Tôhoku Math. Journ.
Vol. 18, No. 3, 1966

ÜBER DIE RELATIVKLASSENZAHL EINES RELATIV-GALOISSCHEN ZAHLKÖRPERS VON PRIMZAHLPOTENZGRAD.

AKIO YOKOYAMA

(Received April 20, 1966)

l sei eine fixierte Primzahl und k ein endlicher algebraischer Zahlkörper, der als Grundkörper behandelt wird. Durch die Klassenkörpertheorie wird der Zusammenhang zwischen der Klassenzahl von k und eines zyklischen Erweiterungskörpers von Primzahlgrad ziemlich klar gemacht. In dieser Arbeit werden eine Aussage für die Teilbarkeit der Relativklassenzahl eines Galoisschen Erweiterungskörpers von Primzahlpotenzgrad über k durch eine beliebige Primzahl gemacht und eine grobe Abschätzung des Ranges der p-Klassengruppe eines solchen Körpers angegeben. Zur Vereinfachung gebrauche ich die folgenden Ausdrücke:

Unter der *p-Klassengruppe von k* versteht man die Gruppe $\mathfrak{C}_k$ der Divisorenklassen von p-Potenzordnung aus der Divisorenklassengruppe (im weiteren Sinn) von k, wo p eine beliebige Primzahl bezeichnet. Die Ordnung der p-Klassengruppe von k wird mit $h_{k,p}$ bezeichnet.

Es sei K ein relativ-Galoisscher Zahlkörper über k und $\mathfrak{g}$ seine Galoissche Gruppe. Dann operiert $\mathfrak{g}$ auf der vollen Divisorengruppe D und der p-Klassengruppe $\mathfrak{C}_K$ von K und daher werden diese Gruppen zur $\mathfrak{g}$-Gruppen. Es sei H die Untergruppe aller $\mathfrak{a} \in D$ mit $\mathfrak{a}^m \sim 1$ für einen zu p primen geeigneten Exponenten m. Die Faktorgruppe

$$\mathfrak{D} = D/H$$

ist dann $\mathfrak{g}$-isomorph zur p-Klassengruppe $\mathfrak{C}_K$ von K. Der H zugeordnete Klassenkörper $K_{(p)}$ (dieses Bezeichnung werde auch weiterhin festgehalten) ist relativ-Galoissch über k. Es sei $\mathfrak{G}$ die Galoissche Gruppe von $\overline{K}_{(p)}/k$ und $\mathfrak{H}$ die Fixgruppe des Körpers K. Dann ist $\mathfrak{G}$ eine Erweiterung von $\mathfrak{H}$ zur Faktorgruppe $\mathfrak{g}$,

$$\mathfrak{G} = \bigcup_{\sigma} S_\sigma \mathfrak{H},$$

wobei die Summe über alle $\sigma \in \mathfrak{g}$ zu erstrecken ist, und $\mathfrak{H}$ wird zur $\mathfrak{g}$-Gruppe

vermöge

$$S_\sigma^{-1}AS_\sigma=A^\sigma \text{ für } A\in\mathfrak{H},\ \sigma\in\mathfrak{g}.$$

Ist $(\mathfrak{g}:1)\not\equiv 0 \bmod p$, so zerfällt die Erweiterung, d.h. können die Vertreter so wählen, dass sie eine zu $\mathfrak{g}$ isomorphe Gruppe bilden,

$$S_\sigma S_\tau=S_{\sigma\tau} \text{ für } \sigma,\tau\in\mathfrak{g}.$$

Nach dem Artinschen Reziprozitätsgesetz ist $\mathfrak{H}$ $\mathfrak{g}$-isomorph zur Faktorgruppe $\mathfrak{D}$ und daher ist sie $\mathfrak{g}$-isomorph zur p-Klassengruppe $\mathfrak{C}_K$ von K.

