, die offenbar keine Lösung hat. In derselben Art beweist man die Unzerlegbarkeit von 3 und $\beta = \frac{1+\sqrt{-23}}{2}$, ebenso von $\bar{\beta}$.

Wir sind daher gezwungen, einen neuen Begriff einzuführen, zu dem schon in § 14 eine Vorbereitung getroffen ist.

Definition. *Ein Ideal* $\mathfrak{a} = (\alpha_1, \ldots, \alpha_q)$ *in einem Körper* k *ist die Gesamtheit aller Zahlen*

$$\alpha_1 \xi_1 + \cdots + \alpha_q \xi_q$$

im Körper, wobei die ξ_j *ganze Zahlen des Körpers sind.*

Sind alle α_j *ganz, so heißt* $\mathfrak{a}$ *ein ganzes Ideal.* Dann sind alle Zahlen des Ideals ganz. *Ist mindestens eine der Zahlen* α_j *gebrochen, so heißt das Ideal ein gebrochenes Ideal.*

Eine Gleichung zwischen zwei Idealen

$$\mathfrak{a} = \mathfrak{b}$$

ist mengentheoretisch aufzufassen: Die Zahlen des Ideals $\mathfrak{a}$ sind auch Zahlen von $\mathfrak{b}$ und umgekehrt.

Unter $\lambda\mathfrak{a}$, wobei λ eine beliebige Körperzahl ist, verstehen wir das Ideal

$$\lambda\mathfrak{a} = (\lambda\alpha_1, \ldots, \lambda\alpha_q).$$

Es sei $\mathfrak{a}$ ein gebrochenes Ideal. Für $\alpha_1, \ldots, \alpha_q$ gibt es dann natürliche Zahlen $c_1, \ldots, c_q$, so daß $c_1\alpha_1, \ldots, c_q\alpha_q$ ganze algebraische Zahlen sind. Denn genügt z. B. α_1 der normierten nicht ganzzahligen irreduziblen Gleichung (alle a_j ganz!)

$$x^m + \frac{a_{m-1}x^{m-1} + \cdots + a_0}{A} = 0$$

mit A ganz rational > 1, so genügt $A\alpha_1$ der normierten ganzzahligen irreduziblen Gleichung

$$y^m + a_{m-1}y^{m-1} + \cdots + a_0 A^{m-1} = 0.$$

Mit $\{c_1, \ldots, c_q\} = C$ als kleinstem gemeinsamen Vielfachen der c_j, ist dann

$$\mathfrak{b} = C\mathfrak{a}$$

ein ganzes Ideal. Es folgt $\mathfrak{a} = \frac{\mathfrak{b}}{C}$. Wir haben

Satz 1. *Jedes gebrochene Ideal ist gleich einem ganzen Ideal, dividiert durch eine natürliche Zahl.*

Vom Nullideal werde abgesehen.

Satz 2. *Das Ideal hat Moduleigenschaft.*

Beweis: Mit ϱ und σ ist auch $\varrho - \sigma$ im Ideal.

Satz 3. *Mit α liegt auch $\alpha\tau$ im Ideal, wobei τ beliebig ganz im Körper ist.*

Beweis: Klar.
Ein Spezialfall ist

Satz 4. *Mit α liegt auch $\alpha\eta$ im Ideal, wobei η eine Einheit ist, oder: ein Ideal enthält mit einer Zahl auch alle assoziierten Zahlen.*

Definition. *Ein Hauptideal (α) besteht aus allen $\alpha\xi$, ξ beliebig ganz in k.*

Satz 5. *Ist α zu β assoziiert, so ist $(\alpha) = (\beta)$.*

Satz 6. *Ist $(\alpha) = (\beta)$, so ist β zu α assoziiert, also $\beta = \alpha\varepsilon$, wobei ε eine Einheit ist.*

Definition. *Das Produkt zweier Ideale $\mathfrak{a} = (\alpha_1, \ldots, \alpha_q)$, $\mathfrak{b} = (\beta_1, \ldots, \beta_r)$ ist das Ideal*

$$\mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \ldots, \alpha_q\beta_1, \alpha_1\beta_2, \ldots, \alpha_q\beta_r).$$

Daraus folgt unmittelbar

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}, \quad (\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}), \quad (\alpha)\mathfrak{a} = \alpha\mathfrak{a}$$

und somit

Satz 7. *Die Multiplikation von Idealen erfüllt das kommutative und assoziative Gesetz.*

Definition. *$\mathfrak{b}$ ist durch $\mathfrak{a}$ teilbar, geschrieben $\mathfrak{a} \mid \mathfrak{b}$, wenn $\mathfrak{a} \supseteqq \mathfrak{b}$. Wir schreiben auch $\mathfrak{b} \equiv 0 \bmod \mathfrak{a}$. $\mathfrak{a} \mid \alpha$ heißt $\mathfrak{a} \mid (\alpha)$.*
Mit Beschränkung auf ganze Ideale als Modul definieren wir auch allgemein eine Kongruenz

$$\alpha \equiv \beta \bmod \mathfrak{a} \text{ heißt } \mathfrak{a} \mid \beta - \alpha,$$

wobei wir zunächst α, β auch als ganz annehmen.

Diese Kongruenz erfüllt, wie man sofort sieht, die Eigenschaften der Äquivalenz: Reflexivität, Symmetrie und Transitivität.

Hiervon werde nur der schwierigste Punkt, die Transitivität, bewiesen. Ist $\alpha \equiv \beta$, $\beta \equiv \gamma$, so liegt $\beta - \alpha$, $\gamma - \beta$, also

$$\beta - \alpha + \gamma - \beta = \gamma - \alpha$$

im Ideal, es ist daher $\alpha \equiv \gamma \bmod \mathfrak{a}$. In analoger Art wie früher können wir also auch von Restklassen nach einem Ideal sprechen.
Mit der vorigen Definition haben wir sofort die üblichen Eigenschaften der Kongruenz:

1. Aus $\alpha \equiv \beta \bmod \mathfrak{b}$, $\mathfrak{b} \equiv 0 \bmod \mathfrak{c}$ folgt $\alpha \equiv \beta \bmod \mathfrak{c}$.
Denn $\beta - \alpha$ liegt in $\mathfrak{b}$, also in $\mathfrak{c}$.

2. Aus $\alpha \equiv \beta \bmod \mathfrak{a}$, $\gamma \equiv \delta \bmod \mathfrak{a}$ folgt $\alpha \pm \gamma \equiv \beta \pm \delta \bmod \mathfrak{a}$.
Denn mit $\beta - \alpha$, $\delta - \gamma$ in $\mathfrak{a}$ liegt auch $(\beta + \delta) - (\alpha + \gamma)$ in $\mathfrak{a}$.
Analog bei der Subtraktion.

3. Aus $\alpha \equiv \beta \bmod \mathfrak{a}$ folgt mit beliebigem ganzen γ, daß $\gamma\alpha \equiv \gamma\beta \bmod \gamma\mathfrak{a}$ ist. Denn $\gamma(\beta - \alpha)$ liegt in $\gamma\mathfrak{a}$.

4. Insbesondere: Aus $\alpha \equiv \beta \bmod \mathfrak{a}$, γ ganz folgt $\gamma\alpha \equiv \gamma\beta \bmod \mathfrak{a}$.

5. Aus $\alpha \equiv \beta$, $\gamma \equiv \delta \bmod \mathfrak{a}$ folgt $\alpha\gamma \equiv \beta\delta \bmod \mathfrak{a}$. Denn zunächst folgt $\alpha\gamma \equiv \beta\gamma \bmod \mathfrak{a}$, auch $\beta\gamma \equiv \beta\delta \bmod \mathfrak{a}$, also wegen der Transitivität ergibt sich $\alpha\gamma \equiv \beta\delta \bmod \mathfrak{a}$.

Satz 8. *Jedes Ideal enthält natürliche Zahlen.*

Beweis: Mit einer Zahl $\gamma \neq 0$ des Ideals gibt es eine natürliche Zahl A, so daß $A\gamma$ ganz ist, dann ist auch $A\gamma$ im Ideal sowie die natürliche Zahl $|(A\gamma)^{\mathfrak{N}}|$. (Ist das Ideal ganz, so kann $A = 1$ gesetzt werden.) Denn die letzte Zahl ist durch $A\gamma$ teilbar.

Die Rechenregeln 2 und 5 für Ideale können zusammengefaßt werden als

Satz 9. *Die Restklassen nach einem ganzen Ideal bilden einen Ring.*

Satz 10. *Der Restklassenring nach einem ganzen Ideal ist ein endlicher Ring, also ein Vollring.*

Beweis: Sei $\mathfrak{a}$ das Ideal. Unter den natürlichen Zahlen in $\mathfrak{a}$ gibt es eine kleinste, sie heiße a. Ein beliebiges ganzes ξ im Körper: $\xi = x_1\omega_1 + \cdots + x_n\omega_n$ mit $[\omega_1, \ldots, \omega_n]$ als Körperbasis ist dann mod a einer Zahl $x_1'\omega_1 + \cdots + x_n'\omega_n$ mit x_j' ganz, $0 \leqq x_j' < a$ kongruent. Der Restklassenring hat also höchstens a^n Elemente.

Definition. $N(\mathfrak{a}) = \mathfrak{a}^{\mathfrak{N}}$ (*Norm von* $\mathfrak{a}$) *ist die Anzahl der Elemente des Restklassenrings mod* $\mathfrak{a}$.

Bemerkungen:

1. Die Norm eines Ideals ist also zunächst nur für ganze Ideale definiert. Sehr spät erst werden wir diesen Begriff auf gebrochene Ideale erweitern.

2. Die Schreibweise $\mathfrak{a}^N$, die wir überwiegend anwenden, setzt die Richtigkeit des Satzes $(\mathfrak{ab})^N = \mathfrak{a}^N\mathfrak{b}^N$ voraus. Wir werden diesen Satz erst später beweisen.

3. Aus der Definition folgt, daß $\mathfrak{a}^N$ für ganzes $\mathfrak{a}$ eine natürliche Zahl ist.

Definition. *Die Gesamtheit aller ganzen Zahlen eines Körpers bildet das Einheitsideal* (1).

Satz 11. *Enthält ein ganzes Ideal die Zahl* 1, *oder enthält es überhaupt eine Einheit, so ist es das Einheitsideal.*

Beweis: Klar.

Definition. *Ein ganzes Ideal, dessen Restklassenring ein nicht nur aus dem Nullelement bestehender Integritätsbereich ist, heißt Primideal.*

Bemerkungen:

1. Durch die Definition ist automatisch das Einheitsideal aus dem Begriff der Primideale ausgeschlossen.

2. Als Vollring ist der Restklassenring nach einem Primideal ein Körper, als endlicher Ring ein endlicher Körper, also ein Galoisfeld $GF(p^f)$, wobei p eine rationale (positive) Primzahl ist. f heißt *Grad des Primideals.*

Satz 12. *Sei* $\mathfrak{p}$ *ein Primideal. Aus* $\alpha\beta \equiv 0 \bmod \mathfrak{p}$ *folgt* $\alpha \equiv 0 \bmod \mathfrak{p}$ *oder* $\beta \equiv 0 \bmod \mathfrak{p}$, *oder, ein Primideal kann nur dann in einem Produkt aufgehen (das Produkt durch das Primideal teilbar sein), wenn es mindestens in einem Faktor aufgeht.*

Beweis: Er folgt unmittelbar daraus, daß der Restklassenring mod $\mathfrak{p}$ ein Körper ist.

Satz 13. *Ein Primideal* $\mathfrak{p}$ *kann in dem Produkt zweier Ideale* $\mathfrak{a}$, $\mathfrak{b}$ *nur aufgehen, wenn es mindestens in einem Faktor aufgeht, oder, sind* $\mathfrak{a}$, $\mathfrak{b}$ *nicht durch* $\mathfrak{p}$ *teilbar, dann auch ihr Produkt* $\mathfrak{ab}$ *nicht.*

Beweis: Nach den Voraussetzungen des Satzes gibt es ein $\alpha \not\equiv 0 \bmod \mathfrak{p}$ in $\mathfrak{a}$, ein $\beta \not\equiv 0 \bmod \mathfrak{p}$ in $\mathfrak{b}$; dann ist $\alpha\beta \equiv 0 \bmod \mathfrak{ab}$, aber $\alpha\beta \not\equiv 0 \bmod \mathfrak{p}$, also $\mathfrak{ab} \not\equiv 0 \bmod \mathfrak{p}$.

Satz 14. *Ein Primideal kann durch kein anderes ganzes Ideal außer durch* (1) *teilbar sein.*

Beweis: Es wäre $\mathfrak{a}$ ein ganzes Ideal, $\mathfrak{p} \equiv 0 \bmod \mathfrak{a}$, aber $\mathfrak{a} > \mathfrak{p}$ und $(1) > \mathfrak{a}$. Nun sei α eine Zahl, die zu $\mathfrak{a}$, aber nicht zu $\mathfrak{p}$ gehört. Da der Restklassenring von $\mathfrak{p}$ ein Körper ist, gibt es ein ganzes ξ in k mit $\alpha\xi \equiv 1 \bmod \mathfrak{p}$; damit auch $\alpha\xi \equiv 1 \bmod \mathfrak{a}$. Es gehört

aber $\alpha\xi$ zu $\mathfrak{a}$ und damit 1 zu $\mathfrak{a}$. Also wäre $\mathfrak{a}$ doch das Einheitsideal.

Satz 15. *Ein ganzes von* (1) *verschiedenes Nichtprimideal* $\mathfrak{a}$ *hat mindestens einen ganzen Teiler, der weder mit* $\mathfrak{a}$ *noch mit* (1) *zusammenfällt.*

Beweis: Der Restklassenring mod $\mathfrak{a}$ hat eigentliche Nullteiler. Sei α ein solcher, also $\alpha\beta \equiv 0 \bmod \mathfrak{a}$, aber α und β nicht in $\mathfrak{a}$. Das Ideal $\mathfrak{a}_1 = (\mathfrak{a}, \alpha)$ ist ein Teiler von $\mathfrak{a}$. Es ist ein echter (mit $\mathfrak{a}$ nichtzusammenfallender) Teiler wegen $\alpha \equiv 0 \bmod \mathfrak{a}_1$, $\alpha \not\equiv 0 \bmod \mathfrak{a}$; $\mathfrak{a}_1$ ist aber auch nicht das Einheitsideal (1), denn seine Zahlen sind die Gesamtheit der durch $\alpha\xi$ repräsentierten Restklassen mod $\mathfrak{a}$. Nun folgte aus $\alpha\xi \equiv 1 \bmod \mathfrak{a}$, $\alpha\beta \equiv 0 \bmod \mathfrak{a}$ sofort $\alpha\xi\beta \equiv 0 \bmod \mathfrak{a}$ und damit auch $\beta \equiv 0 \bmod \mathfrak{a}$ im Gegensatz zur Voraussetzung über β.

Die Fortführung dieses Verfahrens,

$$\mathfrak{a} \equiv 0 \bmod (\mathfrak{a}, \alpha) \equiv 0 \bmod (\mathfrak{a}, \alpha, \alpha_1) \equiv 0 \ldots$$

führt nach endlich vielen Schritten zu einem Ideal $\mathfrak{a}_t$, das nicht (1) ist, aber keine Nullteiler im Restklassenring hat. Es ist also $\mathfrak{a}_t$ ein Primideal, $\mathfrak{a} \equiv 0 \bmod \mathfrak{a}_t$ und wir haben

Satz 16. *Jedes von* (1) *verschiedene ganze Ideal ist durch ein Primideal teilbar.*

Wir definieren, wenn

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_q),\ \mathfrak{b} = (\beta_1, \ldots, \beta_r)$$

ist, das Ideal

$$(\mathfrak{a}, \mathfrak{b}) = (\alpha_1, \ldots, \alpha_q, \beta_1, \ldots, \beta_r)$$

und nennen $(\mathfrak{a}, \mathfrak{b})$ den *größten gemeinsamen Teiler der Ideale* $\mathfrak{a}, \mathfrak{b}$. Es ist klar, daß, wenn ein Ideal $\mathfrak{a}$ und $\mathfrak{b}$ teilen soll, d. h. umfassender als die Vereinigungsmenge der Ideale $\mathfrak{a}, \mathfrak{b}$, die im allgemeinen kein Ideal ist, sein soll, es $(\mathfrak{a}, \mathfrak{b})$ umfassen muß. Da $(\mathfrak{a}, \mathfrak{b})$ aber selbst die Vereinigungsmenge $\mathfrak{a} \cup \mathfrak{b}$ der Ideale umfaßt, so ist jedes der oben genannten Ideale Teiler von $(\mathfrak{a}, \mathfrak{b})$ und damit die Bezeichnung größter (mengentheoretisch wenigst umfassender) gemeinsamer Teiler gerechtfertigt.

Der g.g.T. zweier Ideale $(\mathfrak{a}, \mathfrak{b})$ erfüllt die Beziehungen

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a}),$$
$$((\mathfrak{a}, \mathfrak{b}), \mathfrak{c}) = (\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})),$$
$$(\mathfrak{a}, \mathfrak{b})\,\mathfrak{c} = (\mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}).$$

Manchmal wird er symbolisch $\mathfrak{a}+\mathfrak{b}$ geschrieben. Dann drücken sich die drei Beziehungen viel durchsichtiger aus:

$$\mathfrak{a}+\mathfrak{b}=\mathfrak{b}+\mathfrak{a},$$
$$(\mathfrak{a}+\mathfrak{b})+\mathfrak{c}=\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}),$$
$$(\mathfrak{a}+\mathfrak{b})\,\mathfrak{c}=\mathfrak{a}\mathfrak{c}+\mathfrak{b}\mathfrak{c}.$$

Wir haben es also mit einer Art Addition zu tun, die das kommutative, assoziative und im Verein mit der Multiplikation das distributive Gesetz erfüllt.

Die rationale positive Primzahl p, wobei $GF(p^f)$ Restklassenkörper nach einem Primideal $\mathfrak{p}$ ist, erfüllt $p \equiv 0 \bmod \mathfrak{p}$. Sie ist durch $\mathfrak{p}$ eindeutig bestimmt.

Bemerkung: Da die Restklassengruppe additiv betrachtet nach einem Ideal $\mathfrak{a}$ genau $\mathfrak{a}^N$ Elemente hat, so ist $\mathfrak{a}^N \equiv 0 \bmod \mathfrak{a}$. Denn $\mathfrak{a}^N$ ist die Gruppenordnung.

§ 33. Die eindeutige Zerlegbarkeit in Primideale

Satz 1. *Zu jedem ganzen Ideal $\mathfrak{a}$ gibt es ein ganzes Ideal $\mathfrak{b}$, so daß $\mathfrak{a}\mathfrak{b}=(a)$ gilt, wobei a eine natürliche Zahl ist.*

Beweis: Es sei $\mathfrak{a}=(\xi_1,\ldots,\xi_0)$, ϑ eine erzeugende ganze Zahl von k über P, $\xi_i=\xi_i^{(1)}$. Die Anordnung (A) werde nicht vorausgesetzt. Ferner sei $\xi_i=r_i(\vartheta)$ mit $r_i(x)$ als rationalzahligem Polynom; sodann bilden wir das Polynom $g(x)=\xi_l x^l+\cdots+\xi_0$, und setzen

$$h(x)=\prod_{j=2}^{n}\{\xi_l^{(j)}x^l+\cdots+\xi_0^{(j)}\}.$$

Im Polynom

$$F(x)=g(x)\,h(x)=c_{l+m}\,x^{l+m}+\cdots+c_0$$

sind die Koeffizienten rational als symmetrische Funktionen der $\xi_i^{(j)}$ bezüglich j $(1\leqq j\leqq n)$ und ganz, da die elementarsymmetrischen Funktionen der $\xi_i^{(j)}$ ganz sind. Mit

$$h(x)=\eta_m x^m+\cdots+\eta_0$$

liegen die η_j in $k^{(1)}$, da

$$h(x)=\frac{F(x)}{g(x)}$$

ist, weiter sind sie ganz, da die $\xi_i^{(j)}$ es sind.

Mit $\mathfrak{b} = (\eta_m, \ldots, \eta_0)$ gilt dann, wie gezeigt werden soll,

$$\mathfrak{a}\mathfrak{b} = (a),$$

wobei $a = (c_{l+m}, \ldots, c_0)$ ist.
Wir brauchen nur zu zeigen:
1. Es gibt ganze Zahlen a_{ij}, so daß

$$a = \sum_{i,j} a_{ij} \xi_i \eta_j$$

ist.
2. Es ist $\xi_i \eta_j = \lambda_{ij} a$ mit λ_{ij} ganz.
Die erste Behauptung folgt fast sofort aus der Existenz ganzer rationaler Zahlen x_j mit

$$a = x_{l+m} c_{l+m} + \cdots + x_0 c_0,$$

da

$$c_j = \sum_{\lambda+\mu=j} \xi_\lambda \eta_\mu$$

ist.
Die zweite Behauptung folgt aus dem Satz 5 in § 30.

Satz 2. *Gilt für ganze Ideale* $\mathfrak{a}$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ *die Idealgleichung* $\mathfrak{a}\mathfrak{c}_1 = \mathfrak{a}\mathfrak{c}_2$, *so ist* $\mathfrak{c}_1 = \mathfrak{c}_2$.

Beweis: Multiplikation mit $\mathfrak{b}$, wie es im Beweise von Satz 1 vorkommt, gibt $a\mathfrak{c}_1 = a\mathfrak{c}_2$, daraus $\mathfrak{c}_1 = \mathfrak{c}_2$.

Satz 3. *Gilt für ganze Ideale* $\mathfrak{a} \mid \mathfrak{c}$, *so gibt es ein ganzes Ideal* $\mathfrak{d}$ *mit* $\mathfrak{c} = \mathfrak{a}\mathfrak{d}$.

Beweis: Es ist $\mathfrak{b}\mathfrak{c} \equiv 0 \bmod (a)$, also $\mathfrak{b}\mathfrak{c} = a\mathfrak{d}$ mit ganzem $\mathfrak{d}$, oder $\mathfrak{b}\mathfrak{c} = \mathfrak{a}\mathfrak{b}\mathfrak{d}$, also haben wir nach Satz 2 $\mathfrak{c} = \mathfrak{a}\mathfrak{d}$.
Satz 3 kann auch wie folgt ausgesprochen werden:

Satz 4. *Für ganze Ideale gilt* $\mathfrak{a} \mid \mathfrak{c}$ *oder* $\mathfrak{c} \equiv 0$ *mod* $\mathfrak{a}$ *dann und nur dann, wenn es ein ganzes Ideal* $\mathfrak{d}$ *mit* $\mathfrak{c} = \mathfrak{a}\mathfrak{d}$ *gibt.*

Die Sätze 2 und 3 übertragen sich ohne weiteres auf gebrochene Ideale (bei denen die ganzen Ideale ein Spezialfall der gebrochenen sind).

Satz 5. *Gilt für Ideale* $\mathfrak{a}$, $\mathfrak{c}_1$, $\mathfrak{c}_2$, *daß* $\mathfrak{a}\mathfrak{c}_1 = \mathfrak{a}\mathfrak{c}_2$ *ist, so ist* $\mathfrak{c}_1 = \mathfrak{c}_2$.

Beweis: Es ist $\mathfrak{a} = \frac{\mathfrak{a}_1}{A}$, $\mathfrak{c}_1 = \frac{\mathfrak{c}_{11}}{C_1}$, $\mathfrak{c}_2 = \frac{\mathfrak{c}_{12}}{C_2}$ mit A, C_1, C_2 als natürlichen Zahlen, $\mathfrak{a}_1, \mathfrak{c}_{11}, \mathfrak{c}_{12}$ als ganzen Idealen.
Aus

$$\frac{\mathfrak{a}_1}{A} \frac{\mathfrak{c}_{11}}{C_1} = \frac{\mathfrak{a}_1 \mathfrak{c}_{12}}{A C_2}$$

folgt

$$C_2 \mathfrak{c}_{11} \mathfrak{a}_1 = C_1 \mathfrak{c}_{12} \mathfrak{a}_1,$$

d. h. nach Satz 2

$$C_2 \mathfrak{c}_{11} = C_1 \mathfrak{c}_{12}$$

oder

$$\frac{\mathfrak{c}_{11}}{C_1} = \frac{\mathfrak{c}_{12}}{C_2},$$

d. h.

$$\mathfrak{c}_1 = \mathfrak{c}_2.$$

Satz 6. *Gilt für Ideale* $\mathfrak{a} \mid \mathfrak{c}$, *so gibt es genau ein ganzes Ideal* $\mathfrak{b}$ *mit* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

Beweis: Sei $\mathfrak{a} = \frac{\mathfrak{a}_1}{A}$, $\mathfrak{c} = \frac{\mathfrak{c}_1}{C}$, wobei A, C natürliche Zahlen, $\mathfrak{a}_1$ und $\mathfrak{c}_1$ ganze Ideale sind. Es ist $\frac{\mathfrak{a}_1}{A} \geqq \frac{\mathfrak{c}_1}{C}$, also $C\mathfrak{a}_1 \geqq A\mathfrak{c}_1$, somit gibt es ein ganzes Ideal $\mathfrak{b}$ mit $A\mathfrak{c}_1 = C\mathfrak{a}_1\mathfrak{b}$, und es wird $\frac{\mathfrak{c}_1}{C} = \frac{\mathfrak{a}_1}{A}\mathfrak{b}$ oder $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Nach Satz 2 ist $\mathfrak{b}$ eindeutig.

