ACTA ARITHMETICA
XXVI (1974)

Über die Anzahl der Erweiterungen eines algebraischen Zahlkörpers mit einer gegebenen abelschen Gruppe als Galoisgruppe*

von

K. Haberland (Wrocław–Berlin)

1. Einleitung. Es geht um einige Berechnungen über die Häufigkeit, mit der eine vorgegebene endliche abelsche Gruppe als Galoisgruppe unter den normalen Erweiterungen eines festen algebraischen Zahlkörpers auftritt. Jedenfalls ist das für jede solche Gruppe unendlich oft der Fall. Wir müssen also eine geeignete Art wählen, wie wir diese unendlich vielen Erweiterungen zählen wollen. Ein natürlicher Weg scheint folgender zu sein: Sei k ein fester algebraischer Zahlkörper, G eine endliche abelsche Gruppe, und x ein positiver reeller Parameter. Dann sei

$$(*)\qquad \varrho(G,x) = \operatorname{card}\{K\colon K/k \text{ ist eine normale Körpererweiterung mit der Galoisgruppe } G(K/k) \cong G, \text{ und alle in } K \text{ verzweigten Primideale } \mathfrak{p} \text{ aus } k \text{ erfüllen } N\mathfrak{p} \leqslant x\}.$$

Diese Zahl ist endlich. Unser Ziel ist es, eine Formel der Art

$$\log \varrho(G,x) \sim C(G)\,\frac{x}{\log x} \qquad (x\to\infty)$$

zu beweisen, wo C eine nur von G und k abhängige positive reelle Konstante ist. Wir benutzen die Klassenkörpertheorie.

2. Herleitung der Formel. Wir suchen einen gemeinsamen Erklärungsmodul für alle Körpererweiterungen K/k, die in $\varrho(G,x)$ gezählt werden. Es zeigt sich, daß es eine von x unabhängige Zahl r gibt, so daß

$$\mathfrak{m} = \mathfrak{m}(x) = \prod_{N\mathfrak{p}\leqslant x} \mathfrak{p}^r \cdot \mathfrak{m}_\infty .$$

Erklärungsmodul für alle Erweiterungen K/k aus $\varrho(G,x)$ ist. Denn die

---

* Als Diplomarbeit vom Mathematischen Institut der Boleslaw Bierut Universität Wrocław angenommen.

Ich danke an dieser Stelle meinem Betreuer Doz. W. Narkiewicz. Der Ansatz (*) ist von Prof. H. Koch (Berlin).

Relativdiskriminante $\delta_{K/k}$ hat an den Stellen $\mathfrak{p} \in S_x = \{\mathfrak{p} \in I_k\colon N\mathfrak{p} \leqslant x\}$, die nicht die Ordnung g der Gruppe G teilen (zahme Verzweigungen), den Beitrag $e(\mathfrak{P}/\mathfrak{p})-1 \leqslant g-1$, weil aber der endliche Teil des Führers die Diskriminante teilt, ist an diesen Stellen die Beschränktheit von r bezüglich x gezeigt. An den Stellen $\mathfrak{p} \in S_x$, die g teilen (wilde Verzweigungen), hilft uns folgende topologische Überlegung: Es gibt nur beschränkt viele lokale Erweiterungen $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, $\mathfrak{p} \in S_x$, $\mathfrak{p} \mid p$, K/k aus $\varrho(G, x)$. Der Durchschnitt aller Normgruppen $N_{k_{\mathfrak{p}}}^{K_{\mathfrak{P}}} K_{\mathfrak{P}}^*$ in $k_{\mathfrak{p}}^*$ ist folglich offen. Also existiert eine von x unabhängige natürliche Zahl r, so daß an allen Stellen $\mathfrak{p} \in S_x$, $\mathfrak{p} \mid p$ die Führer aller Erweiterungen $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ das Ideal $\mathfrak{p}^r$ teilt. Damit ist das Verlangte gezeigt; alle Körper K aus $\varrho(G, x)$ liegen also im Strahlklassenkörper modulo $\mathfrak{m}$. Unsere Aufgabe besteht nun darin, in der Strahlklassengruppe modulo $\mathfrak{m}$ die Anzahl der Untergruppen zu bestimmen, nach der die Strahlklassengruppe faktorisiert eine zu G isomorphe Gruppe ergibt. Wir haben also folgendes gruppentheoretisches Problem zu lösen: Gegeben sind zwei endliche abelsche Gruppen G und H, für wieviele Untergruppen von H gibt H nach dieser faktorisiert eine zu G isomorphe Gruppe? Oder durch Dualisierung: Wieviele zu G isomorphe Untergruppen hat H? Wir untersuchen das unter der Voraussetzung, daß G zyklisch von Primzahlpotenzordnung p^n ist. H werde folgendermaßen zerlegt:

$$H = H_0 \oplus H_1 \oplus \dots,$$

wo H_0 von zu p primer Ordnung ist, und H_j, $j \geqslant 1$, die direkte Summe von $h_j(p)$ zyklischen Gruppen der Ordnung p^j ist. Solch eine Zerlegung gibt es, und die $h_j(p)$ sind eindeutig erklärt. Sei noch

$$\bar{H}_n = H_n \oplus H_{n+1} \oplus \dots$$

und

$$\bar{h}_n(p) = h_n(p) + h_{n+1}(p) + \dots.$$

Dann ist

$$H = H_0 \oplus H_1 \oplus \dots \oplus H_{n-1} \oplus \bar{H}_n.$$

Wir zählen die Elemente $x \in H$ der Ordnung p^n. $x = (x_0, x_1, \dots, x_n)$ ist der Ordnung p^n dann und nur dann, wenn $x_0 = 0$, $x_1, \dots, x_{n-1}$ beliebig, x_n der Ordnung p^n ist. Es gibt also genau

$$p^{\sum_{j=1}^{n-1} j h_j(p)} (p^{n\bar{h}_n(p)} - p^{(n-1)\bar{h}_n(p)})$$

viele solche Elemente. Wollen wir die Anzahl der zu G isomorphen Untergruppen haben, müssen wir obige Zahl noch durch $\varphi(p^n)$ teilen, denn auf jede solche Gruppe fallen $\varphi(p^n)$ Generatoren.

Wir wenden das auf die Strahlklassengruppe mod $\mathfrak{m}$ an. Für diese haben wir die folgenden exakten Sequenzen (Lang [2], Kap. 6, § 1)

$$(1) \qquad 0 \to G'_{\mathfrak{m}} \to G_{\mathfrak{m}} \to Cl_k \to 0,$$

$$(2) \qquad 0 \to U_k/U_k^{\mathfrak{m}} \to G'_{\mathfrak{m}} \to \prod_{\mathfrak{p} \in Sx} (\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^r)^* \oplus \prod_{\mathfrak{p} \mid \mathfrak{m}\infty} \boldsymbol{R}^*/\boldsymbol{R}_+^* \to 0.$$

Hier ist $G_{\mathfrak{m}}$ die Strahlklassengruppe mod $\mathfrak{m}$, Cl_k die Gruppe der Idealklassen von k, U_k die Gruppe der Einheiten im Ring der ganzen Zahlen von k, $U_k^{\mathfrak{m}}$ die Gruppe der Einheiten $u \in U_k$ für die $u \equiv 1 \pmod{\mathfrak{m}}$ gilt, $\mathfrak{o}_{\mathfrak{p}}$ der Ring der ganzen Zahlen in $k_{\mathfrak{p}}$, $\mathfrak{p}$ das maximale Ideal in $\mathfrak{o}_{\mathfrak{p}}$, $G'_{\mathfrak{m}}$ eine Hilfsgruppe die uns nicht näher interessiert. Wir zeigen jetzt, daß $U_k/U_k^{\mathfrak{m}}$ „klein" ist. Sei $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}$, dann ist für jedes $u \in U_k$

$$U^{\varphi(\mathfrak{m}_{\mathfrak{p}})} \equiv 1 \pmod{\mathfrak{m}_{\mathfrak{p}}},$$

$$U^{\text{k.g.V.}\{\varphi(\mathfrak{m}_{\mathfrak{p}})\colon \mathfrak{p} \in S_x\}} \equiv 1 \pmod{\mathfrak{m}}.$$

Die Potenz, mit der p in k.g.V. $\{\varphi(\mathfrak{m}_{\mathfrak{p}})\colon \mathfrak{p} \in S_x\}$ aufgeht, ist gleich

$$r_x = \max\{v_p(N\mathfrak{p}-1)\colon \mathfrak{p} \in S_x\}^* \cup \{f(\mathfrak{p}/p) v_{\mathfrak{p}}(\mathfrak{m})\colon \mathfrak{p} \in S_x, \mathfrak{p} \mid p\}.$$