Die Untergruppe aller $C\in\mathfrak{C}_K$ mit $C^\sigma=C$ für alle $\sigma\in\mathfrak{g}$ heisst die *ambige p-Klassengruppe von K in bezug auf k.*

SATZ 1. *Es sei K ein relativ-Galoisscher Zahlkörper vom Primzahlpotenzgrade l^n über k. Ist dann p eine von l verschiedene Primzahl, so ist $h_{K,p}$ teilbar durch $h_{k,p}$ und ferner gilt*

$$h_{K,p}/h_{k,p}\equiv 1 \pmod{l}.$$

Anders gesagt ist der Exponent von p in $h_{K,p}/h_{k,p}$ das Vielfache von f, wo f die Ordnung der Restklasse p mod *l bezeichnet.*

BEWEIS. Es bezeichne $\mathfrak{C}_K$ bzw. $\mathfrak{C}_k$ die p-Klassengruppen von K und k. Es sei C eine von der Hauptklasse verschiedene Divisorenklasse aus $\mathfrak{C}_k$ und $\mathfrak{a}$ ein Nichthauptideal in C. Nehmen wir an, dass $\mathfrak{a}$ in ein Hauptideal von K überginge, so wäre auch $N_{K/k}\mathfrak{a}=\mathfrak{a}^{l^n}$ in k ein Hauptideal. Aber dies ist unmöglich, da $\mathfrak{a}$ zu C gehört. Also sind die zwei Ideale von k, die in k nicht äquivalent sind, auch in K nicht äquivalent. Daher wird $\mathfrak{C}_k$ bei der Einbettung in $\mathfrak{C}_K$ monomorph abgebildet. Die Normabbildung auf den Divisorengruppen induziert einen Normhomomorphismus der p-Klassengruppen $N_{K/k}$: $\mathfrak{C}_K\to\mathfrak{C}_k$, der ein Epimorphismus ist, da $\mathfrak{C}_K$ und die Galoissche Gruppe teilerfremde Ordnungen haben. Es bezeichne $\mathfrak{R}_{K/k}$ den Kern des Normhomomorphismus $N_{K/k}$: $\mathfrak{C}_K\to\mathfrak{C}_k$. Man sieht leicht ein, dass $\mathfrak{R}_{K/k}$ keine von der Hauptklasse verschiedene Divisorenklasse aus $\tilde{\mathfrak{C}}_k$ enthält, wo $\tilde{\mathfrak{C}}_k$ bei der Einbettung in $\mathfrak{C}_K$ das monomorphe Bild von $\mathfrak{C}_k$ bezeichnet. Also gilt

$$\mathfrak{C}_K=\tilde{\mathfrak{C}}_k\times\mathfrak{R}_{K/k} \qquad \text{(direkt)}.$$

Daraus folgt ersichtlich, dass $\tilde{\mathfrak{C}}_k$ mit der ambigen p-Klassengruppe von K in bezug auf k übereinstimmt und $h_{K,p}$ teilbar durch $h_{k,p}$ ist. Im Falle $h_{K,p}/h_{k,p}=1$ ist, ist die Behauptung richtig. Also sei $h_{K,p}/h_{k,p}\neq 1$, d.h. ist $\mathfrak{R}_{K/k}$ nichttrivial. Nun sei C_1 eine von der Hauptklasse verschiedene Divisorenklasse aus $\mathfrak{R}_{K/k}$. Dann existieren mindestens l von einander verschiedene mit C_1 konjugierte

Divisorenklassen, die in $\mathfrak{R}_{K/k}$ enthalten sind, weil $\widetilde{\mathfrak{S}}_k$ mit der ambigen p-Klassengruppe von K in bezug auf k übereinstimmt. Wenn keine von Hauptklasse verschiedene Divisorenklasse C_2 aus $\mathfrak{R}_{K/k}$ zu C_1 konjugiert ist, dann sind die zu C_2 konjugierten Divisorenklassen von der Hauptklasse und von den zu C_1 konjugierten Divisorenklassen verschieden. Dies sieht man leicht aus der Tatsache ein dass die Galoissche Gruppe von K/k auf die konjugierten Divisorenklassen transitiv wirkt. Daher ist die Ordnung von $\mathfrak{R}_{K/k}$ kongruent zu 1 modulo l, folgt somit, dass $h_{K,p}/h_{k,p}\equiv 1 \bmod l$.