Satz 7. *Zu jedem Ideal* $\mathfrak{a}$ *gibt es ein Ideal* $\mathfrak{a}^{-1}$ *(und nach Satz 6 nur eines) mit* $\mathfrak{a}\mathfrak{a}^{-1} = (1)$ *(Einheitsideal).*

Beweis: $\mathfrak{a}\mathfrak{b} = (a)$ mit a als natürlicher Zahl ergibt $\mathfrak{a}\frac{\mathfrak{b}}{a} = (1)$. Das Ideal $\frac{\mathfrak{b}}{a}$ erfüllt die Bedingungen, die der Satz für $\mathfrak{a}^{-1}$ stellt. Es folgt

Satz 8. *Die vom Nullideal verschiedenen (ganzen und gebrochenen) Ideale bilden bezüglich Multiplikation eine Gruppe.*

Aus Satz 3 dieses Paragraphen, sowie aus Satz 16 in § 32 kann gefolgert werden:

Satz 9. *Jedes von* (1) *verschiedene ganze Ideal, das kein Primideal ist, ist als Produkt zweier oder mehrerer Primideale darstellbar.*

Beweis: Jedenfalls hat das Ideal, es heiße $\mathfrak{a}$, ein Primideal $\mathfrak{p}$ als Teiler. Das Ideal $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}^{-1}$ ist ein ganzes Ideal. Es ist aber $\mathfrak{a}_1^N < \mathfrak{a}^N$, denn es gibt durch $\mathfrak{a}_1$ teilbare Zahlen, die nicht in $\mathfrak{a}$ liegen. Andernfalls fiele ja $\mathfrak{a}_1$ mit $\mathfrak{a}$ zusammen; wir hätten $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ und nach Satz 5 wäre $(1) = \mathfrak{p}^{-1}$, also $\mathfrak{p} = (1)$, was ausgeschlossen ist. Wir bekommen eine eigentlich abnehmende Folge positiver ganzer Zahlen

$$\mathfrak{a}^N > \mathfrak{a}_1^N > \mathfrak{a}_2^N > \ldots,$$

die abbrechen muß. $\mathfrak{a}_2$ geht aus $\mathfrak{a}_1$ wie $\mathfrak{a}_1$ aus $\mathfrak{a}$ hervor.
Wir erhalten eine Zerlegung $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_s$. Es ist die Frage, ob eine andere Zerlegung $\mathfrak{a} = \mathfrak{q}_1 \ldots \mathfrak{q}_t$ im wesentlichen (d. h. bis auf die Reihenfolge) damit übereinstimmt.

Wir wollen also als Analogon zum Satz von der eindeutigen Zerlegbarkeit in Primzahlen, der in P gilt, den Satz von der eindeutigen Zerlegbarkeit von Idealen in Primideale, kurz Z.P.I. genannt, herleiten.

Der Z.P.I. gilt jedenfalls für Primideale. Als Induktionsvoraussetzung werde er als richtig angenommen für Ideale, die sich in weniger als s Primideale zerlegen lassen. Dann ist $s \leqq t$ anzunehmen. Wegen $\mathfrak{p}_1 \mid \mathfrak{q}_1 \ldots \mathfrak{q}_t$ ist $\mathfrak{p}_1$ Teiler eines $\mathfrak{q}_j$, fällt also mit einem $\mathfrak{q}_j$ zusammen. Durch Umnumerierung kann dies als $\mathfrak{q}_1$ angenommen werden. Also $\mathfrak{q}_1 = \mathfrak{p}_1$, $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s = \mathfrak{p}_1\mathfrak{q}_2 \ldots \mathfrak{q}_t$,

somit $$\mathfrak{p}_2 \ldots \mathfrak{p}_t = \mathfrak{q}_2 \ldots \mathfrak{q}_t,$$

d. h. die $\mathfrak{p}_2, \ldots, \mathfrak{p}_s$ stimmen nach der Induktionsvoraussetzung bis auf die Reihenfolge mit den $\mathfrak{q}_2, \ldots, \mathfrak{q}_t$ überein. Es muß auch $s = t$ sein. Wir haben damit den Z.P.I.:

Satz 10. *Jedes Ideal ist im wesentlichen eindeutig als Primidealprodukt darstellbar.*

Der Satz überträgt sich sofort auf gebrochene Ideale.

Die Zusammenfassung der gleichen Primidealfaktoren in Potenzen gibt die kanonische Zerlegung

$$\mathfrak{a} = \prod \mathfrak{p}_i^{a_i},$$

wobei die a_i bei ganzem $\mathfrak{a}$ durchweg natürliche Zahlen, bei einem gebrochenen Ideal auch teilweise negative ganze rationale Zahlen sind.

Der Z.P.I. gestattet eine wesentliche Vereinfachung der Rechnung bei Bildung einer Potenz eines Ideals mit natürlichem Exponenten.

Satz 11. *Ist zunächst $\mathfrak{a}$ ein ganzes Ideal, und zwar*

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_s),$$

so ist, wenn m eine natürliche Zahl ist,

$$\mathfrak{a}^m = (\alpha_1{}^m, \ldots, \alpha_s{}^m).$$

Beweis: Es sei

$$(\alpha_j) = \prod_{k=1}^{t} \mathfrak{p}_k^{a_{jk}}$$

die kanonische Zerlegung, so gilt mit

$$\min (a_{1k}, \ldots, a_{sk}) = a_k$$

für $\mathfrak{a}$ die kanonische Zerlegung

$$\mathfrak{a} = \prod_{k=1}^{t} \mathfrak{p}_k^{a_k}.$$

Daher hat $\mathfrak{a}^m$ die kanonische Zerlegung

$$\mathfrak{a}^m = \prod_{k=1}^{t} \mathfrak{p}_k^{m a_k},$$

und es gilt

$$m a_k = \min\ (m a_{1k}, \ldots, m a_{sk}),$$

wir erhalten

$$\mathfrak{a}^m = (\alpha_1^m, \ldots, \alpha_s^m).$$

Für den Fall eines gebrochenen Ideals beweist man den Satz durch den Ansatz $\mathfrak{a} = \frac{\mathfrak{b}}{A}$, $\mathfrak{b}$ ganzes Ideal, A natürliche Zahl.

§ 34. Modulbasis und kanonische Darstellung, Zerlegung in Primideale

Wir gehen aus von einem Modul $\mathfrak{a}$ aus Körperzahlen, der nicht aus Null allein bestehe, und endlich - gliedrig sei. Weiter habe $\mathfrak{a}$ die folgenden Eigenschaften: Mit α gehöre auch $\eta\alpha$ zu $\mathfrak{a}$, wobei η beliebig ganz in k ist, es sei M eine natürliche Zahl, so daß $M\mathfrak{a}$ nur aus ganzen Zahlen des Körpers besteht.

Satz 1. *Der so definierte Modul* $\mathfrak{a}$ *gestattet eine Basisdarstellung* $[\alpha_1, \ldots, \alpha_n]$ *mit n linear unabhängigen Basiselementen* α_j.

Das heißt: Jedes $\gamma = \sum_{j=1}^{n} h_j \cdot \alpha_j$ mit ganzen rationalen h_j gehört zu $\mathfrak{a}$; ist mindestens ein h_j nicht ganz, aber alle h_j rational, so gehört γ nicht zu $\mathfrak{a}$.

Beweis: Wir können annehmen: $\mathfrak{a}$ bestehe aus lauter ganzen Zahlen. Andernfalls betrachten wir $M\mathfrak{a}$ statt $\mathfrak{a}$.

I. Es gibt in $\mathfrak{a}$ ein System von n linear unabhängigen Zahlen. Denn ist $\alpha \neq 0$ in $\mathfrak{a}$, weiter $\eta_1, \ldots, \eta_n$ ein System linear unabhängiger ganzer Zahlen in k, so ist $\alpha\eta_1, \ldots, \alpha\eta_n$ ein System linear unabhängiger ganzer Zahlen in $\mathfrak{a}$.

II. Ein System solcher Zahlen $[\alpha_1, \ldots, \alpha_n]$, wobei $|\Delta(\alpha_1, \ldots, \alpha_n)|$ den Minimalwert von $|\Delta(\xi_1, \ldots, \xi_n)|$ mit den ξ_j als linear unabhängig in $\mathfrak{a}$ annimmt, erfüllt die Behauptungen unseres Satzes.

Zunächst liegen alle $\sum_{j=1}^{n} h_j \alpha_j$ in $\mathfrak{a}$, wenn alle Zahlen ganz rational sind. Weiter ist durch $\sum_{j=1}^{n} x_j \alpha_j$ mit rationalen (nicht mehr notwendig ganzen) x_j jede Zahl des Körpers erfaßt. Zu zeigen bleibt, daß

$$\alpha = \sum_{j=1}^{n} h_j \alpha_j$$

mit rationalen h_j, die nicht alle ganz sind, nicht in $\mathfrak{a}$ liegt. Keine Einschränkung der Allgemeinheit ist die Annahme: h_1 ist nicht ganz. Sei $[h_1] = g$. Wir nehmen an: α liege doch in $\mathfrak{a}$. Dann liegt $\beta = \alpha - g\alpha_1 = r\alpha_1 + h_2\alpha_2 + \cdots + h_n\alpha_n$ in $\mathfrak{a}$. Hier ist

$$0 < r < 1.$$

Wir haben

$$|\Delta(\beta, \alpha_2, \ldots, \alpha_n)| = \begin{vmatrix} r & h_2 & \ldots & h_n \\ 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \ldots & \cdot \\ 0 & 0 & \ldots & 1 \end{vmatrix}^2 |\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$$

$$= r^2 |\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)| < |\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|.$$

Wir sind also zu einem Widerspruch gelangt.

Bezeichnen wir nun mit $\mathfrak{a}^* = (\alpha_1, \ldots, \alpha_n)$ das Ideal, das g.g.T. aller α_j ist, so gilt mengentheoretisch

$$\mathfrak{a} \subseteq \mathfrak{a}^*.$$

Es ist aber auch umgekehrt $\mathfrak{a}^* \subseteq \mathfrak{a}$,

denn es liegt mit α_1 auch $\alpha_1\xi_1$ in $\mathfrak{a}$, wenn ξ_1 beliebig ganz ist, ebenso $\alpha_2\xi_2$ mit ξ_2 beliebig ganz, ..., kurz jedes Element $\alpha_1\xi_1 + \cdots + \alpha_n\xi_n$ von $\mathfrak{a}^*$ liegt in $\mathfrak{a}$. Mithin gilt

$$\mathfrak{a}^* = (\alpha_1, \ldots, \alpha_n) = \mathfrak{a}.$$

Damit haben wir die Existenz einer *Modulbasis* $[\alpha_1, \ldots, \alpha_n]$ *des Ideals* nachgewiesen.

Ist α der Vektor der Modulbasis, $\mathfrak{A}$ eine beliebige n-reihige quadratische Matrix mit ganzen rationalen Zahlen als Elementen und als $|\mathfrak{A}| = 1$, so ist $\mathfrak{A}\alpha$ der Vektor einer anderen Modulbasis.

Im folgenden seien die Ideale ganz. Die Ergebnisse übertragen sich teilweise auf gebrochene Ideale.

Satz 2. *Jedes ganze Ideal* $\mathfrak{a}$ *hat eine kanonische Modulbasis*

$$[a_{11}\omega_1,\ a_{21}\omega_1 + a_{22}\omega_2,\ \ldots,\ a_{n1}\omega_1 + \cdots + a_{nn}\omega_n]$$

mit ganzen rationalen a_{ij} *und durchweg* $a_{ii} > 0$.

Beweis: Jeder Modul des Körpers $x_1\omega_1 + \cdots + x_m\omega_m$ hat Zahlen des Ideals mit $x_m \neq 0$, z. B. $\mathfrak{a}^N\omega_m$. Sei $a_{mm} = \min |x_m|$. Die $\alpha_j = a_{j1}\omega_1 + \cdots + a_{jj}\omega_j$ bilden dann schon eine Modulbasis des Ideals.

Denn erstens sind sie linear unabhängig wegen

$$\Delta(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} a_{11} & 0 & \ldots & 0 \\ a_{21} & a_{22} & \ldots & 0 \\ \cdot & \cdot & \ldots & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 d = d \prod a_{ii}^2 \neq 0.$$

Nun sei $\alpha = \sum_{j=1}^{n} b_j\omega_j$ Element von $\mathfrak{a}$; die b_j sind ganz rational.

Mit $b_n = q_n a_{nn} + r_n$, $0 \leqq r_n < a_{nn}$, gehört

$$\alpha - q_n\alpha_n = b_1'\omega_1 + \cdots + b_{n-1}'\omega_{n-1} + r_n\omega_n,$$

wobei die b_j' ganz rational sind, zu $\mathfrak{a}$, also ist $r_n = 0$.

Es bleibt $b_n \equiv 0 \bmod a_{nn}$, analog $b_{n-1}' \equiv 0 \bmod a_{n-1,n-1}$, $\alpha - q_n\alpha_n - q_{n-1}\alpha_{n-1} = b_1''\omega_1 + \cdots + b_{n-2}''\omega_{n-2}$ usf., schließlich

$$\alpha - q_n\alpha_n - q_{n-1}\alpha_{n-1} - \ldots - q_1\alpha_1 = 0$$

mit ganzen rationalen q_j.

Satz 3. *Die so definierte Zahl* $|\Delta(\alpha_1, \ldots, \alpha_n)|$ *ist* $(\mathfrak{a}^N)^2\,|d|$.

Beweis: Es hat sich $\Delta(\alpha_1, \ldots, \alpha_n) = d\prod a_{ii}^2$ ergeben. Es genügt $\prod a_{ii} = \mathfrak{a}^N$ zu beweisen. Hierzu zeigen wir: $\sum_{j=1}^{n} r_j\omega_j$ mit $0 \leqq r_j < a_{jj}$ ist ein volles Restsystem mod $\mathfrak{a}$ (r_j ganz rational).

I. $$\sum_{j=1}^{n} r_j\omega_j \equiv \sum_{j=1}^{n} r_j'\omega_j \bmod \mathfrak{a}.$$

hätte zur Folge:

$$\pm \sum_{j=1}^{n-1} (r_j - r_j')\,\omega_j + |r_n - r_n'|\,\omega_n \equiv 0 \bmod \mathfrak{a}, \quad \text{also} \quad r_n = r_n',$$

worauf ebenso weiter geschlossen werden kann. Wir haben also $\prod a_{ii}$ verschiedene Restklassen.

II. Für jede ganze Körperzahl $\eta = x_1\omega_1 + \cdots + x_n\omega_n$ folgt mit $x_n = h_n a_{nn} + r_n$ und $0 \leqq r_n < a_{nn}$

$$\eta - h_n\alpha_n = x_1'\omega_1 + \cdots + x_{n-1}'\omega_{n-1} + r_n\omega_n,$$

und weiter

$$x_1'\omega_1 + \cdots + x_{n-1}'\omega_{n-1} - h_{n-1}\alpha_{n-1} = x_1''\omega_1 + \cdots + x_{n-2}''\omega_{n-2} + r_{n-1}\omega_{n-1},$$

wobei

$$x_{n-1}' = h_{n-1}a_{n-1,\,n-1} + r_{n-1},\ 0 \leqq r_{n-1} < a_{n-1,\,n-1}$$

ist, usf., schließlich

$$\eta \equiv r_1\omega_1 + \cdots + r_n\omega_n \bmod \mathfrak{a}.$$

Satz 4. *Ist* $[\alpha_1, \ldots, \alpha_n]$ *eine Modulbasis des Ideals* $\mathfrak{a}$, *weiter*

$$\alpha_k = \sum_{l=1}^{n} c_{kl}\,\omega_l,$$

so gilt abs $|c_{kl}|$ *(Determinante!)* $= \mathfrak{a}^N$.

Beweis: $\Delta(\alpha_1, \ldots, \alpha_n) = |c_{kl}|^2\, d = (\mathfrak{a}^N)^2 d$.

Satz 5. *Ist* $\alpha \neq 0$ *ganz,* $\mathfrak{a} = (\alpha)$, *also* $\mathfrak{a}$ *ein Hauptideal, so ist* $\mathfrak{a}^N = |\alpha^N|$.

Beweis: $\alpha\omega_k$ ist offenbar Element einer Modulbasis von $\mathfrak{a} = (\alpha)$. Weiter gilt

$$(\mathfrak{a}^N)^2 d = \Delta(\alpha\omega_1, \ldots, \alpha\omega_n) = \begin{vmatrix} \alpha^{(1)}\omega_1^{(1)} & \cdots & \alpha^{(1)}\omega_n^{(1)} \\ \cdots & \cdots & \cdots \\ \alpha^{(n)}\omega_1^{(n)} & \cdots & \alpha^{(n)}\omega_n^{(n)} \end{vmatrix}^2$$

$$= (\alpha^N)^2 \begin{vmatrix} \omega_1^{(1)} & \cdots & \omega_n^{(1)} \\ \cdots & \cdots & \cdots \\ \omega_1^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2 = (\alpha^N)^2 d,$$

also, da d von Null verschieden ist,

$$(\mathfrak{a}^N)^2 = (\alpha^N)^2,$$

und da $\mathfrak{a}^N$ eine natürliche Zahl ist

$$\mathfrak{a}^N = |\alpha^N|.$$

Wir wollen einige Bezeichnungen einführen: Ist $\mathfrak{a}$ ein Ideal, $\mathfrak{p}$ ein Primideal und kommt in der kanonischen Zerlegung von $\mathfrak{a}$ das Primideal $\mathfrak{p}$ mit dem Exponenten a vor, so schreiben wir analog wie bei Primzahlen im Körper der rationalen Zahlen $\mathfrak{p}^a \parallel \mathfrak{a}$, gelesen: $\mathfrak{p}$ geht genau zur a-ten Potenz in $\mathfrak{a}$ auf. Ist $\mathfrak{a}$ ein ganzes Ideal und $a > 0$, so ist dies mit $\mathfrak{a} \equiv 0 \bmod \mathfrak{p}^a$, $\not\equiv 0 \bmod \mathfrak{p}^{a+1}$ gleichbedeutend. Analog gelte bei Zahlen $\mathfrak{p}^a \parallel \alpha$ gleichbedeutend mit $\mathfrak{p}^a \parallel (\alpha)$. $\mathfrak{p}^0 \parallel \mathfrak{a}$ bzw. α ist gleichbedeutend damit, daß in der kanonischen Zerlegung von $\mathfrak{a}$ bzw. α das Primideal $\mathfrak{p}$ nicht vorkommt. Eine Primzahl π nach $\mathfrak{p}$ ist eine ganze Zahl $\equiv 0 \bmod \mathfrak{p}$, $\not\equiv 0 \bmod \mathfrak{p}^2$. Es gilt also $\mathfrak{p} \parallel \pi$. Solche Primzahlen π nach $\mathfrak{p}$ gibt es, denn jede von der Nullklasse verschiedene Nullteilerrestklasse $\bmod \mathfrak{p}^2$ besteht aus lauter solchen Zahlen.

Der größte gemeinsame Teiler zweier Ideale $(\mathfrak{a}, \mathfrak{b})$ mit

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_n), \quad \mathfrak{b} = (\beta_1, \ldots, \beta_\iota)$$

besteht aus allen Zahlen $\sum \alpha_i \xi_i + \sum \beta_j \eta_j$, wobei ξ_i, η_j beliebige ganze Zahlen des Körpers sind. Er besteht also aus der Gesamtheit aller Zahlen $\alpha + \beta$, wobei α beliebig in $\mathfrak{a}$, β beliebig in $\mathfrak{b}$ ist. Die vorübergehend eingeführte Schreibweise $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ setzt dies besonders schön in Evidenz.

Ist für den g.g.T. zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$

$$(\mathfrak{a}, \mathfrak{b}) = (1),$$

so heißen die Ideale zueinander *relativ prim* oder *teilerfremd*. Dies ist genau dann der Fall, wenn in den kanonischen Zerlegungen der beiden Ideale

$$\mathfrak{a} = \prod \mathfrak{p}_i^{a_i}, \quad \mathfrak{b} = \prod \mathfrak{q}_i^{b_j}$$

jedes $\mathfrak{p}_i$ von jedem $\mathfrak{q}_j$ verschieden ist, und alle $a_i \geqq 0$, $b_j \geqq 0$ sind.

Bemerkung: Ist z. B. ein $a_i < 0$, so kann dieser Fall nicht eintreten, denn dann enthält $\mathfrak{a}$ auch gebrochene Zahlen, der größte gemeinsame Teiler der beiden Ideale, der ja mengentheoretisch umfassender als jedes der Ideale ist, kann dann nicht (1) sein, was ja die Gesamtheit der ganzen Zahlen des Körpers ist. Da wir überflüssige Ideale (solche $\mathfrak{p}$ mit $\mathfrak{p}^0 \parallel \mathfrak{a}$) in der kanonischen Zerlegung nicht beizusetzen pflegen, so bezieht sich das $\geqq 0$ nur auf den Fall, daß $\mathfrak{a}$ oder $\mathfrak{b}$ (oder ganz trivialerweise beide) das Einheitsideal sind.

Also sagt $(1) = (\mathfrak{a}, \mathfrak{b})$ von selbst weiter aus: $\mathfrak{a}$ und $\mathfrak{b}$ sind beide ganze Ideale. Daher hat dies zur Folge: es gibt ganze Zahlen $\alpha \equiv 0 \bmod \mathfrak{a}$, $\beta \equiv 0 \bmod \mathfrak{b}$ mit $\alpha + \beta = 1$.

Wir verstehen unter einem *vollständigen Restsystem* mod $\mathfrak{a}$ die Gesamtheit der Restklassen von $\mathfrak{a}$. Das vollständige Restsystem bildet bezüglich Addition als Komposition eine abelsche Gruppe mit der Nullklasse als Einselement. Die Nullklasse ist hierbei die Klasse der durch $\mathfrak{a}$ teilbaren Zahlen. Die Ordnung der Gruppe ist $\mathfrak{a}^N$. Wir können uns ein volles Restsystem durch Repräsentanten der Restklassen

$$\xi_1 \equiv 0,\ \xi_2,\ \xi_3,\ \ldots,\ \xi_{\mathfrak{a}^N}$$

gegeben denken.

Es seien nun $\mathfrak{a}$, $\mathfrak{b}$ zwei Ideale mit $(\mathfrak{a}, \mathfrak{b}) = (1)$, also $\mathfrak{a}$, $\mathfrak{b}$ ganze Ideale. Es gibt dann Zahlen $\alpha \equiv 0 \bmod \mathfrak{a}$, $\beta \equiv 0 \bmod \mathfrak{b}$, $\alpha + \beta = 1$. Wir bilden die Ausdrücke $\alpha\eta + \xi$, wobei η ein volles Restsystem mod $\mathfrak{b}$, ξ ein volles Restsystem mod $\mathfrak{a}$ durchläuft, das sind formal $\mathfrak{a}^N \mathfrak{b}^N$ Zahlen. Wir behaupten: Keine zwei dieser Zahlen sind mod $\mathfrak{a}\mathfrak{b}$ kongruent. Denn wäre $\alpha\eta + \xi \equiv \alpha\eta' + \xi' \bmod \mathfrak{a}\mathfrak{b}$, so folgte zunächst wegen $\alpha \equiv 0 \bmod \mathfrak{a}$, wenn man die Kongruenz als solche mod $\mathfrak{a}$ auffaßt, daß $\xi \equiv \xi' \bmod \mathfrak{a}$, also $\xi = \xi'$ ist. Weiter ist $\alpha \equiv 1 \bmod \mathfrak{b}$, also gibt Auffassung der Kongruenz als solche mod $\mathfrak{b}$, daß $\alpha\eta \equiv \alpha\eta' \bmod \mathfrak{b}$, $\eta \equiv \eta' \bmod \mathfrak{b}$, $\eta = \eta'$ ist. Also sind in der Tat diese $\mathfrak{a}^N \mathfrak{b}^N$ Zahlen alle untereinander inkongruent mod $\mathfrak{a}\mathfrak{b}$.

Ist nun γ eine beliebige ganze Zahl des Körpers, $\gamma \equiv \xi_1 \bmod \mathfrak{a}$, $\gamma - \alpha\eta_1 \equiv \xi_1 \bmod \mathfrak{b}$, wobei ξ_1, η_1 den Systemen der ξ und η entnommen sind, so folgt $\gamma \equiv \alpha\eta_1 + \xi_1 \bmod \mathfrak{a}\mathfrak{b}$. Denn es ist $\gamma - \alpha\eta_1 - \xi_1$ durch $\mathfrak{a}$ und $\mathfrak{b}$, also durch ihr Produkt $\mathfrak{a}\mathfrak{b}$ teilbar. Es ist also durch $\alpha\eta + \xi$ jede Restklasse von $\mathfrak{a}\mathfrak{b}$ erfaßt, diese Zahlen repräsentieren die $(\mathfrak{a}\mathfrak{b})^N$ Restklassen von $\mathfrak{a}\mathfrak{b}$. Es ist also für $(\mathfrak{a}, \mathfrak{b}) = (1)$ die Beziehung $(\mathfrak{a}\mathfrak{b})^N = \mathfrak{a}^N \mathfrak{b}^N$ erfüllt. Wir erhalten

Satz 6. *Ist* $(\mathfrak{a}, \mathfrak{b}) = (1)$, *so ist die Norm des Produkts der beiden Ideale* $\mathfrak{a}$, $\mathfrak{b}$ *gleich dem Produkte der Normen*; *in Formeln*:

$$(\mathfrak{a}\mathfrak{b})^N = \mathfrak{a}^N \mathfrak{b}^N \text{ oder } N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\, N(\mathfrak{b}).$$

Zugleich sehen wir, daß mit der Unbekannten σ das Simultansystem der Kongruenzen $\sigma \equiv \lambda \bmod \mathfrak{a}$, $\sigma \equiv \mu \bmod \mathfrak{b}$ eine Lösung mod $\mathfrak{a}\mathfrak{b}$ hat, wenn λ, μ gegebene ganze Zahlen sind, sofern $(\mathfrak{a}, \mathfrak{b}) = (1)$ ist. Denn ist $\lambda \equiv \xi_1 \bmod \mathfrak{a}$, $\mu \equiv \eta_1 \bmod \mathfrak{b}$, so entspricht $\sigma \equiv \alpha\eta_1 + \xi_1 \bmod \mathfrak{a}\mathfrak{b}$ der Aufgabe, und nur diese eine Lösung ist da. Das überträgt sich sofort auf ein Simultansystem von m Kongruenzen $\sigma \equiv \lambda_1 \bmod \mathfrak{a}_1$, $\sigma \equiv \lambda_2 \bmod \mathfrak{a}_2$, $\ldots$,

$\sigma \equiv \lambda_m \bmod \mathfrak{a}_m$, wenn nur die (ganzen) Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ paarweise teilerfremd sind, das heißt stets $(\mathfrak{a}_i, \mathfrak{a}_j) = (1)$ für $i \neq j$ ist. Wir haben

Satz 7. *Sind die ganzen Ideale $\mathfrak{a}_i$ paarweise teilerfremd und das System von Simultankongruenzen $\sigma \equiv \lambda_1 \bmod \mathfrak{a}_1, \ldots, \sigma \equiv \lambda_m \bmod \mathfrak{a}_m$ mit σ als Unbekannter gegeben, so hat das System mod $\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_m$ genau eine Lösung.*

Man dehnt manchmal den Begriff „teilerfremd" oder „relativ prim" auch auf gebrochene Ideale aus, wenn in den kanonischen Primidealzerlegungen der beiden Ideale durchweg verschiedene Primidealfaktoren vorkommen. In diesem Falle ist der größte gemeinsame Teiler der beiden Ideale nicht das Einheitsideal.

