Journal of the Mathematical Society of Japan Vol. 3, No. 1, May, 1951.

Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern

Sigekatu KURODA

Wenn auch die Theorie der relativ-abelschen Zahlkörper als Klassenkörpertheorie zu einem vollständigen Abschluss gebracht worden ist, haben wir noch heute um nicht-abelsche Fälle doch nur geringe Kenntnisse. Während wir das Zerlegungsgestz der Primideale des Grundkörpers im relativ-abelschen Oberkörper in voller Klarheit überblicken können, sehen wir es doch im relativ-galoisschen Oberkörper nur durch einen Nebel. Dieser unbefriedigende Zustand mag wohl zum Teil darauf beruhen, dass wir heute nur über recht wenige Erfahrungen über nicht-abelsche galoissche Körper verfügen können, wovon das betreffende Zerlegungsgesetz lauter durch Begriffe im Grundkörper aufgefasst wird.

Ich werde hier allereinfachste absolute nicht-abelsche galoissche Körper vom Grade 2^n betrachten und das Zerlegungsgesetz der rationalen Primzahlen in ihnen durch Begriffe im rationalen Zahlkörper bestimmen (Satz 1). Dabei spielen biquadratische Reste und Nichtreste im rationalen Zahlkörper wesentliche Rolle. Das Symbol $\left(\frac{m}{p}\right)_4$ in der Formel (16) zeigt eine nicht-klassenkörpertheoretische Erscheinung der nicht-abelschen galoisschen Körper. Es ergibt sich aus dem hier herzuleitenden Zerlegungsgesetze in der galoisschen Erweiterung, dass diejenigen Primzahlen, wonach irgendeine Zahl biquadratischer Rest oder Nichtrest ist, durchkreuzt in gewissen Kongruenzklassen gleichverteilt sind (Satz 2). Es ist also wahrscheinlich, dass sich die Betrachtungen gewisser nicht-abelschen galoisschen Zahlkörper auf neue Kenntnisse, wie diejenigen Primideale, nach denen irgendeine Zahl n-ter Potenzrest ist, in Kongruenzklassen von einem n-te Einheitswurzeln nicht enthaltenden Zahlkörper verteilt sind, beziehen mögen.

1. Bezeichnungen: Falls folgende Bezeichnungen stillschweigend verwendet werden, so sind

R rationaler Zahlkörper;

k Gaussscher Zahlkörper $R(\sqrt{-1})$;

μ Gausssche ganze Zahl, welche keine Quadratzahl ausser ± 1 als Faktor hat und weder reell noch rein-imaginär ist;

$\mu = c\alpha$, $N\alpha = m$, wobei c der positive rationale Teiler von μ ist und α keinen rationalen Teiler hat;

l ungerader Primteiler von m;

$k_1 = R(\sqrt{m})$, $k_2 = R(\sqrt{-m})$, $\Lambda = k(\sqrt{\mu})$, $\bar{\Lambda} = k(\sqrt{\bar{\mu}})$, wobei $\bar{\mu}$ die konjugiert komplexe Zahl von μ bezeichnet;

$V = k_1 k_2$, $K = \Lambda\bar{\Lambda}$, also ist K/R ein nicht-abelscher galoisscher Körper achten Grades;

R^* Kompositum gewisser quadratischen Körper;

$K^* = R^*K$, also ist K^*/R ein nicht-abelscher galoisscher Körper;

$H(\mathfrak{Q}/\Delta)$, im Falle, wo $\mathfrak{Q}/\Delta$ relativ-abelsch ist, die $\mathfrak{Q}$ zugeordnete Idealgruppe von Δ; falls Δ rational ist, so soll Δ weggelassen werden;

$\left(\frac{r}{s}\right)$ Jacobisches Symbol;

$\left[\frac{\rho}{\sigma}\right]$ quadratischer Restcharakter im Gaussschen Körper;

$\left[\frac{\rho}{\sigma}\right]_4$ biquadratischer Restcharakter im Gaussschen Körper;

p rationale Primzahlen, welche in der Diskriminante von K^*/R nicht aufgehen.

