DIE ZERLEGUNG VON PRIMZAHLEN IN ALGEBRAISCHEN ZAHLKÖRPERN*

VON

ANDREAS SPEISER

In den folgenden Zeilen wird gezeigt, dass das Problem der Zerlegung einer Primzahl in einem algebraischen Körper identisch ist mit einem Problem der Theorie der linearen Substitutionen in einem Galois-Feld,† das folgendermassen formuliert werden kann:

Gegeben ist eine ganzzahlige quadratische Matrix M. Nimmt man die Reste modulo einer Primzahl p, so erhält man die Matrix einer linearen Substitution in einem $GF(p)$. Ihre Ordnung hat die Gestalt $p^s u$, wobei u prim ist zu p und eine gewisse Zahl $p^f - 1$ teilt. Hier ist f von der Gestalt $f = n_1 n_2 \ldots n_r$, wobei $n_1 + n_2 + \cdots + n_r \leqq n$ und n ist der Grad der Substitution. Wir nennen die niedrigste Zahl f, für welche $p^f - 1 \equiv 0 \pmod{u}$, die *Exponentialzahl* von M mod p und zeigen in § 1, dass sie den *Grad* der in p aufgehenden Primideale darstellt für denjenigen algebraischen Zahlkörper, der durch die Wurzeln der characteristischen Gleichung dieser Matrix bestimmt ist. Hierbei müssen die Primteiler der Discriminante dieser Gleichung ausgenommen werden, deren Untersuchung in dieser Arbeit nicht durchgeführt werden soll, da sie weitere Hilfsmittel erfordert. In § 2 werden die bekannten Criterien für die Zerlegung in zyklischen und relativ-zyklischen Körpern hergeleitet. Hierbei tritt klar zutage, dass das Zerlegungsproblem für den Fall von Körpern, die nicht durch Wurzelzeichen herstellbar sind, mit den bisher benutzten Methoden nicht mehr zu behandeln ist. Damit man aber wenigstens in der Lage ist, für die niedrigsten Primzahlen den Grad zu bestimmen, so wird in §3 eine rekurrente Reihe benutzt, welche wohl schon öfters in der Literatur aufgetreten ist, ohne dass ihre enge Beziehung zum Zerlegungsproblem bisher erkannt worden wäre.

1. Die Zerlegung von Primzahlen in Zahlkörpern

Gegeben sei die Gleichung:

$$x^n - (a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n) = 0$$

mit ganzen rationalen Koeffizienten. Wir fragen nach der Zerlegung der Primzahl p in dem durch die Wurzeln dieser Gleichung erzeugten Galois' schen Körper.

* Presented to the Society, April 14, 1922.

† L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig, 1901.

Wenn ein Primidealteiler $\mathfrak{p}$ von p vom Grade f ist, so bilden bekanntlich die Reste mod $\mathfrak{p}$ ein $GF(p^f)$. Es gilt nun der

SATZ 1. *$GF(p^f)$ ist das GF mit niedrigstem Exponenten f, in welchem bei gegebenem p die linke Seite der Gleichung in ihre Linearfaktoren zerfällt. Hierbei muss p prim sein zur Diskriminante der Gleichung.*

Beweis: Zunächst ist klar, dass die Funktion im $GF(p^f)$ in ihre Linearfaktoren zerfällt, denn jede der Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ gibt mod $\mathfrak{p}$ ein bestimmtes Element des $GF(p^f)$. Es muss also nur noch gezeigt werden, dass diese Zerlegung in keinem GF mit niedrigerem Exponenten, der übrigens ein Teiler von f sein müsste, möglich ist. Angenommen nämlich, sie sei bereits im $GF(p^{f_1})$ möglich, so müssten die Reste der Wurzeln $\alpha_1, \alpha_2, \cdots, \alpha_n$ mod $\mathfrak{p}$ wegen des Satzes von der eindeutigen Zerlegung der Funktionen in einem GF, durch Addition, Subtraktion und Multiplikation gerade das $GF(p^{f_1})$ erzeugen. Nun entsteht aber durch die genannten drei Operationen aus den Wurzeln selbst ein Ring, dessen Diskriminante nur diejenigen Primteiler enthält, die bereits in der Diskriminante der Gleichung aufgehen. Die Basis des Ringes geht daher aus einer Körperbasis durch eine Substitution hervor, deren Determinante auch nur solche Primteiler enthält, und infolgedessen zu p prim ist. Hieraus folgt ohne weiteres, dass das Restesystem mod $\mathfrak{p}$ im Körper und im Ring identisch ist, d. h. dass $f_1 = f$.

