Zeitschrift: L'Enseignement Mathématique

Band: 19 (1973)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ERWEITERUNGSKÖRPER VON PRIMZAHLGRAD MIT DURCH DIESE PRIMZAHL TEILBARER KLASSENZAHL

Autor: Gut, Max

DOI: https://doi.org/10.5169/seals-46288

ERWEITERUNGSKÖRPER VON PRIMZAHLGRAD MIT DURCH DIESE PRIMZAHL TEILBARER KLASSENZAHL

von Max Gut

Wir beweisen in dieser Note mit elementaren Mitteln den *Satz:* Ist k^* ein beliebiger algebraischer Zahlkörper von endlichem Grade, und ist q eine Primzahl, so gibt es immer unendlich viele Erweiterungskörper k vom Relativgrade q in bezug auf k^*, deren Klassenzahl durch q teilbar ist.

Für weitere Sätze aus dem Ideenkreis der vorliegenden Note verweise ich auf die inhaltsreiche Arbeit des Herrn *Erich Lamprecht:* „Existenz von Zahlkörpern mit nicht abbrechendem Klassenkörperturm", *Archiv der Math.*, vol. 18 (1967), pg. 140—152.

Verwendet wird immer folgende Bezeichnung: ist S eine beliebige Substitution, so bedeute $\{S\}$ die von S erzeugte Gruppe. Alle auftretenden Gruppen sind Abel'sche Gruppen. Ferner bedeute k_0 den Körper der rationalen Zahlen.

Wir behandeln zuerst den Fall, dass die Primzahl q *ungerade* ist. Wir werden später sehen, dass der Beweis für den Fall $q = 2$ ganz analog geführt werden kann.

Durch direkte Konstruktion zeigen wir zunächst die Existenz *eines* solchen Erweiterungskörper k vom k^*, der die im Satze erwähnten Eigenschaften besitzt.

Es seien p_1 und p_2 zwei voneinander verschiedene ungerade Primzahlen, die $\equiv 1 \pmod{q}$ und teilerfremd zur Diskriminanten von k^* sind.

Für $t = 1$ und $t = 2$ bedeute ζ_t eine primitive p_t − te Einheitswurzel und g_t eine Primitivwurzel mod. p_t. Weiter bedeute s_t die Substitution, die ζ_t in $\zeta_t^{g_t}$ überführt; sie soll aber die Grösse ζ_j mit $j \neq t$ festlassen. Eine $\frac{1}{q}(p_t - 1)$ — gliedrige Periode des Körpers der p_t − ten Einheitswurzeln wird dann durch die Grösse

$$\eta_t = \sum_n s_t^{nq} \zeta_t$$

gegeben, wo in der Summe n die Werte $0, 1, 2, \ldots, \frac{1}{q}(p_t - 1 - q)$ durchläuft.

Für sie ist

$$s_t^q \eta_t = \eta_t ,$$

und die Grössen $s_t^m \eta_t$, wo m die Werte $0, 1, 2, \ldots, q-1$ durchläuft, sind alle voneinander verschieden. Da

$$s_t^{m+qz} \eta_t = s_t^m \eta_t$$

für jede ganze rationale Zahl z gilt, ist es für die Wirkung auf die q — gliedrigen Perioden bequemer, die Substitution S_t von der Primzahlordnung q einzuführen, für welche

$$S_t^m \eta_t = s_t^{m+qz} \eta_t = s_t^m \eta_t , \quad m = 0, 1, 2, \ldots, q-1$$

ist. Dabei soll S_t aber die Grösse η_j mit $j \neq t$ festlassen.

Der Körper $k_0 (\eta_t)$ ist absolut Galois'sch, die Grössen $S_t^m \eta_t$, wo $m = 0, 1, 2, \ldots, q-1$, bilden eine Basis für die ganzen Zahlen des Körpers, und

$$\sum_{m=0}^{q-1} S_t^m \eta_t = -1 . \tag{1}$$

Die (absolute) Differente der Zahl ζ_t ist ein Teiler von $p_t^{p_t-2}$. Mithin ist auch die (absolute) Differente der Zahl η_t ein Teiler von $p_t^{p_t-2}$, also auch von $p_t^{p_t}$.