Betrachten wir nun den Restklassenring mod $\mathfrak{p}^2$, dem Quadrat eines Primideals $\mathfrak{p}$. Er enthält eigentliche (von der Nullklasse verschiedene) Nullteiler, nämlich genau die Klassen, die durch Primzahlen π nach $\mathfrak{p}$ repräsentiert werden. Lassen wir α_2 bei gegebenem π ein volles Restsystem mod $\mathfrak{p}$ durchlaufen, so ist jedes $\alpha_2 \pi$, wenn nicht $\alpha_2 \equiv 0 \bmod \mathfrak{p}$ ist, wieder eine Primzahl nach $\mathfrak{p}$. Umgekehrt wollen wir annehmen, τ' sei ein Repräsentant einer Nullteilerklasse. Es ist etwa $(\pi) = \mathfrak{p}\mathfrak{a}$, wobei $\mathfrak{a}$ zu $\mathfrak{p}$ prim, ein ganzes Ideal ist, aber kein Primideal zu sein braucht, auch z. B. das Einheitsideal sein könnte. (Eine Kongruenz nach dem Einheitsideal sagt selbstverständlich nichts aus.) Dann ist das System der Simultankongruenzen mit τ als Unbekannter $\tau \equiv \tau' \bmod \mathfrak{p}^2$, $\tau \equiv 0 \bmod \mathfrak{a}$ lösbar; es ergibt sich eine Zahl τ als Repräsentant der bezüglichen Restklasse mod $\mathfrak{p}^2$, die durch die beiden zueinander primen Ideale $\mathfrak{p}$ und $\mathfrak{a}$, also durch ihr Produkt $\mathfrak{p}\mathfrak{a} = (\pi)$ teilbar ist, es wird $\tau = \beta\pi$, wobei β eine ganze Zahl des Körpers ist. Es ist $\mathfrak{p} \parallel \tau$, also wegen $\mathfrak{p} \parallel \pi$ bleibt $\mathfrak{p}^0 \parallel \beta$, β ist zu $\mathfrak{p}$ prim, es wird etwa $\beta \equiv \alpha_2 \bmod \mathfrak{p}$, daraus $\tau \equiv \alpha_2 \pi \bmod \mathfrak{p}\pi \equiv 0 \bmod \mathfrak{p}^2$. Damit ist die Restklasse von τ', da wegen $\tau \equiv \tau' \bmod \mathfrak{p}^2$ auch $\tau' \equiv \alpha_2 \pi \bmod \mathfrak{p}^2$ gilt, im früheren System $\alpha_2 \pi$ ausgedrückt. Also: Jeder Nullteiler mod $\mathfrak{p}^2$ läßt sich durch $\alpha_2 \pi \bmod \mathfrak{p}^2$ repräsentieren, wenn π eine Primzahl nach $\mathfrak{p}$ ist, und α_2 einem gegebenen vollen Restsystem mod $\mathfrak{p}$ entnommen ist.

Lassen wir nun ebenso α_1 unabhängig von α_2 ein volles Restsystem mod $\mathfrak{p}$ durchlaufen, so ergibt der Ausdruck

$$\alpha_1 + \alpha_2 \pi$$

formal $(\mathfrak{p}^N)^2$ Zahlen; diese sind alle mod $\mathfrak{p}^2$ inkongruent. Denn ist etwa

$$\alpha_1 + \alpha_2\pi \equiv \alpha_1' + \alpha_2'\pi \bmod \mathfrak{p}^2,$$

so gibt Auffassung der Kongruenz als solcher mod $\mathfrak{p}$ sofort $\alpha_1 \equiv \alpha_1'$ mod $\mathfrak{p}$, also $\alpha_1 = \alpha_1'$. Die verbleibende Kongruenz

$$\alpha_2\pi \equiv \alpha_2'\pi \bmod \mathfrak{p}^2$$

gibt $\mathfrak{p}^2 \mid (\alpha_2 - \alpha_2')\pi$, also wegen $\mathfrak{p} \parallel \pi$, bleibt $\mathfrak{p} \mid \alpha_2 - \alpha_2'$, $\alpha_2' = \alpha_2$. Weiter gibt es bei einer beliebigen ganzen Zahl γ des Körpers zunächst eine Zahl α_1' des Systems der ξ_j mit $\gamma \equiv \alpha_1' \bmod \mathfrak{p}$. Es ist dann die Restklasse der Zahl $\gamma - \alpha_1' \bmod \mathfrak{p}^2$ im Restklassenring mod $\mathfrak{p}^2$ ein eigentlicher oder uneigentlicher Nullteiler, also in der Form $\alpha_2'\pi$ ausdrückbar, wobei α_2' dem System der ξ_j entnommen ist. Es ist $\gamma \equiv \alpha_1' + \alpha_2'\pi \bmod \mathfrak{p}^2$. Mithin ergeben diese $(\mathfrak{p}^N)^2$ Ausdrücke gerade die sämtlichen Restklassen mod $\mathfrak{p}^2$. Es ergeben sich die Sätze:

Satz 8. *Die Norm des Quadrats eines Primideals $\mathfrak{p}$ ist gleich dem Quadrat der Norm von $\mathfrak{p}$, in Formeln* $(\mathfrak{p}^2)^N = (\mathfrak{p}^N)^2$ *oder* $N(\mathfrak{p}^2) = N^2(\mathfrak{p})$.

Satz 9. *Jede Restklasse mod $\mathfrak{p}^2$ ist in der Form $\alpha_1 + \alpha_2\pi$ mod $\mathfrak{p}^2$ eindeutig darstellbar, wenn π eine Primzahl nach $\mathfrak{p}$ ist, dagegen α_1, α_2 einem vollen Restsystem mod $\mathfrak{p}$ entnommen sind.*

Nun sei die Induktionsvoraussetzung: Es sei bewiesen, daß $(\mathfrak{p}^t)^N = (\mathfrak{p}^N)^t$ ist und, daß mit den α_j als Elementen eines vollständigen Restsystems mod $\mathfrak{p}$ jede Restklasse mod $\mathfrak{p}^t$ sich als $\alpha_1 + \alpha_2\pi + \cdots + \alpha_t\pi^{t-1}$ eindeutig darstellen läßt. Nun ist zunächst, wenn wir die $(\mathfrak{p}^N)^{t+1}$ Zahlen

$$\alpha_1 + \alpha_2\pi + \cdots + \alpha_t\pi^{t-1} + \alpha_{t+1}\pi^t$$

aufstellen, fast unmittelbar klar, daß sie durchweg mod $\mathfrak{p}^{t+1}$ inkongruent sind. Denn die Annahme

$$\sum_{j=1}^{t+1} \alpha_j\pi^{j-1} \equiv \sum_{j=1}^{t+1} \alpha_j'\pi^{j-1} \bmod \mathfrak{p}^{t+1}$$

hat, wenn wir die Kongruenz mod $\mathfrak{p}^t$ lesen, unmittelbar die Gleichheit $\alpha_j = \alpha'_j$, für jedes $j \leqq t$ zur Folge. Die verbleibende Kongruenz gibt $\mathfrak{p}^{t+1} \mid \pi^t(\alpha_{t+1} - \alpha'_{t+1})$ und wegen $\mathfrak{p} \parallel \pi$ folgt

$\alpha_{t+1} \equiv \alpha'_{t+1} \bmod \mathfrak{p}$, d. h. $\alpha_{t+1} = \alpha'_{t+1}$. Nun sei γ eine beliebige ganze Zahl in k. Nach der Induktionsvoraussetzung gilt

$$\gamma \equiv \beta_1 + \cdots + \beta_t \pi^{t-1} \bmod \mathfrak{p}^t,$$

wobei die β_j irgendwelche ξ_i sind. Sei γ' die rechtsstehende Zahl, also $\gamma \equiv \gamma' \bmod \mathfrak{p}^t$. Das System der Simultankongruenzen $\sigma \equiv \gamma - \gamma' \bmod \mathfrak{p}^{t+1}$, $\sigma \equiv 0 \bmod \mathfrak{a}^{t+1}$ hat eine Lösung, die durch $\mathfrak{p}^t \mathfrak{a}^t$ (wegen $\gamma \equiv \gamma' \bmod \mathfrak{p}^t$), d. h. durch π^t teilbar ist. Mithin wird $\gamma \equiv \gamma' + \pi^t \varrho \bmod \mathfrak{p}^{t+1}$ mit ϱ als ganzer Zahl. Ist $\varrho \equiv \beta_{t+1} \bmod \mathfrak{p}$, wobei β_{t+1} dem System der ξ_j entnommen ist, so ist

$$\varrho \pi^t \equiv \beta_{t+1} \pi^t \bmod \mathfrak{p}\pi^t \equiv 0 \bmod \mathfrak{p}^{t+1}.$$

Damit ist

$$\gamma \equiv \beta_1 + \cdots + \beta_t \pi^{t-1} + \beta_{t+1} \pi^t \bmod \mathfrak{p}^{t+1}$$

nachgewiesen. Zugleich ist gezeigt: $(\mathfrak{p}^{t+1})^{\mathfrak{N}} = (\mathfrak{p}^{\mathfrak{N}})^{t+1}$. Damit sind die Sätze 8 und 9 verallgemeinert:

Satz 10. *Die Norm der t-ten Potenz eines Primideals $\mathfrak{p}$ ist gleich der t-ten Potenz der Norm. Hierbei ist t eine natürliche Zahl. In Formeln wird dies* $(\mathfrak{p}^t)^{\mathfrak{N}} = (\mathfrak{p}^{\mathfrak{N}})^t$ *oder* $N(\mathfrak{p}^t) = N^t(\mathfrak{p})$.

Satz **11.** *Jede Restklasse mod $\mathfrak{p}^t$ läßt sich eindeutig als*

$$\alpha_1 + \alpha_2 \pi + \cdots + \alpha_t \pi^{t-1}$$

darstellen, wenn eine Primzahl π nach $\mathfrak{p}$ gegeben ist. Hierbei sind die α_j ein für allemal festgesetzte Repräsentanten eines vollen Restsystems mod $\mathfrak{p}$.

Nun folgt als Verallgemeinerung von Satz 6

Satz 12. *Die Norm des Produktes zweier ganzen Ideale ist gleich dem Produkt der Idealnormen. In Formeln geschrieben heißt dies, wenn $\mathfrak{a}, \mathfrak{b}$ die beiden Ideale sind:* $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\, N(\mathfrak{b})$ *oder* $(\mathfrak{a}\mathfrak{b})^{\mathfrak{N}} = \mathfrak{a}^{\mathfrak{N}} \mathfrak{b}^{\mathfrak{N}}$.

Beweis: Satz 6 überträgt sich ohne weiteres auf das Produkt von drei oder mehr paarweise teilerfremden Idealen. Ist nun $\mathfrak{a} = \Pi \mathfrak{p}_i^{a_i}$, $\mathfrak{b} = \Pi \mathfrak{p}_i^{b_i}$, wobei wir ausnahmsweise in $\mathfrak{b}$, aber nicht in $\mathfrak{a}$ und in $\mathfrak{a}$, aber nicht in $\mathfrak{b}$ aufgehende Primideale $\mathfrak{p}_j$ mit dem Exponenten $a_j, b_j = 0$ ansetzen, so ist

$$(\mathfrak{a}\mathfrak{b})^{\mathfrak{N}} = (\prod \mathfrak{p}_i^{a_i + b_i})^{\mathfrak{N}} = \prod (\mathfrak{p}_i^{a_i + b_i})^{\mathfrak{N}} = \prod (\mathfrak{p}_i^{a_i})^{\mathfrak{N}} (\mathfrak{p}_i^{b_i})^{\mathfrak{N}} = \mathfrak{a}^{\mathfrak{N}} \mathfrak{b}^{\mathfrak{N}}.$$

Es habe die rationale Primzahl p die Zerlegung

$$(p) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_g^{e_g}.$$

Dann ist etwa $\mathfrak{p}_i^N = p^{f_i}$, also f_i der Grad von $\mathfrak{p}_i$. Die Zahl e_i (natürliche Zahl) heißt *Ordnung* von $\mathfrak{p}_i$. Normenbildung gibt (n ist wieder der Körpergrad)

$$p^n = p^{e_1 f_1} \cdots p^{e_g f_g}$$

oder

$$n = e_1 f_1 + \cdots + e_g f_g.$$

Wir haben also

Satz 13. *Die Summe der Produkte von Ordnung und Grad der Primidealteiler einer rationalen Primzahl p ist gleich dem Körpergrad.*

Nun sei wiederum p eine rationale Primzahl. Wir nehmen an, es gebe eine kanonische Basis (§ 29)

$$\omega_1 = 1, \ldots, \omega_j = \frac{a_{j1} + \cdots + a_{j,j-1}\vartheta^{j-2} + \vartheta^{j-1}}{b_j},$$

$$\ldots, \omega_n = \frac{a_{n1} + \cdots + a_{n,n-1}\vartheta^{n-2} + \vartheta^{n-1}}{b_n},$$

wobei $b_j \mid b_{j+1}$ $(b_1 = 1)$ gilt, und zwar so, daß $b_n \not\equiv 0 \bmod p$ ist. Dann ist von selbst $b_j \not\equiv 0 \bmod p$, wenn $j < n$ ist.

$$F(x) = a_0 + \cdots + x^n$$

sei das normierte ganzzahlige irreduzible Polynom, das ϑ, eine erzeugende ganze Körperzahl als Wurzel hat. Es sei $h(x)$ in $\mathsf{P}_p[x]$ ein normierter Faktor von $F(x)$; wir ziehen nur die Fälle in Betracht, in denen $h(x)$ irreduzibel oder eine Potenz eines irreduzibeln Polynoms mit Exponenten > 1 ist. Sei

$$h(x) = c_0 + \cdots + x^f.$$

Wir bilden $\mathfrak{a} = (p, h(\vartheta))$. Untersuchen wir zunächst, ob $\mathfrak{a}$ nicht das Einheitsideal ist. Wäre dies der Fall, so müßte es eine Gleichung

$$1 = \alpha_1 p + \beta_1 h(\vartheta)$$

mit α_1, β_1 als ganzen Zahlen in k geben. Multiplikation mit b_n gibt

$$b_n = p\,a(\vartheta) + h(\vartheta)\,b(\vartheta) \tag{1}$$

mit $a(x)$, $b(x)$ als ganzzahligen Polynomen. Die in $\mathsf{P}_p[x]$ gültige Gleichung

$$F(x) = h(x)\,G(x)$$

hat eine Gleichung in $\mathsf{P}[x]$ zur Folge

$$F(x) = h(x)\,G(x) + p\,H(x)$$

mit $H(x)$ als Polynom mit nach p ganzzahligen Koeffizienten, so daß

$$h(\vartheta)\, G(\vartheta) + p\, H(\vartheta) = 0$$

gilt. Deshalb folgt aus (1)

$$G(\vartheta)\, b_n = p\big(G(\vartheta)\, a(\vartheta) - H(\vartheta)\, b(\vartheta)\big)$$

und daraus, da $G(x)$ normiert ist

$$b_n \equiv 0 \bmod p$$

im Widerspruch zur Voraussetzung.

Sei nun eine Zahl $\gamma \equiv 0 \bmod \mathfrak{a}$, $\gamma = x_1\omega_1 + \cdots + x_j\omega_j$ mit $j > f$ und $x_j \not\equiv 0$. Die Zahl a_{jj} in Satz 2 ist offenbar ein Teiler von b_j, denn es gibt Zahlen $\equiv 0 \bmod \mathfrak{a}$ mit $x_j = b_j$ z. B. $\vartheta^{j-f-1} h(\vartheta)$. Wegen $p\,\omega_j \equiv 0 \bmod \mathfrak{a}$ gilt aber offenbar auch $a_{jj} \mid p$. Da $(b_j, p) = 1$ ist, ist $a_{jj} = 1$. Damit ist die Existenz einer Teilbasis von $\mathfrak{a}$:

$$c_{f+1,1}\omega_1 + \cdots + c_{f+1,f}\ \omega_f + \omega_{f+1}, \ldots,$$
$$c_{n1}\omega_1 + \cdots + c_{n,n-1}\omega_{n-1} + \omega_n$$

sichergestellt. Hingegen kann ein Element $\gamma = x_1\omega_1 + \cdots + x_j\omega_j$ mit $j \leqq f$ nur bei Teilbarkeit aller x_j durch p zu $\mathfrak{a}$ gehören. Denn es ergibt die Zugehörigkeit von γ zu $\mathfrak{a}$ auch die von $b_j\gamma$ zu $\mathfrak{a}$ und umgekehrt, das letzte, weil $b_j \not\equiv 0 \bmod p$, $\mathfrak{a}$ ein Teiler von p ist. Wir haben, wenn $b_j\gamma = v(\vartheta)$ mit $v(\vartheta)$ als ganzzahligem Polynom in ϑ von einem Grade $j < f$ ist, eine Darstellung

$$b_j\gamma = v(\vartheta) = A(\vartheta)\, p + B(\vartheta)\, h(\vartheta)$$

mit $A(\vartheta)$ und $B(\vartheta)$ als Polynomen, deren Koeffizienten nicht notwendig ganz, aber mod p ganz sind. Das gibt wegen der Irreduzibilität von $F(x)$ eine Gleichung in $\mathsf{P}[x]$:

$$v(x) = A(x)p + B(x)\, h(x) + M(x)\, F(x) \tag{2}$$

mit $M(x)$ als Polynom, dessen Koeffizienten mod p ganz sind, und dies wieder hat in $\mathsf{P}_p[x]$ eine Gleichung

$$v(x) = B(x)\, h(x) + M(x)\, F(x) \tag{3}$$

zur Folge, die aus (2) hervorgeht, wenn man die eventuell gebrochenen, aber mod p ganzen Koeffizienten durch ihre Restklassen mod p ersetzt. Wegen der in $\mathsf{P}_p[x]$ gültigen Beziehung $h(x) \mid F(x)$ gilt aber in diesem Bereich $h(x) \mid v(x)$. Da ein eventueller Grad von $v(x)$ aber $< f$, also kleiner als der Grad von $h(x)$ wäre, so ist dies nur bei der Annahme möglich, daß $v(x)$ gar keinen

Grad hat, also das Nullpolynom ist, es sind also alle Koeffizienten von $v(x)$ in $\mathsf{P}_p[x]$ Null, alle Koeffizienten von $v(x)$ in $\mathsf{P}[x]$ sind durch p teilbar, es ist

$$x_1 \equiv x_2 \equiv x_3 \equiv \cdots \equiv x_j \equiv 0 \bmod p.$$

Da aber $p\omega_j$ in $\mathfrak{a}$ liegt, so ist $a_{jj} = p$. Damit ist eine kanonische Modulbasis des Ideals $\mathfrak{a}$ in der Gestalt

$$p\omega_1, \ldots, p\omega_f, c_{f+1,1}\omega_1 + \cdots + \omega_{f+1}, \ldots, c_{n1}\omega_1 + \cdots + \omega_n$$

nachgewiesen. Es bleibt $\mathfrak{a}^N = p^f$.
Ist nun erstens $h(x)$ irreduzibel, so ist $\mathfrak{a} = \mathfrak{p}_1$ Primideal. Denn der Restklassenring wird das Galoisfeld $GF(p^f)$.
Ist zweitens $h(x) = h_1^t(x)$, wobei $h_1(x)$ in $\mathsf{P}_p[x]$ irreduzibel ist, so ist $\mathfrak{a} \equiv 0 \bmod \mathfrak{p}_1$, wenn jetzt $\mathfrak{p}_1 = (p, h_1(\vartheta))$ ist. Es ist $\mathfrak{p}_1^t = (p^t, h_1^t(\vartheta)) = (p^t, h(\vartheta))$, mithin $\mathfrak{p}_1^t \equiv 0 \bmod \mathfrak{a}$. Es habe $h_1(x)$ den Grad f_1, es sei also $f = tf_1$.
Wegen $(\mathfrak{p}_1^t)^N = p^{tf_1} = \mathfrak{a}^N$ ist aber $\mathfrak{a} = \mathfrak{p}_1^t$.
Ist nun

$$F(x) = h_1^{e_1}(x)\, h_2^{e_2}(x) \ldots h_g^{e_g}(x)$$

die Zerlegung von $F(x)$ in $\mathsf{P}_p[x]$ in Potenzprodukte paarweise verschiedener normierter irreduzibler Faktoren, so folgt mit $\mathfrak{p}_j = (p, h_j(\vartheta))$ die Beziehung

$$p \equiv 0 \bmod \prod \mathfrak{p}_j^{e_j}.$$

Da aber mit f_j als Grad von h_j die Beziehung $\sum_{j=1}^{g} e_j f_j = n$ gilt, folgt aus Satz 12, daß weitere Primidealfaktoren von p nicht vorkommen können und stets $\mathfrak{p}_j^{e_j} \parallel p$ ist. Es bleibt der überaus wichtige

Satz 14. *Ist p eine rationale Primzahl, läßt sich eine kanonische Basis zur ganzen Körpererzeugenden ϑ angeben, so daß die dabei auftretenden Nenner b_j zu p prim sind, und ist weiter $F(x)$ das normierte ganzzahlige irreduzible Polynom mit der Wurzel ϑ, ferner*

$$F(x) = h_1^{e_1}(x)\, h_2^{e_2}(x) \ldots h_g^{e_g}(x)$$

die Zerlegung von $F(x)$ in paarweise verschiedene irreduzible Faktoren in $\mathsf{P}_p[x]$, so zerfällt

$$(p) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$$

in g Primideale der bezüglichen Ordnungen e_j. Es ist $\mathfrak{p}_j = (p, h_j(\vartheta))$, und dieses Primideal hat als Grad f_j den Grad von $h_j(x)$.

Bemerkung: Ist $\mathfrak{a} = (\alpha_1, \ldots, \alpha_q)$, so heißt $\alpha_1, \ldots, \alpha_q$ eine Idealbasis. Sie braucht keine Modulbasis zu sein. Es ist offenbar auch $\mathfrak{a} = (\alpha_1 \varepsilon_1, \ldots, \alpha_q \varepsilon_q)$, wenn die ε_i beliebige Einheiten sind. Insbesondere ist $(\alpha) = (\alpha\varepsilon)$, wenn ε Einheit ist, d. h. assoziierte Zahlen erzeugen dasselbe Hauptideal. Ist γ zu α prim, α, β, γ ganz, so ist $(\alpha, \beta) = (\alpha, \beta\gamma)$.

Nun ergibt sich sehr schnell die Primidealzerlegung einer rationalen Primzahl p im quadratischen Zahlkörper $\mathsf{P}(\sqrt{m})$, wobei m eine quadratfreie ganze rationale Zahl und von Eins verschieden ist. Wir müssen die Fälle $p > 2$ und $p = 2$ unterscheiden.

Wir haben für $m \equiv 2, 3 \bmod 4$ eine Körperbasis $[1, \sqrt{m}]$, für $m \equiv 1 \bmod 4$ hingegen eine solche $\left[1, \frac{1+\sqrt{m}}{2} = \omega\right]$. Die normierten irreduziblen ganzzahligen Polynome, von denen $\sqrt{m}$, ω Wurzeln sind, werden

1. für $\sqrt{m}$ das Polynom $F(x) = x^2 - m$,
2. für ω das Polynom $F_1(x) = x^2 - x - \frac{m-1}{4}$.

Das letzte gilt für $m \equiv 1 \bmod 4$.

Haben wir $p > 2$, so können wir, da immer p zu dem in der kanonischen Basis vorkommenden Nenner b_2 prim ist, stets $\vartheta = \sqrt{m}$ setzen. Es ist dann $F(x) = x^2 - m$.

Ist nun $\left(\frac{m}{p}\right) = 1$, also $x^2 - m \equiv (x + A)(x - A) \bmod p$, wobei A eine Lösung von $x^2 \equiv m \bmod p$ ist, so wird $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ mit $\mathfrak{p}_1 = (p, A + \sqrt{m})$, $\mathfrak{p}_2 = (p, \sqrt{m} - A) = (p, A - \sqrt{m})$. Ist hingegen $\left(\frac{m}{p}\right) = -1$, so bleibt p in k Primideal. Ist endlich $m \equiv 0 \bmod p$, also $F(x) \equiv x^2 \bmod p$, so wird $(p) = \mathfrak{p}^2$ mit $\mathfrak{p} = (p, \sqrt{m})$.

Ist $p = 2$, so kann man im Falle $m \equiv 2, 3 \bmod 4$, wobei $[1, \sqrt{m}]$ eine Basis ist, genau so vorgehen. Ist $m \equiv 2 \bmod 4$, so ist $F(x) \equiv x^2 \bmod 2$ und es wird $(2) = \mathfrak{l}^2$ mit $\mathfrak{l} = (2, \sqrt{m})$. Ist $m \equiv 3 \bmod 4$, so haben wir $F(x) \equiv (x+1)^2 \bmod 2$, und es ist $(2) = \mathfrak{l}^2$ mit $\mathfrak{l} = (2, 1 + \sqrt{m})$.

Ganz anders ist der Fall $m \equiv 1 \bmod 4$. Hier müssen wir von der Basis $[1, \omega]$ ausgehen, also $\vartheta = \omega$ setzen, für F tritt ein F_1. Ist $m \equiv 1 \bmod 8$, so ist $F_1(x) \equiv x^2 - x \equiv x(x-1) \bmod 2$, und es

wird (2) das Produkt der beiden voneinander verschiedenen Primideale: $(2) = \mathfrak{l}_1\mathfrak{l}_2$, hierbei ist $\mathfrak{l}_1 = (2, \omega)$, hingegen

$$\mathfrak{l}_2 = (2, \omega - 1) = \left(2, \frac{-1+\sqrt{m}}{2}\right) = \left(2, \frac{1-\sqrt{m}}{2}\right) = (2, \omega'),$$

wobei ω' die zu ω konjugierte Zahl ist. Ist $m \equiv 5 \bmod 8$, so ist $F_1(x) \equiv x^2 + x + 1$ in $\mathsf{P}_2[x]$ irreduzibel, und 2 bleibt Primideal.

Untersuchen wir beispielsweise die Primzahlen $\leqq 23$ im Zahlkörper $\mathsf{P}(\sqrt{-23})$. Eine Basis ist $\left[1, \omega = \frac{1+\sqrt{-23}}{2}\right]$, die Körperdiskriminante ist -23, und wir haben

1. $p = 2$, $m \equiv 1 \bmod 8$, $2 = \mathfrak{l}_1\mathfrak{l}_2$ mit $(2, \omega) = \mathfrak{l}_1$, $(2, \omega') = \mathfrak{l}_2$.

