Über eine Anwendung der Idealtheorie auf die Frage nach der Irreduzibilität algebraischer Gleichungen.

Von

OSKAR PERRON in München.

Zur Entscheidung darüber, ob eine algebraische Gleichung mit numerisch gegebenen rationalen Koeffizienten im Bereich der rationalen Zahlen reduzibel oder irreduzibel ist, hat Kronecker eine allgemeine Methode angegeben, die allerdings in den meisten Fällen wegen der langen Rechnungen praktisch undurchführbar sein wird. Man kennt aber auch eine Reihe von Sätzen, nach welchen aus gewissen Eigenschaften der Koeffizienten, selbst ohne daß diese *numerisch* gegeben sind, auf die Irreduzibilität einer algebraischen Gleichung geschlossen werden kann. Das erste derartige Kriterium ist das bekannte von Eisenstein*) entdeckte, dem später Königsberger**) und Netto***) noch weitere ähnliche zur Seite stellten. Das zunächst sich darbietende und auch von allen Autoren befolgte Verfahren, um derartige Sätze zu beweisen, besteht darin, daß man eine probeweise Zerfällung der als irreduzibel vermuteten Gleichung vornimmt, und daraus einen Widerspruch mit den vorausgesetzten Eigenschaften der Koeffizienten konstruiert.

Mittels einer neuen hiervon gänzlich verschiedenen Methode will ich im folgenden weitere Sätze über die Irreduzibilität algebraischer Gleichungen aufstellen. Dabei werden nämlich gewisse rationale Primzahlen in einem der durch die gegebene Gleichung definierten algebraischen Körper in ihre idealen Faktoren zerlegt, und aus dieser Zerlegung lassen sich dann Schlüsse ziehen auf den Grad des betreffenden Körpers†). Auf diesem

*) Über die Irreduzibilität der Gleichung, von welcher die Teilung der ganzen Lemniskate abhängt. Journal f. Math. Bd. 39, Heft II.

**) Über den Eisensteinschen Satz etc. Journal f. Math. Bd. 115, und: Über die Entwicklungsform algebraischer Funktionen etc. Journal f. Math. Bd. 121.

***) Über die Irreduzibilität ganzzahliger ganzer Funktionen. Math. Ann. Bd. 48, auch „Vorles. über Algebra", Bd. I, 5. Vorles.

†) Das Verfahren ist in gewissem Sinne parallel (erfordert jedoch im allgemeinen weniger Aufwand an Rechnung) dem von Königsberger a. a. O. für algebraische

Weg hat schon Dedekind*) die Irreduzibilität der Kreisteilungsgleichung $\frac{x^p-1}{x-1}=0$, wo p eine Primzahl bedeutet, nachgewiesen, indem er zeigte, daß p im Körper der p^{ten} Einheitswurzeln die $(p-1)^{\text{te}}$ Potenz eines Primideals wird. Der Grad des Körpers ist daher mindestens $p-1$, also obige Gleichung gewiß irreduzibel. Die allgemeinere Verwendbarkeit der angedeuteten, fast ohne alle Rechnung auskommenden Methode scheint jedoch noch nicht erkannt zu sein. Aus der Idealtheorie werden dabei blos die Elemente vorausgesetzt; die hauptsächlich gebrauchten Sätze sind die beiden folgenden, deren Richtigkeit man ohne Schwierigkeit einsieht:

Hilfssatz I. Eine rationale Primzahl kann in einem algebraischen Körper n^{ten} Grades in höchstens n Faktoren zerfallen.

Hilfssatz II. Eine rationale Primzahl kann in einem algebraischen Körper nur dann die n^{te} Potenz eines Ideals sein, wenn der Grad des Körpers durch n teilbar ist.

§ 1.

Ich beginne damit, zunächst das von Eisenstein gefundene Irreduzibilitätskriterium nach meinen Prinzipien neu zu beweisen; dasselbe lautet:

Die algebraische Gleichung

$$x^n + pa_1x^{n-1} + pa_2x^{n-2} + \cdots + pa_n = 0, \tag{1}$$

*wo $a_1, a_2, \cdots, a_n$ beliebige ganze rationale Zahlen bedeuten, deren letzte durch die Primzahl p nicht teilbar ist, ist stets irreduzibel.***)

Beweis: Eine beliebige Wurzel γ der Gleichung (1) ist eine ganze algebraische Zahl, deren n^{te} Potenz wegen

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

durch p teilbar ist. Die Zahlen γ und p haben also in dem aus γ entspringenden Körper $k(\gamma)$ den idealen Faktor (γ, p) gemein, der von 1 verschieden ist.

