Professor Dr. Jürgen Ritter
Lehrstuhl für Algebra und Zahlentheorie
Institut für Mathematik · Universität Augsburg

Protokoll der Vorlesung Algebra 1 · Wintersemester 2006 / 2007

Literaturvorschläge

E. Artin	Galoissche Theorie (Teubner)
M. Artin	Algebra (Birkhäuser)
S. Bosch	Algebra (Springer)
I.N. Herstein	Algebra (Φ)
N. Jacobson	Lectures in abstract algebra, II,III (Springer GTM 31,32)
S. Lang	Algebra (Addison Wesley)
F. Lorenz	Algebra 1,2 (BI)
G. Scheja & U. Storch	Lehrbuch der Algebra 1,2 (Teubner)
G. Stroth	Algebra (de Gruyter)
B.L. van der Waerden	Algebra I,II (Springer HT 12,23)
H. Weber	Lehrbuch der Algebra I,II,III (Chelsea)
O. Zariski & P. Samuel	Commutative Algebra I,II (Springer GTM 28,29)

1. Körper

Dies sind nichtleere Mengen K mit zwei Strukturen, $+$ und $\cdot$ [1], also Abbildungen $K \times K \to K$, die folgendes erfüllen:

$$
\begin{array}{ll}
\text{(A0)} & \exists\, 0 \in K : a + 0 = a \ (\forall a \in K) \\
\text{(A1)} & a + b = b + a \ (\forall a, b \in K) \\
\text{(A2)} & \forall\, a \in K \, \exists\, -a \in K : a + (-a) = 0 \\
\text{(A3)} & a + (b + c) = (a + b) + c \ (\forall a, b, c \in K) \\
\text{(M0)} & \exists\, 1 \in K : a1 = a \ (\forall a \in K) \\
\text{(M1)} & 1 \neq 0 \\
\text{(M2)} & ab = ba \ (\forall a, b \in K) \\
\text{(M3)} & \forall\, 0 \neq a \in K \, \exists\, a^{-1} \in K : a \cdot a^{-1} = 1 \\
\text{(M4)} & a(bc) = (ab)c \ (\forall a, b, c \in K) \\
\text{(M5)} & a(b + c) = ab + ac \ (\forall a, b, c \in K)
\end{array}
$$

Fehlt (M2), gilt aber noch

$$\text{(M5}') \quad (a + b)c = ac + bc \ (\forall a, b, c \in K)\,,$$

so heißt K ein Schiefkörper [2].

[1] $\cdot$ wird allerdings meist nicht ausgeschrieben

[2] Zumindest in diesem Semester werden wir keine Schiefkörper behandeln.

Gilt nur (A0)-(A3), oder (M0),(M3),(M4), so heißt K, bzw. $K^\times \stackrel{\text{def}}{=} K \setminus \{0\}$, eine Gruppe (bezüglich $+$, bzw. $\cdot$); beachte, daß im letzteren Fall die Gruppe nicht kommutativ [3] sein muß: (M2) fehlt! Dennoch gilt immer: $1a = a1, a \cdot a^{-1} = a^{-1} \cdot a = 1$ $(\forall a \in K^\times)$.

Fehlen für K nur (M1) und (M3), so heißt K ein Ring.

Wir reden von Unterstrukturen von K oder $K^\times$, also von Teilkörpern, Teilringen, Untergruppen, wenn wir nichtleere Teilmengen k von K meinen, die abgeschlossen unter $+$ und (bzw.) $\cdot$ sind, sowie außerdem (A0),(A2), bzw. (M0),(M3) bei Gruppen, erfüllen (alle anderen Gesetze folgen dann automatisch für k).