Damit $\mathfrak{l}_1$ ein Hauptideal ist, müßte $(2, \omega)^N = 2$ Norm einer ganzen Zahl des Zahlkörpers sein. Die Möglichkeit, daß -2 Norm ist, scheidet aus, da eine eigentlich komplexe Zahl stets positive Norm hat. Nun sind die ganzen Körperzahlen durch $\frac{x+y\sqrt{-23}}{2}$ mit $x \equiv y \bmod 2$, wobei x, y ganz rational sind, gegeben. Es folgte $x^2 + 23y^2 = 8$, was offenbar keine Lösungen hat. $[2, \omega]$ ist kanonische Modulbasis von $\mathfrak{l}_1$, woraus die Norm folgt.

Bemerkung: Ist $x^2 + 23y^2 \equiv 0 \bmod 4$, ohne daß x, y beide gerade, wenn also beide ungerade sind, so ist es auch durch 8 teilbar. Wollen wir also bei einer ungeraden Zahl untersuchen, ob sie Norm einer ganzen Zahl in k ist, so können wir sagen: Wenn ja, dann von einer Zahl der Form $x + y\sqrt{-23}$ mit ganzzahligen x und y. Analoges gilt für jedes $m \equiv 1 \bmod 8$.

2. $p = 3$, $\left(\frac{-23}{3}\right) = 1$, $1^2 \equiv -23 \bmod 3$, es wird

$$(3) = \mathfrak{p}_1\mathfrak{p}_2 \text{ mit } \mathfrak{p}_1 = \left(3, 1 + \sqrt{-23}\right), \mathfrak{p}_2 = \left(3, 1 - \sqrt{-23}\right).$$

Oder auch $\mathfrak{p}_1 = (3, \omega)$, $\mathfrak{p}_2 = (3, \omega')$, womit zugleich eine Modulbasis der Primideale gegeben ist. Da $x^2 + 23y^2 = 3$ rationalganzzahlig unlösbar ist, sind $\mathfrak{p}_1$ und $\mathfrak{p}_2$ keine Hauptideale.

3. $p = 5$, $\left(\frac{-23}{5}\right) = \left(\frac{2}{5}\right) = -1$; (5) bleibt Primideal.

4. $p = 7$, $\left(\frac{-23}{7}\right) = \left(\frac{-2}{7}\right) = -1$; (7) wird Primideal zweiten Grades.

5. $p = 11$, $\left(\frac{-23}{11}\right) = \left(\frac{-1}{11}\right) = -1$; (11) ist auch in k Primideal.

6. $p = 13$, $\left(\frac{-23}{13}\right) = \left(\frac{-23+39}{13}\right) = \left(\frac{16}{13}\right) = 1$. Die Kongruenz $x^2 \equiv -23 \bmod 13$ hat eine Lösung $x \equiv 4$. Wir erhalten $(13) = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1 = (13,\ 4 + \sqrt{-23})$, $\mathfrak{q}_2 = (13,\ 4 - \sqrt{-23})$ oder auch $\mathfrak{q}_1 = \left(13, \frac{9+\sqrt{-23}}{2}\right)$, $\mathfrak{q}_2 = \left(13, \frac{9-\sqrt{-23}}{2}\right)$. Wir können auch $\mathfrak{q}_1 = (13, 5 - \omega)$, $\mathfrak{q}_2 = (13, 4 + \omega)$ setzen, also $\mathfrak{q}_1 = (13, -5 + \omega)$, $\mathfrak{q}_2 = (13, 4 + \omega)$. Die letzte Idealbasis ist auch Modulbasis. Da $x^2 + 23y^2 = 13$ unlösbar ist, sind $\mathfrak{q}_1$ und $\mathfrak{q}_2$ keine Hauptideale.

7. $p = 17$, $\left(\frac{-23}{17}\right) = \left(\frac{-23+68}{17}\right) = \left(\frac{45}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = -1$. Die Primzahl 17 zerfällt nicht.

8. $p = 19$, $\left(\frac{-23}{19}\right) = \left(\frac{-4}{19}\right) = \left(\frac{-1}{19}\right) = -1$. Auch (19) bleibt Primideal.

9. $p = 23$. Es ist $(23) = (\sqrt{-23})^2$, Quadrat eines Hauptprimideals.

Ein Beispiel, in dem eine Primzahl Produkt zweier verschiedener Hauptprimideale ist: $(59) = (6 + \sqrt{-23})(6 - \sqrt{-23})$.

Die verschiedenen Fälle der Zerlegung rationaler Primzahlen im quadratischen Zahlkörper lassen sich mit Hilfe des Kronecker-Symbols (§ 21) in den übersichtlichen Satz zusammenfassen:

Satz 15. *Sei d die Diskriminante eines quadratischen Körpers, p eine rationale Primzahl. Ist $\left(\frac{d}{p}\right) = -1$, so bleibt (p) Primideal. Ist $\left(\frac{d}{p}\right) = 1$, so wird $(p) = \mathfrak{p}_1\mathfrak{p}_2$, wobei $\mathfrak{p}_1, \mathfrak{p}_2$ voneinander verschiedene Primideale ersten Grades sind. Ist $\left(\frac{d}{p}\right) = 0$, so wird $(p) = \mathfrak{p}^2$, also Quadrat eines Primideals der Ordnung Zwei und des Grades Eins.*

Als letztes Beispiel nehmen wir den kubischen Körper

$$\mathsf{P}(\vartheta) = k,$$

wobei ϑ eine Wurzel des normierten ganzzahligen irreduziblen kubischen Polynoms $f(x) = x^3 - x - 1$ ist. Die Diskriminante von ϑ ist -23. Da dies quadratfrei ist, sieht man sofort, daß -23 auch die Körperdiskriminante und $[1, \vartheta, \vartheta^2]$ eine Körperbasis

ist. Um die Zerlegungen einfacher Primzahlen zu ermitteln, bemerken wir, daß man nach ganz kurzer Rechnung erhält:

$$f(0) = -1, \qquad f(5) = 119 = 17 \cdot 7,$$
$$f(1) = -1, \qquad f(6) = 209 = 19 \cdot 11,$$
$$f(2) = 5, \qquad f(7) = 335 = 5 \cdot 67,$$
$$f(3) = 23, \qquad f(8) = 503 \text{ (Primzahl)},$$
$$f(4) = 59, \qquad f(9) = 719 \text{ (Primzahl)}.$$

Weiter

$$f(-1) = -1, \qquad f(-6) = -211 \text{ (Primzahl)},$$
$$f(-2) = -7, \qquad f(-7) = -337 \text{ (Primzahl)},$$
$$f(-3) = -25, \qquad f(-8) = -505 = -5 \cdot 101,$$
$$f(-4) = -61, \qquad f(-9) = -721 = -7 \cdot 103.$$
$$f(-5) = -121 = -11^2,$$

Nun ist $f(x) = x^3 - x - 1 \bmod 2$ und $\bmod 3$ irreduzibel, es sind also (2) und (3) in k Primideal e dritten Grades. Danach § 24 für $p > 3$, $\left(\frac{d}{p}\right) = 1$ die Kongruenz $f(x) \equiv 0 \bmod p$ entweder keine oder drei Wurzeln, für $\left(\frac{d}{p}\right) = -1$ hingegen genau eine Wurzel hat, so gilt $(d = -23)$: Es ist $\left(\frac{-23}{5}\right) = -1$, wir haben die einzige Wurzel $x \equiv 2 \bmod 5$; Division von $f(x)$ durch $(x - 2) \bmod 5$ gibt das irreduzible Polynom $x^2 + 2x + 3$. Wir haben die Zerlegung $(5) = \mathfrak{p}_1\mathfrak{p}_2$, wobei $\mathfrak{p}_1 = (5, 2 - \vartheta)$ ein Primideal ersten, $\mathfrak{p}_2 = (5, 3 + 2\vartheta + \vartheta^2)$ Primideal zweiten Grades ist. Analog ist $\left(\frac{-23}{7}\right) = -1$, wir haben die einzige Wurzel $x \equiv -2$ und $(7) = \mathfrak{q}_1\mathfrak{q}_2$ mit $\mathfrak{q}_1 = (7, 2 + \vartheta)$ als Primideal ersten, $\mathfrak{q}_2 = (7, 3 - 2\vartheta + \vartheta^2)$ als Primideal zweiten Grades. Man sieht auch: 13 bleibt Primideal, übereinstimmend mit $\left(\frac{-23}{13}\right) = 1$. Ich wiederhole: aus $\left(\frac{d}{p}\right) = 1$ kann man nur ersehen, daß (p) entweder Primideal bleibt oder Produkt dreier Primideale ersten Grades wird, welcher dieser Fälle eintritt, bedarf näherer Untersuchung. Ein Beispiel, in dem $\left(\frac{d}{p}\right) = 1$ und $f(x)$ das Produkt dreier Linearfaktoren in

$\mathsf{P}_p[x]$, demzufolge p das Produkt dreier paarweise verschiedener Primideale ersten Grades ist, ist $p = 59$. Man hat

$$f(x) \equiv (x-4)(x+17)(x-13) \bmod 59$$

und $(59) = \mathfrak{r}_1\mathfrak{r}_2\mathfrak{r}_3$ mit $\mathfrak{r}_1 = (59,\ 4-\vartheta)$, $\mathfrak{r}_2 = (59,\ \vartheta+17)$, $\mathfrak{r}_3 = (59,\ 13-\vartheta)$.
Wir wollen noch $p = 23$ untersuchen. Es wird

$$f'(x) = 3x^2 - 1 \equiv 0 \bmod 23$$

durch $x \equiv \pm 10$ gelöst. Von diesen beiden Restklassen genügt nur $x \equiv 10$ der Kongruenz $f(x) \equiv 0 \bmod 23$, da $f(10) = 989 = 23 \cdot 43$ ist. Also wird $f(x) \equiv (x-10)^2(x-3)$ und wir haben $(23) = \mathfrak{s}_1^2\mathfrak{s}_2$ mit $\mathfrak{s}_1 = (23,\ 10-\vartheta)$ als Primideal der Ordnung 2 und des Grades 1, $\mathfrak{s}_2 = (23,\ 3-\vartheta)$ als Primideal der Ordnung 1 und des Grades 1.
Wir schließen mit einem Satz, der sehr oft die Entscheidung gestattet, ob ein Ideal das Einheitsideal ist.

Satz 16. *Ist A eine natürliche Zahl >1, α eine ganze Zahl des Körpers und ist $\alpha^{\mathsf{N}} \equiv 0$ mod A, so ist das Ideal $\mathfrak{a} = (A, \alpha)$ nicht das Einheitsideal.*

Beweis: $\gamma = A\xi + \alpha\eta$ mit ξ, η beliebig ganz in k ist Repräsentant einer Zahl in $\mathfrak{a}$. Es wird

$$\gamma^{\mathsf{N}} = \prod_{i=1}^{n}\{A\,\xi^{(i)} + \alpha^{(i)}\eta^{(i)}\} \equiv \prod_{i=1}^{n}\alpha^{(i)}\eta^{(i)} = \alpha^{\mathsf{N}}\eta^{\mathsf{N}} \equiv 0 \bmod A\,.$$

Es ist also 1 in $\mathfrak{a}$ nicht enthalten.

§ 35. Inhalt von Polynomen

Aus dem Z.P.I. gewinnt man ohne weiteres einen Satz, der eine Erweiterung des Satzes 1 in § 25 darstellt.
Wir definieren bei einem ganzzahligen Polynom

$$f(x) = \sum_j \alpha_j x^j\,,$$

in dem nur endlich viele α_j von Null verschieden sind, als Inhalt $I(f)$ das Ideal $(\alpha_0, \alpha_1, \ldots)$. Der Satz lautet dann:

Satz 1. *Der Inhalt des Produktes zweier Polynome mit ganzen algebraischen Zahlen als Koeffizienten ist das Produkt der beiden Inhalte.*

Beweis: Die Polynome seien $f(x)$ und $g(x) = \sum \beta_k x^k$. Das Produkt $h(x)$ wird: $h(x) = \sum \gamma_l x^l$, wobei

$$\gamma_l = \sum_{l=j+k} \alpha_i \beta_k$$

ist. Wir haben $I(f) = \Pi \mathfrak{p}_i^{a_i}$, $I(g) = \prod \mathfrak{p}_i^{b_i}$. Jedenfalls gilt

$$\alpha_j \beta_k \equiv 0 \bmod \mathfrak{p}_i^{a_i + b_i},$$

also

$$I(fg) \equiv 0 \bmod I(f)\, I(g).$$

Sei $\mathfrak{p}$ eines der Primideale $\mathfrak{p}_i$, es sei $\mathfrak{p}^A \parallel I(f)$, $\mathfrak{p}^B \parallel I(g)$. Wir nehmen an:

$$\mathfrak{p}^{A+1} \mid \alpha_0, \alpha_1, \ldots, \alpha_{r-1};\ \mathfrak{p}^A \parallel \alpha_r,$$

ebenso

$$\mathfrak{p}^{B+1} \mid \beta_0, \beta_1, \ldots, \beta_{s-1};\ \mathfrak{p}^B \parallel \beta_s.$$

Dann wird

$$\gamma_{r+s} = \alpha_r \beta_s + \alpha_{r+1}\beta_{s-1} + \cdots + \alpha_{r+s}\beta_0 + \alpha_{r-1}\beta_{s+1} + \cdots + \alpha_0 \beta_{r+s}.$$

Es ist $\mathfrak{p}^{A+B+1} \mid \alpha_{r+t}\beta_{s-t}$ mit $t > 0$, ebenso $\mathfrak{p}^{A+B+1} \mid \alpha_{r-t}\beta_{s+t}$. Es bleibt

$$\mathfrak{p}^{A+B} \parallel \alpha_r \beta_s, \qquad \mathfrak{p}^{A+B} \parallel \gamma_{r+s}.$$

§ 36. Der Gitterpunktdeterminantensatz von Minkowski

Gitterpunkt ist ein Punkt mit ganzzahligen Koordinaten.

Gegeben seien n Linearformen:

$$\begin{aligned} f_1 &= a_{11}x_1 + \cdots + a_{1n}x_n, \\ &\vdots \\ f_n &= a_{n1}x_1 + \cdots + a_{nn}x_n \end{aligned}$$

mit der Matrix $\mathfrak{A} = (a_{ik})$, die a_{ik} seien reell, die Determinante $|\mathfrak{A}| \neq 0$. Gegeben seien weiter n positive Größen $\varkappa_1, \varkappa_2, \ldots, \varkappa_n$ mit $\varkappa_1 \varkappa_2 \ldots \varkappa_n = \operatorname{abs} |\mathfrak{A}|$. Wir denken uns um jeden Gitterpunkt $(y_1, y_2, \ldots, y_n)$ des n-dimensionalen Raumes einen Bereich, gegeben durch

$$|a_{i1}(x_1 - y_1) + \cdots + a_{in}(x_n - y_n)| \leqq \frac{\lambda}{2}\varkappa_i \quad (i = 1, \ldots, n)$$

angebracht, und zwar sei λ so klein, daß

$$|f_i| \leqq \lambda \varkappa_i$$

außer dem Ursprung keinen Gitterpunkt enthalte. Es sei

$$\mathfrak{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathfrak{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Kurz geschrieben lauten unsere Annahmen:

1. $|f_i(\mathfrak{x})| \leqq \lambda \varkappa_i$ enthält keinen Gitterpunkt außer dem Ursprung.

2. Die Bereiche sind um jeden Gitterpunkt $\mathfrak{y}$ angebracht, es ist dabei

$$|f_i(\mathfrak{x} - \mathfrak{y})| \leqq \frac{\lambda}{2} \varkappa_i . \tag{1}$$

Behauptung: Zwei um zwei verschiedene Gitterpunkte $\mathfrak{y}$ und $\mathfrak{z}$ angebrachte Bereiche (1) haben keinen Punkt gemeinsam.

Beweis: Wäre

$$|f_i(\mathfrak{y} - \mathfrak{u})| \leqq \frac{\lambda}{2} \varkappa_i ,$$

$$|f_i(\mathfrak{z} - \mathfrak{u})| \leqq \frac{\lambda}{2} \varkappa_i$$

für zwei verschiedene Gitterpunkte $\mathfrak{y}, \mathfrak{z}$ erfüllt, so wäre

$$|f_i(\mathfrak{y} - \mathfrak{z})| \leqq |f_i(\mathfrak{y} - \mathfrak{u})| + |f_i(\mathfrak{z} - \mathfrak{u})| \leqq \lambda \varkappa_i ,$$

und es enthielte

$$|f_i(\mathfrak{x})| \leqq \lambda \varkappa_i$$

doch nichttrivial einen Gitterpunkt nämlich $\mathfrak{y} - \mathfrak{z}$.

Bei Anbringung der entsprechenden Bereiche um die Gitterpunkte $(y_1, y_2, \ldots, y_n)$, wobei die y_j unabhängig voneinander die Zahlen $0, \pm 1, \pm 2, \pm 3, \ldots, \pm N$ durchlaufen, also insgesamt $(2N+1)^n$ Gitterpunkte erreicht werden, haben wir $(2N+1)^n V(\lambda)$ als Gesamtvolumen, wobei die Größe $V(\lambda)$ das Volumen des Bereiches

$$|f_i(\mathfrak{x})| \leqq \frac{\lambda}{2} \varkappa_i$$

gibt. Wird die Größe T als

$$T = \max \{\max |x_1|, \ldots, \max |x_n|\}$$

im Bereich

$$|f_i(\mathfrak{x})| \leqq \varkappa_i$$

bezeichnet, so sind alle unsere Bereiche im Würfel der Kantenlänge $2N+1+\lambda T$ enthalten. Mithin ist

$$(2N+1)^n V(\lambda) \leqq (2N+1+\lambda T)^n$$

oder nach Division durch $2^n N^n$ und Grenzübergang $N \to \infty$

$$V(\lambda) \leqq 1.$$

Es wird durch Transformation mit $f_1, \ldots, f_n$ als neuen Veränderlichen, also dem Absolutbetrag der Funktionaldeterminante

$$\left| \frac{\partial (f_1, \ldots, f_n)}{\partial (x_1, \ldots, x_n)} \right| = \operatorname{abs} |\mathfrak{A}| > 0$$

demzufolge

$$\left| \frac{\partial (x_1, \ldots, x_n)}{\partial (f_1, \ldots, f_n)} \right| = \frac{1}{\operatorname{abs} |\mathfrak{A}|}$$

das Volumen $V(\lambda)$

$$V(\lambda) = \int \ldots \int dx_1 \ldots dx_n = \frac{1}{\operatorname{abs} |\mathfrak{A}|} \int \ldots \int df_1 \ldots df_n$$

$$= \frac{1}{\operatorname{abs} |\mathfrak{A}|} \int_{-\frac{\lambda}{2}\varkappa_1}^{\frac{\lambda}{2}\varkappa_1} df_1 \ldots \int_{-\frac{\lambda}{2}\varkappa_n}^{\frac{\lambda}{2}\varkappa_n} df_n = \frac{\lambda^n \varkappa_1 \ldots \varkappa_n}{\operatorname{abs} |\mathfrak{A}|} = \lambda^n.$$

Es folgt $\lambda^n \leqq 1$, also muß $\lambda \leqq 1$ sein. Aber auch für $\lambda = 1$ ist es ganz ausgeschlossen, daß der Bereich weder am Rand noch im Innern einen Gitterpunkt enthält (immer vom Ursprung abgesehen!), denn sonst müßte für jedes $\lambda = 1+\varepsilon$ mit noch so kleinem $\varepsilon > 0$ ein Gitterpunkt sogar innerhalb des Bereiches liegen, also liegt auch einer für $\lambda = 1$ am Rande oder im Innern. Wir haben den *Satz von Minkowski*:

Satz 1. *Sind n Linearformen mit reellen Koeffizienten*

$$\begin{aligned} f_1 &= a_{11} x_1 + \cdots + a_{1n} x_n \\ &\vdots \\ f_n &= a_{n1} x_1 + \cdots + a_{nn} x_n \end{aligned}$$

mit der Matrix $\mathfrak{A}$, *nichtverschwindender Determinante* $|\mathfrak{A}|$, *ferner n positive Größen* $\varkappa_i$ *mit* $\varkappa_1 \ldots \varkappa_n = \operatorname{abs} |\mathfrak{A}|$ *gegeben, so enthält der Bereich*

$$|f_1(\mathfrak{x})| \leqq \varkappa_1, \ldots, |f_n(\mathfrak{x})| \leqq \varkappa_n$$

am Rande oder im Innern nichttrivial einen Gitterpunkt. Hierbei ist

$$\mathfrak{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Bemerkt sei, daß nur die Existenz des Gitterpunktes nachgewiesen ist; der Satz gibt keine Rechenmethode, den Gitterpunkt wirklich zu finden.

§ 37. Der Minkowskische Diskriminantensatz

Die Linearform in k

$$f = x_1\omega_1 + \cdots + x_n\omega_n$$

mit $[\omega_1, \ldots, \omega_n]$ als Körperbasis heißt Fundamentalform. Sie werde in den n Körpern durch $f_1, \ldots, f_n$ verwirklicht. Dann ist $|\sqrt{d}|$ der Absolutbetrag der Determinante der Formen.
Wir folgen hier nicht der Anordnung (A)[1]), sondern nehmen zuerst die r_1 reellen Körper, sodann die r_2 Paare konjugiertkomplexer Körper, so daß jeweils einem Körper der konjugiertkomplexe folgt. Sind $k^{(j)}$, $k^{(j+1)}$ konjugiertkomplex, so setzen wir

$$h_j = \frac{f_j + f_{j+1}}{\sqrt{2}},$$

$$h_{j+1} = \frac{f_j - f_{j+1}}{i\sqrt{2}},$$

während $h_1 = f_1, \ldots, h_{r_1} = f_{r_1}$ ist.
Wir nehmen, wenn

$$|h_1| \leqq \tau_1, \ldots, |h_n| \leqq \tau_n$$

verwirklicht werden soll, stets bei einem Paare konjugiertkomplexer Körper dasselbe τ_i, so daß wir nur $r_1 + r_2$ Größen

$$\varkappa_1 = \tau_1, \ldots, \varkappa_{r_1} = \tau_{r_1}, \quad \varkappa_{r_1+1} = \tau_{r_1+1} = \tau_{r_1+2}, \ldots \tag{1}$$

haben.
Aus $|h_j| \leqq \tau_j$, $|h_{j+1}| \leqq \tau_j$ folgt wegen $\bar{f}_j = f_{j+1}$ (der Querstrich bedeutet den Übergang zu den konjugiertkomplexen Zahlen)

$$|f_j| = |f_{j+1}| = \sqrt{\frac{h_j^2 + h_{j+1}^2}{2}},$$

also

$$|f_j| = |f_{j+1}| \leqq \tau_j.$$

[1]) Vgl. S. 109

Um Auskunft über zweckmäßige Wahl des Produkts

$$\tau_1 \dots \tau_n = \varkappa_1 \varkappa_2 \dots \varkappa_{r_1} \varkappa_{r_1+1}^2 \varkappa_{r_1+2}^2 \dots \varkappa_{r_1+r_2}^2$$

zu erhalten, brauchen wir den Absolutbetrag der Determinante der h_j. Nehmen wir nur die Transformation, die alle f_k, soweit sie nicht in h_k bzw, soweit sie schon übergeführt sind, unverändert läßt, und nur f_j, f_{j+1} in h_j, h_{j+1} überführt, so haben wir eine Substitutionsmatrix (leere Stellen sind Nullen!)

$$\mathfrak{A} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & & \\ & & & \frac{1}{i\sqrt{2}} & -\frac{1}{i\sqrt{2}} & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}$$

mit abs $|\mathfrak{A}| = 1$. Mithin hat die Determinante der $h_1, \dots, h_n$ auch den Absolutbetrag $|\sqrt{d}|$.

Daher können wir $r_1 + r_2 - 1 = r$ Größen

$$\varkappa_1, \varkappa_2, \dots, \varkappa_r$$

beliebig wählen, dann ist allerdings $\varkappa_{r+1}$ bestimmt.

Entweder sind alle Körper reell, dann ist $r+1 = n$ und

$$\varkappa_1 \varkappa_2 \dots \varkappa_r \varkappa_{r+1} = |\sqrt{d}|$$

zu setzen, also

$$\varkappa_{r+1} = \frac{|\sqrt{d}|}{\varkappa_1 \dots \varkappa_r}.$$

Oder es ist mindestens ein Körper, damit auch ein Körperpaar eigentlich komplex, dann wird

$$\varkappa_1^{a_1} \varkappa_2^{a_2} \dots \varkappa_r^{a_r} \varkappa_{r+1}^2 = |\sqrt{d}|, \qquad \varkappa_{r+1} = \sqrt{\frac{|\sqrt{d}|}{\varkappa_1^{a_1} \dots \varkappa_r^{a_r}}}.$$

Hierbei sind die a_j eins, wenn $1 \leqq j \leqq r_1$ ist (sofern überhaupt reelle Körper vorkommen). Sonst ist $a_j = 2$.

Es wird dann einen Gitterpunkt $\mathfrak{x}$ geben (nichttrivial, also vom Ursprung verschieden) mit

$$\begin{aligned} |f_1(\mathfrak{x})| &\leqq \varkappa_1, \\ &\cdots \\ |f_{r_1}(\mathfrak{x})| &\leqq \varkappa_{r_1}, \\ |f_{r_1+1}(\mathfrak{x})| = |f_{r_1+2}(\mathfrak{x})| &\leqq \varkappa_{r_1+1}, \\ &\cdots \\ |f_{n-3}(\mathfrak{x})| = |f_{n-2}(\mathfrak{x})| &\leqq \varkappa_r, \\ |f_{n-1}(\mathfrak{x})| = |f_n(\mathfrak{x})| &\leqq \varkappa_{r+1}. \end{aligned} \tag{1}$$

Dieser Gitterpunkt definiert dann eine ganze Zahl $\alpha \neq 0$ des Körpers, es ist $\alpha^{(j)} = f_j(\mathfrak{x})$, $|\alpha^{\mathfrak{N}}| \leqq |\sqrt{d}|$.