Natürlich gilt $r_x = O(\log x)$. Seien $\varepsilon_1, \dots, \varepsilon_{r_0}$ Grundeinheiten. Dann gilt

$$\varepsilon_j^{p^{r_x} \cdot q} \equiv 1 \pmod{\mathfrak{m}}, \quad j = 1, \dots, r_0, \text{ für ein gewisses } q \in \boldsymbol{N}.$$

Also ist die Potenz, mit der p in $(U_k : U_k^{\mathfrak{m}})$ aufgeht, höchstens gleich $r_0 \cdot r_x + O(1)$. Folglich gilt

$$\sum_{j=1}^{\infty} j h_j(p) = O(\log x),$$

wo $h_j(p)$ die Invarianten der Gruppe $U_k/U_k^{\mathfrak{m}}$ sind.

Wir berechnen nun die Invarianten $h_j(p)$ für die Gruppe $\prod_{\mathfrak{p} \in S_x} (\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^r)^*$. Die Gruppe $(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^r)^*$ ist das direkte Produkt einer zyklischen Gruppe der Ordnung $N\mathfrak{p}-1$ und einer Gruppe der Ordnung $(N\mathfrak{p})^{r-1}$. Bis auf die beschränkt vielen Ausnahmen $\mathfrak{p} \mid p$, $\mathfrak{p} \in S_x$ ist der zweite Faktor p-frei. Wir haben also die Formeln

$$h_j(p) = \text{card}\{\mathfrak{p}\colon N\mathfrak{p} \leqslant x,\ N\mathfrak{p} \equiv 1 \pmod{p^j},\ N\mathfrak{p} \not\equiv 1 \pmod{p^{j+1}}\} + O(1),$$

$$\bar{h}_n(p) = \text{card}\{\mathfrak{p}\colon N\mathfrak{p} \leqslant x,\ N\mathfrak{p} \equiv 1 \pmod{p^n}\} + O(1).$$

Sei $D_n \subseteq (\boldsymbol{Z}/p^n\boldsymbol{Z})^*$ die Untergruppe der Restklassen mod p^n, in denen Absolutnormen von ganzen Idealen aus k auftreten, ihre Ordnung bezei-

chnen wir mit $d(p^n)$. Seien $\chi_0, \chi_1, \dots, \chi_s$ die gewöhnlichen Dirichletschen Charaktere mod p^n. Diese fassen wir als Heckesche Charaktere auf der Gruppe der zu $S = \{p, \infty\}$ primen Ideale von Q auf. Um die Invarianten $\overline{h}_n(p)$ mit Hilfe der gewöhnlichen analytischen Methode abschätzen zu können, müssen wir wissen, daß $\chi_j \circ N$ Heckesche Charaktere sind. Dazu reicht es, so einen Modul $\mathfrak{m}$ anzugeben, daß $\chi_j \circ N$ gleich 1 ist auf der Gruppe der totalpositiven Hauptideale, die $\equiv 1 \pmod{\mathfrak{m}}$ sind. Wir nehmen $\mathfrak{m} = p^n$, aufgefaßt als Modul über k, dann folgt aus $x \equiv 1 \pmod{\mathfrak{m}}$ $N_Q^k(x) \equiv 1 \pmod{p^n}$, also $\chi_j \circ N(x) = 1$. Die $\varphi(p^n)$ Funktionen $\chi_j \circ N$ sind demnach Heckesche Charaktere mit der Ausschließungsmenge $S = S_\infty \cup \{\mathfrak{p}: \mathfrak{p} | p\}$. Diese sind nicht alle verschieden: Ist $\chi_j | D_n = \chi_k | D_n$, so gilt $\chi_j \circ N = \chi_k \circ N$ und umgekehrt. Wir wählen aus jeder Klasse gleicher Charaktere einen aus, und erhalten eine Gruppe verschiedener Heckescher Charaktere

$$\chi_0, \chi_1, \dots, \chi_{d-1}, \qquad d = d(p^n).$$

Auf diese wenden wir Lang [2], Theorem 5, Kap. 15, § 5 an, und erhalten

$$\overline{h}_n(p) \sim \frac{1}{d(p^n)} \cdot \frac{x}{\log x}.$$

Daraus folgt

$$h_j(p) = \left(\frac{a(p^{j+1}) - 1}{d(p^{j+1})} + O(1) \right) \frac{x}{\log x},$$

