**Zeitschrift:** Commentarii Mathematici Helvetici
**Herausgeber:** Schweizerische Mathematische Gesellschaft
**Band:** 6 (1934)

**Artikel:** Ueber die Primideale im Wurzelkörper einer Gleichung.
**Autor:** Gut, Max
**DOI:** https://doi.org/10.5169/seals-7588

# Ueber die Primideale im Wurzelkörper einer Gleichung

Von MAX GUT, Zürich.

**1.** Herr A. Speiser hat in einer Arbeit[1]) ein Kriterium angegeben, mit Hilfe dessen man den Grad der Primideale im Körper sämtlicher Wurzeln einer vorgelegten (nicht notwendigerweise irreduzibeln) algebraischen Gleichung angeben kann. Dieses Kriterium liefert im Falle der binomischen Gleichungen in sehr durchsichtiger Weise das gesuchte Resultat, hat aber den Nachteil, daß es im allgemeinen Falle bald zu viel zu weitläufigen Rechnungen führt. Es setzt dann außerdem voraus, daß die zugehörige rationale Primzahl weder in der Diskriminante der Gleichung, noch im absoluten Gliede aufgeht[2]).

Indem man im wesentlichen einige bekannte Sätze zusammenhält, kann man aber, wie ich hier bemerken will, ein anderes Kriterium angeben, das im allgemeinen Falle viel rascher zum Ziele führt, und ferner nur voraussetzt, daß die Primzahl nicht in der *Körper*diskriminante des Wurzelkörpers aufgeht. Ich will die Darstellung überdies so halten, daß ich annehme, der Grundkörper sei ein beliebiger algebraischer Zahlkörper $k$.

**2.** Ich schicke voraus folgenden

*Hilfssatz:* Es seien $K_1$ und $K_2$ zwei Körper, die je Galois'sch in bezug auf $k$ sind, $\mathfrak{p}$ ein Primideal in $k$, das zur Relativdiskriminanten von $K_1$ in bezug auf $k$ und zur Relativdiskriminanten von $K_2$ in bezug auf $k$ teilerfremd ist. Es bezeichne $F_1$, bezw. $F_2$ den Relativgrad (in bezug auf $k$) jedes Primidealteilers von $\mathfrak{p}$ in $K_1$, bezw. $K_2$.

Dann ist $\mathfrak{p}$ teilerfremd zur Relativdiskriminanten (in bezug auf $k$) des Kompositums $K$ von $K_1$ und $K_2$, und der Relativgrad $F$ (in bezug auf $k$) jedes Primidealteilers von $\mathfrak{p}$ in $K$ ist gleich dem K.G.V.[3]) von $F_1$ und $F_2$.

*Beweis:* Da bei Galois'schen Körpern jeder Isomorphismus ein Automorphismus ist, so ist zunächst klar, daß sowohl der Durchschnitt $\bar{k}$ von $K_1$ und $K_2$ (d. h. die Gesamtheit aller Zahlen, die sowohl $K_1$, als $K_2$ angehören), als auch das Kompositum $K$ von $K_1$ und $K_2$ (d. h. die Gesamtheit aller rationalen Funktionen mit rationalzahligen Koeffizienten

[1]) *A. Speiser*, Die Zerlegung von Primzahlen in algebraischen Zahlkörpern, Transactions of the American Math. Soc., vol. 23, pg. 173, (1922).

[2]) l. c. pg. 177.

[3]) Kleinstes gemeinschaftliches Vielfaches.

irgend zweier primitiver Zahlen von $K_1$ und $K_2$) Galois'sche Körper über $k$ sind.

Da außerdem sowohl $K_1$ als auch $K_2$ Galois'sch in bezug auf $k$ sind, so haben folgende Bezeichnungen einen Sinn:

$f$ = Relativgrad in bezug auf $k$ irgend eines Primideales $\mathfrak{p}$ von $\bar{k}$, welches $\mathfrak{p}$ teilt.

$N^*$, bezw. $N^{**}$ = Relativgrad von $K_1$, bezw. $K_2$ in bezug auf $k$.