$\varkappa_1, \ldots,$ waren ganz beliebig, $\varkappa_{r+1}$ ergibt sich aus ihnen; also nochmals: wenn alle Körper reell sind, ist

$$\varkappa_{r+1} = \frac{\sqrt{d}}{\varkappa_1 \varkappa_2 \ldots \varkappa_{r-1} \varkappa_r},$$

Wegen $|\alpha^{\mathfrak{N}}| = |\Pi f_j(\mathfrak{x})| \geqq 1$ aber muß

$$\varkappa_1 \ldots \varkappa_r \varkappa_{r+1} \geqq 1$$

gelten, so daß sich in diesem Falle $(r = n-1)$ ergibt

$$\frac{1}{\varkappa_1 \ldots \varkappa_r} \leqq \varkappa_{r+1} = \frac{|\sqrt{d}|}{\varkappa_1 \ldots \varkappa_r}.$$

Sind auch eigentlich komplexe Körper da, so ergibt sich in genau derselben Art

$$\frac{1}{\varkappa_1 \ldots \varkappa_{r_1} \varkappa_{r_1+1}^2 \ldots \varkappa_r^2} \leqq \varkappa_{r+1}^2 = \frac{|\sqrt{d}|}{\varkappa_1 \ldots \varkappa_{r_1} \varkappa_{r_1+1}^2 \ldots \varkappa_r^2}.$$

Es kann nicht $|d| = 1$ sein, sonst würde bei jeder Annahme der $\varkappa_1, \ldots, \varkappa_r$ die Gleichheit

$$|f_j(\mathfrak{x})| = \varkappa_{j'}$$

bestehen, wobei j' durch j aus dem Gleichungssystem (1) bestimmt ist Das ist aber ganz unmöglich, z. B. schon, wenn man $\varkappa_1$ als positive transzendente Zahl annimmt.

Damit erhalten wir den

Diskriminantensatz von Minkowski. *Die Körperdiskriminante d hat einen Absolutbetrag >1.*

Für quadratischimaginäre Körper gilt der Beweis nicht. Hier folgt er aus Satz 3 in § 29.

§ 38. Die Einheiten im quadratischen Zahlkörper

Grundlegend für mehrere weitere Sätze ist der folgende Satz über die Endlichkeit der Menge ganzer Ideale unter bestimmten Voraussetzungen:

Satz 1. *Ist $M > 1$ beliebig vorgegeben, so gibt es nur endlich viele ganze Ideale $\mathfrak{a}$ mit $\mathfrak{a}^N < M$.*

Beweis: Es gibt nur endlich viele natürliche Zahlen $< M$, also nur endlich viele solche, die Normen ganzer Ideale sind. Ist eine Zahl Norm eines ganzen Ideals, dann nur von endlich vielen ganzen Idealen, da sie nur endlich viele ganze Idealteiler hat.

Spezialisierung des Satzes ergibt:

Satz 2. *Es gibt nur endlich viele ganze Hauptideale $\mathfrak{a} = (\alpha)$ mit $\mathfrak{a}^N = |\alpha^N| < M$, wenn $M > 1$ vorgegeben ist.*

Es sei nun eine natürliche Zahl $m > 1$ vorgegeben, $m = m_1 m_2^2$, wobei m_1 quadratfrei und kein Quadrat, also m_2^2 das größte in m enthaltene Quadrat einer ganzen Zahl ist. Es ist $k = \mathsf{P}(\sqrt{m}) = \mathsf{P}(\sqrt{m_1})$ ein quadratischer Körper. Nach dem Minkowskischen Determinantensatz gibt es Paare ganzer Zahlen $[x, y]$, die nicht beide Null sind und

$$|x + y\sqrt{m}| \leqq 2\sqrt{m}, \tag{1a}$$

$$|x - y\sqrt{m}| \leqq 1 \tag{1b}$$

erfüllen. Es ist dann $(x + y\sqrt{m})^N \leqq 2\sqrt{m}$. Bei dieser Normenangleichung ist Gleichheit ausgeschlossen, da die Norm eine ganze rationale Zahl $\neq 0$, $\sqrt{m}$ aber irrational ist. Mithin ist

$$|(x + y\sqrt{m})^N| \leqq 2[\sqrt{m}].$$

Es erfülle etwa $[x_1, y_1]$ die Ungleichungen (1a), (1b). Dann sei $\alpha_1 = x_1 + y_1\sqrt{m}$. Es wird $|\alpha_1^N| \leqq 2[\sqrt{m}]$.

Wir setzen $\left|\frac{x_1 - y_1\sqrt{m}}{2}\right| = \varkappa_1$. Es ist $\varkappa_1 > 0$, denn $\sqrt{m}$ ist irrational, weiter kann nicht x_1 verschwinden, sonst wäre $|y_1| \geqq 1$ und $|x_1 - y_1\sqrt{m}| = |y_1|\sqrt{m} \geqq \sqrt{m} > 1$ im Widerspruch zu (1b).

Nun gibt es wieder ein Paar ganzer nichtverschwindender ganzer Zahlen $[x_2, y_2]$ mit

$$|x_2 + y_2\sqrt{m}| \leqq \frac{4\sqrt{m}}{\varkappa_1} \tag{2a}$$

$$|x_2 - y_2\sqrt{m}| \leqq \frac{\varkappa_1}{2}. \tag{2b}$$

Das Paar fällt wegen $|x_2 - y_2\sqrt{m}| < \left|\frac{x_1 - y_1\sqrt{m}}{2}\right|$ nicht mit $[x_1, y_1]$ zusammen. Wieder ist $\varkappa_2 = \left|\frac{x_2 - y_2\sqrt{m}}{2}\right| > 0$, es ist mit $\alpha_2 = x_2 + y_2\sqrt{m}$ die Ungleichung $|\alpha_2^N| \leqq 2[\sqrt{m}]$ erfüllt usf.

Wir bekommen eine Folge ganzer Zahlen des Körpers $\alpha_1, \alpha_2, \alpha_3, \ldots,$ deren Normen absolut $\leqq 2[\sqrt{m}]$ sind. Jedes α_i ist von jedem α_j verschieden, wenn $i > j$ ist, da

$$|x_i - y_i\sqrt{m}| < |x_j - y_j\sqrt{m}|$$

gilt. Es muß also

$$(\alpha_u) = (\alpha_v)$$

mit $v > u$ sein, also

$$\alpha_v \alpha_u^{-1} = \varepsilon$$

eine Einheit in k, die von ± 1 verschieden ist. Es wird

$$\varepsilon^N = \pm 1.$$

Wir haben:

Satz 3. *In jedem reellen quadratischen Zahlkörper gibt es von* ± 1 *verschiedene Einheiten.*

Es ist etwa $\varepsilon = A + B\sqrt{m_1}$. Dann wird $A^2 - B^2 m_1 = \pm 1$. Es folgt: Gilt das Minuszeichen, so wird $\varepsilon^2 = C + D\sqrt{m_1}$ und $C^2 - D^2 m_1 = 1$ mit $C = A^2 + m_1 B^2$, $D = 2AB$. Wir haben

Satz 4. *Die Pellsche Gleichung* $x^2 - my^2 = 1$ *hat für quadratfreie* $m > 1$ *Lösungen in ganzen Zahlen* $[x, y]$, *wobei* $y \neq 0$ *ist.*

Bei der Pellschen Gleichung schließen wir die Lösung $[\pm 1, 0]$ stets aus. Die Gleichung $x^2 - my^2 = -1$ heißt *Nicht-Pellsche Gleichung*. Fast trivial ist

Satz 5. *Hat* m *einen Primfaktor* $p \equiv 3 \bmod 4$, *so ist die Nicht-Pellsche Gleichung* $x^2 - my^2 = -1$ *ganzzahlig unlösbar.*

Beweis: Aus einer Lösung folgte wegen $(x, m) = 1$, daß $\left(\frac{-1}{p}\right) = 1$ im Widerspruch zum zweiten Ergänzungssatz ist.

Zunächst sei jetzt $m_2 = 1$, also $m = m_1$ quadratfrei. Für $m \equiv 2, 3, 6, 7 \bmod 8$ kann eine ganze Zahl des Körpers k, damit auch eine Einheit nur die Gestalt $A + B\sqrt{m}$ mit A, B ganz rational haben. Bei Einheiten gilt dies auch bei $m \equiv 1 \bmod 8$, denn die noch vorkommenden ganzen Zahlen $\gamma = \frac{A + B\sqrt{m}}{2}$ mit ungeradem A, B

erfüllen $\gamma^N = \frac{A^2 - B^2 m}{4} \equiv 0 \bmod 2$, sind also keine Einheiten. Bei Zahlen $m \equiv 5 \bmod 8$ kann es allerdings Einheiten $\eta = \frac{A + B\sqrt{m}}{2}$ geben, z. B. $\frac{1+\sqrt{5}}{2}$ in $\mathsf{P}(\sqrt{5})$, $\frac{39+5\sqrt{61}}{2}$ in $\mathsf{P}(\sqrt{61})$. Es gilt aber folgender

Satz 6. *Ist* $k = \mathsf{P}(\sqrt{m})$, $m \equiv 5 \bmod 8$, *sowie* $\eta = \frac{A + B\sqrt{m}}{2}$ *mit* $A \equiv B \equiv 1 \bmod 2$ *eine Einheit, so ist* $\eta^3 = H + K\sqrt{m}$ *mit* H, K *ganz.*

Beweis: Es ist $\eta^3 = (X + Y\sqrt{m})/8$ mit

$$X = A\,(A^2 + 3B^2 m) \equiv A\,(1 + 3 \cdot 5) \equiv 0 \bmod 8.$$

Da μ ganz ist, ist μ_3, also mit $\chi/8$ auch $y/8$ ganz.

Eine solche „Halbeinheit" erfüllt also

$$A^2 - m B^2 = \pm 4$$

mit ungeradem A und B. Selbstverständlich ist die Halbeinheit wie jede Einheit eine ganze Zahl.

Wir wollen die Lösungen dadurch normieren, daß wir x, y als positiv auffassen. Sind etwa $\alpha = x + y\sqrt{m}$, $\beta = X + Y\sqrt{m}$ mit $x, y, X, Y > 0$ aus den Lösungen von

$$x^2 - m y^2 = k$$

hervorgegangen, wobei k nicht ± 1 zu sein braucht, so bezeichnen wir das Lösungspaar $[x, y]$ als eine kleinere Lösung als $[X, Y]$, wenn $\alpha < \beta$ ist.

Die Tatsache, daß die Lösung $[x, y]$ kleiner als die Lösung $[X, Y]$ ist, wird auch durch $x < X$ oder $y < Y$ charakterisiert, denn y wächst monoton mit x, wie aus $y = \frac{1}{\sqrt{m}}\sqrt{x^2 - k}$, $y' = \frac{x}{\sqrt{m}\sqrt{x^2 - k}}$ für $x > 0$, $y > 0$ hervorgeht.

Sei $\varepsilon_0' = a + b\sqrt{m}$ die kleinste Lösung mit $\varepsilon_0'^N = 1$, also

$$a^2 - b^2 m = 1 \quad (a > 0,\ b > 0)$$

oder $[a, b]$ die kleinste Lösung der Pellschen Gleichung

$$x^2 - m y^2 = 1.$$

Sei $\varepsilon'^N = 1$, $\varepsilon' = A + B\sqrt{m}$, $A > 0$, $B > 0$. Wir behaupten:

ε' ist eine Potenz von ε_0'. Wäre $\varepsilon_0'^u < \varepsilon' < \varepsilon_0'^{u+1}$, $\varepsilon_0'^u = R + S\sqrt{m}$, so wäre

$$\varepsilon'' = \varepsilon' \varepsilon_0'^{-u} = \frac{A + B\sqrt{m}}{R + S\sqrt{m}}$$
$$= (AR - BSm) + \sqrt{m}(-AS + BR) = k + l\sqrt{m}$$

mit $k > 0$. Dies folgt sofort aus $A > B\sqrt{m}$, $R > S\sqrt{m}$. Wäre $l \leqq 0$, so wäre $1 < \varepsilon'' = k + l\sqrt{m} \leqq \varepsilon''^{-1} = k - l\sqrt{m} < 1$, also ein Widerspruch. Aber nun wäre $[k, l]$ eine kleinere Lösung als $[a, b]$. Es folgt

Satz 7. *Aus der kleinsten Lösung* $[a, b]$ *der Pellschen Gleichung* $x^2 - my^2 = 1$, $\varepsilon_0' = a + b\sqrt{m}$ *gehen alle Lösungen* $[A, B]$ *durch die Potenzen von* ε_0', *also* $\varepsilon_0'^u = A + B\sqrt{m}$ *(u natürliche Zahl) hervor.*

Beim Beweis von Satz 7 wurde die Voraussetzung „m ist quadratfrei" nicht verwendet. *Man nennt* ε_0' *die Grundeinheit der Norm* $+1$ *im Ringe der Zahlen* $A + B\sqrt{m}$. Alle Einheiten der Norm $+1$ in diesem Ring haben die Gestalt $\pm \varepsilon_0'^u$, wobei u eine ganze (positive oder negative) rationale Zahl ist; $u = 0$, wo die trivialen Einheiten ± 1 herauskommen, interessiert wenig.

Wir müssen noch bei nicht quadratfreien $m = m_1 m_2^2, m_2 > 1$ den Nachweis für die Existenz von Lösungen der Pellschen Gleichung erbringen. Sei $\varepsilon_{0'}$ die Grundeinheit der Norm $+1$ im Ring der Zahlen $X + Y\sqrt{m_1}$. Wir bilden $\varepsilon_0'^j$ (für $1 \leqq j \leqq m_2^2 + 1$) $= a_j + b_j\sqrt{m_1}$ $(a = a_1, b = b_1)$, also $m_2^2 + 1$ Zahlen. Da mod m_2 nur m_2^2 Restklassenpaare $[L, M]$ existieren, aber $m_2^2 + 1$ Zahlenpaare $[a_j, b_j]$ da sind, so muß es mindestens ein Paar $a_{j'} \equiv a_{j''}$, $b_{j'} \equiv b_{j''}$ mod m_2 geben (Schubfachschluß!), wobei $j' < j''$ ist. Mit $a_{j'} = R$, $b_j = S$, $a_{j''} = T$, $b_{j''} = U$ wird $R \equiv T$, $S \equiv U$ mod m_2, also

$$\varepsilon_0'^{j''-j'} = \begin{vmatrix} R & S \\ Um_1 & T \end{vmatrix} + \begin{vmatrix} R & S \\ T & U \end{vmatrix} \sqrt{m} = F + Gm_2\sqrt{m_1} = F + G\sqrt{m}$$

und $x = F$, $y = G$ löst $x^2 - my^2 = 1$. Wir erhalten als Verallgemeinerung von Satz 4 den folgenden

Satz 8. *Ist* m *ganz rational* > 1, *nicht das Quadrat einer rationalen Zahl, so ist die Pellsche Gleichung* $x^2 - my^2 = 1$ *stets nichttrivial ganzzahlig lösbar. Aus* ε_0' *folgen alle Einheiten.*

Nun ein wichtiger Satz, der oft die Beantwortung der schwierigen Frage über Existenz von Lösungen der Nicht-Pellschen Gleichung erleichtert! Der Satz ist trivial wenn $4/m$ oder m Quadrat ist.

Satz 9. *Für $m > 2$ ist gleichzeitige Lösbarkeit zweier der Gleichungen*

$$x^2 - my^2 = -1 \text{ (Nicht-Pellsche Gleichung)}, \tag{3}$$

$$x^2 - my^2 = 2, \tag{4}$$

$$x^2 - my^2 = -2 \text{ unmöglich}. \tag{5}$$

Beweis: Es genügt der Beweis für quadratfreie m. Für $m \equiv 1 \bmod 4$ sind (4), (5) schon als Kongruenzen mod 4 ein Widerspruch. Für $m \equiv 3 \bmod 4$ ist (3) wegen $\left(\frac{-1}{m}\right) = -1$ unmöglich, ebenso mindestens eine der Gleichungen (4), (5), da von den Symbolen $\left(\frac{2}{m}\right), \left(\frac{-2}{m}\right)$ nur eines den Wert 1 hat. Es genügt die Annahme $m = 2F$, F ungerade, quadratfrei.

Für beliebige natürliche $m > 2$, die keine Quadrate in $\mathbf{P}$ sind, gilt: Eine Kleinstlösung $[a, b]$ von (4) oder (5), $\varkappa = a + b\sqrt{m}$, gibt $\varepsilon_0' = \frac{\varkappa^2}{2}$. Denn $\frac{\varkappa^2}{2}$ ist von der Form $X + Y\sqrt{m}$ (X, Y ganz rational); ferner ist $\frac{\varkappa^2}{2} > 1$ und hat die Norm 1; also gilt

$$\frac{\varkappa^2}{2} = \varepsilon_0'^{A}$$

mit A als natürlicher Zahl. $A = 2B$ hätte $(\varkappa \varepsilon_0^{-B})^2 = 2$, also $\sqrt{2}$ im Ringe, damit $m = 2$ zur Folge. $A = 2B + 1$ mit $B > 0$ ergäbe für $\varkappa' = \varkappa \varepsilon_0'^{-B}$ die Beziehungen $\varkappa' = \sqrt{2\varepsilon_0'} > 1$, $\varkappa'^{\mathsf{N}} = \pm 2$ mit dem oberen oder unteren Vorzeichen, je nachdem (4) oder (5) vorliegt; es folgte aus $\varkappa'$ eine kleinere Lösung von (4) bzw. (5).

Nun sei wieder wie vorhin $m = 2F$.

Gleichzeitige Lösbarkeit von (4), (5) durch $[r, s]$, bzw. $[t, u]$ ergibt, da m gerade, also r, t gerade ist:

$$\alpha = \frac{t + u\sqrt{m}}{r + s\sqrt{m}} = \frac{1}{2}\{(rt - msu) + \sqrt{m}(ru - st)\}$$

ist ganz, liegt im Ring, und es ist $\alpha^{\mathsf{N}} = -1$. Wir können also gleichzeitige Lösbarkeit von (3), (4), bzw. (3), (5) annehmen.

Da auch (3) etwa durch $[g, h]$ als kleinster Lösung erfüllt wird, so ist mit $\eta = g + h\sqrt{m}$ auch $\varepsilon_0' = \eta^2$, $\eta^2 = \frac{\varkappa^2}{2}$, $\sqrt{2}$ im Ring, $m = 2$ $(F = 1)$.

Bemerkungen:

1. Bei $m = 2$ sind alle drei Gleichungen lösbar:

$$1^2 - 2 \cdot 1^2 = -1,\ 2^2 - 2 \cdot 1^2 = 2,\ 0^2 - 2 \cdot 1^2 = -2,$$

oder, wenn man die letzte Lösung wegen $x = 0$ nicht gelten lassen will, $4^2 - 2 \cdot 3^2 = -2$.

2. Möglicherweise sind alle drei Gleichungen unlösbar, z. B. für

$$m = 105 = 3 \cdot 5 \cdot 7,$$

wobei (3) als Kongruenz mod 3 oder mod 7, (4), (5) hingegen als Kongruenz mod 5 ausgeschlossen sind.

Beispiele:

1. Es ist $6^2 - 34 \cdot 1^2 = 2$, also ist die Nicht-Pellsche Gleichung

$$x^2 - 34y^2 = -1,$$

obwohl $\left(\frac{-1}{17}\right) = 1$ ist, und ebenso $x^2 - 34y^2 = -2$ unlösbar.

2. Es gilt $12^2 - 146 \cdot 1^2 = -2$, damit ist $x^2 - 146y^2 = -1$ (Nicht-Pellsche Gleichung) und ebenso $x^2 - 146y^2 = +2$ unlösbar, obwohl $\left(\frac{2}{73}\right) = \left(\frac{-1}{73}\right) = 1$ ist.

3. Wegen $9^2 - 82 \cdot 1^2 = -1$ ist $x^2 - 82y^2 = \pm 2$ unlösbar.

4. Es ist $68^2 - 3^2 \cdot 514 = 4624 - 4626 = -2$.
Für $2p = 514$, $p = 257$ (Primzahl) ist also $x^2 - 2py^2 = -1$ (Nicht-Pellsche Gleichung) und ebenso $x^2 - 2py^2 = 2$ unlösbar.

Beim Beweis hat sich der Satz ergeben:

Satz 10. *Die aus den kleinsten Lösungen der Nicht-Pellschen Gleichung $x^2 - my^2 = -1$, bzw. aus den kleinsten Lösungen der Gleichungen $x^2 - my^2 = 2$, $x^2 - my^2 = -2$, wenn eine dieser Gleichungen lösbar, sich ergebenden ganzen algebraischen Zahlen η, $\varkappa$, λ ergeben $\varepsilon_0' = \eta^2$, $\frac{\varkappa^2}{2}$, $\frac{\lambda^2}{2}$. Bei $m = 2$, $x^2 - my^2 = -2$ ist hierbei von der Lösung $[0, 1]$ abzusehen.*

Der Beweis für den Fall der Lösbarkeit von $x^2 - my^2 = -2$ wird völlig analog geliefert.

Es ergibt sich z. B. aus $(68 + 3\sqrt{514})^N = -2$ mit λ als Zahl in der Klammer

$$\frac{\lambda^2}{2} = 4625 + 204\sqrt{514}\ ;$$

und $x = 4625$, $y = 204$ löst $x^2 - 514y^2 = 1$.

Nun kann im Falle $k = \mathsf{P}(\sqrt{m})$, wobei jetzt m wieder quadratfrei ist (natürlich bleibt immer die Bedingung bestehen: m ist kein Quadrat einer rationalen Zahl), ein vollständiger Überblick über die möglichen Fälle von Einheiten im reellen quadratischen Zahlkörper erreicht werden:

1. Es gebe in k „Halbeinheiten", und zwar sei $\varepsilon_0 = \frac{A + B\sqrt{m}}{2}$ davon die kleinste mit der Norm -1. Dann ist $\varepsilon_0^3 = C + D\sqrt{m}$ die Grundringeinheit der Norm -1 und gibt eine Lösung, genauer die kleinste Lösung der Nicht-Pellschen Gleichung. Weiter ist $\varepsilon_0^6 = E + G\sqrt{m} = \varepsilon_0'$ *Grundringeinheit* der Norm $+1$; diese ergibt die kleinste Lösung der Pellschen Gleichung.
Der Fall kann nur eintreten, wenn jeder Primteiler p von m die Kongruenz $p \equiv 1 \bmod 4$ erfüllt, überdies $m \equiv 5 \bmod 8$ ist.

2. Es gebe keine „Halbeinheiten" der Norm -1, aber es sei $\varepsilon_0 = \frac{a + b\sqrt{m}}{2}$ (a, b ungerade) die kleinste Halbeinheit der Norm $+1$. Dann ist $\varepsilon_0^3 = \varepsilon_0'$.

3. Es gibt Einheiten der Gestalt $A + B\sqrt{m}$ der Norm -1 (A, B ganz), aber keine Halbeinheiten, sei also die Nicht-Pellsche Gleichung lösbar. Dann ist $\varepsilon_0' = \varepsilon_0^2$, wenn ε_0 die kleinste Lösung dieser Gleichung ergibt.

4. Es gebe keine Halbeinheiten, die Nicht-Pellsche Gleichung ist unlösbar. Dann ist

$$\varepsilon_0' = \varepsilon_0.$$

In jedem Falle ist jede Einheit von der Form $\pm \varepsilon_0^u$ mit u ganz rational. Wir haben

Satz 11. *Alle Einheiten eines reellen quadratischen Körpers sind von der Form* $\pm \varepsilon_0^u$; ε_0 *heißt Grundeinheit.*

Im Falle der Halbeinheiten $\frac{a + b\sqrt{m}}{2}$ löse $[a, b]$ die Gleichung

$$x^2 - my^2 = 4,$$

wobei x, y ungerade sind. Diese Gleichung wird manchmal auch als Pellsche Gleichung bezeichnet.

Satz 12. Es sei p *eine ungerade Primzahl.* Dann ist für $p \equiv 1 \bmod 4$ *die Nicht-Pellsche Gleichung* $x^2 - py^2 = -1$, *für* $p \equiv 7 \bmod 8$ *die Gleichung* $x^2 - py^2 = 2$, und *für* $p \equiv 3 \bmod 8$ *die Gleichung* $x^2 - py^2 = -2$ *lösbar.*

Beweis: Sei $[a, b]$ die kleinste Lösung der Pellschen Gleichung, also $a^2 - pb^2 = 1$ oder $a^2 - 1 = b^2 p$.

Sind $a+1$, $a-1$ gerade, so ist $(a+1, a-1) = 2$. Sind beide ungerade, so ist $(a+1, a-1) = 1$.

Es sind nur folgende Fälle möglich:

1. $a+1 = 2A^2$,
   $a-1 = 2pB^2$

gibt $A^2 - pB^2 = 1$, also einen Widerspruch gegen die Voraussetzung, daß $[a, b]$ die kleinste Lösung ist.

2. $a+1 = 2pA^2$,
   $a-1 = 2B^2$

gibt $B^2 - pA^2 = -1$, dies ist nur für $p \equiv 1 \bmod 4$ möglich. Da aber aus $a^2 - pb^2 = 1$, wenn wir dies als Kongruenz mod 4 auffassen, b gerade, a ungerade, also $(a+1, a-1) = 2$ folgt, muß für $p \equiv 1 \bmod 4$ dieser Fall eintreten. Wir haben bereits die Lösbarkeit der Nicht-Pellschen Gleichung für $p \equiv 1 \bmod 4$ bewiesen. Wir können also jetzt $p \equiv 3 \bmod 4$ annehmen. Dann wird a gerade; denn b gerade, a ungerade führte auf 2.

3. $a+1 = A^2$,
   $a-1 = pB^2$

gibt $A^2 - pB^2 = 2$, was nur für $p \equiv 7 \bmod 8$ möglich ist.

4. $a+1 = pA^2$,
   $a-1 = B^2$.

Das hat $B^2 - pA^2 = -2$ zur Folge, was nur für $p \equiv 3 \bmod 8$ zulässig ist.

Da einer der Fälle 3., 4. bei $p \equiv 3 \bmod 4$ eintreten muß, ist der Satz in allen Teilen bewiesen. Wir haben weiter

Satz 13. *Ist p eine ungerade Primzahl, so ist für $p \equiv 5 \bmod 8$ die Nicht-Pellsche Gleichung $x^2 - 2py^2 = -1$ lösbar, für $p \equiv 7 \bmod 8$ die Gleichung $x^2 - 2py^2 = 2$, endlich für $p \equiv 3 \bmod 8$ die folgende $x^2 - 2py^2 = -2$* lösbar.

Für $p \equiv 1 \bmod 8$ ist es nicht so leicht, allgemeine Aussagen zu machen.