Man hat des weiteren die Beziehung

$$\frac{\gamma^n}{p} = -\gamma(a_1\gamma^{n-2} + a_2\gamma^{n-3} + \cdots + a_{n-1}) - a_n;$$

Hier ist das erste Glied auf der rechten Seite durch γ, also auch durch

---

Funktionen eingeschlagenen Weg, wobei die Irreduzibilität aus dem Zusammenhang der Riemannschen Fläche erschlossen wird. Für algebraische *Zahlen* jedoch bedient sich auch Königsberger ausschließlich der Methode der probeweisen Zerfällung.

*) Dirichlets Vorlesungen über Zahlentheorie, 4. Auflage § 185.

**) Es ist offenbar, daß der Satz auch dann gilt, wenn der Koeffizient von x^n nicht 1, sondern eine beliebige zu p prime ganze Zahl a_0 ist. Denn wenn man $a_0x = y$ setzt, so erfüllen die Koeffizienten der Gleichung für y die Bedingungen des Satzes.

(γ, p) teilbar, das letzte Glied aber nach Voraussetzung prim zu p, also auch prim zu (γ, p). Daraus folgt, daß auch $\frac{\gamma^n}{p}$ prim ist zu (γ, p), da aber der Zähler γ^n offenbar durch $(\gamma, p)^n$ teilbar ist, so muß auch der Nenner p durch $(\gamma, p)^n$ teilbar sein. Andrerseits ist $(\gamma, p)^n = (\gamma^n, p^n)$ gewiß teilbar durch p, und folglich $p = (\gamma, p)^n$. Daraus schließt man nach Hilfssatz I oder II sofort, daß der Körper $k(\gamma)$ mindesten vom n^{ten} Grad ist; da aber γ auch wirklich einer Gleichung n^{ten} Grades genügt, so ist $k(\gamma)$ genau vom n^{ten} Grad, und folglich Gleichung (1) irreduzibel. Zugleich ergibt sich, daß (γ, p) in $k(\gamma)$ ein Primideal darstellt, was jedoch für die gegenwärtige Betrachtung unwesentlich ist.

Der gegebene Beweisgang schließt sich möglichst nahe an den von Dedekind a. a. O. für die Kreisteilungsgleichungen gegebenen an.*) Eine leichte Modifikation dieses Gedankengangs stellt sich in folgender Überlegung dar, die ich deshalb noch anfügen will, weil durch fast wörtlich entsprechende Schlüsse die Beweise der in den folgenden Paragraphen zu gebenden Erweiterungen des Eisensteinschen Satzes ihre präziseste Form erhalten.

Da p und γ nicht relativ prim sind, so sei $\mathfrak{p}$ ein sowohl in p als in γ aufgehendes Primideal des Körpers $k(\gamma)$, und es sei p genau durch $\mathfrak{p}^a$, γ genau durch $\mathfrak{p}^b$ teilbar. Dann ist

$$\begin{aligned} &\gamma^n \quad \text{genau durch } \mathfrak{p}^{bn}, \\ &pa_i\gamma^{n-1} \text{ mindestens durch } \mathfrak{p}^{a+b(n-i)}, \quad (i=1,2,3,\cdots,n-1) \\ &pa_n \text{ genau durch } \mathfrak{p}^a \end{aligned}$$

teilbar. In dem Ausdruck

$$\gamma^n + pa_1\gamma^{n-1} + \cdots + pa_n$$

ist also das zweite, dritte, $\cdots$, vorletzte Glied durch eine höhere Potenz von $\mathfrak{p}$ teilbar als das letzte. Da der Ausdruck aber verschwindet, also durch jede beliebige Potenz von $\mathfrak{p}$ teilbar ist, so müssen das erste und letzte Glied dieselbe Potenz von $\mathfrak{p}$ enthalten, d. h. es ist $a = bn$. Daher ist p teilbar durch $\mathfrak{p}^{bn}$, und daraus folgt wieder nach Hilfssatz I, und mit Rücksicht darauf, daß γ einer Gleichung n^{ten} Grades genügt, die Tatsache, daß $k(\gamma)$ vom n^{ten} Grad ist, w. z. b. w. Zugleich ergibt sich $b = 1$.

§ 2.

Durch $[\alpha]$ soll in der Folge stets, wie üblich, die in der reellen Zahl α enthaltene größte ganze Zahl bezeichnet werden.