$F^*$, bezw. $F^{**}$ = Relativgrad in bezug auf $\bar{k}$ irgend eines Primideales $\mathfrak{P}^*$ von $K_1$, bezw. $\mathfrak{P}^{**}$ von $K_2$, welches $\mathfrak{p}$ teilt; $F^* = \frac{F_1}{f}$, $F^{**} = \frac{F_2}{f}$.

$\mathfrak{G}^*$, bezw. $\mathfrak{G}^{**}$ = Relativgruppe von $K_1$, bezw. $K_2$ in bezug auf $\bar{k}$.

$\mathfrak{P}$ irgend ein festes Primideal von $K$. $\mathfrak{P}$ sei dann Teiler von $\bar{\mathfrak{p}}$ in $k$, von $\mathfrak{P}^*$ in $K_1$ und von $\mathfrak{P}^{**}$ in $K_2$.

$\mathfrak{Z}^*$, bezw. $\mathfrak{Z}^{**}$ = Relative Zerlegungsgruppe von $\mathfrak{P}^*$, bezw. $\mathfrak{P}^{**}$ in bezug auf $\bar{k}$. Sie ist zyklisch vom Grade $F^*$, bezw. $F^{**}$.

$\mathfrak{G}^* = \mathfrak{Z}^* G_1^* + \mathfrak{Z}^* G_2^* + \ldots + \mathfrak{Z}^* G_{\overline{N^*}}^{*}$; $G_1^* =$ Identität;

$\mathfrak{G}^{**} = \mathfrak{Z}^{**} G_1^{**} + \mathfrak{Z}^{**} G_2^{**} + \ldots + \mathfrak{Z}^{**} G_{\overline{N^{**}}}^{**}$; $G_1^{**} =$ Identität.

Nach unseren Definitionen ist dann die Relativgruppe $\mathfrak{G}$ von $K$ in bezug auf $\bar{k}$ das direkte Produkt der beiden Gruppen $\mathfrak{G}^*$ und $\mathfrak{G}^{**}$.

Zunächst ist die Relativdifferente von $\bar{k}$ in bezug auf $k$ als Teiler der Relativdifferenten von $K_1$ (oder von $K_2$) in bezug auf $k$ teilerfremd zu $\mathfrak{p}$.

Ferner ist die Relativdifferente von $K$ in bezug auf $\bar{k}$ gleich dem Produkt der Elemente:

$$\Pi' \ (\Omega_1 - G^* G^{**} \Omega_1, \ \Omega_2 - G^* G^{**} \Omega_2, \ \ldots),$$

wo in der Klammer $\Omega$ alle ganzen Zahlen von $K$ durchläuft, und das Produkt über alle möglichen Paare von Elementen $G^*$ aus $\mathfrak{G}^*$ und $G^{**}$ aus $\mathfrak{G}^{**}$ zu erstrecken ist, mit Ausnahme des einzigen Paares, wo sowohl $G^*$ als auch $G^{**}$ die Identität bedeuten.

Würde man nun annehmen, daß irgend ein fester Faktor einen vom Einheitsideal verschiedenen Idealteiler gemein hätte mit $\mathfrak{p}$, so würde das auch für alle seine Zahlen gelten, die in $K_1$, bezw. $K_2$ liegen, und daher hätte wenigstens eine der beiden Relativdifferenten von $K_1$ oder von $K_2$ in bezug auf $\bar{k}$ einen vom Einheitsideal verschiedenen Idealteiler mit $\mathfrak{p}$ gemein, gegen Voraussetzung.

Folglich ist $\mathfrak{p}$ zur Relativdiskriminanten von $K$ in bezug auf $k$ teiler-

fremd, ferner besteht die Trägheitsgruppe von $\mathfrak{P}$ in bezug auf $\bar{k}$ aus der Einheitsoperation, und die Zerlegungsgruppe $\mathfrak{Z}$ von $\mathfrak{P}$ in bezug auf $\bar{k}$ ist zyklisch.