Bemerkung: Da -1 in k Quadratzahl ist, nehmen wir das Vorzeichen von μ geeignet, so dass die Zahl μ eine der folgenden Kongruenzbedingungen erfüllt: (1) $\mu \equiv 1$, (2) $\mu \equiv 1+2i$, (3) $\mu \equiv i$, $2+i$ oder (4) $\mu \equiv 1+i$, $1+3i$ (mod. 4). Die Diskriminante von K/R ist gleich $4^e c^4 m^4$, wobei $e=4$, 6, 8 oder 9 ist, je nachdem μ der obigen Kongruenzbedingung (1), (2), (3) oder (4) genügt. Die Relativdiskriminante[1] von Λ/k ist gleich $2^e\mu$, wobei $e=0$, 1, 2 oder 2 ist, der obigen vier Fällen entsprechend.

2. Die Primzahl p zerfällt in K in Primidealen ersten, zweiten oder vierten Grades und die Kroneckersche Dichtigkeit solcher Primzahlen p ist 1/8, 5/8 bzw. 1/4. Dies sieht man wegen eines Satzes von Artin[2] mit Hilfe der regulären Darstellung (als Produkt zyklischer Permutationen) der galoisschen Gruppe von K/R. Die Primzahl p zerfällt auch in K^* in

---

1) Bezüglich des Körpers Λ/k vergleiche man meine frühere Arbeit: Über den Dirichletschen Körper, J. Fac. Sci. Tokyo, Sec. I. Vol. IV, Part 5 (1943).

2) Math. Ann. **89** (1928).

Primidealen ersten, zweiten oder vierten Grades. Die Dichtigkeit solcher Primzahlen ist $1/2^n$, $3/4-1/2^n$ bzw. $1/4$, wobei 2^n den Grad von K^* bezeichnet. Dies sieht man auch, wie oben, unter Berücksichtigung der Tatsache, dass die galoissche Gruppe von K^*/R direktes Produkt aus der von K/R und der abelschen Gruppe vom Typus $(2, 2,\ldots, 2)$ ist.

Wenn p in K nicht vollzerfällt, so haben die Primteiler von p in K und die in K^* denselben Grad. Dies ersieht man leicht, wenn man den Zerlegungskörper des Primteilers von p in K und in K^* bestimmt. Für solche p ist also das Zerlegungsgesetz in K^* schon durch dasjenige in K bestimmt.

Es sei nun $p \notin H(V)$. Ist überdies $p \in H(k_2)$, so zerfällt p in K, also auch in K^*, in Primidealen vierten Grades. Ist dagegen $p \in H(k)$ oder $p \in H(k_1)$, so zerfällt p in K, also auch in K^*, in Primidealen zweiten Grades.

Die $H(V)$ gehörige Primzahl p ist in K (und auch in K^*) entweder vollzerfällt oder Produkt von Primidealen zweiten Grades. Wir werden im folgenden für spezielle K^* diese zwei Arten von Primzahlen abspalten.

3. Wir schalten hier die Betrachtungen über biquadratische Reste im rationalen Zahlkörper ein. Es sei p beliebige ungerade Primzahl. Ist $p \equiv -1 \pmod 4$, so ist biquadratischer Rest mit quadratischem Rest nach p gleichbedeutend. So sei $p \equiv 1 \pmod 4$ und m eine zu p prime Zahl, für die $\left(\frac{m}{p}\right) = +1$ gilt. Für solche p und m soll das Symbol[3] $\left(\frac{m}{p}\right)_4$ gleich $+1$ oder -1 sein, je nachdem die Zahl m biquadratischer Rest nach p ist oder nicht. Es ist also

$$\left(\frac{m}{p}\right)_4 = i^{\mathrm{Ind}\, m} \qquad (i = \sqrt{-1}).$$

Wir setzen ferner

$$\left(\frac{m}{n}\right)_4 = \prod_{p/n} \left(\frac{m}{p}\right)_4, \tag{1}$$

falls jeder Faktor rechter Seite definiert ist. Dies Symbol hat natürlich folgende Eigenschaften.

$$\text{Ist } m \equiv m' \pmod n, \text{ so ist } \left(\frac{m}{n}\right)_4 = \left(\frac{m'}{n}\right)_4. \tag{2}$$

---

3) Herr L. Rédei hat auch dieses Symbol verwendet, um tief liegende Eigenschaften quadratischer Zahlkörper herzuleiten. J. für reine und ang. Math. **171** (1934), **173** (1935).