Es läßt sich nun ganz entsprechend wie vorhin auch die folgende

*) Dort ist (γ, p) ein Hauptideal, wodurch der Beweis noch einfacher wird.

von Königsberger*) ohne vollständig durchgeführten Beweis angegebene Erweiterung des Eisensteinschen Satzes ableiten:

Theorem I. *Die algebraische Gleichung*

$$(2)\quad x^n + p^{\left[\frac{e}{n}\right]+1} a_1 x^{n-1} + p^{\left[\frac{2e}{n}\right]+1} a_2 x^{n-2} + \cdots + p^{\left[\frac{(n-1)e}{n}\right]+1} a_{n-1} x + p^e a_n = 0,$$

wo $a_1, \cdots, a_n$ *beliebige ganze rationale Zahlen bedeuten, deren letzte zur Primzahl* p *prim ist, ferner* e *irgend eine zu* n *prime Zahl, ist irreduzibel.*

Beweis: Ist γ eine Wurzel der Gleichung (2), so ist wieder ersichtlich, daß γ^n durch p teilbar ist, also γ und p einen von 1 verschiedenen idealen Faktor gemein haben. Es sei daher $\mathfrak{p}$ ein sowohl in p als in γ aufgehendes Primideal des Körpers $k(\gamma)$, und zwar sei p genau durch $\mathfrak{p}^a$, γ genau durch $\mathfrak{p}^b$ teilbar. Dann ist

$$\begin{aligned} &\gamma^n \text{ genau durch } \mathfrak{p}^{bn}, \\ &p^{\left[\frac{ie}{n}\right]+1} a_i \gamma^{n-i} \text{ mindestens durch } \mathfrak{p}^{a\left(\left[\frac{ie}{n}\right]+1\right)+b(n-i)}, \quad (i=1,2,\cdots,n-1) \\ &p^e a_n \text{ genau durch } \mathfrak{p}^{ae} \end{aligned}$$

teilbar. Hieraus läßt sich leicht schließen, daß $bn = ae$ ist.

In der Tat, wäre nämlich $bn > ae$, so würde hieraus folgen

$$a\left(\left[\frac{ie}{n}\right]+1\right) + b(n-i) > a\frac{ie}{n} + \frac{ae}{n}(n-i) = ae.$$

In dem Ausdruck

$$(3)\qquad \gamma^n + p^{\left[\frac{e}{n}\right]+1} a_1 \gamma^{n-1} + p^{\left[\frac{2e}{n}\right]+1} a_2 \gamma^{n-2} + \cdots + p^e a_n$$

wäre daher das letzte Glied genau durch $\mathfrak{p}^{ae}$ teilbar, alle andern aber durch eine höhere Potenz von $\mathfrak{p}$, was nicht möglich ist, da der Ausdruck verschwindet.

Wäre dagegen umgekehrt $ae > bn$, so folgte weiter

$$a\left(\left[\frac{ie}{n}\right]+1\right) + b(n-i) > a\frac{ie}{n} + b(n-i) > bn\frac{i}{n} + b(n-i) = bn.$$

In dem Ausdruck (3) wäre also jetzt das erste Glied nur durch $\mathfrak{p}^{bn}$ teilbar, und alle andern durch eine höhere Potenz von $\mathfrak{p}$, was wieder nicht möglich ist.

Man hat daher in der Tat $bn = ae$, und da n und e als teilerfremd vorausgesetzt sind, so folgt hieraus $a = rn$, $b = re$, wo r eine natürliche Zahl ist. Somit ist p teilbar durch $\mathfrak{p}^{rn}$, und also nach Hilfssatz I der Grad des Körpers $k(\gamma)$ mindestens gleich rn. Da aber γ einer Gleichung n^{ten} Grades genügt, so folgt wieder, daß $r = 1$, und der Grad von $k(\gamma)$ gleich n sein muß. Hierdurch ist die Irreduzibilität erwiesen.

*) Vergl. die erste der eingangs erwähnten Abhandlungen.

Für $e=1$ erhält man wieder den Eisensteinschen Satz. Die Schlüsse dieses Paragraphen lassen sich nicht mehr anwenden auf die Gleichung

$$x^n + p^{e_1} a_1 x^{n-1} + \cdots + p^{e_{n-1}} a_{n-1} x + p^e a_n = 0, \tag{4}$$

wo die e_i kleinere Werte haben als die oben angegebenen. Das ganze Verfahren beruht vielmehr darauf, daß für $x=\gamma$ die mittleren Glieder der linken Seite von (4) durch eine höhere Potenz von $\mathfrak{p}$ teilbar werden als die beiden äußeren. Sucht man nun die e_i so zu bestimmen, daß dies sicher eintritt, so findet man gerade $e_i = \left[\frac{ie}{n}\right]+1$. Ist $e_i < \left[\frac{ie}{n}\right]+1$, so kann die Gleichung in der Tat reduzibel sein.