Beispiele:

> Körper sind $\mathbb{Q}$ (die rationalen), $\mathbb{R}$ (die reellen), $\mathbb{C}$ (die komplexen Zahlen); aber auch $\mathbb{F}_2 = \{0, 1\}$ mit $1 + 1 = 0$ ist ein Körper.
>
> Ringe sind $\mathbb{Z}$ (die ganzen Zahlen), $\mathbb{R}[x]$ (der Ring der Polynome in der Unbestimmten x mit reellen Koeffizienten) oder $\mathbb{R}_{n\times n}$ (der Ring der $n \times n$-Matrizen mit reellen Einträgen.
>
> Aus der lineraren Algebra sind die Gruppen S_n (die symmetrische [Permutations]-Gruppe auf n Elementen), und $\mathrm{GL}_n(\mathbb{R})$ (die Gruppe der invertierbaren $n \times n$-Matrizen mit reellen Einträgen) bekannt. Beide Gruppen sind (mit Ausnahme von kleinen n) nichtkommutativ.

In einem Körper K bilden die ganzrationalen Vielfachheiten $n1 = \underbrace{1 + \ldots + 1}_{n}, n \in \mathbb{N}$, und $(-n)1 = n(-1) = \underbrace{-1 + \ldots + -1}_{n}$ des Eiselementes $1 \in K$ einen Teilring. Gilt für alle $0 \neq n \in \mathbb{N}$, daß $n1 \neq 0$, so ist dieser Teilring vermöge $z1 \mapsto z$ isomorph zu $\mathbb{Z}$, d.h. die gezeigte Abbildung ist bijektiv sowie verträglich mit $+$ und $\cdot$. Wegen (M3) gehören alle Quotienten $z_1 1 \cdot (z_2 1)^{-1}$, $z_1, 0 \neq z_2 \in \mathbb{Z}$, zu K; diese zusammen bilden den kleinsten Teilkörper von K, den sogenannten Primkörper in K. Er ist vermöge $z_1 1 \cdot (z_2 1)^{-1} \mapsto z_1/z_2$ isomorph zu $\mathbb{Q}$.

Falls es ein $n \neq 0$ mit $n1 = 0$ gibt, so können wir das kleinste solche $n \in \mathbb{N}$ wählen. Dieses n ist dann eine Primzahl p, und die Elemente $0, 1, 2 \cdot 1, \ldots, (p-1)1$ bilden den kleinsten Teilkörper in K. Vermöge $n1 \mapsto \overline{n}$, $0 \leq n \leq p-1$, ist dieser isomorph zu $\mathbb{F}_p$, dem Primkörper mit p Elementen, der aus $\mathbb{Z}$ dadurch entsteht, daß man die Gleichheit "$=$" durch "$\equiv \mod p$" ersetzt, also durch die neue modulo p - Gleichheit "$a \equiv b \mod p \iff p \mid a - b$" für $a, b \in \mathbb{Z}$ [4]. Damit gilt: $a + b \equiv c \mod p$ mit c als dem Rest von $a - b$ nach Division durch p; entsprechend $ab \equiv c \mod p$ mit c als dem Rest von ab nach Division durch p. In beiden Fällen ist also c eine natürliche Zahl zwischen 0 und $p - 1$. Dies beweist die Abgeschlossenheit von $\mathbb{Z}$ mit der neuen Gleichheit bei $+$ und $\cdot$. Daß es sich bei $\mathbb{F}_p$ tatsächlich um einen Körper handelt, also (M3) erfüllt ist, sieht man am einfachsten so: die Multiplikation mit $\overline{0} \neq \overline{z}$ ist eine injektive Selbstabbildung der endlichen Menge $\mathbb{F}_p$, also auch surjektiv und damit die Gleichung $\overline{z} \cdot \overline{x} = \overline{1}$ lösbar, i.e. $\overline{x} = (\overline{z})^{-1}$.

DEFINITION. *Ist $\mathbb{Q}$ der Primkörper in K, so sagen wir, daß K die Charakteristik 0 hat; ist $\mathbb{F}_p$ der Primkörper, so setzen wir* $\mathrm{char}(K) = p$.

[3] statt kommutativ sagt man auch abelsch

[4] $p \mid z$ heißt: p teilt die ganze Zahl z. Die neue Gleichheitsklasse der ganzen Zahl z wird mit $\overline{z}$ bezeichnet, also $\overline{z}_1 = \overline{z}_2 \iff z_1 \equiv z_2 \mod p$.