SATZ 2. *Es sei u die niedrigste ganze positive Zahl, für welche die n Gleichungen gelten: $\alpha_i^u \equiv 1$ oder $0 \pmod{\mathfrak{p}}$ und f die kleinste Zahl, für welche $p^f \equiv 1 \pmod{u}$, dann ist f der Grad von $\mathfrak{p}$.*

Beweis: Ist f der Grad von $\mathfrak{p}$, so bilden die zu p primen Reste eine zyklische Gruppe von der Ordnung $p^f - 1$. Wenn nun die Zahl u bereits einer Kongruenz mit niedrigerem Exponenten genügte, der alsdann bekanntlich ein Teiler von f wäre, so würden die Reste der Wurzeln mod $\mathfrak{p}$ nicht das ganze $GF(p^f)$ erzeugen, was dem Satz 1 widerspricht.

SATZ 3. *Ist (a_i^{ν}) $(i, k = 1, 2, \cdots, n)$ eine ganzzahlige Matrix und ist f ihre Exponentialzahl* mod p *(vgl. die Einleitung), so zerfällt p in dem durch die Wurzeln der characteristischen Gleichung gebildeten Galois'schen Körper in Primideale vom Grade f. Immer sind ausgenommen die Teiler der Diskriminante der Gleichung.*

Beweis: Setzt man die Matrix (a_{ik}) h-mal mit sich selbst zusammen, so sind die Wurzeln der charakteristischen Gleichung die h-ten Potenzen von $\alpha_1, \alpha_2, \ldots, \alpha_n$. Bildet man daher insbesondere die $(p^f - 1)$-ste Potenz, so sind die Wurzeln der so entstehenden Matrix $\equiv 0$ oder $1 \pmod{\mathfrak{p}}$. Die Ordnung einer solchen Matrix ist aber mod p immer gleich einer Potenz von p. Da die auftretenden Matrizen sämtlich ganze rationale Koeffizienten besitzen, so darf man den Modul $\mathfrak{p}$ durch p ersetzen.

Die Einschränkung, der die Moduln p unterliegen, kann dadurch aufgehoben werden, dass an die Stelle einer beliebigen Gleichung die Fundamentalgleichung

des Körpers gesetzt wird. Ferner ist zu bemerken, dass die Gleichung nicht als irreduzibel vorausgesetzt werden muss, was sich z. B. bei den Kreiskörpern vorteilhaft bemerkbar macht.

Jede Gleichung $x^n = a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ ist charakteristische Gleichung einer Matrix, nämlich der folgenden:

$$\left\|\begin{array}{l} 0, 0, 0, \ldots, 0, a_n \\ 1, 0, 0, \ldots, 0, a_{n-1} \\ 0, 1, 0, \ldots, 0, a_{n-2} \\ 0, 0, 1, \ldots, 0, a_{n-3} \\ \ldots\ldots\ldots\ldots\ldots \\ 0, 0, 0, \ldots\ldots, a_1 \end{array}\right\| = M$$

und in dieser Gestalt werden wir das Kriterium des Satzes im folgenden benutzen.

2. Die Kriterien für die Kreiskörper und die relativ-zyklischen Körper

1. **Kreiskörper.** Die Gleichung lautet hier:

$$x^n = 1,$$

wobei n irgend eine ganze positive Zahl bedeutet. Bildet man die zugehörige Matrix, so findet man, dass ihre Ordnung modulo jeder Primzahl gleich n ist, denn sie ist gleichbedeutend mit einer zyklischen Permutation. Ist daher p kein Teiler von n, so folgt das bekannte Kriterium:

Der Grad f eines Primteilers von p im Körper der n-ten Einheitswurzeln ist gleich dem Exponenten der niedrigsten Potenz von p, welche der Gleichung genügt:

$$p^f \equiv 1 \pmod{n}.$$

2. **Reine Gleichungen.** Gegeben ist die Gleichung:

$$x^l = a,$$

wobei l eine Primzahl bedeutet und a keine l-te Potenz einer rationalen Zahl ist. Wenn $a \pmod{p}$ zum Exponenten q gehört: $a^q \equiv 1 \pmod{p}$, so wird $u = l \cdot q$. Die Primteiler von p sind dann und nur dann vom ersten Grad, wenn $p \equiv 1 \pmod{lq}$, d. h. wenn die Gleichung $x^l \equiv a \pmod{p}$ lösbar ist. In diesem Fall sagt man: *a ist l-ter Potenzrest* mod p.

Ferner gilt der

Satz 4. *Der Grad f der Primidealteiler von p in einem aus zwei Galois'schen Körpern zusammengesetzten Körper ist gleich dem kleinsten gemeinschaftlichen Vielfachen der entsprechenden Grade in den beiden Teilkörpern.*

Beweis: In dem $GF(p^f)$ werden die Fundamentalgleichungen beider Teilkörper zerlegbar in ihre Linearfaktoren. Ausgenommen sind auch hier die Diskriminantenteiler.