$\left(\frac{abc\cdots}{n}\right)_4=\left(\frac{a}{n}\right)_4\left(\frac{b}{n}\right)_4\left(\frac{c}{n}\right)_4\cdots$, falls jeder Faktor rechter Seite definiert ist. (3)

$$\left(\frac{-1}{n}\right)_4=(-1)^{\frac{n-1}{4}} \tag{4}$$

$$\left(\frac{m}{n}\right)_4=\left[\frac{m}{\nu}\right]_4=\left[\frac{m}{\bar{\nu}}\right]_4, \text{ wobei } n=\nu\bar{\nu} \text{ ist.} \tag{5}$$

Es seien nun m und n zueinander prime ungerade positive Zahlen und für jeden Primteiler p von m und q von n seien $p\equiv q\equiv 1$ (mod. 4) und $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=+1$. Ferner sei $m=\mu\bar{\mu}$, $n=\nu\bar{\nu}$, $\mu\equiv\nu\equiv 1$ (mod. $(1+i)^3$). Dann gilt das " Reziprozitätsgesetz "

$$\left(\frac{m}{n}\right)_4\left(\frac{n}{m}\right)_4=\left[\frac{\nu}{\mu}\right]=\left[\frac{\mu}{\nu}\right]. \tag{6}$$

Dass es unmöglich ist, den Ausdruck der linken Seite von (6) bloss mit Hilfe der Kongruenzklasse im rationalen Zahlkörper auszudrücken, ist, wie man unten ersieht, eine Folgerung aus dem Abschliessungssatze der Klassenkörpertheorie. Wie die Formel (6) zeigt, kann man doch das Symbol $\left(\frac{m}{n}\right)_4$ auf Kongruenzklasse im Gaussschen Körper beziehen, indem man $\left(\frac{m}{n}\right)_4$ und $\left[\frac{\mu}{\nu}\right]$ doppelt " reziprozieıt."

Es braucht nur die Formel (6) zu beweisen für den Fall, wo m und n Primzahlen sind. Es seien also p, q Primzahlen, für welche $p\equiv q\equiv 1$ (mod. 4) und $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=+1$ ist. Im Gaussschen Körper sind dann $p=\pi\bar{\pi}$, $q=\varkappa\bar{\varkappa}$, $\pi\equiv\bar{\pi}\equiv\varkappa\equiv\bar{\varkappa}\equiv 1$ (mod. $(1+i)^3$). Es gilt nun $\left(\frac{p}{q}\right)_4=\left[\frac{p}{\varkappa}\right]_4$ und wegen des Reziprozitätsgesstzes biquadratischer Reste im Gaussschen Körper $\left[\frac{p}{\varkappa}\right]_4=\left[\frac{\varkappa}{p}\right]_4$. Aber ist $\left[\frac{\varkappa}{p}\right]_4=\left[\frac{\varkappa}{\pi}\right]_4\left[\frac{\varkappa}{\bar{\pi}}\right]_4$. Weil anderseits $\left[\frac{\bar{\varkappa}}{\pi}\right]_4=\left[\frac{\varkappa}{\bar{\pi}}\right]_4$ ist, ist $\left[\frac{\varkappa}{\bar{\pi}}\right]_4=\left[\frac{\bar{\varkappa}}{\pi}\right]_4\left[\frac{\varkappa}{\bar{\pi}}\right]_4^2$. Daher ist $\left(\frac{p}{q}\right)_4=\left[\frac{\varkappa}{\pi}\right]_4\times\left[\frac{\bar{\varkappa}}{\pi}\right]_4\left[\frac{\varkappa}{\bar{\pi}}\right]=\left[\frac{q}{\pi}\right]_4\left[\frac{\varkappa}{\bar{\pi}}\right]=\left(\frac{q}{p}\right)_4\left[\frac{\varkappa}{\pi}\right]$ w.z.b.w.

