Über affektlose Gleichungen.

Von *Ph. Vassiliou* in Saloniki.

---

1. Eine kürzlich erschienene Arbeit von van der Waerden [1]), betreffend die Zerlegungs- und die Trägheitsgruppe eines Primideals im Galoisschen Wurzelkörper einer algebraischen Gleichung, erlaubt es uns, einige ältere Sätze über affektlose Gleichungen, sowie manche neue Konstruktion solcher Gleichungen, in überaus einfacher Weise zu erhalten.

Der in der genannten Arbeit von van der Waerden aufgestellte Hauptsatz stellt eine Verallgemeinerung eines bekannten Satzes von Artin [2]) dar; er vermittelt auch für den Fall eines Diskriminantenteilers den Zusammenhang, der zwischen der Primidealzerlegung in einem algebraischen Körper und den Zerlegungs- und Trägheitssubstitutionen der zugehörigen Galoisschen Gruppe besteht. Zu seiner Formulierung gehen wir gleich über.

2. Es seien $x_1, \ldots, x_n$ die voneinander verschiedenen Wurzeln einer algebraischen Gleichung $F(x) = 0$ im Grundkörper P (einem Zahl- oder Funktionenkörper), Ω der zugehörige Galoissche Wurzelkörper $\mathsf{P}(x_1, \ldots, x_n)$. Die Galoissche Gruppe von $F(x) = 0$ ist eine Gruppe von Permutationen dieser Wurzeln. Außerdem zerfalle im Körper $\mathsf{P}(x_1)$ das Primideal p des Grundkörpers P folgendermaßen:

$$p = \mathfrak{p}_{f_1}^{e_1} \mathfrak{p}_{f_2}^{e_2} \cdots \mathfrak{p}_{f_\varrho}^{e_\varrho},$$

also in ϱ verschiedene Primideale $\mathfrak{p}_{f_j}$ von den Graden f_j und den Exponenten e_j.

Für die Zerlegungsgruppe $\mathfrak{Z}$ und die Trägheitsgruppe $\mathfrak{T}$ (betrachtet als Permutationsgruppen) eines Primteilers $\mathfrak{P}$ von p in Ω sagt dann der genannte Satz folgendes aus:

Hilfssatz 1. *Die Wurzeln $x_1, \ldots, x_n$ zerfallen gegenüber $\mathfrak{Z}$ in ϱ Transitivitätsgebiete zu je $e_j f_j$ Wurzeln und gegenüber $\mathfrak{T}$ in f_j Transitivitätsgebiete zu je e_j Wurzeln.*

3. Wir beschränken uns jetzt auf den Fall des rationalen Grundkörpers R und nehmen an,

$$(1) \qquad F(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

sei in R irreduzibel (die a_i gewöhnliche ganze Zahlen).

Wir machen ferner die Voraussetzungen, daß für die Primzahl p eine Kongruenz der Form:

$$(2) \qquad F(x) \equiv x^h f(x) \pmod{p}$$

---

[1]) B. L. van der Waerden, Die Zerlegungs- und die Trägheitsgruppe als Permutationsgruppen, Math. Annalen **111** (1935), 731.

[2]) E. Artin, Über die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann. **89** (1923), oder H. Hasse, Zahlbericht, Teil II, Jahresbericht D. M.-V., Ergänzungsband VI (1930), 126.

mit $h > 1$ besteht, und daß die Diskriminante Δ_1 des Polynoms $f(x)$ zu p teilerfremd ist. Letzteres bedingt, daß in der Primfunktionzerlegung von $f(x)$ mod. p alle Primfunktionen in der ersten Potenz aufgehen.

Es bezeichne weiter Δ die Diskriminante von $F(x)$, D die Diskriminante des Körpers $R(x_1)$ und d den sogenannten Index der Zahl x_1; die Relation, welche diese drei Zahlen verbindet, lautet bekanntlich

$$\Delta = d^2 D.$$

Wir wenden nun ein Kriterium von Dedekind an [3]), das uns erlaubt zu entscheiden, ob die Primzahl p ein Teiler des Index d ist, und das folgenden Wortlaut hat:

Hilfssatz 2. *Ist*

$$F(x) = f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_\varrho(x)^{e_\varrho} + p\, M(x)$$

($f_j(x)$ die verschiedenen Primfunktionen von $F(x)$ in der Zerlegung mod. p), *so ist die Primzahl p dann und nur dann ein Teiler des Index, wenn das Polynom $M(x)$* mod. p *durch eine der Primfunktionen $f_j(x)$ mit $e_j > 1$ teilbar ist.*