Es mag noch bemerkt werden, daß nicht mehr wie in § 1 (γ, p) selbst ein Primideal ist in $k(\gamma)$, sondern es ist, wie man leicht sieht, $(\gamma, p) = \mathfrak{p}^e$ oder $\mathfrak{p}^n$, je nachdem $e<n$ oder $e>n$ ist.

§ 3.

Königsberger hat in seiner zuerst genannten Arbeit einen noch allgemeineren Satz aufgestellt, als den eben bewiesenen. Ich will jedoch gleich ein noch viel weiter gehendes Theorem angeben, das diesen, sowie die in § 1 und § 2 bewiesenen Sätze als Spezialfälle umfaßt:

Theorem II. *Die algebraische Gleichung*

$$x^n + p_1^{\left[\frac{e_1}{n}\right]+1} p_2^{\left[\frac{e_2}{n}\right]+1} \cdots p_k^{\left[\frac{e_k}{n}\right]+1} a_1 x^{n-1} + p_1^{\left[\frac{2e_1}{n}\right]+1} \cdots p_k^{\left[\frac{2e_k}{n}\right]+1} a_2 x^{n-2} + \cdots$$
$$+ p_1^{\left[\frac{(n-1)e_1}{n}\right]+1} \cdots p_k^{\left[\frac{(n-1)e_k}{n}\right]+1} a_{n-1} x + p_1^{e_1} \cdots p_k^{e_k} a_n = 0, \tag{5}$$

wo $a_1, \cdots, a_n$ beliebige ganze rationale Zahlen bedeuten, deren letzte zu den Primzahlen $p_1, p_2, \cdots, p_k$ prim ist, wo ferner die $k+1$ Zahlen $n, e_1, e_2, \cdots, e_k$ keinen gemeinsamen Teiler haben, ist irreduzibel.

Beweis: Ist wieder γ eine Wurzel der Gleichung (5), so ist γ^n durch p_1 teilbar; daher ist auch γ durch jedes in p_1 enthaltene Primideal des Körpers $k(\gamma)$ teilbar. Sei $\mathfrak{p}_1$ ein solches Primideal, und es sei p_1 genau durch $\mathfrak{p}_1^{a_1}$, γ genau durch $\mathfrak{p}_1^{b_1}$ teilbar; dann folgt durch wörtlich dieselbe Überlegung wie im vorigen Paragraphen, daß $b_1 n = a_1 e_1$ ist. Ist daher d_1 der größte Teiler von n und e_1, so muß $a_1 = r_1 \frac{n}{d_1}$, $b_1 = r_1 \frac{e_1}{d_1}$ sein, wo r_1 eine natürliche Zahl ist. Es ist daher p_1 genau durch $\mathfrak{p}_1^{r_1 \frac{n}{d_1}}$ teilbar. Da nun diese Überlegung für jedes in p_1 enthaltene Primideal gilt, so hat offenbar p_1 in $k(\gamma)$ eine Zerlegung der folgenden Art:

$$p_1 = (\mathfrak{p}_1^{r_1} \mathfrak{p}_1'^{r_1'} \mathfrak{p}_1''^{r_1''} \cdots)^{\frac{n}{d_1}} = \mathfrak{a}^{\frac{n}{d_1}},$$

so daß nach Hilfssatz II der Grad des Körpers $k(\gamma)$ gewiß durch $\frac{n}{d_1}$ teilbar ist. Dieselbe Betrachtung, die hier für die Primzahl p_1 durchgeführt ist, gilt aber auch für $p_2, p_3, \cdots, p_k$. Bezeichnet also allgemein d_i den größten Teiler von n und e_i $(i = 1, 2, \cdots, k)$, so ist der Grad des Körpers $k(\gamma)$ teilbar durch die Zahlen $\frac{n}{d_1}, \frac{n}{d_2}, \cdots, \frac{n}{d_k}$. Nach der Voraussetzung haben aber $d_1, d_2, \cdots, d_k$ keinen gemeinsamen Teiler, und demnach ist der Grad des Körpers auch durch n teilbar; er ist also genau gleich n, und somit die Irreduzibilität der Gleichung (5) bewiesen.

Der zu Beginn dieses Paragraphen erwähnte Satz von Königsberger geht aus dem allgemeinen Theorem hervor, wenn man $k = 2$, und $n = e_1 e_2$ setzt; die Zahlen e_1 und e_2 müssen dann nach den obigen Bedingungen relativ prim sein.

§ 4.

Ich gehe jetzt zu einer neuen Klasse von Sätzen über, und beweise zunächst das

Theorem III. *Die algebraische Gleichung*

$$x^n + a_1 x^{n-1} + p a_2 x^{n-2} + \cdots + p a_n = 0, \tag{6}$$

wo $a_1, a_2, \cdots, a_n$ ganze rationale Zahlen bedeuten, deren erste und letzte durch die Primzahl p nicht teilbar sind, und wo kein Teiler von a_n (± 1 eingeschlossen) nach dem Modul p kongruent a_1 ausfällt, ist irreduzibel.