Wir wollen nun das Symbol $\left(\frac{m}{n}\right)_4$ zum solchen Falle ausdehen, worin

n gerade Zahl ist. Da $\left(\frac{2}{p}\right)=+1$ für $p\equiv+1 \pmod 8$ ist, ist das Symbol $\left(\frac{2}{p}\right)_4$ für solche Primzahl p definiert. Also betrachten wir nur solche p, wofür $p\equiv 1 \pmod 8$ ist, und sei $p=\pi\bar{\pi}$, $\pi\equiv 1 \pmod{(1+i)^3}$ in k. Dann ist

$$\left(\frac{2}{p}\right)_4=\left[\frac{2}{\pi}\right]_4=\begin{cases}+1\\-1\end{cases} \text{ für } \pi\equiv\begin{cases}1\,,\quad -3\\-3+4i,\ 1+4i\end{cases} \pmod 8. \tag{7}$$

Wir setzen nun für $p\equiv 1 \pmod 8$

$$\left(\frac{p}{2}\right)_4=\begin{cases}+1\\-1\end{cases} \text{ für } p\equiv\begin{cases}1\\9\end{cases} \pmod{16}. \tag{8}$$

Falls aber $p\equiv 1 \pmod{16}$ ist, so ist $\pi\equiv 1$ oder $1+4i \pmod 8$, und falls $p\equiv 9 \pmod{16}$ ist, so ist $\pi\equiv -3$ oder $-3+4i \pmod 8$. Also folgt aus (7) und (8)

$$\left(\frac{2}{p}\right)_4\left(\frac{p}{2}\right)_4=\left[\frac{1+i}{\pi}\right] \tag{9}$$

unter Berücksichtigung des Ergänzungssatzes des Reziprozitätsgesetzes von quadratischen Resten in k:

$$\left[\frac{1+i}{\pi}\right]=\begin{cases}+1\\-1\end{cases} \text{ für } \pi\equiv\begin{cases}1\\-3\end{cases} \pmod{(1+i)^5}.$$

Das Symbol $\left(\frac{m}{n}\right)_4$ ist jetzt für zueinander prime gerade oder ungerade positive Zahlen m und n durch (1) definiert, wenn für jeden ungeraden Primteiler p von m und q von n $p\equiv q\equiv 1 \pmod 8$ und $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=+1$ sind. Für diese m und n gilt auch (6), wenn wir

$$\left[\frac{\pi}{1+i}\right]=\left[\frac{1+i}{\pi}\right] \quad \text{für } \pi\equiv 1 \pmod{(1+i)^3} \tag{10}$$

setzen und wenn ferner $m=\mu\bar{\mu}$, $n=\nu\bar{\nu}$, $\frac{\mu}{1+i}\equiv\nu\equiv 1 \pmod{(1+i)^3}$ für gerades m, $\mu\equiv\frac{\nu}{1+i}\equiv 1 \pmod{(1+i)^3}$ für gerades n seien.

4. Nun kehren wir auf das Problem, welches am Schluss von Nr. 2. gestellt ist, zurück, und suchen zunächst unter den Primzahlen p, wofür $p\in H(V)$ sind, diejenige, welche in K vollzerfallen. Es sei also $p\in H(V)$

und $p=\pi\bar{\pi}$, $\pi\equiv\bar{\pi}\equiv 1 \pmod{(1+i)^3}$ in k. Dafür, dass diese Primzahl p in K vollzerfalle, ist notwendig und hinreichend, dass π in $\Lambda=k(\sqrt{\mu})$ zerfällt, d. h. $\pi\in H(\Lambda/k)$. Dafür ist notwendig und hinreichend, dass

$$X(\pi)=\prod_{\lambda}\chi_\lambda(\pi)=+1, \quad \pi\equiv 1 \pmod{(1+i)^3} \tag{11}$$

gilt.[1] Dabei durchläuft λ entweder alle in der Relativdiskriminante von Λ/k aufgehenden Primzahlen λ von k oder alle solche Primzahlen ausser $1+i$. Letzteres geschieht dann und nur dann, wenn $\mu\equiv 1+2i \pmod{(1+i)^3}$ ist. Für die von $1+i$ verschiedenen Primzahl λ ist $\chi_\lambda(\pi)$ quadratischer Restcharakter von π nach λ; für $\lambda=1+i$ und für π, deren Norm $N(\pi)=p\equiv 1 \pmod 8$ ist, ist

$$\chi_{1+i}(\pi)=\begin{cases} +1 \\ \left[\dfrac{1+i}{\pi}\right] \end{cases} \text{ für } \mu\equiv\begin{cases} i\ ,\ 2+i \\ 1+i,\ 1+3i \end{cases} \pmod 4. \tag{12}$$