Infolge der angenommenen Voraussetzung $(\Delta_1, p) = 1$ und wegen dieses Satzes von Dedekind ist p kein Teiler von d, sobald a_n, welches gemäß (2) ja $\equiv 0 \pmod{p}$ ist, $\not\equiv 0 \pmod{p^2}$ ist. Setzt man also $\mathfrak{p}_1 = (p, x_1)$, so ist $\mathfrak{p}_1$ Primideal ersten Grades des Körpers $R(x_1)$, und die Primzahl p zerfällt im Körper $R(x_1)$ folgendermaßen:

$$p = \mathfrak{p}_1^h \mathfrak{p}_{f_2} \cdots \mathfrak{p}_{f_\nu} \ ^{4)},$$

also derart, daß nur das Primideal $\mathfrak{p}_1$ in einer höheren als der ersten Potenz aufgeht.

Wenn nun $(h, p) = 1$ wäre, so wäre die Diskriminante D höchstens durch die $(h - 1)$-te Potenz der Primzahl p teilbar [5]). Nehmen wir also weiter an, daß die Primzahl p mindestens in der n-ten Potenz in der Diskriminante Δ von $F(x)$ aufgeht, was wegen $(d, p) = 1$ gleichbedeutend damit ist, daß D mindestens die n-te Potenz von p enthält, so müssen wir den Schluß ziehen, daß h durch p teilbar ist.

Nach dem unter 2 formulierten Satze von van der Waerden, nämlich wegen der darin behaupteten Transitivität der Trägheitsgruppe $\mathfrak{T}$ als Gruppe von h Wurzeln, ist die Ordnung der Galoisschen Gruppe unserer Gleichung (1) durch h und folglich dann durch p teilbar.

Zusammenfassend haben wir damit folgenden Satz von I. Schur [6]):

Satz 1. *Hat man eine im Körper der rationalen Zahlen irreduzible ganzzahlige Gleichung* (1) *vom Grade n, deren Diskriminante die Primzahl p mindestens in der n-ten Potenz enthält, und bei der das konstante Glied a_n durch p, aber nicht durch p^2 teilbar ist, besteht ferner eine Kongruenz der Form* (2), *wo $h > 1$ und die Diskriminante des Polynoms $f(x)$ zu p teilerfremd ist, so besitzt die Galoissche Gruppe der Gleichung eine durch p teilbare Ordnung.*

4. Genau von denselben Schlüssen ausgehend, kann man, unter Heranziehung von bekannten Sätzen über Permutationsgruppen, ebenso leicht verschiedene Klassen von affektlosen Gleichungen oder solchen mit alternierender Gruppe angeben.

Dazu benötigen wir noch den

---

[3]) R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Göttinger Abhandlungen 1878, § 3.

[4]) Siehe Weber-Fricke, Algebra III, 57.

[5]) Siehe Weber-Fricke, l. c. 119.

[6]) I. Schur, Gleichungen ohne Affekt, Sitz.Berichte Akad. Berlin 1930, 443—449.

Hilfssatz 3. *Sind in der Primidealzerlegung*

$$p = \mathfrak{p}_{f_1}^{e_1} \cdots \mathfrak{p}_{f_\varrho}^{e_\varrho}$$

alle Exponenten zu p teilerfremd, so ist die Verzweigungsgruppe von $\mathfrak{P}$ in Ω gleich der Einheit.

Zum Beweise dieser Tatsache verweisen wir auf einen kürzlich erschienenen Aufsatz von U. Wegner [7]).

5. Wir sind jetzt in der Lage, folgenden Satz zu beweisen:

Satz 2. *Hat man eine im Körper der rationalen Zahlen irreduzible ganzzahlige Gleichung* (1) *ungeraden Grades n, sind alle Koeffizienten a_i außer dem ersten a_1 durch eine Primzahl $p > n$ teilbar, insbesondere der letzte genau durch p^1, sind ferner für eine von p verschiedene Primzahl $q > n$ alle Koeffizienten außer den beiden ersten a_1, a_2 durch q^2 teilbar, insbesondere der letzte genau durch q^1, und ist $a_1^2 - 4a_2 \equiv 0$ (mod. q^2), so besitzt die Gleichung* (1) *die symmetrische Gruppe als Galoissche Gruppe.*