Eine leichte Erweiterung, die der in § 2 gegebenen Erweiterung des Eisensteinschen Satzes parallel läuft, führt zu dem folgenden

Theorem IV. *Die algebraische Gleichung*

$$x^n + a_1 x^{n-1} + p^{\left[\frac{e}{n-1}\right]+1} a_2 x^{n-2} + p^{\left[\frac{2e}{n-1}\right]+1} a_3 x^{n-3} + \cdots + p^{\left[\frac{(n-2)e}{n-1}\right]+1} a_{n-1} x + p^e a_n = 0, \tag{7}$$

wo e prim zu $n-1$ ist, und die $a_1, \cdots, a_n$ genau die Bedingungen des vorigen Theorems erfüllen, ist irreduzibel.

Für $e = 1$ geht Theorem IV in das Theorem III über.

Zum Beweis will ich $n > 2$ voraussetzen, da für quadratische Gleichungen die Sätze ja ziemlich evident sind. Da das Produkt aller Wurzeln von (7) gleich $\pm p^e a_n$ ist, so muß mindestens eine Wurzel mit p einen Faktor gemein haben. γ sei eine solche Wurzel, und $\mathfrak{p}$ ein sowohl in p als in γ enthaltenes Primideal des Körpers $k(\gamma)$; p sei genau durch $\mathfrak{p}^a$, γ genau durch $\mathfrak{p}^b$ teilbar. Es wird dann die Zahl $\gamma + a_1$, da a_1 prim zu p ist, gewiß nicht durch $\mathfrak{p}$ teilbar sein, und folglich ist

$\gamma^{n-1}(\gamma+a_1)$ genau durch $\mathfrak{p}^{b(n-1)}$,

$p^{\left[\frac{(i-1)e}{n-1}\right]+1} a_i \gamma^{n-i}$ mindestens durch $\mathfrak{p}^{a\left(\left[\frac{(i-1)e}{n-1}\right]+1\right)+b(n-i)}$, $(i=2,3,\cdots,n-1)$

$p^e a_n$ genau durch $\mathfrak{p}^{ae}$

teilbar. Durch genau dieselben Schlüsse wie in § 2 ergibt sich hieraus, daß $b(n-1)=ae$ ist, und weil e und $n-1$ als relativ prim vorausgesetzt sind, so hat man notwendig $a=r(n-1)$, $b=re$, wo r eine natürliche Zahl ist. Die Primzahl p ist daher durch $\mathfrak{p}^{r(n-1)}$ teilbar, und da der Grad von $k(\gamma)$ wegen Gleichung (7) höchstens n ist, so muß $r(n-1)\leqq n$ sein. Wegen $n>2$ ergibt sich hieraus $r=1$, und somit ist p genau durch $\mathfrak{p}^{n-1}$ teilbar, γ genau durch $\mathfrak{p}^e$.

Enthält nun p noch einen weiteren Primfaktor $\mathfrak{q}$ in $k(\gamma)$, so ist notwendig $p=\mathfrak{p}^{n-1}\mathfrak{q}$, folglich nach Hilfssatz I der Grad von $k(\gamma)$ gleich n und Gleichung (7) irreduzibel. Es werde daher jetzt angenommen, p enthalte keinen von $\mathfrak{p}$ verschiedenen Primfaktor, so daß also $p=\mathfrak{p}^{n-1}$ ist. Nach Hilfssatz II ist dann der Grad von $k(\gamma)$ ein Multiplum von $n-1$, und da er höchstens gleich n sein kann und $n>2$ angenommen ist, so muß er genau gleich $n-1$ sein.

Die Gleichung (7) enthält somit einen irreduzibeln Faktor $(n-1)^{\text{ten}}$ Grades, folglich auch einen linearen Faktor, und sie hat somit eine rationale Wurzel β. β ist notwendig prim zu p, denn sonst könnte man genau wie oben folgern, daß der Grad von $k(\beta)$ entweder n oder $n-1$ ist, also β nicht rational. Da aber nach der Form der Gleichung (7) gewiß $\beta^{n-1}(\beta+a_1)$ durch p teilbar ist, so muß schon $\beta+a_1$ durch p teilbar sein, so daß $\beta=-(a_1+kp)$ wird, wo k eine ganze rationale Zahl bedeutet. Setzt man aber diese Wurzel in Gleichung (7) ein, so erhält man