Da $\mu=c\alpha$ ist (vgl. Nr. 1), so sei $X_c(\pi)=\prod_{\lambda/c}\chi_\lambda(\pi)$ gesetzt. Dann gilt

$$X_c(\pi)=\left[\frac{\pi}{c}\right]=\left(\frac{N\pi}{c}\right)=\left(\frac{p}{c}\right).$$

Sei also

$$X(\pi)=\left(\frac{p}{c}\right)X_\alpha(\pi), \tag{13}$$

so ist $X_\alpha(\pi)=+1$ dann und nur dann, wenn π in $k(\sqrt{\alpha})$ zerfällt. Denn, da $\mu\equiv\pm\alpha \pmod 4$ ist, ist der Charakter $\chi_{1+i}(\pi)$ in $X_\alpha(\pi)$ genau demjenigen für $k(\sqrt{\alpha})$ gleich.

5. Erstens sei $\mu\equiv\pm\alpha\equiv 1$ oder $1+2i \pmod 4$. Dann ist für jede $\pi\equiv 1 \pmod{(1+i)^3}$

$$X_\alpha(\pi)=\prod_{\lambda/\alpha}\chi_\lambda(\pi)=\prod_{\lambda/\alpha}\left[\frac{\pi}{\lambda}\right]=\left[\frac{\pi}{\alpha}\right]. \tag{14}$$

Mithin gilt wegen (6) und $N\alpha=m$

$$\left(\frac{p}{m}\right)_4\left(\frac{m}{p}\right)_4=\left[\frac{\pi}{\alpha}\right]=X_\alpha(\pi), \tag{15}$$

wenn nur für p das Symbol $\left(\dfrac{m}{p}\right)_4$ definiert ist. Dies ist der Fall, wenn

$p \equiv 1 \pmod 4$ ist und überdies wenn für jeden Primteiler l von m $\left(\frac{l}{p}\right)=\left(\frac{p}{l}\right)=+1$ gilt; mit anderen Worten, wenn p in $R^*=R(\sqrt{-1}, \sqrt{l},\ldots\ldots)$ vollzerfällt. Mithin folgt aus (11), (13) und (14), dass die Primzahl p, welche in R^* vollzerfällt, dann und nur dann auch in K vollzerfällt, wenn

$$\left(\frac{p}{c}\right)\left(\frac{p}{m}\right)_4\left(\frac{m}{p}\right)_4=+1 \tag{16}$$

gilt. Es sei nun $K^*=R^*K$. Das Zerlegungsgesetz der Primzahl p in K^*, für welche $p \notin H(V)$ ist, ist mit Hilfe der Kongruenzklasse in Nr. 2 bestimmt worden. Die Primzahl p, für welche $p \in H(V)$ ist, zerfällt in K^* dann und nur dann voll, wenn $p \in H(R^*)$ ist und überdies die Formel (16) gilt. Damit ist das Zerlegungsgesetz der Primzahlen in K^* vollständig bestimmt worden.

Zweitens sei $\mu \equiv \pm a \equiv 1+i,\ 1+3i \pmod 4$. In diesem Falle ist $Na=m$ gerade. Für $\pi \equiv 1 \pmod{(1+i)^3}$ gilt aber auch (14) wegen (10) und (12). Also gilt auch (15) wegen (9) oder wegen (6) mit geradem m, wenn nur $\left(\frac{m}{p}\right)_4$ definiert ist. Wenn also $R^*=R(\sqrt{-1}, \sqrt{2}, \sqrt{l},\ldots\ldots)$, $K^*=R^*K$ gesetzt werde, so erschliessen wir das Zerlegungsgesetz in K^* ähnlich wie oben.

Drittens sei $\mu \equiv \pm a \equiv i,\ 2+i \pmod 4$. Ist $N\pi \equiv p \equiv 1 \pmod 8$, so gilt wegen (12) $\chi_{1+i}(\pi)=+1$, also ist $\chi_{1+i}(\pi)$ als Faktor von $X_a(\pi)$ überflüssig. Also gilt auch die Formel (14). Alles geht dann ganz ähnlich wie oben, falls $R^*=R(\sqrt{-1}, \sqrt{2}, \sqrt{l},\ldots\ldots)$, $K^*=R^*K$ ist.