KOROLLAR. *Es sei K ein relativ-Galoisscher Zahlkörper vom Primzahlpotenzgrade l^n über k und es sei h_K bzw. h_k die Klassenzahlen von K und k. Wenn h_K und h_k zu l prim sind, dann gilt*

$$h_K/h_k\equiv 1 \pmod{l}.$$

Zum Beweise beachte man, dass h_K, wenn h_k zu l prim ist, teilbar durch h_k ist und dass der p-Betrag von h_K/h_k mit $h_{K,p}/h_{k,p}$ übereinstimmt. (vgl. [4])

BEMERKUNG. i) Die Voraussetzung, dass h_K und h_k zu l prim sind, kann man durch etwas derartiges ersetzen, zum Beispiel, dass kein in K enthaltener unverzweigter Abelscher Körper über k existiert und dass h_K zu l prim ist.

ii) Dies ist eine Verallgemeinerung des Resultat von S.N. Kuroda [3].*)

Wenn K ein relativ-zyklischer Zahlkörper über k ist, gilt der

ZUSATZ 1. *K sei ein relativ-zyklischer Zahlkörper von Primzahlpotenzgrad und E sei ein in K enthaltener relativ-zyklischer Körper vom Relativgrade l^{n-1} über k. Ferner sei p eine von l verschiedene Primzahl. Dann gilt*

$$h_{K,p}/h_{E,p}\equiv 1 \pmod{l^n}.$$

Anders gesagt ist der Exponent von p in $h_{K,p}/h_{E,p}$ das Vielfache der Ordnung der primen Restklasse p mod l^n.

BEWEIS. Es bezeichne $\mathfrak{S}_K$ bzw. $\mathfrak{S}_E$ die p-Klassengruppen von K und E. Wie im Beweise von Satz 1 erhält man die direkte Zerlegung

$$\mathfrak{S}_K=\widetilde{\mathfrak{S}}_E\times\mathfrak{R}_{K/E} \qquad \text{(direkt)},$$

wobei $\widetilde{\mathfrak{S}}_E$ bei der Einbettung in $\mathfrak{S}_K$ das monomorphe Bild von $\mathfrak{S}_E$ und $\mathfrak{R}_{K/E}$ den Kern der Normabbildung $N_{K/E}$: $\mathfrak{S}_K\to\mathfrak{S}_E$ bezeichnet. Ferner, wie leicht

*) Zusatz bei der Korrektur (10. 20, 1966) : Siehe etwa H. Yokoi, On the class number of a relatively cyclic number field. Erssheint in Nagoya Math. Journ.

einzusehen ist, stimmt die ambige p-Klassengruppe von K in bezug auf E mit $\widetilde{\mathfrak{C}}_E$ überein. Im Falle $\mathfrak{R}_{K/E}=1$ ist, ist die Behauptung richtig. Also sei $\mathfrak{R}_{K/E}\neq 1$. Wenn eine Divisorenklasse $C\,(\neq 1)$ aus $\mathfrak{R}_{K/E}$ bei einer Substitution σ von der Galoisschen Gruppe von K/k invariant bleibt, so ist C auch bei der von σ erzeugten zyklischen Gruppe $\{\sigma\}$ invariant. Es sei F der in K enthaltene Oberkörper l-ten Grades von E. Es ist dann leicht zu sehen, dass die zyklische Gruppe $\{\sigma\}$ eine Untergruppe der Galoisschen Gruppe von K/F ist, da die ambige p-Klassengruppe von K in bezug auf E mit $\widetilde{\mathfrak{C}}_E$ übereinstimmt. Daher hat jede von Hauptklasse verschiedene Divisorenklasse aus $\mathfrak{R}_{K/E}$ mindestens l^n von einander verschiedene mit ihr konjugierte Klassen. Wie im Beweise von Satz 1 folgt also $h_{K,p}/h_{E,p}\equiv 1 \bmod l^n$.