$$0=kp(a_1+kp)^{n-1}+p^{\left[\frac{e}{n-1}\right]+1}a_2(a_1+kp)^{n-2}-p^{\left[\frac{2e}{n-1}\right]+1}a_3(a_1+kp)^{n-3}+\cdots\pm p^e a_n;$$

folglich muß a_n durch a_1+kp teilbar sein. Es ist also

$$a_n=c(a_1+kp)$$

oder

$$\frac{a_n}{c}\equiv a_1(p).$$

Diese Kongruenz widerspricht aber der Voraussetzung über die Koeffizienten a_1 und a_n; die Annahme $p=\mathfrak{p}^{n-1}$ ist also unstatthaft, und es bleibt nur die Möglichkeit $p=\mathfrak{p}^{n-1}\mathfrak{q}$, womit die Irreduzibilität von (7) nachgewiesen ist.

§ 5.

Aus dem Beweisgang des vorigen Paragraphen erkennt man unmittelbar auch die Richtigkeit des folgenden etwas allgemeineren

Theorem V. *Die algebraische Gleichung*

$$(8)\quad x^n + a_1 x^{n-1} + p^{\left[\frac{e}{n-1}\right]+1} a_2 x^{n-2} + \cdots + p^{\left[\frac{(n-2)e}{n-1}\right]+1} a_{n-1} x + p^e a_n = 0,$$

wo $a_1, a_2, \cdots, a_n$ ganze rationale Zahlen bedeuten, deren erste und letzte prim zur Primzahl p sind, und wo e und $n-1$ relativ prim sind, ist entweder irreduzibel, oder sie zerfällt in einen irreduzibeln Faktor $(n-1)^{ten}$ Grades und einen linearen Faktor. Die aus dem linearen Faktor entspringende rationale Wurzel ist dabei notwendig $\equiv -a_1 \left(\mathrm{mod}\, p^{\left[\frac{e}{n-1}\right]+1}\right)$*).

Königsberger hat in der zweiten der genannten Arbeiten die Irreduzibilität der Gleichung

$$(9)\quad x^5 + qa_1 x^4 + pqa_2 x^3 + p^2 q^2 a_3 x^2 + p^3 q^3 a_4 x + p^3 q^3 a_5 = 0$$

nachgewiesen, wo p, q verschiedene Primzahlen sind, a_1 nicht durch p, a_2 nicht durch q, a_5 weder durch p noch durch q teilbar ist.

Dies folgt nun leicht auch aus unserm gegenwärtigen Theorem; denn die Koeffizienten erfüllen die Bedingungen desselben, und für die Irreduzibilität ist daher nur erforderlich nachzuweisen, daß Gleichung (9) keine rationale Wurzel der Form $x = -(qa_1 + kp)$ hat.

Setzt man aber diesen Wert in (9) ein, so ergibt sich nach Division durch p

$$0 = k(qa_1 + kp)^4 + qa_2(qa_1 + kp)^3 - pq^2 a_3 (qa_1 + kp)^2 + p^2 q^3 (qa_1 + kp) - p^2 q^3 a_5.$$

Daher muß k durch q teilbar sein; alsdann ist aber das letzte Glied nur durch die dritte, alle andern durch eine höhere Potenz von q teilbar, was nicht möglich ist. Gleichung (9) ist daher irreduzibel.

Theorem VI. *Das Polynom*

$$x^n + a_1 x^{n-1} + \cdots + a_i x^{n-i} + p a_{i+1} x^{n-i-1} + \cdots + p a_n,$$

oder allgemeiner

$$(10)\quad x^n + a_1 x^{n-1} + \cdots + a_i x^{n-i} + p^{\left[\frac{e}{n-i}\right]+1} a_{i+1} x^{n-i-1} + \cdots + p^{\left[\frac{(n-i-1)e}{n-i}\right]+1} a_{n-1} x + p^e a_n,$$

wo a_i und a_n durch die Primzahl p nicht teilbar sind, und wo e zu $n-i$ relativ prim ist, enthält mindestens einen irreduzibeln Faktor, dessen Grad

*) Der angegebene Beweis gilt bloß für $n > 2$, für $n = 2$ ist ohne Schwierigkeit einzusehen, wie sich der Satz modifiziert.

$\geqq n-i$ *ist. Eine in* (10) *eventuell noch enthaltene Wurzel* β, *die diesem Faktor nicht angehört, erfüllt notwendig die Kongruenz*

$$\beta^i + a_1\beta^{i-1} + \cdots + a_i \equiv 0 \ (p),$$

und wenn man von dem bedeutungslosen Fall $i = n-1$ *absieht, dieselbe Kongruenz auch nach dem Modul* $p^{\left[\frac{e}{n-i}\right]+1}$.