6. Zusammenfassend erhalten wir folgendes Resultat.

Satz 1. *Die Zeichen* μ, m, c, l, k, k_1, k_2, V, K *haben dieselbe Bedeutung wie in Nr.* 1. *Ist* $\mu \equiv 1$ *oder* $1+2i \pmod 4$, *so sei* $R^*=R(\sqrt{-1}, \sqrt{l},\ldots\ldots)$. *Sonst sei* $R^*=R(\sqrt{-1}, \sqrt{2}, \sqrt{l},\ldots\ldots)$. *Es sei ferner* $K^*=R^*K$. *Dann zerfällt die Primzahl* p, *welche in der Diskriminante von* K^* *nicht aufgeht, in* K^* *in Idealen*

1. *ersten Grades, wenn* $p \in H(R^*)$ *und* $\left(\frac{p}{c}\right)\left(\frac{p}{m}\right)_4\left(\frac{m}{p}\right)_4=+1$ *ist,*
2. *zweiten Grades, wenn* $p \in H(R^*)$ *und* $\left(\frac{p}{c}\right)\left(\frac{p}{m}\right)_4\left(\frac{m}{p}\right)_4=-1$ *ist,*

oder wenn $p \notin H(R^*)$ *und* $p \in H(V)$ *ist,*

oder aber wenn $p \notin H(V)$ *und* $p \in H(k) \cup H(k_1)$ *ist,*

3. vierten Grades, wenn $p \notin H(V)$ *und* $p \in H(k_2)$ *ist.*

Vergleichen wir die Kroneckersche Dichtigkeit der Primzahlen, welche in K^* vollzerfallen, mit derjenigen der in Kongruenzklassen enthaltenen Primzahlen, so erhalten wir aus Satz 1 Aussagen über Verteilung der Primzahlen. Ich erwähne hier nur ein Spezialfall von denen:

Satz 2. Es sei m Produkt $t-1$ *verschiedener Primzahlen* l, *wofür* $l \equiv 1 \pmod 4$ *ist. Es sei ferner p Primzahl mit der Bedingung*

$$p \equiv 1 \pmod 4 \text{ und } \left(\frac{p}{l}\right) = +1 \text{ für jeden Primteiler } l \text{ von } m. \quad (17)$$

Die Dichtigkeit dieser Primzahlen p ist offenbar gleich $1/2^t$. *Unter diesen Primzahlen haben dann die Primzahlen p mit der Bedingung*

$$\left(\frac{p}{m}\right)_4 \left(\frac{m}{p}\right)_4 = +1. \quad (18)$$

die Dichtigkeit $1/2^{t+1}$.

Für die im Satze 2 erwähnte Zahl m sei $m=\mu\bar{\mu}$ in k. Und sei $\mu \equiv 1$ oder $1+2i \pmod 4$. Es seien $R^*=k(\sqrt{l},\ldots)$, $K=k(\sqrt{\mu})$ und $K^*=R^*K$. Wegen Satz 1, zerfällt die Primzahl p, welche (17) genügt, dann und nur dann in K^* voll, wenn sie (18) genügt. Aber die Primzahl p, welche (17) genügt, nichts anders als diejenige, welche nach der Diskriminante des quadratischen Körpers $k_2=R(\sqrt{-m})$ Normenrest bezüglich k_2/R ist. Andererseits ist R^* unverzweigt und abelsch über k_2 und vom Relativgrade $(R^*/k_2)=2^{t-1}$, also der dem Hauptgeschlecht von k_2 zugeordnete Klassenkörper[4]. Ist $\mu \equiv 1 \pmod 4$, so ist auch K^* unverzweigt über k_2. Wenn überdies K^* absoluter Klassenkörper von k_2 ist, d. h. wenn die Klassenzahl von k_2 gleich 2^t ist, so ist (18) die notwendige und hinreichende Beningung dafür, dass die Primzahl p, welche Normenrest ist, wirklich Norm einer Zahl aus k_2 ist. Darin fallen die Zahlen $m=17, 65, 73, 97$ usw. Des Interesses halber füge ich ein Zahlenbeispiel hinzu.