Es sei K/k ein relativ-Galoisscher Zahlkörper vom Relativgrade m und es sei p eine nicht im Grade m aufgehende Primzahl. Wie zuvor, besitzt die p-Klassengruppe $\mathfrak{C}_K$ von K die direkte Zerlegung

$$\mathfrak{C}_K=\widetilde{\mathfrak{C}}_k\times\mathfrak{R}_{K/k} \qquad \text{(direkt)}.$$

Es bezeichne $\mathfrak{g}$ bzw. $\mathfrak{H}$ die Galoisschen Gruppen von K/k und $\overline{K}_{(p)}/K$. Dann ist $\mathfrak{H}$ $\mathfrak{g}$-isomorph zur p-Klassengruppe $\mathfrak{C}_K$ von K. Dementsprechend zerfällt $\mathfrak{H}$ in das direkte Produkt

$$\mathfrak{H}=\mathfrak{h}_1\times\mathfrak{h}_2 \qquad \text{(direkt)},$$

wobei $\mathfrak{h}_1$ und $\mathfrak{h}_2$ die Bilder der entsprechenden Faktoren $\widetilde{\mathfrak{C}}_k$, $\mathfrak{R}_{K/k}$ der p-Klassengruppe $\mathfrak{C}_K$ von K bezeichnen. Nun sei L_i $(i=1, 2)$ der Invariantenkörper des Komplementärfaktors von $\mathfrak{h}_i$ in $\mathfrak{H}$. Dann zerfällt der Klassenkörper $K_{(p)}$ in das Kompositum

$$\overline{K}_{(p)}=L_1\cdot L_2;$$

und wir bemerken, dass $L_1\cap L_2=K$. Auch L_i ist relativ-Galoissch über k und seine Galoissche Gruppe $\mathfrak{G}_i$ eine zerfallende Erweiterung von $\mathfrak{h}_i$ zur Faktorgruppe $\mathfrak{g}$ $(i=1, 2)$. Daher können wir eine Untergruppe $\mathfrak{N}$ von $\mathfrak{G}_2$ so finden, dass sie die folgenden Bedingungen erfüllt:

$$\mathfrak{G}_2=\mathfrak{h}_2\cdot\mathfrak{N}, \quad \mathfrak{h}_2\cap\mathfrak{N}=1, \quad (\mathfrak{N}:1)=m.$$

Dann induziert jedes Element aus $\mathfrak{N}$ einen Automorphismus von $\mathfrak{h}_2$. Hier verwenden wir die bekannte Tatsache für die Ordnung der Automorphismengruppe der p-Gruppe, die für beliebige endliche p-Gruppe angegeben worden ist und für $\mathfrak{h}_2$ so lautet, dass die Ordnung der Automorphismengruppe von $\mathfrak{h}_2$ ein Teiler der ganzen Zahl $\eta(p)$ ist:

$$\eta(p)=p^{\rho(e-\rho)}(p^{\rho}-1)(p^{\rho}-p)\cdots(p^{\rho}-p^{\rho-1}),$$

wo e durch $h_{K,p}/h_{k,p}=p^e$, d.h. die Ordnung von $\mathfrak{h}_2$ erklärt ist und ρ den Range von $\mathfrak{h}_2$, d.h. die Anzahl der zyklischen direkten Faktoren bezeichnet. (vgl. [1]) Nun seien $q_1,q_2,\cdots,q_r$ alle verschiedenen im m aufgehenden Primzahlen und sei f die Minimalzahl von allen f_i, $i=1,2,\cdots,r$, die die Ordnung der Restklasse p mod q_i bedeuten. Ist $\rho<f$, so ist m zu $\eta(p)$ prim. Daraus folgt wegen der obigen Tatsache, dass alle von jedes aus $\mathfrak{N}$ induzierten Automorphismen von $\mathfrak{h}_2$ trivial operieren und daher folgt, dass alle in $\mathfrak{h}_2$ mit jedem Element von $\mathfrak{N}$ vertauschbar sind. Damit ist gleichzeitig gezeigt, dass $\mathfrak{N}_{K/k}$ elementwise invariant bei jedem Element der Galoisschen Gruppe von K/k ist. Aber dies ist unmöglich, da die ambige p-Klassengruppe von K in bezug auf k mit $\widetilde{\mathfrak{C}}_k$ übereinstimmt. Also ist $\rho\geqq f$. Damit ist die folgende Aussage gewonnen:

SATZ 2. *Es sei K/k ein relativ-Galoisscher Zahlkörper vom Relativgrade m und es sei p eine nicht im Grade m aufgehende Primzahl. Ferner seien $q_1,q_2,\cdots,q_r$ alle verschiedenen in m aufgehenden Primzahlen und sei f die Minimalzahl von allen f_i, $i=1,2,\cdots,r$, die die Ordnung der Restklasse p* mod q_i *bedeuten. Ist dann $h_{K,p}/h_{k,p}$ durch p teilbar, so gilt für den Rang ρ des Normabbildungskerns $N_{K/k}$: $\mathfrak{C}_K\to\mathfrak{C}_k$*

$$f\leqq\rho.$$

Aus diesem Satz folgt sofort:

KOROLLAR. *Es sei K/k ein relativ-Galoisscher Zahlkörper vom Relativgrade m und es sei p eine nicht in m aufgehende Primzahl. f habe dieselbe Bedeutung wie in Satz 2. Ist dann $h_{K,p}/h_{k,p}$ durch p teilbar, so gilt für die Ränge ρ_1,ρ_2 der p-Klassengruppen von K bzw. k die Ungleichung*

$$\rho_2+f\leqq\rho_1.$$

Im Falle K/k ein relativ-zyklischer Zahlkörper von Primzahlpotenzgrad ist, gilt der

ZUSATZ 2. *Die Zahlkörper K, E erfüllen die Voraussetzungen von Zusatz 1; es sei f die Ordnung der Restklasse p* mod l *und es sei s die ganze Zahl derart, dass p^f-1 durch l^s, aber nicht durch l^{s+1} teilbar ist. Ist dann $h_{K,p}/h_{E,p}$ durch p teilbar, so ist*

$$nf/s\leqq\rho,$$

wobei ρ den Rang des Normabbildungskerns $N_{K/k}$: $\mathfrak{C}_K\to\mathfrak{C}_k$ bezeichnet.

BEWEIS. Wie oben, zerfällt die p-Klassengruppe $\mathfrak{C}_K$ von K in das direkte Produkt

$$\mathfrak{C}_K = \tilde{\mathfrak{C}}_k \times \mathfrak{R}_{K/k} \qquad \text{(direkt)}$$

und der Klassenkörper $\overline{K}_{(p)}$ in das Kompositum

$$\overline{K}_{(p)} = L_1 \cdot L_2,$$

wo L_1 bzw. L_2 die zu $\tilde{\mathfrak{C}}_k$ bzw. $\mathfrak{R}_{K/k}$ isomorphe Galoissche Gruppe $\mathfrak{h}_1, \mathfrak{h}_2$ über K besitzt. Auch L_2 ist relativ-Galoissch über k und seine Galoissche Gruppe $\mathfrak{G}$ eine zerfallende Erweiterung von $\mathfrak{h}_2$ zur Galoisschen Gruppe von K/k. Daher können wir die Vertreter so wählen, dass sie eine zur Galoisschen Gruppe von K/k isomorphe Gruppe bilden. Diese Vertreter induzieren dann die Automorphismen von $\mathfrak{h}_2$, die eine Untergruppe $\mathfrak{N}$ der Automorphismengruppe von $\mathfrak{h}_2$ bilden. Nun sei F der minimale Unterkörper von K, dessen p-Klassengruppe zu $\mathfrak{C}_K$ isomorph ist. Weil $h_{K,p}/h_{E,p}$ durch p teilbar ist, sieht man ein, dass E ein Unterkörper von F ist und folglich die Galoissche Gruppe von L_2/F den Zentralisator von $\mathfrak{h}_2$ in $\mathfrak{G}$ enthält (vgl. [1]). Also gibt es in $\mathfrak{N}$ mindestens l^n voneinander verschiedene Automorphismen von $\mathfrak{h}_2$ und daher muss die im Beweise von Satz 2 behandelte ganze Zahl $\eta(p)$ mindestens durch l^n teilbar sein, da die Ordnung der Automorphismengruppe von $\mathfrak{h}_2$ ein Teiler der ganzen Zahl $\eta(p)$ ist. Damit ist die Ungleichung $nf/s \leqq \rho$ gewonnen.