Beweis: Wieder sei $[a, b]$ die kleinste Lösung der Pellschen Gleichung $x^2 - 2py^2 = 1$. Es sind $a+1$, $a-1$ gerade, da a ungerade sein muß. Es sind folgende Fälle möglich:

1. $a+1=2A^2$,
   $a-1=4pB^2$.
Daraus folgt $A^2-2pB^2=1$ im Widerspruch dazu, daß $[a, b]$ kleinste Lösung der Pellschen Gleichung ist.
2. $a+1=4pA^2$,
   $a-1=2B^2$
gibt $B^2-2pA^2=-1$; dies ist nur für $p\equiv 1, 5 \bmod 8$ möglich.
3. Aus
   $a+1=A^2$,
   $a-1=2pB^2$
erhalten wir $A^2-2pB^2=2$, was nur für $p\equiv 1, 7 \bmod 8$ geht.
4. $a+1=2pA^2$,
   $a-1=B^2$
hat $B^2-2pA^2=-2$ zur Folge. Das ist nur für $p\equiv 1, 3 \bmod 8$ möglich.
Da einer der Fälle 2., 3., 4. eintreten muß, folgt der Satz.
Um $x^2-my^2=1$ wirklich zu lösen, suche man zuerst die Lösungen der Kongruenz $x^2\equiv 1 \bmod m$. Man braucht, wenn x_1 eine Wurzel der Kongruenz ist, nur $x=x_1+mt$ zu setzen, kann die Wurzel $-x_1$ vernachlässigen, darf aber nicht vergessen, daß für t alle ganzzahligen Werte (auch negative!) zulässig sind.
Ähnlich kann bei $x^2-my^2=\pm 2$ vorgegangen werden, bzw. bei der Nicht-Pellschen Gleichung $x^2-my^2=-1$. Hier ist allerdings wichtig, daß man von irgendwoher weiß, daß überhaupt Lösungen vorhanden sind.
Es wurde absichtlich eine Pellsche Gleichung mit unverhältnismäßig großen Zahlen in der kleinsten Lösung gewählt, nämlich

$$x^2-94y^2=1. \tag{6}$$

Wir lösen zuerst

$$x^2-94y^2=2. \tag{7}$$

Nach Satz 13 ist (7) lösbar.
Es ist y ungerade, $\left(\frac{2}{y}\right)=1$, $(-1)^{\frac{y^2-1}{8}}=1$, $y^2-1\equiv 0 \bmod 16$, $-94y^2\equiv 2y^2\equiv 2 \bmod 32$, $x^2\equiv 0 \bmod 32$, $x\equiv 0 \bmod 8$. Da $x^2\equiv 2 \bmod 94$ die Lösung $x\equiv 40$ (und $x\equiv -40) \bmod 94$ hat, so gilt genauer $x\equiv 40 \bmod 4\cdot 94=376$, oder $x=40+376t$, wobei aber für t auch negative Werte zugelassen werden müssen. Da

(7) als Kongruenz mod 3 betrachtet $x^2 - y^2 \equiv 2 \bmod 3$ lautet, so ergibt $y^2 \not\equiv 2 \bmod 3$ sofort $x^2 \not\equiv 4 \bmod 3$, $x \not\equiv 1, 2 \bmod 3$. Es muß also $x \equiv 0 \bmod 3$ oder $|x| \equiv \pm 792 \bmod 1128$ sein. Die kleinsten Werte von (x) sind 792, 336, 1464.

Da für jeden Primteiler p von χ die Beziehung $1 = \left(\frac{-47}{p}\right)$ erfüllt ist, aber $11 \mid 792$ gilt, fällt $x = 792$ aus. $x = 336$ gibt nichts.

$x = 1464$ gibt $y = 151$. Mit $\alpha = 1464 + 151\sqrt{94}$ wird $\frac{\alpha^2}{2} = 2143295 + 221064\sqrt{94}$, daher löst $x = 2143295$, $y = 221064$ die Pellsche Gleichung $x^2 - 94y^2 = 1$.

Satz 14. *Ist $p \equiv 9$ mod 16 eine Primzahl, 2 biquadratischer Nichtrest von p, was auf $p = m^2 + 8n^2$ mit geradem n herausläuft, so sind die Gleichungen*

$$r'^2 - 2ps^2 = 2, \tag{8}$$

$$r'^2 - 2ps^2 = -2 \tag{9}$$

beide ganzzahlig unlösbar.

Beweis: Wir gehen vom Gegenteil der Behauptung aus.

I. Sei (8) lösbar. Es ist $r' \equiv 0 \bmod 2$. Wir setzen $r' = 2^t r$, r ungerade, $t \geqq 1$.

Gleichung (8) wird

$$2^{2t-1}r^2 - ps^2 = 1.$$

s ist also ungerade. Es folgt $\left(\frac{2}{s}\right) = 1$, $s \equiv 1,7 \bmod 8$, $s^2 \equiv 1 \bmod 16$, $ps^2 \equiv 9 \bmod 16$, $2^{2t-1}r^2 \equiv 10 \bmod 16$, also $t = 1$, schließlich $r^2 \equiv 5 \bmod 8$, was unmöglich ist.

II. Nun sei (9) lösbar. Mit den gleichen Bezeichnungen können wir

$$2^{2t-1}r^2 - ps^2 = -1 \tag{10}$$

schreiben. Es ist $2^{2t-1}r^2$ biquadratischer Rest von p, weil -1 biquadratischer Rest von p ist. Also ist r^2 biquadratischer Nichtrest, r quadratischer Nichtrest mod p, also $\left(\frac{r}{p}\right) = -1$. Aber (10) gibt sofort $\left(\frac{p}{r}\right) = 1$ und nach dem Reziprozitätsgesetz kommt $\left(\frac{r}{p}\right) = 1$, also ein Widerspruch.

Aus der Beweisführung von Satz 13 geht hervor, daß entweder eine der Gleichungen (8), (9) oder die Nicht-Pellsche Gleichung $x^2 - 2py^2 = -1$ lösbar sein muß. Wir haben

Satz 15. *Ist* $p \equiv 9 \bmod 16$ *eine Primzahl, die Zahl* 2 *ein biquadratischer Nichtrest mod* p, *so ist die Nicht-Pellsche Gleichung* (3) *für* $m = 2p$ *lösbar.*

Satz 16. *Sind* $p \equiv 1$, $q \equiv 1 \bmod 4$ *Primzahlen und* p *kein biquadratischer Rest von* q, *so ist die Gleichung*

$$px'^2 - qy^2 = -1 \tag{11}$$

unlösbar.

Die Bedingungen des Satzes sind z. B. erfüllt, wenn $\left(\frac{q}{p}\right) = -1$, also nach dem Reziprozitätsgesetz auch $\left(\frac{p}{q}\right) = -1$ ist.

Beweis: (11) gibt sofort $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. Es bleibt nur der Fall zu erledigen, daß $\left(\frac{p}{q}\right) = 1$, aber p biquadratischer Nichtrest mod q ist.

Es ist x' gerade, sei $2^t \parallel x'$, also $x' = 2^t x$ mit ungeradem x. Die Gleichung (11) wird

$$p \cdot 2^{2t}x^2 - qy^2 = -1. \tag{12}$$

1. Sei $q \equiv 5 \bmod 8$, also die Zahl $p \cdot 2^{2t}x^2$ biquadratischer Nichtrest mod q. Es muß $t = 1$ sein, da sonst (12) schon als Kongruenz mod 8 unmöglich wäre. Also ist $p \cdot 2^2x^2$ ein biquadratischer Nichtrest mod q, da -1 es ist. Nun ist aber nach Voraussetzung p ein biquadratischer Nichtrest mod q. Also ist 2^2x^2 ein biquadratischer Rest, $2x$ ein quadratischer Rest. Weiter ist $\left(\frac{2}{q}\right) = -1$, also ist $\left(\frac{x}{q}\right) = -1$. Aus (12) folgt aber $\left(\frac{q}{x}\right) = 1$, nach dem R.G. wird $\left(\frac{x}{q}\right) = 1$. Damit ist für $q \equiv 5 \bmod 8$ die Unmöglichkeit von (12) bewiesen.

2. Sei $q \equiv 1 \bmod 8$. Dann ist in (12) die Zahl $p \cdot 2^{2t}x^2$ ein biquadratischer Rest von q, also $2^{2t}x^2$ nicht biquadratischer Rest, da p es nicht ist. Mithin ist wegen $\left(\frac{2}{q}\right) = 1$ die Zahl x^2 kein biquadratischer Rest. Es bleibt: x ist kein quadratischer Rest, also $\left(\frac{x}{q}\right) = -1$, während aus der Gleichung und dem R.G. im Gegensatz hierzu $\left(\frac{x}{q}\right) = 1$ folgt.

Nun nehmen wir an, daß auch q biquadratischer Nichtrest mod p sei. Dann ist auch eine Gleichung

$$qx'^2 - py^2 = -1 \tag{13}$$

unmöglich. Gehen wir nun aus von der kleinsten Lösung der Pellschen Gleichung

$$x^2 - pqy^2 = 1$$

— sie heiße $[a, b]$ —, so ist a ungerade, also $a+1$, $a-1$ gerade, und aus

$$a^2 - pqb^2 = 1$$

ergeben sich wieder folgende Möglichkeiten:

$$a+1 = 2a'^2,\ a-1 = 2pqb'^2, \tag{14}$$
$$a+1 = 2qa'^2,\ a-1 = 2pb'^2, \tag{15}$$
$$a+1 = 2pa'^2,\ a-1 = 2qb'^2, \tag{16}$$
$$a+1 = 2pqa'^2,\ a-1 = 2b'^2. \tag{17}$$

Es ist $a>1$, somit in allen Fällen $0<a'<a$. (14) ergibt einen Widerspruch, da sich dann $[a', b']$ als noch kleinere Lösung der Pellschen Gleichung ergeben würde. (15), (16) hätten eine Lösung von (11), (13) zur Folge. Es bleibt nur (17), somit

$$b'^2 - pqa'^2 = -1.$$

Wir haben

Satz 17. *Sind die Primzahlen p, q, beide von der Form $4n+1$ und gegenseitig biquadratische Nichtreste (z. B. gegenseitige quadratische Nichtreste), so ist die Nicht-Pellsche Gleichung*

$$x^2 - pqy^2 = -1$$

lösbar.

Gewöhnlich erfolgt die Auflösung der Pellschen und Nicht-Pellschen Gleichung mit Hilfe der Kettenbrüche, die wir in diesem Buche nicht besprechen wollen.

§ 39. Einiges über Kreisteilungskörper

Ist l eine ungerade Primzahl, so heißt die Gleichung $(l-1)$-ten Grades

$$f(x) = \frac{x^l - 1}{x - 1} = x^{l-1} + x^{l-2} + \cdots + x^2 + x + 1 = 0$$

Kreisteilungsgleichung, $f(x)$ ein Kreisteilungspolynom. Die Wurzeln sind

$$x_j = e^{\frac{2\pi ij}{l}}$$

mit $0 < j < l$. Sie sind die primitiven l-ten Einheitswurzeln.

Im folgenden werden wir unter ζ eine nicht näher bestimmte primitive l-te Einheitswurzel verstehen. Dies rechtfertigt sich dadurch, daß $f(x)$ irreduzibel ist. Wir wollen dies gleich allgemeiner für das Kreisteilungspolynom der l^u-ten Einheitswurzeln

$$F(x) = \frac{x^{l^u} - 1}{x^{l^{u-1}} - 1} = x^{l^{u-1}(l-1)} + x^{l^{u-1}(l-2)} + \cdots + x^{l^{u-1}} + 1$$

nachweisen. Dazu brauchen wir das Eisensteinsche Irreduzibilitätskriterium, das wir im folgenden Satze wiedergeben:

Satz 1. *Ist das ganzzahlige Polynom*

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n,$$

wobei alle a_j $(0 \leqq j < n)$ durch eine Primzahl l teilbar sind, reduzibel, so ist $a_0 \equiv 0 \bmod l^2$.

Beweis: Sei $f(x) = g(x)\, h(x)$, wobei die Gradzahlen r, s der normierten, ganzzahligen Polynome $g(x)$, $h(x)$ beide positiv sind, weiter $r + s = n$ ist. Dieser Zerlegung in $\mathsf{P}[x]$ entspricht eine in $\mathsf{P}_l[x]$. In $\mathsf{P}_l[x]$ kann aber $f(x) = x^n$ gesetzt werden. Dies hat mit den Gradzahlen r, s als bezügliche Zerlegung nur $x^r \cdot x^s$. Mithin ist

$$g(x) = b_0 + \cdots + b_{r-1} x^{r-1} + x^r \equiv x^r \bmod l,$$
$$h(x) = c_0 + \cdots + c_{s-1} x^{s-1} + x^s \equiv x^s \bmod l,$$

also alle b_j und $c_j \equiv 0 \bmod l$ und $a_0 = b_0 c_0 \equiv 0 \bmod l^2$.
Wir können dies auch so aussprechen (gewöhnliche Formulierung des Eisensteinschen Irreduzibilitätskriteriums):

Satz 2. *Ist in $f(x) = a_0 + \cdots + a_{n-1} x^{n-1} + x^n$, wobei die a_j ganzzahlig und durch eine Primzahl l teilbar sind, $l \parallel a_0$, so ist $f(x)$ irreduzibel.*

Nun wird

$$F(1 - z) = \frac{(1 - z)^{l^u} - 1}{(1 - z)^{l^{u-1}} - 1} = \sum_{j=0}^{l-1} (1 - z)^{j l^{u-1}} = l + \cdots,$$

es wird jeder Koeffizient von z^t $(0 \leqq t < l^{u-1}(l-1))$ durch l teilbar. Denn dieser Koeffizient ist

$$(-1)^t \sum_j \binom{j\, l^{u-1}}{t}.$$

Es sei $u - 1 = v$.
In irgendeinem Körper der Charakteristik l ist

$$(a + b)^{l^v} = a^{l^v} + b^{l^v},$$

mithin

$$(a+b)^{jl^v} = \sum_{k=0}^{l-1} \binom{j}{k} a^{(j-k)l^v} b^{kl^v}.$$

Es brauchen nur die Werte $\sum_{j=0}^{l-1} \binom{j}{t}$ für $0 < t < l$ in Betracht gezogen zu werden.

Hier gilt

$$\binom{0}{t} + \binom{1}{t} + \cdots + \binom{l-1}{t} = \left(\frac{1+x+x^2+\cdots+x^{l-1}}{t!}\right)^{(t)}\Bigg|_{x=1},$$

also bleiben die Koeffizienten von $\frac{(1+h)^l - 1}{h}$, die offenbar bis auf den von h^{l-1} durch l teilbar sind, übrig.

Es sind also die Voraussetzungen des Eisensteinschen Irreduzibilitätskriteriums erfüllt. Es folgt

Satz 3. *Das Kreisteilungspolynom der l^u-ten Einheitswurzeln ist irreduzibel. Dabei ist $u \geqq 1$, l eine Primzahl.*

Bemerkung: Im Beweis von Satz 3 ist nirgends die Voraussetzung $l > 2$ vorgekommen. Der Satz gilt auch für $l = 2$.

Nun betrachten wir mit $l > 2$ den Kreisteilungskörper der l-ten Einheitswurzeln. Es ist

$$1, \zeta, \zeta^2, \ldots, \zeta^{l-2} \tag{1}$$

eine Basis für alle Körperzahlen. Sicher sind alle Zahlen $\sum_{j=0}^{l-2} a_j \zeta^j$ mit ganzen rationalen a_j ganz. Nun ist aber die Frage, ob (1) eine Körperbasis ist.

Wir haben

$$f(x) = 1 + x + \cdots + x^{l-1} = (x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{l-1}).$$

Durch Einsetzen von $x = 1$ ergibt sich

$$l = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{l-1})$$

oder mit der ein für allemal eingeführten Abkürzung $\lambda = 1 - \zeta$:

$$l = \lambda^{l-1} \varepsilon_2 \varepsilon_3 \ldots \varepsilon_{l-1}, \tag{2}$$

wobei $\varepsilon_j = \frac{1-\zeta^j}{1-\zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{j-1}$ eine ganze Zahl des Körpers ist. Nun ist aber auch

$$\varepsilon_j^{-1} = \frac{1-\zeta}{1-\zeta^j}$$

ganz. Denn es sei $jk \equiv 1 \bmod l$. Wegen $1 < j < l$ hat diese Kongruenz sicher eine Wurzel k, die wir im Intervall $(0, l)$ annehmen können. Es wird

$$\varepsilon_j^{-1} = \frac{1-\zeta^{jk}}{1-\zeta^j} = 1 + \zeta^j + \zeta^{2j} + \cdots + \zeta^{(k-1)j},$$

also ganz. Die in (2) auftretenden Größen ε_j sind daher Einheiten. (2) hat somit die Gleichung in Idealen

$$(l) = (\lambda)^{l-1} \tag{3}$$

zur Folge. Es ist (λ) Primideal, denn die kanonische Zerlegung von (l) in $k = \mathsf{P}(\zeta)$ hat die Form

$$(l) = \mathfrak{l}_1^{e_1} \mathfrak{l}_2^{e_2} \cdots \mathfrak{l}_g^{e_g}$$

mit $e_1 f_1 + e_2 f_2 + \cdots + e_g f_g = l - 1$, wenn f_j der Grad von $\mathfrak{l}_j$ ist. Es muß (λ) durch $\mathfrak{l}_1, \ldots, \mathfrak{l}_g$ teilbar sein, etwa $\mathfrak{l}_j^{A_j} \parallel (\lambda)$.
Es folgt

$$(l-1) \sum_{j=1}^{g} e_j f_j A_j = l - 1$$

oder

$$\sum_{j=1}^{g} e_j f_j A_j = 1,$$

was nur für $g = 1$, $e_1 = f_1 = A_1 = 1$ möglich ist. Es wird $(\lambda) = \mathfrak{l}_1$. Also haben wir

Satz 4. *In $k = \mathsf{P}(\zeta)$ wird die Primzahl l die $(l-1)$-te Potenz des Hauptprimideals ersten Grades (λ).*

Die Diskriminante $\Delta(\zeta)$ ist leicht zu bestimmen. Zunächst gibt es keinen reellen Körper, aber $\frac{l-1}{2}$ Paare konjugiertkomplexer Körper. Mit den eingeführten Bezeichnungen ist also $r_1 = 0$, $r_2 = \frac{l-1}{2}$, $r = r_1 + r_2 - 1 = \frac{l-3}{2}$. Somit ist

$$\operatorname{sgn} \Delta(\zeta) = (-1)^{r_2} = (-1)^{\frac{l-1}{2}}.$$

Weiter ist

$$\Delta(\zeta) = \prod_{0<j<i<l} (\zeta^i - \zeta^j)^2,$$

also

$$|\Delta(\zeta)| = \left| \prod_{j,\, i \atop j \neq i} (\zeta^i - \zeta^j) \right|.$$

Bei festem i ist

$$\prod_{j \neq i} (\zeta^i - \zeta^j) = \zeta^i \prod_{j \neq i} (1 - \zeta^{j-i})$$

$$= \zeta^i \prod_{\substack{t=1 \\ t \neq l-i}}^{l-1} (1 - \zeta^t) = \frac{\zeta^i}{1 - \zeta^{-i}} \prod_{t=1}^{l-1} (1 - \zeta^t)$$

oder einfach

$$\left| \prod_{j \neq i} (\zeta^i - \zeta^j) \right| = \frac{l}{|1 - \zeta^{-i}|} = \frac{l}{|1 - \zeta^i|}.$$

Endgültig kommt

$$|\Delta(\zeta)| = \frac{l^{l-1}}{\Pi |1 - \zeta^i|} = \frac{l^{l-1}}{l} = l^{l-2}$$

oder

$$\Delta(\zeta) = (-1)^{\frac{l-1}{2}} l^{l-2}. \tag{4}$$

Die Körperdiskriminante d ist gleich $\Delta(\zeta)$, eventuell dividiert durch das Quadrat einer ganzen rationalen Zahl, also hier durch eine Potenz von l mit geradem Exponenten. Die Frage, ob (1) eine Körperbasis ist, kann als gleichwertig mit der betrachtet werden, ob

$$1, \lambda, \lambda^2, \ldots, \lambda^{l-2} \tag{5}$$

eine solche ist. Denn wegen

$$1 = 1,$$

$$\lambda = 1 - \zeta,$$

$$\lambda^2 = 1 - \binom{2}{1}\zeta + \zeta^2,$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\lambda^{l-2} = 1 - \binom{l-2}{1}\zeta + \ldots - \zeta^{l-2}$$

geht (5) aus (1) durch eine lineare Transformation mit der Matrix

$$\mathfrak{A} = \begin{pmatrix} 1 & & \\ 1 & -1 & \\ 1 & -\binom{2}{1} & 1 \\ \vdots & \vdots & \vdots \\ 1 & -\binom{l-2}{1} & \binom{l-2}{2} \ldots -1 \end{pmatrix}.$$

hervor, wobei abs $|\mathfrak{A}| = 1$ ist und leere Stellen Nullen bedeuten. Bei Aufstellung einer kanonischen Basis muß also zunächst untersucht werden, ob eine Zahl

$$\gamma = \frac{a_1 + a_2\lambda + \cdots + a_{t-1}\lambda^{t-2} + \lambda^{t-1}}{l} \tag{6}$$

eine ganze Zahl darstellen kann.

Es ist $$g(x) = f(1-x) = \frac{(1-x)^l - 1}{-x}$$

$$= x^{l-1} - \binom{l}{1}x^{l-2} + \binom{l}{2}x^{l-3} + \cdots + l$$

das normierte ganzzahlige irreduzible Polynom $g(x)$, dessen Wurzel λ ist. Es folgt $\lambda^{\mathfrak{N}} = l$, $\left(\frac{1}{\lambda}\right)^{\mathfrak{N}} = \frac{1}{l}$. Die Zahl γ ist sicher nicht ganz, wenn

$$\delta = \frac{a_1 + a_2\lambda + \cdots + a_{t-1}\lambda^{t-2} + \lambda^{t-1}}{\lambda}$$

nicht ganz ist (nach Formel (3)). Es ist aber

$$\delta = \frac{a_1}{\lambda} + \sigma,$$

wobei $\sigma = a_2 + a_3\lambda + \ldots a_{t-1}\lambda^{t-3} + \lambda^{t-2}$ ganz ist, somit δ genau dann ganz, wenn $\frac{a_1}{\lambda}$ ganz ist. Es ist aber $\left(\frac{a_1}{\lambda}\right)^{\mathfrak{N}} = \frac{a_1^{l-1}}{l}$, das ist also nur im Falle $l \mid a_1$ ganz, wo in der Formel (6) die Zahl a_1 weggelassen werden kann. Die verbleibende Zahl

$$\gamma' = \frac{a_2\lambda + \cdots + \lambda^{t-1}}{l}$$

kann ebenso behandelt werden, es bleibt $a_2 \equiv 0 \bmod l$, und Fortsetzung des Verfahrens gibt schließlich $a_t = 1 \equiv 0 \bmod l$, also einen Widerspruch. Es folgt

Satz 5. *Im Kreisteilungskörper der l-ten Einheitswurzeln, in denen l eine ungerade Primzahl ist, ist* $1, \lambda, \lambda^2, \ldots, \lambda^{l-2}$ *oder auch*

eine Körperbasis. $$1, \zeta, \zeta^2, \ldots, \zeta^{l-2}$$

Zugleich folgt aus Formel (4)

Satz 6. *Die Diskriminante d des Kreisteilungskörpers der l-ten Einheitswurzeln erfüllt*

$$d = (-1)^{\frac{l-1}{2}} l^{l-2}.$$

Nun sei p eine von l verschiedene Primzahl in P, p gehöre mod l zum Exponenten $f \mid l-1 = fg$. Es sei $h(x)$ ein irreduzibles Polynom f-ten Grades in $\mathsf{P}_p[x]$. Adjungieren wir zu P_p symbolisch eine Wurzel α von h, so erhalten wir $\mathsf{P}_p(\alpha) = GF(p^f)$. Jedes Element $\xi \neq 0$ des Galoisfeldes ist dann von der Form

$$\xi = \alpha^t$$

mit $0 \leqq t < p^f - 1$. Es sei speziell

$$\xi = \alpha^{\frac{p^f-1}{l}}.$$

Dann ist

$$\xi^l = 1. \tag{7}$$

Wir haben aber $\xi \neq 1$, da erst die (p^f-1)-te Potenz von α gleich Eins (Einselement in P_p oder $GF(p^f)$) ist, keine mit einem niedrigeren ganzen positiven Exponenten. Das Polynom $u(x)$, dem ξ genügt, ist also in $\mathsf{P}_p[x]$ ein Teiler von $\frac{x^l-1}{x-1} = x^{l-1} + x^{l-2} + \cdots + 1$. Es ist ein irreduzibler Teiler. Dies zeigen wir so: Das Galoisfeld $\mathsf{P}_p(\xi) = GF(p^t)$ erfüllt zunächst $t \leqq f$. Es ist

$$\xi^{p^t-1} = 1, \tag{8}$$

also folgte wegen (7) im Falle $p^t - 1 \not\equiv 0 \bmod l$ nach Angabe zweier ganzer rationaler X, Y mit

$$(p^t-1)\,X + l\,Y = 1$$

durch Erhebung von (7) zur Potenz Y, von (8) zur Potenz X und Multiplikation die Gleichung $\xi = 1$, also ein Widerspruch. Damit ist $p^t \equiv 1 \bmod l$ gezeigt, zugleich $t \geqq f$, da $p \bmod l$ zu f gehört. Es ist also $u(x)$ irreduzibel in $\mathsf{P}_p[x]$. Die Gleichung

$$x^{l-1} + x^{l-2} + \cdots + x + 1 = 0$$

kann in einem Erweiterungskörper von P_p keine mehrfache Wurzel haben, denn sonst hätte auch

$$v(x) = x^l - 1$$

in einem solchen Körper über P_p mehrfache Wurzeln; $v(x)$ hat aber mit $v'(x)$ keine Wurzel gemein, denn

$$v'(x) = l x^{l-1}.$$

Wohlgemerkt: $v'(x)$ ist nicht das Nullpolynom, denn l ist von p verschieden. Mithin hat $u(x)$ die Wurzeln

$$\xi,\ \xi^p,\ \xi^{p^2},\ \ldots,\ \xi^{p^{f-1}},$$

die alle voneinander verschieden und primitive l-te Einheitswurzeln im Galoisfeld sind. Ist $l-1=fg>f$, d. h. $g>1$, oder die Primzahl p keine primitive Wurzel mod l, so hat die zyklische Gruppe $\mathfrak{G}$ der zu l primen Reste mod l die Gruppe $\{p\}$, wobei jede Potenz von p durch ihren Rest mod l zu ersetzen ist, als Normalteiler vom Index g. Ist dann

$$\mathfrak{G}=\{p\}+c_2\{p\}+\cdots+c_g\{p\}$$

eine Lagrangesche Verteilung von $\mathfrak{G}$ nach $\{p\}$, so ist für jedes $j\,(2\leqq j\leqq g)$ die Gesamtheit

$$\xi^{c_j},\ \xi^{c_j p},\ \ldots,\ \xi^{c_j p^{f-1}} \tag{9}$$

wieder ein System von f primitiven l-ten Einheitswurzeln, und das aus ihnen aufgebaute Polymon

$$u_j(x)=\prod_{t=0}^{f-1}(x-\xi^{c_j p^t}), \tag{10}$$

dessen Koeffizienten in $\mathsf{P}_p[x]$ liegen, ist ebenfalls Teiler des Kreisteilungspolynoms und irreduzibel. Nach den Ausführungen in § 34 gilt

Satz 7. *Gehört eine von l verschiedene Primzahl p mod l zum Exponenten f, so wird in k die kanonische Zerlegung von p*

$$(p)=\mathfrak{p}_1\cdots\mathfrak{p}_g\ ,$$

wobei die $\mathfrak{p}_j$ Primideale f-ten Grades sind und $fg=l-1$ ist.