Es liege uns eine Körpererweiterung L/K vor, also ein Paar L, K von Körpern mit $L \supset K$, so daß $+, \cdot, 0, 1$ dasselbe in L und K bedeuten. Wir können L in natürlicher Weise als K-Vektorraum betrachten und sodann von der Dimension reden.

DEFINITION. $[L : K] = \dim_K L$ *heißt der Grad der Körpererweiterung* L/K. *Beachte, daß* $[L : K] = \infty$ *möglich ist.*

LEMMA. *Der Grad von Körpererweiterungen verhält sich multiplikativ* [5]*:*

$$[F : K] = [F : L][L : K]$$

für Körper $K \subset L \subset F$.

DEFINITION. L/K *sei eine Körpererweiterung und* $a \in L$. *Dann bezeichnet* $K(a)$ *den kleinsten in* L *gelegenen Körper, der* K *und* a *enthält, also* $K(a) = \bigcap k$, *der Duchschnitt genommen über alle Teilkörper* k *von* L, *die* K *und* a *enthalten. Des weiteren wird* a *algebraisch über* K *genannt, wenn* $[K(a) : K]$ *endlich ist, sonst transzendent.*

Beispiel: $L = \mathbb{C}, a = i = \sqrt{-1}, K = \mathbb{Q}$. Hier ist $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Für $a = \pi$ ist dagegen $[Q(\pi) : \mathbb{Q}] = \infty$, wie wir später noch sehen werden.

Wir beschreiben im folgenden $K(a)$. Sei zunächst $[K(a) : K] < \infty$. Ist $a \in K$, so ist $K(a) = K$. Ist $a \notin K$, also $1 \neq [K(a) : K] = n < \infty$, so existiert eine Gleichung $g(a) = \sum_{j=0}^{n_1} \alpha_j a^j = 0$ mit $n_1 > 1$ und $\alpha_{n_1} \neq 0$, denn $1, a, a^2, \ldots, a^n \in K(a)$ sind linear abhängig über K. Die Gleichung $f(a) = 0$ von kleinster Länge und mit $\alpha_{n_1} = 1$ ist eindeutig durch a und K bestimmt, weil das Polynom $f(x)$ (mit der Unbestimmten x anstelle von a) jedes Polynom $g(x)$ mit Koeffizienten aus K und mit Nullstelle a in L teilt; $f(x)$ ist insbesondere irreduzibel. Es folgt, daß der Grad von $f(x)$ gleich n ist und daß $K(a) = \{\sum_{j=0}^{n-1} \gamma_j a^j : \gamma_j \in K\}$ gilt. Die Irreduzibilität von $f(x)$ garantiert (M3) für $\{\sum_{j=0}^{n-1} \gamma_j a^j : \gamma_j \in K\}$. Nämlich: $\{\sum_{j=0}^{n-1} \gamma_j a^j : \gamma_j \in K\}$ ist ein K-Vektorraum der Dimension n und (dieser Schluß ist ähnlich dem vom Nachweis von (M3) für $\mathbb{F}_p$) die Multiplikation mit $b \stackrel{\text{def}}{=} \sum_{j=0}^{n-1} \beta_j a^j \neq 0$ ein injektiver K-Vektorraumendomorphismus von $\{\sum_{j=0}^{n-1} \gamma_j a^j : \gamma_j \in K\}$, also auch ein surjektiver, mithin ist die Gleichhung $b \cdot X = 1$ lösbar mit einem $X \in \{\sum_{j=0}^{n-1} \gamma_j a^j : \gamma_j \in K\}$ und $X = b^{-1}$. Schließlich ist die Darstellung eines Elementes aus $K(a)$ in der angegebenen Form eindeutig.

Sei nun a transzendent über K. Dann stimmen zwei endliche Summen $f(a) = \sum_{j=0}^{n_1} \alpha_j a^j$, $g(a) = \sum_{j=0}^{n_2} \beta_j a^j$ in $K(a) \subset L$ mit Koeffizienten $\alpha_j, \beta_j \in K$ nur überein, wenn $\alpha_j = \beta_j$ für alle j gilt. Die Menge aller dieser Summen (Polynome in a) bezeichnen wir mit $K[a]$ und erhalten einen K und a enthaltenden Teilring von L, der allerdings noch kein Körper ist: $a^{-1} \notin K[a]$. Offenbar gilt aber $K(a) = \{f(a)/g(a) : f(a), g(a) \in K[a], g \neq 0\}$ [6]. Dies ist der Körper der rationalen Funktionen in a über K.