Es sei m eine beliebige ganze rationale Zahl, und wir betrachten die ganzen algebraischen Zahlen

$$\xi_m = \sum_{n=0}^{q-1} (S_1^{m+n} \eta_1 S_2^n \eta_2) . \tag{2}$$

Man erkennt sofort, dass für jede ganze rationale Zahl w

$$\xi_{m+qw} = \xi_m$$

ist, d.h. der Index mod. q genommen werden darf.

Ferner folgt aus (1) sofort, dass

$$\sum_{m=0}^{q-1} \xi_m = 1 \tag{3}$$

ist.

Die Zahlen ξ_m sind invariant unter den Substitutionen der Gruppe $\{S_1 \, S_2\}$, und für jede ganze rationale Zahl w ist

$$S_1{}^w \xi_m = \xi_{m+w}, \tag{4}$$

und daher auch

$$S_2^w \xi_m = (S_1 S_2)^w S_1^{-w} \xi_m = S_1^{-w} \xi_m = \xi_{m-w}. \tag{5}$$

Die Grössen

$$\xi_0, \xi_1, \xi_2, \ldots, \xi_{q-1} \tag{6}$$

sind gewiss alle voneinander verschieden. Denn nimmt man an, dass zwei von ihnen den gleichen Wert haben, so haben gemäss (4) oder (5) *alle* diesen gleichen Wert, und dieser müsste gemäss (3) gleich $\frac{1}{q}$, also nicht ganz sein. Ebenso erkennt man, dass keine der Zahlen (6) in k^* liegt.

Da unter jeder Substitution $S_1{}^m S_2{}^n$, wo m und n zwei beliebige ganze rationale Zahlen sind, die Grössen (6) nur untereinander permutiert werden, sind die symmetrischen Grundfunktionen der Grössen (6) ganz rational, und die Grössen (6) genügen einer Gleichung vom Grade q mit ganzen rationalen Zahlkoeffizienten, wobei der Koeffizient der höchsten Potenz gleich 1 ist. Diese Gleichung ist in k^* irreduzibel, da ihre Galoisgruppe $\mathfrak{G}$ — man kann für sie etwa $\{S_1\}$ oder $\{S_2\}$ nehmen — transitiv ist.

Der Körper $k = k^* (\xi_0)$ ist also vom Primzahlgrade q in bezug auf den Grundkörper k^*. Ferner ist er relativ Galois'sch, d.h.

$$k = k^* (\xi_0) = k^* (\xi_0, \xi_1, \xi_2, \ldots, \xi_{q-1}),$$

denn durch die Adjunktion von ξ_0 zu k^* wird die Galoisgruppe $\mathfrak{G}$ sicher reduziert. Aber $\mathfrak{G}$ hat nur die Identität als eigentliche Untergruppe.

Der Körper $K = k^* (\eta_1, \eta_2)$ hat in bezug auf k^* den Relativgrad q^2. Folglich ist K vom Relativgrad q in bezug auf $k = k^* (\xi_0)$. Es können also nicht beide Grössen η_1 und η_2 in k liegen. Aus Symmetriegründen liegen daher *beide* nicht in k. (Man könnte dies übrigens auch ersehen aus dem Gleichungssystem, das sich ergibt, wenn man die Formel (2) für die Werte $m = 0, 1, 2, \ldots, q-1$ hinschreibt.)

Daraus folgt aber sofort, dass die Erweiterung K ein Stück des Hilbert'schen Klassenkörpers von k ist. Denn die Relativdifferente $\mathfrak{D}_{K/k}$ von K in bezug auf k ist der grösste gemeinschaftliche Teiler der Relativdifferenten aller ganzen Zahlen von K in bezug auf k. Nun gilt für $t = 1$ und $t = 2$: Die Relativdifferente $\mathfrak{D}_{K/k}(\eta_t)$ von K in bezug auf k der Zahl η_t ist jedenfalls gleich einem Teiler der absoluten Differenten von η_t, also ein Teiler von $p_t^{p_t}$.