Beweis. Wegen der angenommenen Teilbarkeit der Koeffizienten durch p besteht die Kongruenz

$$F(x) \equiv x^{n-1}(x + a_1) \quad (\text{mod. } p),$$

und p ist nach Hilfssatz 2 kein Indexteiler. Folglich zerfällt p im Körper $R(x_1)$ folgendermaßen:

$$p = \mathfrak{p}_1^{n-1}\mathfrak{p}_1', \tag{3}$$

wo

$$\mathfrak{p}_1 = (p, x_1), \quad \mathfrak{p}_1' = (p, x_1 + a_1),$$

und die voneinander verschiedenen Primideale $\mathfrak{p}_1$, $\mathfrak{p}_1'$ sind beide vom ersten Grad. Gemäß der Voraussetzung $p > n$ sind die Exponenten in der Zerlegung (3) zu p teilerfremd; folglich ist nach Hilfssatz 3 die Verzweigungsgruppe eines Primteilers $\mathfrak{P}$ von p in Ω gleich der Einheit, und nach Hilfssatz 1 enthält die Galoissche Gruppe von $F(x)$ einen $(n-1)$-gliedrigen Zyklus.

Ebenso folgt aus den Voraussetzungen des Satzes über q, daß die Zerlegung von q im Körper $R(x_1)$ folgendermaßen lautet:

$$q = \mathfrak{q}_1^{n-2}\mathfrak{q}_1'^2,$$

und daß q nach Hilfssatz 2 kein Indexteiler ist. Nach Hilfssatz 3 und 1 folgt dann wieder die Existenz des Produktes eines $(n-2)$-gliedrigen und eines zweigliedrigen Zyklus, also weil n ungerade ist, die Existenz eines zweigliedrigen Zyklus in der Galoisschen Gruppe von $F(x)$.

Da $F(x)$ als irreduzibel angenommen ist, so ist die Galoissche Gruppe transitiv, und weil sie einen $(n-1)$-gliedrigen und einen zweigliedrigen Zyklus enthält, ist sie die symmetrische Gruppe [8]).

6. Gleichungen mit den obigen Voraussetzungen kann man ersichtlich sehr leicht explizit angeben, wie das z. B. von O. Perron [9]) geschieht.

Was die Irreduzibilität des Polynoms $F(x)$ in der obigen Konstruktion betrifft, so können wir uns am einfachsten des Eisensteinschen Kriteriums bedienen, wie das bei Perron der Fall ist, oder die folgende Modifikation anwenden:

---

[7]) U. Wegner, Zur Theorie der affektlosen Gleichungen, Math. Ann. **111** (1935), 738.

[8]) Siehe z. B. B. L. van der Waerden, Moderne Algebra I, 191.

[9]) O. Perron, Algebra II, 2. Aufl., 220, Satz 111.

$F(x)$ vom Grade $n = p^\alpha$ (p Primzahl) ist irreduzibel, wenn alle Koeffizienten bis auf den letzten a_n durch p teilbar sind und

$$F(-a_n) \not\equiv 0 \pmod{p^2}$$

ist.

Beweis. Wenn $F(x)$ reduzibel wäre, so sei $F(x) = \varphi(x) \cdot \psi(x)$, wo $\varphi(x)$, $\psi(x)$ mindestens vom ersten Grade sind und nach dem Gaußschen Lemma ganze rationale Koeffizienten haben.

Nun ist aber

$$F(x) = \varphi(x)\,\psi(x) \equiv x^n + a_n \equiv (x + a_n)^n \quad (\mathrm{mod.}\ p),$$

also wegen der Eindeutigkeit der Zerlegung mod. p

$$\varphi(x) \equiv (x + a_n)^\varrho \quad (\mathrm{mod.}\ p)$$
$$\psi(x) \equiv (x + a_n)^\sigma \quad (\mathrm{mod.}\ p),$$

mit $\varrho, \sigma \geqq 1$, $\varrho + \sigma = n$, d. h.

$$\varphi(-a_n) \equiv 0, \qquad \psi(-a_n) \equiv 0 \quad (\mathrm{mod.}\ p),$$

und somit

$$F(-a_n) = \varphi(-a_n)\,\psi(-a_n) \equiv 0 \quad (\mathrm{mod.}\ p^2),$$

gegen die Voraussetzung.

Derselbe Beweis überträgt sich ohne weiteres auf den Fall eines beliebigen Grundkörpers P statt R.

Eingegangen 3. Mai 1936.