Beweis. Da das Produkt aller Wurzeln des Polynoms (10) den Wert $\pm p^e a_n$ hat, so gibt es gewiß eine Wurzel γ, die zu p nicht prim ist. Sei also $\mathfrak{p}$ ein sowohl in p als in γ enthaltenes Primideal des Körpers $k(\gamma)$, und sei p genau durch $\mathfrak{p}^a$, γ genau durch $\mathfrak{p}^b$ teilbar. Da nach Voraussetzung a_i und a_n zu p prim, ferner auch e und $n-i$ relative Primzahlen sind, so führt die Wiederholung der früheren Schlüsse dazu, daß $a = r(n-i)$, $b = re$ ist, wo r eine natürliche Zahl bedeutet. Es ist also p genau durch $\mathfrak{p}^{r(n-i)}$ teilbar, und folglich der Grad von $k(\gamma)$ mindestens $n-i$, womit der erste Teil unserer Behauptung bewiesen ist. Des weiteren ist γ genau durch $\mathfrak{p}^{re}$ teilbar, und wenn $\mathfrak{p}$ etwa ein Primideal f^{ten} Grades ist, so ist die Norm von γ durch p^{fre} teilbar. Da aber das Produkt aller Wurzeln von (10) nur durch die e^{te} Potenz von p teilbar ist, so stellt sich $f=1$, $r=1$ heraus, so daß p genau durch $\mathfrak{p}^{n-i}$, γ genau durch $\mathfrak{p}^e$ teilbar und außerdem $\mathfrak{p}$ ein Primideal ersten Grades ist. Zugleich folgt, daß eine Wurzel β von (10), die nicht demselben irreduzibeln Faktor angehört wie γ, notwendig zu p prim ist. Da aber aus der Form des Polynoms (10) hervorgeht, daß $\beta^n + a_1\beta^{n-1} + \cdots + a_i\beta^{n-i}$ durch $p^{\left[\frac{e}{n-i}\right]+1}$ teilbar ist, so gilt dasselbe schon von $\beta^i + a_1\beta^{i-1} + \cdots + a_i$ und damit ist auch die zweite Aussage unseres Theorems bewiesen.

Theorem VII. *Wenn die algebraische Gleichung*

$$(11)\quad x^n + a_1 x^{n-1} + p_1^{\left[\frac{e_1}{n-1}\right]+1} \cdots p_k^{\left[\frac{e_k}{n-1}\right]+1} a_2 x^{n-2} + p_1^{\left[\frac{2e_1}{n-1}\right]+1} \cdots p_k^{\left[\frac{2e_k}{n-1}\right]+1} a_3 x^{n-1} + \cdots$$
$$+ p_1^{\left[\frac{(n-2)e_1}{n-1}\right]+1} \cdots p_k^{\left[\frac{(n-2)e_k}{n-1}\right]+1} a_{n-1} x \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = 0$$

keine der beiden Zahlen ± 1 *als Wurzel hat, so ist sie irreduzibel. Dabei ist* a_1 *prim zu den Primzahlen* $p_1, p_2, \cdots, p_k$, *die Exponenten* $e_1, e_2, \cdots, e_k$ *alle prim zu* $n-1$, *und* $n > 2$ *vorausgesetzt.*

Besonders bemerkenswert ist der Fall, daß alle e_i einander gleich sind.

Zum Beweis bemerke man, daß Gleichung (11) sicher eine Wurzel γ hat, die zu p_1 nicht prim ist, und nach den früheren Erörterungen dieses Paragraphen entspringt hieraus ein Körper $k(\gamma)$ vom n^{ten} oder $(n-1)^{\text{ten}}$ Grad. Ist $k(\gamma)$ nur vom $(n-1)^{\text{ten}}$ Grad, so hat Gleichung (11) noch eine rationale Wurzel β. Diese müßte aber notwendig ± 1 sein; denn wäre β

etwa durch p_ϱ teilbar, so könnte man wieder schließen, daß der Körper $k(\beta)$ vom Grad n oder $n-1$ sein muß, während doch β rational ist. Da jedoch Gleichung (11) keine der Zahlen ± 1 als Wurzel haben soll, so ist die Annahme, daß $k(\gamma)$ nur vom $(n-1)^{\text{ten}}$ Grad sei, hinfällig; es ist $k(\gamma)$ vom n^{ten} Grad, und daher die Gleichung irreduzibel, wie behauptet war.

Die Irreduzibilität steht insbesondere dann fest, wenn

$$a_1 \neq \pm 1 \left(p_1^{\left[\frac{e_1}{n-1}\right]+1} \cdots p_k^{\left[\frac{e_k}{n-1}\right]+1}\right),$$

was man entweder unter Zuziehung des Theorems V erkennt, oder auch direkt, wenn man $x = \pm 1$ in Gleichung (11) einsetzt

§ 6.