Indem wir mit Polynomen in einer Unbestimmten und Koeffizienten aus einem Körper K irgendwie schon vertraut zu sein scheinen (wir erinnern in dem Zusammenhang etwa an die Theorie der Eigenwerte einer Matrix), können wir uns jetzt auch Körpererweiterungen konstruieren. Zum Beispiel den Körper $K(x)$ der rationalen Funktionen in einer Unbestimmten x. Oder, zu gegebenem irreduziblen Polynom $f(x)$ mit Koeffizienten aus K einen Erweiterungskörper $L = K(a)$ von K, der eine Nullstelle a von $f(x)$ enthält und von dieser über K aufgespannt wird. Das tun wir so: Setze $K(a) = \{\sum_{j=0}^{n-1} \gamma_j a^j : \gamma_j \in K\}$ mit

[5] bei vernünftiger Interpretation der Multiplikation mit ∞

[6] $g \neq 0$ bedeutet, daß das Polynom $g(a)$ einen von Null verschiedenen Koeffizienten besitzt.

n als dem Grad von $f(x)$ und identifiziere dabei die Summe $\sum_{j=0}^{n-1}\gamma_j a^j$ mit dem n-tupel $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})\in K\times\ldots\times K=K^n$, so daß $K(a)$ zunächst einmal eine wohldefinierte Menge ist. Wir addieren komponentenweise in K^n und multiplizieren $\sum_{j=0}^{n-1}\gamma_j a^j$ mit $\sum_{j=0}^{n-1}\delta_j a^j$ gemäß der Regel: Ist $g(x)=\sum_{j=0}^{n-1}\gamma_j x^j$ und $h(x)=\sum_{j=0}^{n-1}\delta_j x^j$, so berechne das Produkt der Polynome $g(x)$ und $h(x)$, dividiere das Ergebnis mit Rest $r(x)=\sum_{j=0}^{n-1}\theta_j x^j$ durch $f(x)$ und setze a für x in $r(x)$ ein; $r(a)$ ist dann das Produkt. Als Beispiel betrachte man $K=\mathbb{R}$ und $f(x)=x^2-2$ oder $f(x)=x^2+1$. Wir erhalten $\mathbb{R}(a)=\mathbb{R}$ im ersten und $\mathbb{R}(a)=\mathbb{C}$ im zweiten Fall.

Man beachte, daß obiges $K(a)$ zwar eine Wurzel von $f(x)$ enthält, aber im allgemeinen nicht alle, und daß mit dieser Konstruktion nicht zwischen den verschiedenen Wurzeln von $f(x)$ unterschieden werden kann. Dies führt notwendig dazu, nicht nur Erweiterungsköper L von K allein, sondern solche L zusammen mit K-Isomorphismen $\tau: L\to F$, $\tau(\alpha)=\alpha$ $(\forall\alpha\in K)$, in ausreichend große Erweiterungskörper F von K zu betrachten [7]. Unter F stellen wir uns am besten Körper vor, die K und alle Wurzeln von $f(x)$ enthalten (die es erst noch zu konstruieren gilt). Beispiel: Statt $\mathbb{C}/\mathbb{R}$ betrachten wir $\mathbb{C}$ zusammen mit dem Automorphismus $\tau:\alpha+i\beta\mapsto\alpha-i\beta$ als Erweiterungskörper von $\mathbb{R}$. Die Unbestimmtheit, welche Wurzel aus -1 wir mit i meinen, ist jetzt dadurch ausgeräumt, daß wir $\mathbb{C}$ durch das Paar $\mathbb{C},\tau$ ersetzt haben; wir reden sozusagen von i und $-i$ gleichzeitig; $\tau(i)=-i$.