Wir schließen mit einigen Bemerkungen:

Ist eine allgemeine primitive M-te Einheitswurzel gegeben, so ist diese eine Lösung von $T(x)=x^{M-1}+x^{M-2}+\cdots+1=0$, was aber (außer im Falle $M=l$, wie eben besprochen) nicht irreduzibel ist. Heißt diese Einheitswurzel wieder ζ, so ist

$$T(x)=(x-\zeta)\,(x-\zeta^2)\ldots(x-\zeta^{M-1}),$$

und analog wie früher gibt $x=1$

$$M=(1-\zeta)\,(1-\zeta^2)\ldots(1-\zeta^{M-1}).$$

Es sei noch gegeben

$$U(x)=x^{R-1}+x^{R-2}+\cdots+1,$$

ϱ sei eine primitive Wurzel von $U(x)$, wir nehmen $(M,\,R)=1$ und selbstverständlich $\min(M,\,R)>1$ an. Genau wie früher gilt

$$R=(1-\varrho)\ldots(1-\varrho^{R-1}).$$

Es bleibt $1-\zeta \mid M$, $1-\varrho \mid R$.
Wir betrachten $\varrho\zeta$, also eine primitive MR-te Einheitswurzel, insbesondere sei $1-\varrho\zeta=\alpha$. Es ist $\alpha \mid 1-\varrho^M\zeta^M=1-\varrho^M$.
Es ist $\beta=\frac{1-\varrho}{1-\varrho^M}$ ganz, denn mit x als Lösung von $xM \equiv 1 \bmod R$,
was wegen $(M, R)=1$ löslich ist, wird $\beta=1+\varrho^M+\cdots+\varrho^{M(x-1)}$.
Offenbar ist β Einheit. Es folgt $\alpha \mid 1-\varrho \mid R$, genau so $\alpha \mid 1-\zeta \mid M$ daher $\alpha \mid (R, M)=1$, also α ist Einheit. Es bleibt

Satz 8. *Sind M, R natürliche Zahlen >1, $(M, R)=1$, ζ eine primitive M-te, ϱ eine primitive R-te Einheitswurzel, so ist $1-\varrho\zeta$ eine Einheit.*

Von allgemeinem Interesse und auch später von großer Wichtigkeit sind die folgenden Sätze.

Satz 9. *In einem Körper vom Grade n gibt es nur endlich viele ganze algebraische Zahlen, deren sämtliche Konjugierte einen Absolutbetrag $<M$ (vorgegebene positive Größe) haben.*

Beweis: $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ sei das Polynom der Hauptgleichung für ein solches α mit $|\alpha^{(j)}|<M, j=1, 2, 3, \ldots, n$.
Dann ist $|a_j| \leqq \binom{n}{j} M^j$. Es bleiben nur endlich viele ganzzahlige Polynome.

Satz 10. *Eine ganze algebraische Zahl, deren sämtliche Konjugierte den Absolutbetrag Eins haben, ist eine Einheitswurzel.*

Beweis: Die Potenzen einer solchen Zahl α haben die gleiche Eigenschaft, also müssen unter ihnen gleiche vorkommen; mit A und B als natürlichen Zahlen muß $\alpha^{A+B}=\alpha^A$ sein. Dann ist $\alpha^B=1$.

Satz 11. *Im Körper der primitiven l-ten Einheitswurzeln ist jede Einheit Produkt einer Einheitswurzel und einer reellen Einheit. (l sei jetzt wieder Primzahl >2.)*

Beweis: $1, \zeta, \zeta^2, \ldots, \zeta^{l-2}$ ist eine Körperbasis, $f(\zeta)$, wobei f ein ganzzahliges Polynom eines Grades $<l-1$ ist, ist eine ganze algebraische Zahl. Sei speziell $\eta=f(\zeta)$ Einheit. Dann ist $\frac{f(\zeta)}{f(\zeta^{-1})}$ eine Einheit mit den Eigenschaften des Satzes 10, also eine Einheitswurzel in $\mathsf{P}(\zeta)$, also

$$\frac{f(\zeta)}{f(\zeta^{-1})}=\pm\zeta^{-2t}.$$

Hierbei ist t ganzzahlig, oder

$$\frac{\zeta^t f(\zeta)}{\zeta^{-t} f(\zeta^{-1})} = \pm 1.$$

Nun kommt alles darauf an, zu zeigen, daß das negative Vorzeichen ausgeschlossen ist.
Stets ist, wenn $g(x)$ ein Polynom mit ganzen rationalen Zahlen als Koeffizienten ist, die Beziehung

$$g(\zeta) \equiv g(\zeta^a) \bmod \lambda$$

erfüllt. Ist

$$\frac{\zeta^t f(\zeta)}{\zeta^{-t} f(\zeta^{-1})} = -1,$$

so erhalten wir

$$f(\zeta) \equiv -(f(\zeta) \bmod \lambda,$$
$$2f(\zeta) \equiv 0 \bmod \lambda;$$

da 2 zu λ (Hauptprimidealfaktor von l) prim ist, sehen wir:

$$f(\zeta) \equiv 0 \bmod \lambda,$$

was unmöglich ist, da $f(\zeta)$ eine Einheit ist.
Es ist also $\zeta^t f(\zeta)$ total reell (in allen konjugierten Körpern reell) und

$$f(\zeta) = \zeta^{-t}\varepsilon,$$

wobei ε eine total reelle Einheit ist.

§ 40. Die Endlichkeit der Klassenzahl

Gegeben sei eine positivhomogene Funktion $f(\mathfrak{x})$ des n-dimensionalen Vektors $\mathfrak{x}$, die das Dreiecksaxiom

$$f(\mathfrak{x} + \mathfrak{y}) \leqq f(\mathfrak{x}) + f(\mathfrak{y})$$

erfüllt. Die Dimension der homogenen Funktion sei 1, also gelte

$$f(t\mathfrak{x}) = |t| f(\mathfrak{x}).$$

Insbesondere ist $f(-\mathfrak{x}) = f(\mathfrak{x})$. Jeder Bereich $f(\mathfrak{x}) \leqq \alpha$ liege ganz im Endlichen. Es enthalte

$$f(\mathfrak{x}) \leqq 2\lambda$$

keinen Gitterpunkt. (Der in jedem dieser Bereiche liegende Anfangspunkt werde nicht gerechnet.) Nach Anbringung parallelverschobener Bereiche

$$f(\mathfrak{x} - \mathfrak{x}_1) \leqq \lambda$$

um jeden Gitterpunkt $\mathfrak{x}_1$ sind zwei solche elementfremd, denn wären $\mathfrak{x}_1, \mathfrak{x}_2$ zwei voneinander verschiedene Gitterpunkte, und es gäbe einen Vektor $\mathfrak{y}$, der

$$f(\mathfrak{y}-\mathfrak{x}_1) \leqq \lambda, \quad f(\mathfrak{y}-\mathfrak{x}_2) \leqq \lambda$$

erfüllte, so wäre

$$f(\mathfrak{x}_2-\mathfrak{x}_1) \leqq f(\mathfrak{y}-\mathfrak{x}_1)+f(\mathfrak{y}-\mathfrak{x}_2) \leqq 2\lambda,$$

es enthielte $f(\mathfrak{x}) \leqq 2\lambda$ doch nichttrivial einen Gitterpunkt.

Nun definieren wir $\alpha = \max\{\max|x_i|\}$ in $|f(\mathfrak{x})| \leqq 2\lambda$. Wir geben den x_i unabhängig voneinander die Werte $0, \pm 1, \pm 2, \ldots, \pm T$, haben also $(2T+1)^n$ Gitterpunkte, um die wir jeweils die aus $f(\mathfrak{x}) \leqq \lambda$ durch Parallelverschiebungen hervorgehenden Bereiche anbringen. V_λ sei das Volumen von $f(\mathfrak{x}) \leqq \lambda$. Wir erhalten

$$(2T+\alpha)^n > (2T+1)^n V_\lambda$$

oder

$$\left(\frac{2T+\alpha}{2T+1}\right)^n > V_\lambda.$$

$T \to \infty$ gibt $1 \geqq V_\lambda$.

Nun ist $V_\lambda = \lambda^n V_1$; für $\lambda^n V_1 > 1$ oder $\lambda > \frac{1}{\sqrt[n]{V_1}}$ liegt in $f(\mathfrak{x}) \leqq 2\lambda$ bestimmt nichttrivial ein Gitterpunkt. Mit $2\lambda = \varkappa$ gilt dasselbe für $\varkappa > \sqrt[n]{\frac{2^n}{V_1}} = \sqrt[n]{\frac{1}{V_{\frac{1}{2}}}}$. Auch bei Gleichheitszeichen gilt dasselbe, denn sonst müßte der Bereich nichttrivial keinen Gitterpunkt enthalten, weder an der Oberfläche noch im Innern, aber bei jeder beliebig kleinen Vergrößerung von $\varkappa$.

Wir erhalten

Satz 1. *Ist* $\varkappa \geqq V_{\frac{1}{2}}^{-\frac{1}{n}}$, *so enthält der Bereich* $f(\mathfrak{x}) \leqq \varkappa$ *bestimmt nichttrivial einen Gitterpunkt.*

Die zu einem ganzen Ideal $\mathfrak{a}$ mit der Modulbasis $[\alpha_1, \ldots, \alpha_n]$ gehörige Linearform $f = \sum \alpha_t x_t$ werde in den n Körpern durch die n Linearformen $f_j = \sum \alpha_t^{(j)} x_t$ realisiert. Dabei seien $k^{(1)}, \ldots, k^{(r_1)}$ die reellen Körper, hierauf seien $k^{(r_1+1)}$, $k^{(r_1+2)}$ konjugiertkomplex, ebenso $k^{(r_1+3)}$, $k^{(r_1+4)}$ usf. Die Anordnung (A)[1] werde hier nicht eingehalten.

---

[1]) Vgl. S. 109.

Mit $j \leqq r_1$ sei $f_j = g_j$.
Für $j > r_1$ setzen wir der Reihe nach mit reellen g_j

$$f_{r_1+1} = g_{r_1+1} + i g_{r_1+2},$$
$$f_{r_1+2} = g_{r_1+1} - i g_{r_1+2},$$
$$f_{r_1+3} = g_{r_1+3} + i g_{r_1+4},$$
$$f_{r_1+4} = g_{r_1+3} - i g_{r_1+4},$$
$$\cdots\cdots\cdots\cdots$$

Wir fragen uns, in welchem Bereich sicher eine von Null verschiedene (ganze) Zahl von $\mathfrak{a}$ liegt. Hierzu rechnen wir das Volumen des Bereichs.

$$\frac{1}{n}\sum |f_j| \leqq \frac{1}{2}$$

aus, also $V_{\frac{1}{2}}$. Um die Schreibweise zu verkürzen, schreiben wir den Absolutbetrag einer Funktionaldeterminante $\left|\frac{\partial(x_1, \ldots, x_n)}{\partial(y_1, \ldots, y_n)}\right|$ kurz mit $\mathfrak{x}/\mathfrak{y}$, wenn $\mathfrak{x} = (x_1, \ldots, x_n)$, $\mathfrak{y} = (y_1, \ldots, y_n)$ ist. Es ist

$$V_{\frac{1}{2}} = \int \cdots \int dx_1 \ldots dx_n$$

mit $\frac{1}{n}\sum |f_j| \leqq \frac{1}{2}$. Mit $z_j = f_j$, $\mathfrak{z} = (z_1, \ldots, z_n)$ ist $\mathfrak{x}/\mathfrak{z} = \frac{1}{\mathfrak{a}^N |\sqrt{\bar{d}}|}$.
Mit $z_1 = y_1, \ldots, z_{r_1} = y_{r_1}, z_{r_1+1} = y_{r_1+1} + i y_{r_1+2}, z_{r_1+2} = y_{r_1+1} - i y_{r_1+2}$, ..., also reellem Vektor $\mathfrak{y}$, wird (leere Stellen sind Nullen) bei analoger Bezeichnung

$$\mathfrak{z}/\mathfrak{y} = \operatorname{abs}\begin{vmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & i & \\ & & & 1 & -i & \\ & & & & & \ddots \end{vmatrix} = 2^{r_2}.$$

Somit berechnet sich

$$V_{\frac{1}{2}} = \frac{2^{r_2}}{\mathfrak{a}^N |\sqrt{\bar{d}}|} \int \cdots \int dy_1 \ldots dy_n$$

über den Bereich

$$\frac{1}{n}\left(|y_1| + |y_2| + \cdots + |y_{r_1}| + 2\sqrt{y_{r_1+1}^2 + y_{r_1+2}^2} + 2\sqrt{y_{r_1+3}^2 + y_{r_1+4}^2} + \cdots\right) \leqq \frac{1}{2}.$$

Denn es ist

$$|z_{r_1+1}| = |z_{r_1+2}| = \sqrt{y_{r_1+1}^2 + y_{r_1+2}^2}.$$

Dies läßt sich aber mit allen $y_j \geqq 0$ in

$$V_{\frac{1}{2}} = \frac{2^{r_2}}{\mathfrak{a}^N |\sqrt{\vec{d}}|} \int \cdots \int d y_1 \cdots d y_n$$

umgestalten, wobei jetzt aber der Bereich

$$\frac{1}{n} \left(y_1 + y_2 + \cdots + y_{r_1} + 2\sqrt{y_{r_1+1}^2 + y_{r_1+2}^2} + \cdots\right) \leqq 1$$

ist.

Nun kommt die letzte Transformation

$y_1 = w_1, \ldots, y_{r_1} = w_{r_1}, y_{r_1+1} = w_{r_1+1} \cos\varphi_1, y_{r_1+2} = w_{r_1+1} \sin\varphi_1, \ldots$ mit der Funktionaldeterminante $w_{r_1+1} w_{r_1+2} \cdots w_{r_1+r_2}$. Wir erhalten

$$V_{\frac{1}{2}} = \frac{2^{r_2}}{\mathfrak{a}^N |\sqrt{\vec{d}}|} \int \cdots \int w_{r_1+1} \cdots w_{r_1+r_2} d w_1 \cdots d w_{r_1} d w_{r_1+1} \cdots d w_{r_1+r_2} I,$$

wobei

$$I = \int_0^{\frac{\pi}{2}} d\varphi_1 \int_0^{\frac{\pi}{2}} d\varphi_2 \cdots \int_0^{\frac{\pi}{2}} d\varphi_{r_2} = \left(\frac{\pi}{2}\right)^{r_2}$$

ist. Es wird

$$V_{\frac{1}{2}} = \frac{\pi^{r_2}}{\mathfrak{a}^N |\sqrt{\vec{d}}|} \int \cdots \int w_{r_1+1} \cdots w_{r_1+r_2} d w_1 \cdots d w_{r_1+r_2}$$

mit dem Bereich, daß alle $w_j \geqq 0$ und

$$\frac{1}{n} (w_1 + \cdots + w_{r_1} + 2 w_{r_1+1} + \cdots + 2 w_{r_1+r_2}) \leqq 1 \quad \text{ist.}$$

Nun gehen wir an die Verwendung der Dirichlet-Formel. Sind alle $x_j \geqq 0$, $\left(\frac{x_1}{a_1}\right)^{\lambda_1} + \cdots + \left(\frac{x_m}{a_m}\right)^{\lambda_m} \leqq 1$, so ist das m-fache Integral über diesen Bereich

$$\int \cdots \int x_1^{\alpha_1 - 1} \cdots x_m^{\alpha_m - 1} d x_1 \cdots d x_m$$

$$= \frac{a_1^{\alpha_1} \cdots a_m^{\alpha_m}}{\lambda_1 \cdots \lambda_m} \frac{\Gamma\left(\frac{\alpha_1}{\lambda_1}\right) \cdots \Gamma\left(\frac{\alpha_m}{\lambda_m}\right)}{\Gamma\left(1 + \frac{\alpha_1}{\lambda_1} + \frac{\alpha_2}{\lambda_2} + \cdots + \frac{\alpha_m}{\lambda_m}\right)}.$$

Hier ist $\frac{\alpha_j}{\lambda_j}=1$ für $j \leqq r_1$, dagegen $\frac{\alpha_j}{\lambda_j}=2$ für $j>r_1$. Die Gammafunktionen im Zähler werden also alle gleich eins. Hingegen wird das Argument der Gammafunktion im Nenner $1+r_1+2r_2=n+1$, die Gammafunktion selbst $\Gamma(n+1)=n!$ Es ist der Reihe nach

$$\frac{1}{a_1}=\frac{1}{n}, \ldots, \frac{1}{a_{r_1}}=\frac{1}{n}, \quad \frac{1}{a_{r_1+1}}=\frac{2}{n}, \ldots,$$

also

$$a_1=n, \ldots, a_{r_1}=n, \; a_{r_1+1}=\frac{n}{2}, \ldots$$

Weiter ist

$$\alpha_1=1, \ldots, \alpha_{r_1}=1, \; \alpha_{r_1+1}=2, \ldots, \alpha_{r_1+r_2}=2.$$

Die λ_j sind alle $=1$. Es wird

$$a_1^{\alpha_1} \ldots a_n^{\alpha_n}=n^{r_1+2r_2}\frac{1}{4^{r_2}}=\frac{n^n}{4^{r_2}},$$

und es bleibt

$$V_{\frac{1}{2}}=\frac{\pi^{r_2}}{\mathfrak{a}^{\mathsf{N}}|\sqrt{d}|}\frac{n^n}{4^{r_2}\,n!}=\left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!\,\mathfrak{a}^{\mathsf{N}}|\sqrt{d}|}.$$

Da in $\frac{1}{n}\sum|f_j(\mathfrak{x})| \leqq V_{\frac{1}{2}}^{\frac{1}{n}}$ nichttrivial ein Gitterpunkt liegt, haben wir

Satz 2. *In jedem ganzen Ideal* $\mathfrak{a}$ *gibt es eine von Null verschiedene Zahl* α *mit*

$$\left\{\sum\frac{1}{n}|\alpha^{(j)}|\right\}^n \leqq \left(\frac{4}{\pi}\right)^{r_2}\frac{\mathfrak{a}^{\mathsf{N}}n!\,|\sqrt{d}|}{n^n}.$$

Da bei ungleichen positiven Zahlen das geometrische Mittel immer kleiner als das arithmetische Mittel ist, so bleibt die Ungleichung verstärkt bestehen, wenn wir die linke Seite durch $\Pi\,|\alpha^{(j)}|=|\alpha^{\mathsf{N}}|$ ersetzen, also

Satz 3. *Für ein ganzes Ideal* $\mathfrak{a}$ *gibt es ein von Null verschiedenes* $\alpha \equiv 0 \bmod \mathfrak{a}$ *mit*

$$|\alpha^{\mathsf{N}}| \leqq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!\,\mathfrak{a}^{\mathsf{N}}|\sqrt{d}|}{n^n}.$$

Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ (vom Nullideal werde immer abgesehen) heißen *äquivalent*, wenn es eine Zahl β gibt, so daß $\mathfrak{b}=\beta\mathfrak{a}$ ist. Sofort sieht man, daß diese Eigenschaft die Postulate: Reflexivität, Symmetrie und Transitivität erfüllt. Man schreibt $\mathfrak{a} \sim \mathfrak{b}$. Äquivalente Ideale faßt man in eine *Klasse* zusammen. Die Hauptideale bilden eine Klasse für sich, die *Hauptklasse*. Liegt $\mathfrak{a}$ in der Klasse C_1, $\mathfrak{b}$ in der Klasse C_2, so definieren wir mit $C_1\,C_2$ die Klasse

von $\mathfrak{a}\mathfrak{b}$. Diese Definition ist von den speziellen Idealen $\mathfrak{a}$ in C_1, $\mathfrak{b}$ in C_2 unabhängig, denn ist $\mathfrak{c} = \gamma\mathfrak{a}$ ein anderes Ideal als $\mathfrak{a}$ in C_1, $\mathfrak{d} = \delta\mathfrak{b}$ ein anderes Ideal als $\mathfrak{b}$ in C_2, so ist $\mathfrak{c}\mathfrak{d} = \gamma\delta\mathfrak{a}\mathfrak{b}$ und $\mathfrak{c}\mathfrak{d}$ liegt in $C_1 C_2$. Ist $\mathfrak{a}$ ein Ideal, α eine Zahl in $\mathfrak{a}$, so ist $(\alpha) = \mathfrak{a}\mathfrak{b}$. Liegt $\mathfrak{a}$ in der Klasse K, so $\mathfrak{b}$ in der Klasse K^{-1}. Für diese *Multiplikation der Klassen*, die offenbar auch das kommutative und assoziative Gesetz erfüllt, ist die Hauptklasse das Einselement. Es folgt

Satz 4. *Die Idealklassen bilden bezüglich der Multiplikation eine abelsche Gruppe.*

Die Hauptklasse wird oft mit 1 bezeichnet.
Nun folgt aus Satz 3: Ist C eine Klasse, so liegt in C^{-1} ein ganzes Ideal $\mathfrak{c}$ und darin eine Zahl $\gamma \neq 0$ mit

$$|\gamma^N| \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!\ \mathfrak{c}^N |\sqrt{d}|}{n^n}.$$

Nun ist $(\gamma) = \mathfrak{a}\mathfrak{c}$ mit $\mathfrak{a}$ als ganzem Ideal in C und $|\gamma^N| = \mathfrak{a}^N \mathfrak{c}^N$. Es folgt

$$\mathfrak{a}^N \mathfrak{c}^N \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!\ \mathfrak{c}^N |\sqrt{d}|}{n^n}$$

oder

$$\mathfrak{a}^N \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!\,|\sqrt{d}|}{n^n}.$$

Wir erhalten

Satz 5. *In jeder Idealklasse C gibt es ein ganzes Ideal $\mathfrak{a} \neq 0$ mit*

$$\mathfrak{a}^N \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!\,|\sqrt{d}|}{n^n}.$$

Hieraus und aus Satz 2 von § 38 erhalten wir unmittelbar

Satz 6. *Die Anzahl h der Idealklassen ist endlich.*

h heißt *Klassenzahl*. Ist $h = 1$, was aber sehr häufig nicht der Fall ist, so sind alle Ideale Hauptideale.
Bevor wir weitergehen, schalten wir ein Beispiel ein: Es sei $k = \mathsf{P}(\zeta)$, wobei ζ eine primitive fünfte Einheitswurzel ist. Die Diskriminante ist $5^3 = 125$ und die rechte Seite von Satz 5 wird, da $r = 2$, $n = 4$, $\frac{n!}{n^n} = \frac{3}{32}$ ist, $\left(\frac{4}{\pi}\right)^2 \frac{3}{32}\sqrt{125}$. Nun machen wir eine weitere Abschätzung nach oben, aber äußerst vorsichtig

$$\left(\frac{4}{\pi}\right)^2 = \frac{16}{\pi^2} < \frac{16}{9{,}76} = \frac{1}{0{,}61},$$

$$\sqrt{125} < 11{,}2.$$

Es ergibt sich

$$\mathfrak{a}^N < \frac{11{,}2 \cdot 3}{0{,}61 \cdot 32} = \frac{33{,}6}{19{,}52} < 2.$$

Es bleibt $\mathfrak{a}^N = 1$, d. h. in jeder Klasse liegt das Hauptideal (1); es ist nur eine Klasse da, nämlich die Hauptklasse: Im Zahlkörper der fünften Einheitswurzeln sind alle Ideale Hauptideale.

Aus dem Begriff der Klassengruppe folgt unmittelbar

Satz 7. *Die h-te Potenz jedes Ideals ist ein Hauptideal.*

Satz 8. *In jeder Klasse C gibt es ein Ideal, das zu einem gegebenen ganzen Ideal* $\mathfrak{b}$ *prim ist.*

Beweis: Sei $\mathfrak{u}$ ein ganzes Ideal in C,

$$\mathfrak{u} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_k^{a_k} \mathfrak{v} \quad \text{mit} \quad \mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_k$$

als Primteilern von $\mathfrak{b}$, die in der kanonischen Zerlegung von $\mathfrak{u}$ vorkommen; das brauchen nicht alle Primfaktoren von $\mathfrak{b}$ zu sein. Dabei sei $\mathfrak{v}$ zu $\mathfrak{b}$ prim. Es sei weiter π_j eine Primzahl nach $\mathfrak{p}_j$, und zwar speziell $\pi_j \equiv 1 \bmod \mathfrak{b}\, \mathfrak{p}_j^{-b_j}$, wenn $\mathfrak{p}_j^{b_j} \parallel \mathfrak{b}$ ist.

Das Ideal

$$\left(\frac{\mathfrak{p}_1}{\pi_1}\right)^{a_1} \left(\frac{\mathfrak{p}_2}{\pi_2}\right)^{a_2} \dots \left(\frac{\mathfrak{p}_k}{\pi_k}\right)^{a_k} \mathfrak{v} = \frac{\mathfrak{m}}{\mathfrak{n}}$$

wobei $\mathfrak{m}, \mathfrak{n}$ ganze Ideale mit $(\mathfrak{m}, \mathfrak{n}) = 1$ sind, erfüllt die Bedingungen des Satzes.

Satz 9. *In jeder Klasse gibt es ein ganzes Ideal, das zu einem gegebenen ganzen Ideal* $\mathfrak{b}$ *prim ist.*

Ist $\frac{\mathfrak{m}}{\mathfrak{n}}$ das im vorigen Satz erhaltene Ideal, so ist $\mathfrak{n}^{h-1}\mathfrak{m}$ ganz, zu $\mathfrak{b}$ prim, und da $\mathfrak{n}^h$ Hauptideal ist, in derselben Klasse.

Satz 8 und 9 gelten, wie man sofort sieht, auch für gebrochene $\mathfrak{b}$.