Die bisherigen Ueberlegungen lassen sich ohne wesentliche Aenderungen auf Gleichungen in einem beliebigen algebraischen Grundkörper k übertragen. Ist $\mathfrak{p}$ ein Primideal vom Grade f_1, so ergibt die Gleichung mod $\mathfrak{p}$ eine Matrix im $GF(p^{f_1})$. Ist f ihre Exponentialzahl, so zerfällt $\mathfrak{p}$ in dem durch die Wurzeln der Gleichung bestimmten relativ zu k Galois'schen Zahlkörper in Primideale vom absoluten Grade f.

3. **Die relativ zyklischen Zahlkörper.** Gegeben ist ein Zahlkörper k und eine Gleichung $x^l = \alpha$, wobei α in k liegt und keine l-te Potenz einer Zahl aus k ist. Der durch diese Gleichung bestimmte Zahlkörper enthält den Körper der l-ten Einheitswurzeln. Adjungiert man diesen zu k, so reduziert sich die Gruppe der Gleichung auf die zyklische Gruppe von der Ordnung l. Ist nun $\mathfrak{p}_1$ ein Primideal in k, so wird seine Zerlegung nach Adjunktion des Kreiskörpers durch den Satz 4 bestimmt. $\mathfrak{p}$ sei ein Primteiler von $\mathfrak{p}_1$. Die Zerlegung von $\mathfrak{p}$ im vollen Körper erfolgt nun genau nach 2 und es gilt der Satz:

SATZ 5. *Das Primideal $\mathfrak{p}$ zerfällt in l Faktoren oder es bleibt Primideal, je nachdem α l-ter Potenzrest ist* (mod $\mathfrak{p}$) *oder nicht im Körper, dem $\mathfrak{p}$ angehört.*

Hiermit sind die bisher bekannten Regeln für die Zerlegung von Zahlen resp. Idealen in Zahlkörpern, abgesehen von den Diskriminantenteilern, hergeleitet. Man sieht, dass sie nur für auflösbare Körper resp. Relativkörper gelten, infolge der besonders einfachen Gestalt der zugehörigen Matrix, die eine monomiale wird. Nimmt man allgemeinere Gleichungen, etwa die im nächsten Paragraphen zu besprechende Gleichung: $x^5 = x + 1$, so gelangt man auf Matrizen, für die eine ähnlich einfache Regel zur Bestimmung der Exponentialzahl nicht mehr zu erwarten ist, und es muss die Frage noch offen gelassen werden, ob überhaupt ein einfaches Zerlegungsgesetz existiert oder ob die bisherige Formulierung das Schlussresultat darstellt. Jedenfalls ist die Zurückführung auf Matrizen in Diagonalform, d. h. auf die Lehre von den Potenzresten nur im Falle auflösbarer Körper möglich, genau wie auch nur in diesem Fall das algebraische Gleichungsproblem auf ein Formenproblem l-ten Grades reduzierbar ist.*

---

* Als Literatur über diese Fragen seien folgende Abhandlungen angemerkt:

D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 4, S. 189, S. 333 und S. 398; *Ueber die Theorie der relativ-abelschen Zahlkörper*, Göttinger Nachrichten, 1898, S. 370–399.

Ueber den Zusammenhang mit den Reziprozitätsgesetzen vgl. R. Fueter, *Die Klassenkörper der komplexen Multiplikation und ihr Einfluss auf die Entwicklung der Zahlentheorie*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 20.

3. Ein Algorithmus zur Berechnung des Grades eines Primideales

Da sich im allgemeinen Fall kein einfaches Gesetz für den Grad eines Primideales angeben lässt, so ist es von Wichtigkeit, ein Verfahren zu kennen, das wenigstens für kleine Primzahlen zum Ziele führt, ohne allzuweitläufige Rechnungen. Es sei wiederum die Gleichung gegeben:

$$x^n = a_1 x^{n-1} + \cdots + a_n.$$

Wir betrachten diejenigen Primzahlen, welche zur Diskriminante sowie zu a_n prim sind. Aus den Koeffizienten dieser Gleichung kann man eine Rekursionsformel herleiten, welche aus der Entwicklung des reziproken Wertes von $x^n - a_1 x^{n-1} - \cdots - a_n$ in eine Potenzreihe bekannt ist. Hiernach bildet man aus n aufeinanderfolgenden Zahlen $y_1, y_2, \ldots, y_n$ die nächstfolgende durch die Formel

$$y_{n+1} = a_n y_1 + a_{n-1} y_2 + \cdots + a_1 y_n.$$

Die ersten n Zahlen können beliebig gewählt werden. Wir wählen sie aber in bestimmter Weise, indem wir setzen: $y_1 = 0$, $y_2 = 0$, $\ldots$, $y_{n-1} = 0$, $y_n = 1$. Indem man die Rekursionsformel successive anwendet, erhält man eine unbegrenzte Reihe ganzer Zahlen. Diese Zahlen reduziere man mod p. Sie wird alsdann zu einer periodischen Reihe der Reste und wir bezeichnen die Anzahl der Terme in einer Periode mit u, alsdann gilt der

Satz 6. *Der Grad der in p aufgehenden Primideale ist die kleinste Zahl f, für welche die Kongruenz gilt:* $p^f \equiv 1 \pmod{u}$.