2. Polynomringe; Grundsätzliches zu Homomorphismen und Faktorstrukturen

Es sei K ein Körper. Der Polynomring $R=K[x]$ in der Unbestimmten x über K ist als die Menge $\{g(x)=\sum_{j=0}^{d}\alpha_j x^j : d\in\mathbb{N},\ \alpha_j\in K\}$ definiert, die wir, ähnlich wie früher, mit $K^\infty=\{(\alpha_0,\alpha_1,\cdots):\alpha_i\in K,\ \text{fast alle } \alpha_i=0\}$ identifizieren. Addiert wird komponentenweise, multipliziert gemäß der Regel $(\sum_{j=0}^{d}\alpha_j x^j)(\sum_{k=0}^{m}\beta_k x^k)=\sum_{i=0}^{d+m}(\sum_{j+k=i}\alpha_j\beta_k)x^i$. Man sieht leicht, daß dadurch ein Ring entsteht (tatsächlich genügt es dafür, von K nur die Ringeigenschaft zu fordern). Ist $\alpha_d\neq 0$ in $g(x)$, so heißt d der Grad des Elementes oder Polynoms g; Bezeichnung: $\deg(g)=d$. Dem Nullelement oder Nullpolynom $0+0x+0x^2+\ldots$ wird kein Grad zugeordnet. Fundamental ist das

LEMMA. *1. Das Produkt zweier Polynome $\neq 0$ ist $\neq 0$.*

2. $\deg(g_1\cdot g_2)=\deg(g_1)+\deg(g_2)$

3. Zu vorgegebenen Polynomen g und $h\neq 0$ existieren Polynome v,r mit

$$g=v\cdot h+r\,,\ r=0 \text{ oder } \deg(r)<\deg(h)\,.$$

Der Beweis von 1. und 2. nützt von K nur die Nullteilerfreiheit aus, also die Eigenschaft $[\,\alpha\beta=0\Longrightarrow\alpha=0 \text{ oder } \beta=0\,]$ [8], der Beweis von 3. die Tatsache, daß der höchste Koeffizient von h, also der mit Index $\deg(h)$, in K invertierbar ist. Die Eigenschaft 3. wird auch als Euklidischer Algorithmus bezeichnet.

Beschäftigt man sich mit Körpern, Ringen oder Gruppen, so muß man immer auch Homomorphismen zwischen den jeweiligen Strukturen betrachten, weil deren Vielfalt einen guten

[7] τ heißt Isomorphismus, wenn $\tau\neq 0$ und $\tau(a\dot{+}b)=\tau(a)\dot{+}\tau(b)$ für alle $a,b\in K$ gilt. Solche τ sind wegen $\tau(aa^{-1})=\tau(1)=1$ automatisch injektiv.

[8] das ist nicht unbedingt in jedem Ring wahr – man denke etwa an Matrizenringe

Einblick in diese Strukturen vermittelt. Ein Homomorphismus ϕ ist eine Abbildung zwischen zwei Körpern, zwei Ringen oder zwei Gruppen, der die jeweiligen Stukturen respektiert, i.e., $\phi(a+b) = \phi(a) + \phi(b)$ und (bzw.) $\phi(ab) = \phi(a)\phi(b)$. Der Homomorphismus ϕ heißt Epimorphismus, falls er surjektiv (auf), Monomorphismus, falls er injektiv (eineindeutig) ist und Endomorphismus, falls Urbild- und Zielbereich übereinstimmen. Ein injektiver und surjektiver, also bijektiver, Endomorphismus wird Automorphismus genannt; bijektive Homomorphismen heißen Isomorphismen. Das alles ist analog zur Sprache der linearen Algebra – mit einem Unterschied: wir reden auch schon von Isomorphismen $\tau : L \to F$ zwischen Körpern L und F, wenn wir nur injektive Homomorphismen meinen.

Beobachtungen:

$\phi(-a) = -\phi(a)\,,\ \phi(a^{-1}) = \phi(a)^{-1}$ für Homomorphismen ϕ (von Gruppen),

ist ϕ ein Isomorphismus (zwischen Gruppen oder Ringen), so auch die Umkehrabbildung ϕ^{-1}.