Da $\mathfrak{P}$ die Primideale $\mathfrak{P}^*$ und $\mathfrak{P}^{**}$ teilt, teilt ein Primideal

$$\mathfrak{Z}^* G_i^* \mathfrak{Z}^{**} G_j^{**} \mathfrak{P}, \text{ wo } 1 \leqq i \leqq \frac{N^*}{F^*}, \; 1 \leqq j \leqq \frac{N^{**}}{F^{**}},$$

die Ideale $G_i^* \mathfrak{P}^*$ und $G_j^{**} \mathfrak{P}^{**}$. Daraus folgt aber, daß $\mathfrak{Z}$ eine Untergruppe des direkten Produktes der beiden zyklischen Gruppen $\mathfrak{Z}^*$ und $\mathfrak{Z}^{**}$ ist. Da $\mathfrak{Z}$ auch zyklisch ist, so ist seine Ordnung, d. h. der Relativgrad von $\mathfrak{P}$ in bezug auf $\bar{k}$ *höchstens* gleich dem K. G. V. von $F^*$ und $F^{**}$.

Anderseits ist der Relativgrad von $\mathfrak{P}$ in bezug auf $\bar{k}$ *mindestens* gleich dem K. G. V. von $F^*$ und $F^{**}$, denn die Relativgrade der Primidealteiler multiplizieren sich analog wie die zugehörigen Relativdifferenten.

Folglich ist der Relativgrad von $\mathfrak{P}$ in bezug auf $\bar{k}$ *genau* gleich dem K. G. V. von $F^*$ und $F^{**}$, und daher der Relativgrad $F$ von $\mathfrak{P}$ in bezug auf $k$ gleich dem K. G. V. von $F_1 = F^* f$ und $F_2 = F^{**} f$. Q. E. D.

**3.** Ein Polynom heiße ein normiertes Polynom in $k$, wenn alle seine Koeffizienten ganze Zahlen in $k$ sind, und der Koeffizient der höchsten Potenz gleich 1 ist.

Ist $H(x)$ das vorgelegte normierte Polynom in $k$, so zerlege man es zunächst in seine in $k$ irreduzibeln Faktoren, die nach einem bekannten Gauß'schen Lemma auch normierte Polynome in $k$ sind:

$$H(x) = C(x)\, D(x) \ldots L(x) .$$

Sei die Zerlegung in Linearfaktoren

$$\begin{aligned} C(x) &= (x - \Gamma_1)(x - \Gamma_2) \ldots (x - \Gamma_c), \\ D(x) &= (x - \Delta_1)(x - \Delta_2) \ldots (x - \Delta_d), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ L(x) &= (x - \Lambda_1)(x - \Lambda_2) \ldots (x - \Lambda_l) . \end{aligned}$$

Ich betrachte jetzt einen dieser Faktoren, z. B. $C(x)$, und bezeichne mit $\bar{k}$ einen Körper, der aus $k$ dadurch entsteht, daß man *eine* beliebige Wurzel von $C(x)$ adjungiert, ferner mit $K_C$ den Körper, der aus $k$ dadurch entsteht, daß man *alle* Wurzeln von $C(x)$ adjungiert. Ein Primideal $\mathfrak{p}$ des Grundkörpers $k$ geht dann immer gleichzeitig in der Relativ-

diskriminanten von $k$ in bezug auf $k$ und in der Relativdiskriminanten von $K_C$ in bezug auf $k$ auf oder nicht auf. Die beiden Hauptsätze der Ore'schen Theorie[4]) gestatten aber, zum mindesten theoretisch, zu entscheiden, ob $\mathfrak{p}$ in der Relativdiskriminanten von $\bar{k}$ in bezug auf $k$ aufgeht oder nicht, und falls der letztere Fall eintritt, falls also $\mathfrak{p}$ sich nicht verzweigt, so liefern sie folgende Aussage:

Ist die Diskriminante von $C(x)$ teilbar durch $\mathfrak{p}^t$, aber nicht mehr durch $\mathfrak{p}^{t+1}$, so zerlege man $C(x)$ in normierte irreduzible Polynome mod $\mathfrak{p}^N$, wo $N$ eine beliebig große natürliche Zahl größer als $t$ ist:

$$C(x) \equiv C_1(x)\, C_2(x) \ldots C_R(x) \qquad (\mathrm{mod}\ \mathfrak{p}^N).$$

Ist dann $C_r(x)$ vom Grade $f_r$, wo $r = 1, 2, \ldots R$; $f_1 + f_2 + \ldots + f_R = c$, so zerlegt sich $\mathfrak{p}$ in $\bar{k}$ in $R$ voneinander verschiedene Primideale:

$$\mathfrak{p} = \bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2 \ldots \mathfrak{p}_R, \text{ wo } N_{\bar{k}/k}(\mathfrak{p}_r) = \mathfrak{p}^{f_r}.$$

Die Ore'sche Zerlegung liefert aber, wie bisher nicht bemerkt worden zu sein scheint, im Falle der unverzweigten Primideale noch mehr[5]). Auf Grund eines von Herrn E. Artin bewiesenen Satzes[6]) folgt nämlich, daß jede erzeugende Substitution der relativen Zerlegungsgruppe in bezug auf $k$ jedes Primideales $\mathfrak{P}_C$ von $K_C$, welches $\mathfrak{p}$ teilt, speziell also auch die „Frobenius-Substitution", aus $R$ Zykeln besteht, wobei der $r$-te Zyklus genau $f_r$ Elemente enthält. Insbesondere ergibt sich daraus, daß der Relativgrad $F_C$ von $\mathfrak{P}_C$ in bezug auf $k$ gleich dem K. G. V. aller $R$ Werte $f_r$ ist.

In analoger Weise kann man jetzt untersuchen, ob $\mathfrak{p}$ in den Relativdiskriminanten von $K_D, \ldots K_L$ in bezug auf $k$ aufgeht oder nicht. Geht $\mathfrak{p}$ in wenigstens einer derselben oder in der von $K_C$ in bezug auf $k$ auf, so ist klar, daß $\mathfrak{p}$ in der Relativdiskriminanten in bezug auf $k$ des Wurzelkörpers $K = K(k; \Gamma_1, \Gamma_2, \ldots \Gamma_c; \Delta_1, \Delta_2, \ldots \Delta_l)$ aufgeht, denn eine Verzweigung kann nie mehr rückgängig gemacht werden. Geht $\mathfrak{p}$ aber in keiner der Relativdiskriminanten von $K_C, K_D, \ldots K_L$ in bezug

---

[4]) *Ö. Ore*, Ueber den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, Math. Ann., Band 96, S. 313—352 (1926), und Band 97, S. 569—598 (1927); vgl. besonders S. 592 und 594.

[5]) insbesondere im Falle der unverzweigten Relativkörper die vollständige Zerlegung im Galois'schen Körper für *alle* Primideale von $k$, falls weiter die Ordnung der Galois'schen Gruppe bekannt ist. In vielen Fällen kann man ja gerade mit Hilfe des Satzes von Artin leicht zeigen, daß die vorgelegte Gleichung in $k$ z. B. ohne Affekt ist.

[6]) *E. Artin*, Ueber die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann., Band 89, S. 147—156, (1923), vgl. besonders S. 148/149.

auf $k$ auf, so folgt aus dem Hilfssatz, daß $\mathfrak{p}$ nicht in der Relativdiskriminanten von $K$ in bezug auf $k$ aufgeht, und daß, falls man in analoger Weise für $D(x)$, ... $L(x)$, die Werte $F_D$, ... $F_L$ bestimmt, der Relativgrad $F$ in bezug auf $k$ von jedem Primideal $\mathfrak{P}$ des Wurzelkörpers $K$, welches $\mathfrak{p}$ teilt, gleich dem K. G. V. aller Werte $F_C$, $F_D$, ... $F_L$, oder was dasselbe ist, gleich dem K. G. V. aller Werte $f$ ist.