$m=65$. Der absolute Klassenkörper von $R(\sqrt{-65})$ ist $K=R(\sqrt{-1}, \sqrt{5}, \sqrt{13}, \sqrt{1+8i})$. Die Primzahl p ist Normenrest nach der Diskriminante $d=-4\cdot 65$ von $R(\sqrt{-65})$, wenn nur $p \equiv 1 \pmod 4$, $\pm 1 \pmod 5$, $\pm 1, \pm 3, \pm 4 \pmod{13}$ ist. Diese Primzahlen p können dann und nur dann in der Form $p=x^2+65y^2$ dargestellt werden, wenn $\left(\frac{65}{p}\right)_4 \left(\frac{p}{65}\right)_4 = +1$ ist. Dabei ist

4) In dieser Hinsicht vergleiche man die vorstehende Arbeit von Herrn Hasse: Zur Geschlechtertheorie in quadratischen Zahlkörpern.

$$\left(\frac{p}{13}\right)_4 = \begin{cases} +1 \\ -1 \end{cases} \quad \text{für} \quad p \equiv \begin{cases} 1, & 3, & -4 \\ -1, & -3, & 4 \end{cases} \quad (\text{mod. } 13)$$

$$\left(\frac{p}{5}\right)_4 = \begin{cases} +1 \\ -1 \end{cases} \quad \text{für} \quad p \equiv \begin{cases} 1 \\ -1 \end{cases} \quad (\text{mod. } 5).$$

Unter der Rubrik $\left(\frac{65}{p}\right)_4$ in folgender Tabelle steht das Symbol $\pm$, je nachdem

$65^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$ d. h. $\left(\frac{65}{p}\right)_4 = \pm 1$ ist.

p	x, y	p mod. 5	p mod. 13	$\left(\frac{65}{p}\right)_4$	p	p mod. 5	p mod. 13	$\left(\frac{65}{p}\right)_4$
101	6, 1	1	−3	−	29	−1	3	+
269	3, 2	−1	−4	−	61	1	−4	−
389	18, 1	−1	−1	+	181	1	−1	+
601	4, 3	1	3	+	521	1	1	−
641	24, 1	1	4	−	569	−1	−3	−
701	21, 2	1	−1	−	809	−1	3	+
1049	3, 4	−1	−4	−	829	−1	−3	−
1069	22, 3	−1	3	−	881	1	−3	+
1361	36, 1	1	−4	+	1109	−1	4	−
1481	21, 4	1	−1	−	1249	−1	1	+
1609	32, 3	−1	3	−	1301	1	1	−
1741	34, 3	1	−1	−	1381	1	3	−
1949	18, 5	−1	−1	+	1429	−1	−1	−
2029	38, 3	−1	1	−	1621	1	−4	−
2129	33, 4	−1	−3	+	1889	−1	4	−
2341	1, 6	1	1	+	1901	1	3	−
2389	7, 6	−1	−3	+	2081	1	1	−
2521	44, 3	1	−1	−	2089	−1	−4	+
2861	51, 2	1	1	+	2141	1	−4	−
3181	29, 6	1	−4	+	2161	1	3	−
3221	6, 7	1	−3	−	2441	1	−3	+
3301	31, 6	1	−1	−	2549	−1	1	+
3329	12, 7	−1	1	−	2609	−1	−4	+
3389	42, 5	−1	−4	−	2729	−1	−1	−
3709	37, 6	−1	4	+	2909	−1	−3	−
3761	24, 7	1	4	−	3041	1	−1	+
3929	48, 5	−1	3	−	3121	1	1	−
4021	41, 6	1	4	−	3169	−1	−3	−
4229	63, 2	−1	4	+	3449	−1	4	−
4241	9, 8	1	3	+	3461	1	3	−
4289	57, 4	−1	−1	+	3701	1	−4	−
4421	66, 1	1	1	+	3769	−1	−1	−
4481	36, 7	1	−4	+	3821	1	−1	+
4549	47, 6	−1	−1	+	4001	1	−3	+
					4261	1	−3	+

Mathematisches Institut, Universität zu Nagoya