Satz 10. *Jedes Ideal* $\mathfrak{a}$ *ist als zweigliedriges Ideal darstellbar.*

Beweis: Es genügt den Satz für ganze Ideale nachzuweisen. Sei $\mathfrak{a}$ in C^{-1}, $\mathfrak{b}$ ganz in C, so ist $\mathfrak{a}\mathfrak{b} = \alpha_1$ ganz. Sei auch $\mathfrak{c}$ ganz in C mit $(\mathfrak{b}, \mathfrak{c}) = 1$, so ist auch $\mathfrak{a}\mathfrak{c} = \alpha_2$ ganz. Dann ist

$$\mathfrak{a} = \mathfrak{a}(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}) = (\alpha_1, \alpha_2).$$

Satz 11. *Ist* α, β *ganz,* $(\alpha) = \mathfrak{a}\mathfrak{m}$, $\beta = \mathfrak{b}\mathfrak{m}$, *wobei* $\mathfrak{a}, \mathfrak{b}, \mathfrak{m}$ *ganz sind mit* $(\mathfrak{a}, \mathfrak{b}) = 1$, *so kann der Bruch* $\frac{\alpha}{\beta}$ *durch* $\frac{\gamma}{\delta}$ *ausgedrückt werden, wobei* γ, δ *ganz, und* $\mathfrak{m}$ *prim sind.*

Beweis: Wir haben

$$\left(\frac{\alpha}{\beta}\right) = \frac{\mathfrak{a}}{\mathfrak{b}},$$

und daher, wenn $\mathfrak{c}$ ein zu $\mathfrak{m}$ primes, zu $\mathfrak{m}$ äquivalentes ganzes Ideal ist,

$$\left(\frac{\alpha}{\beta}\right) = \frac{\mathfrak{a}\mathfrak{c}}{\mathfrak{b}\mathfrak{c}}$$

und mit $\mathfrak{a}\mathfrak{c} = (\gamma_1)$, $\mathfrak{b}\mathfrak{c} = (\delta)$ gilt $\left(\frac{\alpha}{\beta}\right) = \left(\frac{\gamma_1}{\delta}\right)$.
Diese Gleichung in Hauptidealen hat eine Gleichung in Zahlen

$$\frac{\alpha}{\beta} = \frac{\gamma_1 \varepsilon}{\delta}$$

mit ε als einer Einheit zur Folge. Mit $\gamma_1 \varepsilon = \gamma$ haben wir die Forderungen unseres Satzes erfüllt.

Satz 11 zeigt das Analoge zu dem Verfahren, das man im rationalen Zahlkörper als Kürzen von Brüchen bezeichnet. Hier kann man oft die Teilerfremdheit von Zähler und Nenner nicht erreichen.

Wir wollen den Satz, daß die Norm eines ganzen Hauptideals der Absolutwert der Norm der Erzeugenden ist, auf beliebige Ideale in der Form verallgemeinern, daß das Produkt der konjugierten Ideale gleich dem Hauptideal in P, erzeugt durch das Ideal der Norm im bisherigen Sinne, ist. Hierzu sind einige Bemerkungen erforderlich:

Ist $\mathfrak{a}$ ein Ideal in k, das im Körper $k^{(1)}$ durch $\mathfrak{a}^{(1)}$, im Körper $k^{(2)}$ durch $\mathfrak{a}^{(2)}$, ... verwirklicht wird, so ist zunächst im allgemeinen das Produkt $\mathfrak{a}^{(1)}\mathfrak{a}^{(2)}$ und natürlich erst recht $\mathfrak{a}^{(1)}\mathfrak{a}^{(2)} \ldots \mathfrak{a}^{(n)}$ gar nicht definiert, da die Körper $k^{(1)}$ und $k^{(2)}$ in vielen Fällen nicht zusammenfallen. Daher definieren wir zuerst die *Verlagerung* des Ideals k in einen Körper K, von dem k ein Teilkörper ist.

Definition. *Ist k ein Teilkörper von K, so wird das Ideal $\mathfrak{a} = (\alpha, \beta)$, bestehend aus allen Zahlen $\alpha\xi + \beta\eta$ mit ξ, η als ganzen Zahlen in k in den Körper K verlagert, indem man nunmehr unter $\mathfrak{a}$ die Gesamtheit aller Zahlen $\alpha\,\Xi + \beta\,\mathsf{H}$ mit Ξ, H als beliebigen ganzen Zahlen in K versteht. Im Sinne einer Abstraktion, wie sie auch sonst vielfach in der Mathematik vorkommt, betrachtet man die beiden Ideale $\mathfrak{a}$ in k und K als miteinander identisch.*

Beispiele: (2) ist in P Primideal, enthält alle Zahlen $2x$, wobei x ganz rational ist. Nach Verlagerung nach $k = \mathsf{P}(\sqrt{5})$ bleibt (2) Primideal, ist

aber mit $\left[1, \omega = \frac{1+\sqrt{5}}{2}\right]$ als Körperbasis die Gesamtheit aller Zahlen $2x + 2y\omega = 2x + y + y\sqrt{5}$ mit x, y ganz rational.

Das Ideal (5) ist in P Primideal, in $\mathsf{P}(i)$ wird (5) die Gesamtheit der Zahlen $5x + 5yi$ mit x, y ganz rational, aber dann ist (5) kein Primideal mehr, sondern das Produkt der beiden Hauptprimideale $(2+i)$ und $(2-i)$.

Nach Einführung des Begriffes der Verlagerung verlagern wir nunmehr $\mathfrak{a}^{(1)}, \mathfrak{a}^{(2)}, \ldots, \mathfrak{a}^{(n)}$ in den aus $k^{(1)}, k^{(2)}, \ldots, k^{(n)}$ zusammengesetzten Körper $K = k^{(1)}k^{(2)} \ldots k^{(n)}$, den kleinsten (mengentheoretisch wenigst umfassenden) Galoischen Körper über k. Wir bezeichnen mit einer nur hier vorkommenden Abkürzung $\mathfrak{a}^{(1)}\mathfrak{a}^{(2)} \ldots \mathfrak{a}^{(n)}$ mit $\mathfrak{a}^{\Pi}$ und suchen nachzuweisen, daß $\mathfrak{a}^{\Pi} = (\mathfrak{a}^{\mathsf{N}})$ ist. Es sei $\mathfrak{a}$ ganz.

Nun sei $\mathfrak{a} = (\alpha, \beta)$. Es ist $\mathfrak{a}^{\Pi}$ der Inhalt des Polynoms

$$f(x) = \prod_{i=1}^{n} (\alpha^{(i)} + \beta^{(i)} x)$$

nach § 35, Satz 1.

Da dies ein Polynom mit ganzen rationalen Zahlen als Koeffizienten ist, so ist $\mathfrak{a}^{\Pi}$ ein Ideal in P, also Hauptideal, erzeugt durch eine natürliche Zahl.

Wegen

$$f(x) = \alpha^{\mathsf{N}} + \cdots + \beta^{\mathsf{N}} x^n$$

gilt

$$\mathfrak{a}^{\Pi} \mid (\alpha^{\mathsf{N}}, \beta^{\mathsf{N}}).$$

Es existieren aber Zahlen α, β in $\mathfrak{a}$, so daß $\mathfrak{a} = (\alpha, \beta)$ und $(\alpha^{\mathsf{N}}, \beta^{\mathsf{N}}) = \mathfrak{a}^{\mathsf{N}}$ ist. Zunächst gibt es in der zur Klasse C^{-1} von $\mathfrak{a}$ inversen Klasse C ein ganzes Ideal $\mathfrak{c}_1$ mit $\mathfrak{a}\mathfrak{c}_1 = (\alpha)$. Weiter gibt es in derselben Klasse C ein ganzes zu $\mathfrak{c}_1^{\mathsf{N}}$ primes ganzes Ideal $\mathfrak{c}_2$ mit $\mathfrak{a}\mathfrak{c}_2 = (\beta)$. Dann gilt

1. $(\alpha, \beta) = (\mathfrak{a}\mathfrak{c}_1, \mathfrak{a}\mathfrak{c}_2) = \mathfrak{a}(\mathfrak{c}_1, \mathfrak{c}_2) = \mathfrak{a}$.
2. Es ist dann auch $(\mathfrak{c}_1^{\mathsf{N}}, \mathfrak{c}_2^{\mathsf{N}}) = 1$.

Es wird $(\alpha^{\mathsf{N}}, \beta^{\mathsf{N}}) = (\mathfrak{a}^{\mathsf{N}}\mathfrak{c}_1^{\mathsf{N}}, \mathfrak{a}^{\mathsf{N}}\mathfrak{c}_2^{\mathsf{N}}) = \mathfrak{a}^{\mathsf{N}}(\mathfrak{c}_1^{\mathsf{N}}, \mathfrak{c}_2^{\mathsf{N}}) = \mathfrak{a}^{\mathsf{N}}$.

Wir wollen α, β nunmehr so annehmen.

Sofort folgt

$$\mathfrak{a}^{\Pi} \mid \mathfrak{a}^{\mathsf{N}}.$$

Für Hauptideale $\mathfrak{g} = (\alpha)$ ist

$$\mathfrak{g}^{\mathsf{N}} = \left|\alpha^{(1)}\alpha^{(2)} \ldots \alpha^{(n)}\right|,$$

somit $(\mathfrak{g}^{\mathsf{N}}) = \mathfrak{g}^{\Pi}$ bewiesen.

Für Nichthauptideale $\mathfrak{a}$ gehen wir mit den bisherigen Voraussetzungen und Bezeichnungen in der Untersuchung weiter.
Sofort aus der Definition des symbolischen Exponenten Π folgt

$$(\mathfrak{a}\,\mathfrak{b})^{\Pi} = \mathfrak{a}^{\Pi}\,\mathfrak{b}^{\Pi},$$

wodurch ja erst die Schreibweise gerechtfertigt wird. Es ist $(\mathfrak{c}_1^{\Pi}, \mathfrak{c}_2^{\Pi}) = 1$, denn nach dem bereits Bewiesenen ist

$$\mathfrak{c}_1^{\Pi} \mid \mathfrak{c}_1^{\mathsf{N}}, \mathfrak{c}_2^{\Pi} \mid \mathfrak{c}_2^{\mathsf{N}},$$

und $(\mathfrak{c}_1^{\mathsf{N}}, \mathfrak{c}_2^{\mathsf{N}}) = 1$ folgte bereits aus den Voraussetzungen. Es wird

$$(\alpha^{\mathsf{N}}) = \mathfrak{a}^{\Pi}\mathfrak{c}_1^{\Pi},$$
$$(\beta^{\mathsf{N}}) = \mathfrak{a}^{\Pi}\mathfrak{c}_2^{\Pi},$$

daher

$$((\alpha^{\mathsf{N}}, \beta^{\mathsf{N}})) = \mathfrak{a}^{\Pi}(\mathfrak{c}_1^{\Pi}, \mathfrak{c}_2^{\Pi}) = \mathfrak{a}^{\Pi},$$

d. h.

$$(\mathfrak{a}^{\mathsf{N}}) = \mathfrak{a}^{\Pi}.$$

Wir haben

Satz 12. *Das Produkt der zu einem ganzen Ideal konjugierten Ideale ist ein Ideal in* P, *erzeugt durch die Norm des Ideals.*

Satz 12 gestattet den Begriff der Idealnorm auch auf gebrochene Ideale zu übertragen, bei denen die ursprüngliche Definition, Zahl der Elemente des Restklassenrings sinnlos wäre.

§ 41. Beispiele zur Bestimmung der Klassenzahl im quadratischen Zahlkörper

In einfachen Fällen ermöglicht die in § 40 gegebene obere Schranke für die Norm eines ganzen Ideals einer Klasse die Bestimmung der Klassenzahl.
Von hierbei in Betracht kommenden Sätzen sei erwähnt:

Satz 1. *In einem reellen quadratischen Körper sei die Zahl* α *ein Idealquadrat, das heißt:* $(\alpha) = \mathfrak{a}^2$, *und zwar sei* $\alpha^{\mathsf{N}} < 0$, *weiter sei* $\varepsilon_0^{\mathsf{N}}$ *(Norm der Grundeinheit)* $= +1$ *(damit von selbst* α *keine Einheit). Dann kann* $\mathfrak{a}$ *kein Hauptideal sein.*

Beweis: Wegen $\varepsilon_0^{\mathsf{N}} = +1$ sind alle Normen von Einheiten positiv.

Wäre $\mathfrak{a} = (\beta)$, so wäre $\alpha = \beta^2 \varepsilon$ mit ε als Einheit. Wir hätten dann

$$0 > \alpha^N = \beta^{2N} \varepsilon^N = (\beta^N)^2 \varepsilon^N > 0,$$

also einen Widerspruch.

Die in § 40 gegebene Grenze für die Norm des Ideals einer Klasse wird (m ist quadratfrei, kein Quadrat):

I. Bei einem reellquadratischen Körper: $k = \mathsf{P}(\sqrt{m})$, wobei $m > 0$ ist

$$\mathfrak{a}^N \leqq \frac{1}{2}\sqrt{d}\,.$$

II. Bei einem imaginärquadratischen Körper $k = \mathsf{P}(\sqrt{-m'})$ mit $m' > 0$, $m' = -m$ ist

$$\mathfrak{a}^N \leqq \frac{2}{\pi}\left|\sqrt{d}\right|.$$

Nun folgen einige Beispiele:

1. $k = \mathsf{P}(\sqrt{34})$, eine Basis ist $[1, \sqrt{34}]$. Die Körperdiskriminante wird $d = 4 \cdot 34 = 136$. Es bleibt

$$\mathfrak{a}^N < \sqrt{34},$$

also

$$\mathfrak{a}^N \leqq 5.$$

Es sind nur die Primzahlen 2, 3, 5 zu untersuchen. 2 ist Idealquadrat: $(2) = \mathfrak{l}^2$ mit $\mathfrak{l} = (6 + \sqrt{34})$ (Hauptprimideal). Denn $(6 + \sqrt{34})(6 - \sqrt{34}) = 2$.

3 wird wegen $\left(\frac{34}{3}\right) = \left(\frac{1}{3}\right) = 1$ Produkt zweier voneinander verschiedener Primideale: $(3) = \mathfrak{p}_1 \mathfrak{p}_2$ mit $\mathfrak{p}_1 = (3, 1 + \sqrt{34})$, $\mathfrak{p}_2 = (3, 1 - \sqrt{34})$. Es ist $(9, 5 + \sqrt{34}) = \mathfrak{t} = (5 + \sqrt{34})$ ein Hauptideal, denn $5^2 - 34 \cdot 1^2 = (5 + \sqrt{34})^N = -9$. Offenbar ist weiter $5 + \sqrt{34} \equiv 0 \bmod \mathfrak{p}_2$; ferner ist $\mathfrak{t} = [9, 5 + \sqrt{34}]$ eine Darstellung durch eine Modulbasis, also $\mathfrak{t}^N = 9 = (\mathfrak{p}_2^N)^2$, d. h. $\mathfrak{t} = \mathfrak{p}_2^2$. Also ist $\gamma = 5 + \sqrt{34}$ ein Idealquadrat mit negativer Norm. Da aber die Grundeinheit des Körpers die Norm $+1$ hat, kann $\mathfrak{p}_2$ nicht Hauptideal sein. Die Klasse C von $\mathfrak{p}_2$ erfüllt $C^2 = 1$, da $\mathfrak{p}_2^2 = (\gamma) \sim 1$ ist.

Nun ist noch 5 zu untersuchen; wegen $\left(\frac{34}{5}\right) = 1$ ist (5) Produkt zweier voneinander verschiedener Primideale: $(5) = \mathfrak{q}_1 \mathfrak{q}_2$. Es ist $-25 = \sigma^N$ mit $\sigma = 3 + \sqrt{34}$. Wieder kann das Idealquadrat nicht Quadrat eines Hauptideals sein; daher sind $\mathfrak{q}_1 = (5, 3 + \sqrt{34})$,

$\mathfrak{q}_2 = (5, 3 - \sqrt{34})$, wobei die Idealbasis zugleich Modulbasis ist (bei $\mathfrak{q}_2$ mit Annahme der Körperbasis $[1, -\sqrt{34}]$) keine Hauptideale. Es ergibt sich eine Klasse C_2, bei der wir nicht wissen, ob sie mit C identisch ist: $C_2 \neq 1$, $C_2^2 = 1$.
Wir bilden $\mathfrak{p}_1\mathfrak{q}_2$ und sehen nach, ob dies ein Hauptideal ist. Hier führt folgender Satz oft schnell zum Ziele:

Satz 2. *Kann man in einem ganzen Ideal $\mathfrak{a}$ eine Zahl α finden mit $|\alpha^N| = \mathfrak{a}^N$, so ist $\mathfrak{a}$ ein Hauptideal, und zwar $\mathfrak{a} = (\alpha)$.*

Beweis: Es ist $(\alpha) = \mathfrak{a}\mathfrak{g}$ mit $\mathfrak{g}$ als ganzem Ideal; Normenbildung gibt $|\alpha^N| = \mathfrak{a}^N\mathfrak{g}^N$, also $\mathfrak{g}^N = 1$, $\mathfrak{g} = (1)$.
Es ist mit $\alpha = 7 + \sqrt{34}$:

$$\text{a)}\quad \alpha \equiv 6 \equiv 0 \bmod \mathfrak{p}_1,$$

$$\text{b)}\quad \alpha \equiv 10 \equiv 0 \bmod \mathfrak{q}_2,$$

somit $\alpha \equiv 0 \bmod \mathfrak{p}_1\mathfrak{q}_2$, da $\mathfrak{p}_1$ und $\mathfrak{q}_2$ relativ prim zueinander sind; weiter ist $|\alpha^N| = 15 = \mathfrak{p}_1^N\mathfrak{q}_2^N$. Mithin ist $\mathfrak{p}_1\mathfrak{q}_2 = (\alpha)$, $CC_2 = 1$, $C_2 = C^{-1} = C$. Die Untersuchung von 5 bringt also keine neue Klasse hinzu. Es ist $h = 2$.

2. Sei $k = \mathsf{P}(\sqrt{-23})$; eine Basis ist $\left[1, \omega = \frac{1+\sqrt{-23}}{2}\right]$; die Körperdiskriminante wird $d = -23$.
Es wird $\frac{2}{\pi}\sqrt{23} < \frac{2 \cdot 4{,}8}{\pi} = \frac{9{,}6}{\pi} < 4$; es sind also die Primzahlen 2, 3 zu untersuchen. Wegen $m \equiv 1 \bmod 8$ $(k = \mathsf{P}(\sqrt{m}))$ zerfällt 2 in das Produkt zweier verschiedener Primideale: $(2) = \mathfrak{l}_1\mathfrak{l}_2$ mit $\mathfrak{l}_1 = (2, \omega)$, $\mathfrak{l}_2 = (2, \omega')$, wobei $\omega' = \frac{1-\sqrt{-23}}{2}$ ist.
Da $x^2 + 23y^2 = 8$ ganzzahlig unlösbar ist, sind die Ideale $\mathfrak{l}_1, \mathfrak{l}_2$ keine Hauptideale. Weil

$$\frac{x^2 + 23y^2}{4} = 8$$

durch $x = 3$, $y = 1$ ganzzahlig lösbar ist, gilt

$$(8) = \left(\frac{3+\sqrt{-23}}{2}\right)\left(\frac{3-\sqrt{-23}}{2}\right) = (2 - \omega')(2 - \omega).$$

Es ist $2 - \omega \equiv 0 \bmod \mathfrak{l}_1$, $(2 - \omega)^N = (\mathfrak{l}_1^N)^3 = 2^3$. Da $2 - \omega$ durch $\mathfrak{l}_2$ nicht teilbar ist, so ist $(2 - \omega) = \mathfrak{l}_1^3$, mithin ist $\mathfrak{l}_1^3$ ein Hauptideal; die Klasse C von $\mathfrak{l}_1$ erfüllt $C^3 = 1$, $C \neq 1$ (also auch $C^2 \neq 1$). $\mathfrak{l}_2$ liegt in der Klasse $C^2 = C^{-1}$.

Wegen $\left(\frac{-23}{3}\right) = \left(\frac{1}{3}\right) = 1$ zerfällt auch 3 in das Produkt zweier nicht zusammenfallender Primideale: $(3) = \mathfrak{q}_1 \mathfrak{q}_2$. Wegen $1^2 \equiv -23 \bmod 3$ kann etwa gesetzt werden $\mathfrak{q}_1 = (3, 1+\sqrt{-23}) = \left(3, \frac{1+\sqrt{-23}}{2}\right) = (3, \omega)$, wobei die letztangegebene Idealbasis zugleich Modulbasis ist. Es ist $\omega \equiv 0 \bmod \mathfrak{l}_1, \bmod \mathfrak{q}_1$, also $\equiv 0 \bmod \mathfrak{l}_1 \mathfrak{q}_1$, da $(\mathfrak{l}_1, \mathfrak{q}_1) = 1$ ist; zugleich ist $\omega^{\mathsf{N}} = 6 = (\mathfrak{l}_1 \mathfrak{q}_1)^{\mathsf{N}}$, also $\mathfrak{l}_1 \mathfrak{q}_1 = (\omega)$, es steht $\mathfrak{q}_1$ in der Klasse C^2, $\mathfrak{q}_2$ in der Klasse C. Die Klassenzahl h erfüllt $h = 3$.

3. $\mathsf{P}(\sqrt{-127})$, Basis $\left[1, \omega = \frac{1+\sqrt{-127}}{2}\right]$.

Es wird $d = -127$, weiter $\frac{2}{\pi}\sqrt{127} < \frac{2 \cdot 11{,}5}{\pi} = \frac{23}{\pi} < 8$. Es braucht nur 2, 3, 5, 7 untersucht zu werden.

Wegen $-127 \equiv 1 \bmod 8$ wird $2 = \mathfrak{l}_1 \mathfrak{l}_2$. Es ist $2^5 = \frac{1^2 + 127 \cdot 1^2}{4} = \omega^{\mathsf{N}}$, wird $\mathfrak{l}_1 = (2, \omega)$ gesetzt, so folgt wegen $\omega \not\equiv 0 \bmod \mathfrak{l}_2$, daß $\omega \equiv 0 \bmod \mathfrak{l}_1^5$; da $\omega^{\mathsf{N}} = (\mathfrak{l}_1)^{5\mathsf{N}} = 2^5$ ist, wird $\mathfrak{l}_1^5 = (\omega)$. Offenbar sind $\mathfrak{l}_1$ und ebenso $\mathfrak{l}_1^j (1 < j < 5)$ keine Hauptideale. Damit sind 5 Klassen nachgewiesen: $C \neq 1$, C^2, C^3, C^4, $C^5 = 1$.

Es bleibt wegen $\left(\frac{-127}{3}\right) = \left(\frac{-1}{3}\right) = -1$ die Primzahl 3 Primideal, ebenso hat $\left(\frac{-127}{5}\right) = \left(\frac{-2}{5}\right) = -1$ zur Folge, daß (5) Primideal ist. Endlich findet wegen $\left(\frac{-127}{7}\right) = \left(\frac{-1}{7}\right) = -1$ keine Zerlegung von 7 statt. Es wird $h = 5$.

4. $\mathsf{P}(\sqrt{-14})$. Eine Körperbasis wird $[1, \sqrt{-14}]$, die Diskriminante ist $d = -56$. Wir erhalten $\frac{2}{\pi}\sqrt{56} < \frac{2 \cdot 7{,}5}{\pi} = \frac{15}{\pi} < 5$, haben daher nur die Primzahlen 2 und 3 zu untersuchen.

Es wird $(2) = (2, \sqrt{-14})^2 = \mathfrak{l}^2$. Das Primideal $\mathfrak{l}$ ist kein Hauptideal, da $x^2 + 14y^2 = 2$ keine Lösungen in ganzen Zahlen hat, also ist damit eine Klasse A nachgewiesen, die $A^2 = 1$ erfüllt.

Es ist $(3) = (3, 1+\sqrt{-14})(3, 1-\sqrt{-14}) = \mathfrak{p}_1 \mathfrak{p}_2$. Offenbar ist keine niedrigere Potenz von 3 als 3^4 durch $x^2 + 14y^2$ darstellbar. Es ist dagegen $3^4 = 5^2 + 14 \cdot 2^2$; die Zahl $\alpha = 5 + 2\sqrt{-14}$, die $\alpha \equiv 0 \bmod \mathfrak{p}_1$, $\alpha \not\equiv 0 \bmod \mathfrak{p}_2$ erfüllt, ist also, da sie keine weitere Primteiler haben kann, eine Potenz von $\mathfrak{p}_1$, also $\mathfrak{p}_1^4$ wegen $\alpha^{\mathsf{N}} = (\mathfrak{p}_1^4)^{\mathsf{N}}$.

Mithin sind damit 4 Klassen C, C^2, C^3, $C^4 = 1$ nachgewiesen, wobei $C^j \neq 1$ für $1 \leqq j < 4$ gilt. Nun ist die Frage, ob $A = C^2$ ist. Die Zahl $\alpha_1 = 2 - \sqrt{-14}$ erfüllt $\alpha_1 \equiv 0 \bmod \mathfrak{l}$, $\alpha_1 \equiv 0 \bmod \mathfrak{p}_1$, $\alpha_1 \not\equiv 0 \bmod \mathfrak{p}_2$. Wegen $18 = \alpha_1 \mathfrak{N} = (\mathfrak{p}_1^2 \mathfrak{l})\mathfrak{N}$ folgt, da α_1 keine anderen Primteiler haben kann, direkt $(\alpha_1) = \mathfrak{p}_1^2 \mathfrak{l}$, also $C^2 A = 1$, $A = C^{-2} = C^2$. Es bleibt die Klassenzahl $h = 4$.

5. $\mathsf{P}(\sqrt{-163})$. Eine Körperbasis wird $\left[1, \omega = \frac{1+\sqrt{-163}}{2}\right]$, die Körperdiskriminante ist $d = -163$. Es wird $\frac{2}{\pi}\sqrt{163} < \frac{2 \cdot 12{,}8}{\pi} = \frac{25{,}6}{\pi} < 9$. Es brauchen nur 2, 3, 5, 7 untersucht zu werden.

Wegen $-163 \equiv 5 \bmod 8$ bleibt 2 Primideal, wegen $\left(\frac{-163}{3}\right) = \left(\frac{-1}{3}\right) = -1$, $\left(\frac{-163}{5}\right) = \left(\frac{2}{5}\right) = -1$, $\left(\frac{-163}{7}\right) = \left(\frac{-2}{7}\right) = -1$ auch 3, 5, 7. Es wird $h = 1$.

SACHVERZEICHNIS