Mit der Grösse $\mathfrak{D}_{K/k}(\eta_t)$ liegt auch ihr Vielfaches $p_t^{p_t}$ in $\mathfrak{D}_{K/k}$. Da also $p_1^{p_1}$ und $p_2^{p_2}$ im Ideal $\mathfrak{D}_{K/k}$ liegen, ist

$$\mathfrak{D}_{K/k} = 1,$$

was zu beweisen war.

Ich möchte hier noch bemerken, dass die eben bewiesene Aussage schon enthalten ist in einem allgemeineren Satze, den ich bewiesen habe in der Arbeit: „Die Zetafunktion, die Klassenzahl und die Kronecker'sche Grenzformel eines beliebigen Kreiskörpers“, *Comment. Math. Helvet.*, vol. 1 (1929), pg. 160. Denn ich habe dort gezeigt, dass wenn U ein beliebiger Nicht — Ausgangskreiskörper ist, und K der kleinste Ausgangskreiskörper ist, der U enthält, die Relativdifferente von K in bezug auf U gleich 1 ist (vgl. 1.c., pg. 220).

Dass für den Grundkörper k^* *unendlich viele* Erweiterungskörper k vom Relativgrade q mit einer durch q teilbaren Klassenzahl existieren, ist evident. Denn hat man schon s solche Körper, etwa $k_1, k_2, \ldots, k_s$ — für $s = 1$ ist dies ja der Fall — so braucht man für die Konstruktion eines weiteren Körpers k_{s+1} die beiden voneinander verschiedenen ungeraden Primzahlen $p_1{}^{(s+1)}$ und $p_2{}^{(s+1)}$ nur so zu wählen, dass sie $\equiv 1$ (mod. q) und zu den Diskriminanten der Körper $k_1, k_2, \ldots, k_s$ teilerfremd sind.

Wir gehen über zum Fall $q = 2$.

Ist P eine Primzahl, die $\equiv 1$ (mod. 4) ist, oder das Produkt von lauter voneinander verschiedenen Primzahlen, die alle $\equiv 1$ (mod. 4) sind, so ist die (absolute) Differente der ganzen algebraischen Zahl

$$\tfrac{1}{2}(-1+\sqrt{P})$$

gleich $\sqrt{P}$.

Sind p_1 und p_2 zwei voneinander verschiedene Primzahlen, die $\equiv 1$ (mod. 4) und zur Diskriminanten von k^* teilerfremd sind, und nimmt man an Stelle von ξ_0, η_1, η_2 beziehungsweise

$$\tfrac{1}{2}(-1+\sqrt{p_1 p_2}), \qquad \tfrac{1}{2}(-1+\sqrt{p_1}), \qquad \tfrac{1}{2}(-1+\sqrt{p_2}),$$

so erkennt man wie oben, dass für $K = k^*(\sqrt{p_1}, \sqrt{p_2})$ und $k = k^*(\sqrt{p_1 p_2})$ die Relativdifferente $\mathfrak{D}_{K/k} = 1$ ist.

Dass für den Grundkörper k^* *unendlich viele* relativquadratische Erweiterungskörper k mit gerader Klassenzahl existieren, erkennt man ebenfalls wie oben.

Denn hat man schon s solche Körper, etwa $k_1, k_2, \ldots, k_s$ — für $s = 1$ ist dies ja der Fall — so braucht man für die Konstruktion eines weiteren Körpers k_{s+1} die beiden voneinander verschiedenen Primzahlen $p_1^{(s+1)}$ und $p_2^{(s+1)}$ nur so zu wählen, dass sie $\equiv 1 \pmod{4}$ und zu den Diskriminanten der Körper $k_1, k_2, \ldots, k_s$ teilerfremd sind.

(Reçu le 20 décembre 1972)

Max Gut
Glärnischstr. 14
8704 Herrliberg ZH