Weiß man von vorneherein, daß $\mathfrak{p}$ nicht in der Relativdiskriminanten von $K$ in bezug auf $k$ aufgeht, und hat $H(x)$ keine mehrfachen Nullstellen, so liefert die direkte Zerlegung von $H(x)$ in normierte Primpolynome mod $\mathfrak{p}^N$ für genügend großes $N$ die Werte $f$, und damit ihr K. G. V., also $F$. Ist in der Tat die Diskriminante von $H(x)$ durch $\mathfrak{p}^T$, aber nicht durch $\mathfrak{p}^{T+1}$ teilbar, so genügt es jedenfalls immer, $N > 2T$ zu wählen, wie man durch Anwendung eines Satzes von Ore[7]) auf das Polynom

$$H^*(x) = H(x) + \pi^{2T+1} G(x)$$

einsieht. Hiebei ist $\pi$ eine durch $\mathfrak{p}$ teilbare ganze Zahl von $k$, und $G(x)$ ein ganzzahliges Polynom von $k$ von kleinerem Grade als $H(x)$, dessen Koeffizienten so bestimmt sind, daß falls $\mathfrak{q}$ ein zu $\pi$ teilerfremdes Primideal von $k$ ist, alle Koeffizienten von $H^*(x)$ mit Ausnahme des ersten durch $\mathfrak{q}$ teilbar sind, und der letzte nicht durch $\mathfrak{q}^2$ teilbar ist. Denn $H^*(x)$ ist dann nach dem Eisenstein'schen Kriterium irreduzibel, ferner $H^*(x) \equiv H(x) \pmod{\mathfrak{p}^{2T+1}}$, schließlich der Exponent der Potenz, in der $\mathfrak{p}$ in der Diskriminante von $H^*(x)$ aufgeht, auch gleich $T$.

**4.** Es sei wieder $k$ ein algebraischer Körper und $C(x)$ ein in $k$ irreduzibles normiertes Polynom, dessen eine Wurzel einen Erweiterungskörper $\bar{k} = k(k; \Gamma_i)$ von $k$ festlegt und $K = K(k; \Gamma_1, \Gamma_2, \ldots \Gamma_c)$ der zugehörige Galois'sche Erweiterungskörper. Verzweigt sich dann das Primideal $\mathfrak{p}$ von $k$ in $\bar{k}$ und $K$, so ist der Relativgrad $F$ (bezw. die Relativordnung $E$) in bezug auf $k$ jedes Primideales $\mathfrak{P}$ von $K$, welches $\mathfrak{p}$ teilt, im allgemeinen nicht mehr gleich dem K. G. V. der Relativgrade $f_1, f_2, \ldots f_R$ (bezw. der Relativordnungen $e_1, e_2, \ldots e_R$) in bezug auf $k$ aller voneinander verschiedenen Primideale $\bar{\mathfrak{p}}_1, \bar{\mathfrak{p}}_2, \ldots \bar{\mathfrak{p}}_R$ von $\bar{k}$, welche $\mathfrak{p}$ teilen. Bei beliebigem Grundkörper $k$ liefern schon geeignete binomische Gleichungen Gegenbeispiele:

*a) Gegenbeispiel für die Relativgrade.*

Es sei $\mathfrak{p}$ ein Primideal 1. Grades von $k$, und $n(\mathfrak{p}) = p$, ferner $q$ eine Primzahl, welche größer als $p$ ist. Endlich sei $\pi$ eine ganze Zahl von $k$, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist.

[7]) Vgl. *Ö. Ore*, l. c. pg. 332, Satz 5.

Dann sei das nach dem Eisenstein'schen Satze in $k$ irreduzible Polynom:

$$C(x) = x^q - \pi = (x - \sqrt[q]{\pi})\ (x - \varepsilon\sqrt[q]{\pi})\ \ldots\ (x - \varepsilon^{q-1}\sqrt[q]{\pi})$$

vorgelegt, wo $\varepsilon$ eine von 1 verschiedene $q$-te Einheitswurzel bedeutet.