BEMERKUNG. Statt der Bedingung über die Relativklassenzahl $h_{K,p}/h_{E,p}$ ist dieser Zusatz richtig unter der Bedingung, dass die Anzahl der Divisorenklassen des Hauptgeschlechtes von K/E durch p teilbar ist.

Für den Rang der l-Klassengruppe von K, wobei l im Körpergrad aufgeht, ist der

SATZ 3. *K/k sei ein relativ-zyklischer Zahlkörper von Primzahlpotenzgrad derart, dass es wenigstens ein zwischen K und k verzweigtes und zwar reinverzweigtes Primideal von k gibt. Ferner sei E ein in K enthaltener relativ-zyklischer Körper vom Relativgrade l^{n-1} über k. Wenn die Anzahl der Divisorenklassen des Hauptgeschlechtes von K/E durch l teilbar ist, dann gilt für den Rang ρ bzw. den Exponent e der Ordnung l^e der l-Klassengruppe von K die Ungleichung*

$$\beta(n) \leqq \rho \quad bzw. \quad \beta(n)+1 \leqq e,$$

wo $\beta(n)$ gleich $\frac{1}{2}(-1+\sqrt{1+8n})$ ist.

BEWEIS. Es sei $\mathfrak{p}$ ein Primteiler eines reinverzweigten Primideals in $\overline{K}_{(l)}$ und es sei $T_{\mathfrak{p}}$ die Trägheitsgruppe zu $\mathfrak{p}$ für $\overline{K}_{(l)}/k$; es bezeichne $\mathfrak{G}$ bzw. $\mathfrak{A}$ die Galoisschen Gruppen von $\overline{K}_{(l)}/k$ und $\overline{K}_{(l)}/K$. Dann sieht man leicht aus der Hilbertschen Theorie des Galoisschen Körpers, dass $\mathfrak{G}=T_{\mathfrak{p}}\mathfrak{A}$ und $T_{\mathfrak{p}}\cap\mathfrak{A}=1$ sind; und wir bemerken, dass die Ordnung von $T_{\mathfrak{p}}$ mit dem Relativgrad von K/k übereinstimmt. Ist σ eine erzeugende Substitution der Galoisschen Gruppe von K/E, so ist bekanntlich das Hauptgeschlecht von K/E identisch mit der Gesamtheit aller symbolischen $(1-\sigma)$-ten Potenzen von Divisorenklassen aus K (vgl.[2]). Ist nun $\mathfrak{S}$ diejenige Untergruppe der Galoisschen Gruppe von K/k, die alle Divisorenklasse aus der l-Klassengruppe von K festlässt und ist weiter F der zur Untergruppe $\mathfrak{S}$ gehörige Teilkörper von K, so folgt dass F ein Oberkörper von E ist, weil die Anzahl der Divisorenklassen des Hauptgeschlechtes von K/E durch l teilbar ist, d.h. stimmt die l-Klassengruppe von K mit der ambigen l-Klassengruppe von K in bezug auf E nicht überein. Jedes Element aus $T_{\mathfrak{p}}$ induziert einen Automorphismus von $\mathfrak{A}$. Wie im Beweis von Zusatz 2 folgt also die Teilbarkeit der gleichartigen ganzen Zahl $\eta(l)$ wie im Beweis von Satz 2 durch l^n. Andererseits ist der Exponent von l in $\eta(l)$ gleich

$$\rho(e-\rho)+\frac{1}{2}\rho(\rho-1),$$

dessen Maximalbetrag $\frac{1}{2}\rho(\rho+1)$ $(=\frac{1}{2}e(e-1))$ ist. Daher haben wir die Ungleichung $\beta(n)\leqq\rho$ (bzw. $\beta(n)+1\leqq e$) in unserem Falle.

LITERATURVERZEICHNIS

[1] M. HALL, The theory of groups. New York, 1959.
[2] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, J. der D. M. V., 35(1926).
[3] S. N. KURODA, Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrade. Proc. Japan Acad., 40(1964), 623-626.
[4] A. YOKOYAMA, On class numbers of finite algebraic number fields. Tôhoku Math. Journ. 2, Vol. 17(1965), 349-357.

DIE UNIVERSITÄT ZU SHIZUOKA.