wo $a(p^{j+1})$ die Anzahl der Restklassen $\bmod p^{j+1}$ ist, die $\equiv 1 \pmod{p^j}$ sind, und in D_{j+1} liegen, also

$$a(p^{j+1}) = d(p^{j+1})/d(p^j).$$

Wir betrachten nun die Sequenz (2). Die h_j-Invarianten der ersten Gruppe bezeichnen wir mit $h_j'(p)$, die der mittleren mit $h_j(p)$ und die der letzten mit $h_j''(p)$. Dann gilt auf Grund der Exaktheit

$$\sum_{j=1}^{\infty} j h_j(p) = \sum_{j=1}^{\infty} j h_j'(p) + \sum_{j=1}^{\infty} j h_j''(p)$$

und

$$\sum_{j=r}^{\infty} h_j''(p) \leqslant \sum_{j=r}^{\infty} h_j(p)$$

für beliebiges r. Summieren wir die Ungleichungen über r, so erhalten wir

$$\sum_{j=1}^{\infty} j h_j''(p) \leqslant \sum_{j=1}^{\infty} j h_j(p),$$

also gilt wegen

$$\sum_{j=1}^{\infty} j h_j'(p) = O(\log x),$$

$$\sum_{j=r}^{\infty} h_j(p) = \sum_{j=r}^{\infty} h_j''(p) + O(\log x),$$

$$h_j(p) = h_j''(p) + O(\log x),$$

$$\overline{h}_n(p) = \overline{h}_n''(p) + O(\log x).$$

Wir dualisieren nun die Sequenz (1) und die obige Rechnung bleibt auch für die entstandene Sequenz richtig, denn Cl_k hängt ja nicht von x ab. Folglich haben wir eine asymptotische Formel für die Invarianten $h_j(p)$ und $\overline{h}_n(p)$ der Strahlklassengruppe mod $\mathfrak{m}$ erhalten. Es ergibt sich sofort der

Satz. *Sei G eine zyklische Gruppe von Primzahlpotenzordnung p^n, dann gilt die Formel*

$$\log \varrho(G, x) \sim \log p \left(\sum_{j=1}^{n} \frac{1}{d(p^j)} \right) \frac{x}{\log x}.$$

Sei G_1 eine endliche abelsche Gruppe, G_2 eine zyklische Gruppe von Primzahlpotenzordnung p^n. Dann gilt

$$\varrho(G_1 \oplus G_2, x) \leqslant \sum_{H_1 \subseteq G_\mathfrak{m}, H_1 \cong G_1} \operatorname{card}\{H_2 \subseteq G_\mathfrak{m}: H_2 \cong G_2, H_2 \cap H_1 = (1)\},$$

$$\varrho(G_1 \oplus G_2, x) \leqslant \varrho(G_1, x)\, \varrho(G_2, x).$$

(Wir zählen wieder zu $G_1 \oplus G_2$ isomorphe Untergruppen statt Untergruppen mit zu $G_1 \oplus G_2$ isomorphen Faktorgruppen.) Die Ungleichung steht deshalb, weil $H_1 \oplus H_2$ die H_i, $i = 1, 2$ im allgemeinen nicht eindeutig bestimmt. Die Anzahl der Zerlegungen von $H_1 \oplus H_2$ ist aber beschränkt, das heißt unabhängig von x, also

$$\varrho(G_1 \oplus G_2, x) \geqslant C_1 \sum_{H_1 \subseteq G_\mathfrak{m}, H_1 \cong G_1} \operatorname{card}\{H_2 \subseteq G_\mathfrak{m}: H_2 \cong G_2, H_2 \cap H_1 = (1)\}.$$

Aus $0 \to H_1 \to G_\mathfrak{m} \to G_\mathfrak{m}/H_1 \to 0$ gewinnen wir durch Dualisierung eine Einbettung $0 \to G_\mathfrak{m}/H_1 \to G_\mathfrak{m}$ und jede zyklische Untergruppe der Ordnung p^n der Gruppe $G_\mathfrak{m}/H_1$ gibt eine Gruppe H_2 der beschriebenen Art, also

$$\varrho(G_1 \oplus G_2, x) \geqslant C_1 \sum_{H_1 \subseteq G_\mathfrak{m}, H_1 \cong G_1} \operatorname{card}\{H_2 \subseteq G_\mathfrak{m}/H_1: H_2 \cong G_2\}.$$