Offenbar gibt es wegen $(\varepsilon^i\sqrt[q]{\pi})^q = \pi$ in $\bar{k}$ nur ein einziges Primideal $\bar{\mathfrak{p}}$, welches $\mathfrak{p}$ teilt, und

$$\mathfrak{p} = \bar{\mathfrak{p}}^q, \quad N_{\bar{k}/k}(\bar{\mathfrak{p}}) = \mathfrak{p}, \quad \text{d. h. } f = 1.$$

Jedes Primideal des Körpers $k^*$ der $q$-ten Einheitswurzeln, welches $p$ teilt, hat den Grad $f^*$, falls $f^*$ die kleinste positive Zahl ist, für welche

$$p^{f^*} \equiv 1 \pmod{q}.$$

Hier ist $f^* > 1$, denn sonst würde folgen, daß $p - 1$ durch $q$ teilbar ist, was wegen $q > p$ nicht möglich ist. Der Körper $k^*$ ist in $K$; jedes Primideal von $K$, welches $p$ teilt, muß daher einen durch $f^*$ teilbaren Grad haben, mithin muß wegen $n(\bar{\mathfrak{p}}) = p$ auch jedes Primideal $\mathfrak{P}$ von $K$, welches $\bar{\mathfrak{p}}$ teilt, einen durch $f^*$ teilbaren Relativgrad in bezug auf $\bar{k}$ und folglich auch in bezug auf $k$ haben. Es ist daher $F$ durch $f^*$ teilbar, also größer als das K. G. V. aller $f$, welches 1 ist.

*b) Gegenbeispiel für die Relativordnungen.*

Wir wählen die ungerade Primzahl $p$ teilerfremd zur Diskriminanten des Körpers $k$. Sei $\mathfrak{p}$ ein Primideal in $k$, welches $p$ teilt, $\pi$ wie oben eine ganze Zahl von $k$, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist.

Dann sei das nach dem Eisenstein'schen Satze in $k$ irreduzible Polynom:

$$C(x) = x^p - \pi = (x - \sqrt[p]{\pi})\ (x - \eta\sqrt[p]{\pi})\ \ldots\ (x - \eta^{p-1}\sqrt[p]{\pi})$$

vorgelegt, wo $\eta$ eine von 1 verschiedene $p$-te Einheitswurzel bedeutet.

Wie eben folgt zunächst die Primidealzerlegung in $\bar{k}$:

$$\mathfrak{p} = \bar{\mathfrak{p}}^p, \qquad N_{\bar{k}/k}(\bar{\mathfrak{p}}) = \mathfrak{p}, \quad \text{d. h. } e = p.$$

Der Relativgrad von $K$ in bezug auf $\bar{k}$ ist höchstens gleich $p-1$, anderseits ist er nicht kleiner, denn der Körper $k^*$ der $p$-ten Einheitswurzeln steckt in $K$, und in $k^*$ besteht die Primidealzerlegung

$$p = \mathfrak{p}^{*p-1}, \qquad n(\mathfrak{p}^*) = p.$$

Also muß jedes in $K$ liegende Primideal, welches $p$ teilt, eine durch $p-1$ teilbare Ordnung, und da die absolute Ordnung von $\bar{\mathfrak{p}}$ gleich $p$, also zu $p-1$ teilerfremd ist, jeder Primteiler $\mathfrak{P}$ in $K$ von $\bar{\mathfrak{p}}$ eine durch $p-1$ teilbare Relativordnung in bezug auf $\bar{k}$ haben, und

$$\mathfrak{p} = \mathfrak{P}^{p(p-1)}, \qquad N_{K/k}(\mathfrak{P}) = \mathfrak{p}, \quad \text{d. h. } E = p(p-1),$$

und $K$ hat genau den Relativgrad $p-1$ in bezug auf $\bar{k}$.

Es ist folglich $E = (p-1)p$, d. h. größer als das K. G. V. aller $e$, welches gleich $p$ ist.

New Haven, Conn., Juli, 1933.

(Eingegangen den 27. Juli 1933)