Theorem VIII. *Das Polynom*

(12) $x^n + pa_1x^{n-1} + \cdots + pa_{n-k-1}x^{k+1} + p^2a_{n-k}x^k + \cdots + p^2a_{n-1}x + p^2a_n$,

wo a_n prim zur Primzahl p und $n > 2k$ ist, besitzt keinen rationalen Teiler von geringerem als dem $(k+1)^{ten}$ Grad. (Netto a. a. O.)*)

Beweis. Eine beliebige Wurzel γ von (12) hat eine durch p teilbare n^{te} Potenz, also kann sie zu p nicht relativ prim sein. Sei daher $\mathfrak{p}$ ein sowohl in p als in γ aufgehendes Primideal des Körpers $k(\gamma)$, und p genau durch $\mathfrak{p}^a$, γ genau durch $\mathfrak{p}^b$ teilbar. Ferner mag p^{e_i-1} die höchste in a_i aufgehende Potenz von p bedeuten $(i=1,2,\cdots,n-k-1)$. Dann ist

$$\begin{aligned}
&\gamma^n && \text{genau durch } \mathfrak{p}^{bn}, && \\
&pa_i\gamma^{n-i} && \text{genau durch } \mathfrak{p}^{ae_i+b(n-i)}, && (i=1,2,\cdots,n-k-1),\\
&p^2a_j\gamma^{n-j} && \text{mindestens durch } \mathfrak{p}^{2a+b(n-j)}, && (j=n-k,\ n-k+1,\cdots,n-1),\\
&p^2a_n && \text{genau durch } \mathfrak{p}^{2a} && \\
\end{aligned}$$

teilbar. Die beiden hier auftretenden kleinsten Exponenten müssen offenbar wieder einander gleich sein; von den $n-k+1$ Zahlen

$$2a, \quad bn, \quad ae_i + b(n-i) \quad (i=1,2,\cdots,n-k-1)$$

müssen also zwei einander gleich und dabei nicht größer als jede andre sein.

Ist nun $2a = bn$, so folgt $a = \frac{bn}{2} > bk$; ist aber $2a = ae_i + b(n-i)$, so folgt $e_i = 1$, also $a = b(n-i) \geqq b(k+1)$; ist ferner $bn = ae_i + b(n-i)$ der kleinste auftretende Exponent, so kann $2a$ nicht kleiner sein, also ist wieder $2a \geqq bn$; $a > bk$. Die letzte Möglichkeit, daß

$$ae_i + b(n-i) = ae_h + b(n-h) \quad (i,h=1,\cdots,n-k-1)$$

*) Über die interessanten weiteren Folgerungen aus diesem Satz vergl. man die Nettosche Arbeit.

der kleinste Exponent ist, liefert endlich $2a \geqq ae_i + b(n-i)$, woraus wieder $a \geqq b(k+1)$ folgt. Man findet daher in jedem Fall $a \geqq k+1$, und da p durch $\mathfrak{p}^a$ teilbar ist, so muß der Grad von $k(\gamma)$ mindestens $k+1$ sein, w. z. b. w.

Die aufgeführten Sätze sind lediglich Beispiele zur Illustration meiner Methode; sie mögen genügen, um die Fruchtbarkeit derselben darzutun, und zu zeigen, wie überraschend einfach die Beweise selbst komplizierter Irreduzibilitätskriterien sich bei ihrer Anwendung gestalten. Indeß wäre es nicht schwer, die Zahl dieser Sätze beliebig zu vermehren; insbesondere lassen sich z. B. alle von Netto a. a. O. bewiesenen Theoreme in derselben Weise neu begründen.

Ich habe mich der Einfachheit halber im vorstehenden ausschließlich auf die Irreduzibilität in bezug auf den natürlichen Rationalitätsbereich beschränkt. Doch will ich hervorheben, daß nach demselben Prinzip mit ebensolcher Leichtigkeit sich ganz analoge Sätze beweisen lassen über die Irreduzibilität in bezug auf einen beliebigen algebraischen Rationalitätsbereich. Der Eisensteinsche Satz lautet dann z. B.:

Die algebraische Gleichung

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

deren Koeffizienten einem gewissen algebraischen Körper K angehören und sämtlich durch ein bestimmtes Primideal $\mathfrak{p}$ dieses Körpers teilbar sind, und zwar a_n nur durch die erste Potenz von $\mathfrak{p}$, ist im Bereich K irreduzibel.

Eisenstein selbst hat seinen Satz bereits für den Körper $k(\sqrt{-1})$ bewiesen.

München, den 5. Juli 1904.