Bevor wir diesen Satz beweisen, sei ein Beispiel dafür gegeben. Wir wählen die Gleichung: $x^5 = x + 1$. Ihre Diskriminante ist $2869 = 19 \cdot 151$. Als Primzahl nehmen wir 2. Man findet sofort folgende Reihe:

$$0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, \ldots$$

und es erweist sich sonach $u = 21$, und also $f = 6$. Für $p = 3$ findet man: $u = 121$ und also $f = 5$, da $3^5 = 243$. Aus diesen beiden Resultaten folgt übrigens, dass die Gruppe der Gleichung die symmetrische von der Ordnung 120 ist, denn man zeigt in der Zahlentheorie, dass der Grad eines Primideales gleich der Ordnung einer zyklischen Untergruppe der Körpergruppe ist. Nun ist offenbar die symmetrische Gruppe die einzige Permutationsgruppe von 5 Variablen, welche Substitutionen von der Ordnung 5 und 6 enthält.

Um den Satz 6 zu beweisen, stellen wir folgende Ueberlegungen an: Reduziert man die Gleichung mod p, so zerfällt sie in einem gewissen $GF(p^f)$ in ihre Linearfaktoren. Ihre Wurzeln sind wegen unserer Voraussetzung über p unter einander und von 0 verschieden. Daher lässt sich ihre Matrix M (vergl. § 1 am Ende) auf die Diagonalform bringen im $GF(p^f)$. Hieraus folgt, dass die

Ordnung von $M \pmod p$ ein Teiler von $p^f - 1$ ist. f ist der Grad der in p aufgehenden Primideale. Nun gehen wir über zu der rekurrenten Reihe $y_1, y_2, \ldots$ und betrachten irgendwelche $2n - 1$ aufeinanderfolgende Glieder: $y_{i+1}, y_{i+2}, \ldots, y_{i+2n-1}$. Aus diesen bilden wir die folgende (Hankelsche) Matrix:

$$M_i = \left|\left| \begin{matrix} y_{i+1} & y_{i+2} & \cdots & y_{i+n} \\ y_{i+2} & y_{i+3} & \cdots & y_{i+n+1} \\ \cdots & \cdots & \cdots & \cdots \\ y_{i+n} & y_{i+n+1} & \cdots & y_{i+2n-1} \end{matrix} \right|\right|.$$

Diese Matrizen genügen folgender Gleichung: $M_i M = M_{i+1}$, wobei Zeilen mit Kolonnen zusammenzusetzen sind. Aus der besonderen Wahl von $y_1, \ldots, y_n$ folgt, dass die Determinante von M_0 gleich ± 1 ist. Da diejenige von M gleich a_n wird, so sind die Determinanten sämtlicher Matrizen $M_i \not\equiv 0 \pmod p$. Wenn nun die rekurrente Reihe mod p periodisch mit u Gliedern ist, so wird $M_u \equiv M_0$ und also $M_0 M^u \equiv M_0$. Hier kann man mit M_0 kürzen und man findet: $M^u \equiv E$, wo E die Einheitsmatrix darstellt. Umgekehrt folgt aus $M^u \equiv E$, dass die Reihe eine Periode von u Gliedern aufweist. Die Anzahl u der Glieder in einer Periode ist also gleich der Ordnung der Matrix $M \pmod p$, und hieraus folgt die Giltigkeit des Satzes 6.

Durch diesen Satz ist gleichzeitig die zahlentheoretische Natur der rekurrenten Reihen vollständig aufgeklärt. Man sieht, dass auch dieses Problem identisch ist mit der Frage nach dem Grad der in p aufgehenden Primideale in einem Galois'schen Zahlkörper. Was nun das Verhalten der Diskriminantenteiler betrifft, so ist zu bemerken, dass auch diese Untersuchung auf Probleme der Galois'schen Felder führt und Anlass zu interessanten Problemen der Gruppentheorie bietet.*

---

* Vgl. D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 4, S. 250 ff.

A. Speiser, *Die Zerlegungsgruppe*, Journal für Mathematik, Bd. 149, S. 174.

ZURICH,
SWITZERLAND