Die Zahl $\operatorname{card}\{H_2 \subseteq G_m/H_1\colon H_2 \cong G_2\}$ unterscheidet sich von $\varrho(G_2, x)$ nur um einen beschränkten Faktor, denn

$$\operatorname{card}\{H_2 \subseteq G_m/H_1\colon H_2 \cong G_2\} = \frac{1}{\varphi(p^n)} \cdot p^{\sum_{j=1}^{n} j\bar{h}'_j(p)} (p^{n\bar{h}'_n(p)} - p^{(n-1)\bar{h}'_n(p)}).$$

$h'_j(p)$ sind die Invarianten von G_m/H_1. Aber $h_j(p) = h'_j(p) + O(1)$ wo $h_j(p)$ die Invarianten von G_m sind, also

$$\operatorname{card}\{H_2 \subseteq G_m/H_1\colon H_2 \cong G_2\} \geqslant C_2 \varrho(G_2, x),$$

wobei C_2 nicht von H_1 abhängt, sondern bloß von G_1. Demnach ist

$$\varrho(G_1 \oplus G_2, x) \geqslant C_3 \varrho(G_1, x)\varrho(G_2, x),$$

also

$$\log \varrho(G_1 \oplus G_2, x) \sim \log \varrho(G_1, x) + \log \varrho(G_2, x).$$

Wir haben damit für jede endliche abelsche Gruppe G eine asymptotische Formel für $\log \varrho(G, x)$ gewonnen: Man zerlege G in zyklische Gruppen von Primpotenzordnung G_i und summiere die entsprechenden Formeln für $\log \varrho(G_i, x)$ aus dem Satz.

3. Beispiele. Sei k ein Körper, wo $d(p^j) = \varphi(p^j)$ ist für alle j. Das gilt zum Beispiel für $k = \boldsymbol{Q}$ und jede Primzahl oder $k = \boldsymbol{Q}(\zeta_m)$ und $(p, m) = 1$. Dann ist

$$C(p) = \frac{1}{p-1}\log p,$$

$$C(p^2) = \frac{p+1}{p(p-1)}\log p, \quad C(p, p) = \frac{2}{p-1}\log p,$$

$$C(p^3) = \frac{p^2+p+1}{p^2(p-1)}\log p, \quad C(p^2, p) = \frac{2p+1}{p(p-1)}\log p,$$

$$C(p, p, p) = \frac{3}{p-1}\log p.$$

Literatur

[1] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, London and New York 1967.

[2] S. Lang, *Algebraic Number Theory*, Reading–London 1971.

Eingegangen 6. 7. 1973 (432)

ACTA ARITHMETICA
XXVI (1974)

On two problems of R. M. Robinson about sums of roots of unity

by

J. H. Loxton (Cambridge)

1. Introduction. Let β be a cyclotomic integer, that is an algebraic integer in a cyclotomic field. As usual, we define the maximum modulus of β, denoted by $|\overline{\beta}|$, to be the maximum of the absolute values of the conjugates of β. It is well-known that β can be represented as a sum of roots of unity. The aim of this paper is to investigate how these representations depend on the properties of β, such as its degree and maximum modulus. In particular, we consider two problems proposed by R. M. Robinson [4].

First, how can we tell whether a given cyclotomic integer can be expressed as a sum of a prescribed number of roots of unity? This problem was solved by A. Schinzel [6] who proved that a cyclotomic integer of degree d is a sum of n roots of unity only if it is a sum of n roots of unity of common degree less than

$$d(2\log d + 200\, n^2 \log 2n)^{20n^2}. \tag{1.1}$$

We shall show, by quite different methods, that this upper bound can be replaced by

$$10^{n+1} d \log\log 20d,$$

which is the main result of § 4. On the way, in § 3, we shall see that an integer in a given cyclotomic field, K say, is a sum of n roots of unity only if it is a sum of at most n roots of unity lying in the field K.

Second, how can we tell whether there is any cyclotomic integer with a given maximum modulus? For this problem, we consider two cyclotomic integers β and β^* to be equivalent if $\beta^* = \varrho\beta'$ for some conjugate β' of β and some root ϱ of unity. Clearly, equivalent cyclotomic integers have the same maximum modulus. In § 5, we shall show that there are only finitely many inequivalent cyclotomic integers with a given maximum modulus and give a method for finding them.