DEFINITION. *$\phi : R \to S$ sei ein Homomorphismus zwischen Körpern, Ringen oder Gruppen. Dann sei* $\mathrm{im}\,(\phi) \stackrel{\text{def}}{=} \{\phi(r) : r \in R\} \subset S$ *und* $\ker(\phi) \stackrel{\text{def}}{=} \{r \in R : \phi(r) = 0\} \subset R$ [9].

Beides, das Bild $\mathrm{im}\,(\phi)$ und der Kern $\ker(\phi)$ von ϕ sind Unterstrukturen, also wieder Körper (es sei denn $\phi = 0$), Ringe bzw. Gruppen. Für den Kern gilt jedoch mehr.

LEMMA. 1. *Ist R ein Körper, so ist* $\ker(\phi) = 0$ *oder* $= R$.

2. *Ist R ein Ring, so ist* $\ker(\phi)$ *ein Ideal $\mathfrak{a}$ in R, also eine Teilmenge, die abgeschlossen unter $\pm$ ist, die Null enthält und folgendes Gesetz erfüllt:*

$$a \in \mathfrak{a}\ \&\ r \in R \Longrightarrow ra \in \mathfrak{a}\,.$$

Wir notieren die Idealeigenschsft von $\mathfrak{a}$ so: $\mathfrak{a} \lhd R$.

3. *Ist R eine (multiplikativ geschriebene) Gruppe, so ist* $\ker(\phi)$ *ein Normalteiler in R, das ist eine Untergruppe mit der zusätzlichen Eigenschaft*

$$a \in \ker(\phi)\ \&\ r \in R \Longrightarrow r^{-1}ar \in \ker(\phi)\,.$$

Wir notieren die Normalteilereigenschsft von $\ker(\phi)$ *so:* $\ker(\phi) \lhd G$ [10].

In jedem Fall gilt: $\phi(x) = \phi(y) \iff x - y \in \ker(\phi)$ bzw. $xy^{-1} \in \ker(\phi)\,.$

Für Gruppen rufe man sich an dieser Stelle die Vorzeichenabbildung sign: $S_n \to \{\pm 1\}$ mit Kern A_n, der alternierenden Gruppe, ins Gedächtnis.

Ideale $\mathfrak{a}$ bei Ringen R, und Normalteiler N bei Gruppen G, führen zu neuen Ringen $R/\mathfrak{a}$, bzw. neuen Gruppen G/N. Nämlich so: man vergröbert die Gleichheit in R (in G) zu

$$r \equiv s \bmod \mathfrak{a} \stackrel{\text{def}}{\iff} r - s \in \mathfrak{a} \quad \text{bzw.} \quad g \equiv h \bmod N \stackrel{\text{def}}{\iff} gh^{-1} \in N \quad [11]$$

[9] Sind R, S multiplikativ geschriebene Gruppen, so ist die letzte Gleichheit durch $\ker(\phi) = \{r \in R : \phi(r) = 1\}$ abzuändern.

[10] Die Untergruppeneigenschaft einer Teilmenge U einer Gruppe G wird dagegen so notiert: $U \leq G$.

[11] lies: kongruent ... modulo

und stellt fest, daß

$$r_i \equiv s_i \bmod \mathfrak{a}\ (i=1,2) \Longrightarrow r_1 \dot{+} r_2 \equiv s_1 \dot{+} s_2 \bmod \mathfrak{a}$$

und, entsprechend,

$$g_i \equiv h_i \bmod N \Longrightarrow g_1 g_2 \equiv h_1 h_2 \bmod N$$

gilt. Die neue Gleichheit "$\equiv$" ist eine Äquivalenzrelation. Die Menge der Äquivalenzklassen wird mit $\overline{R}$ oder $R/\mathfrak{a}$, bzw. $\overline{G}$ oder G/N, bezeichnet und trägt aufgrund der obigen Eigenschaften auf natürliche Weise eine Ring-, bzw. Gruppenstruktur. Und $\psi : R \to R/\mathfrak{a}, r \mapsto \overline{r}$ (mit $\overline{r}$ als der Äquivalenzklasse von r) ist ein Epimorphismus mit Kern $\mathfrak{a}$. Entsprechend für Gruppen. Wir nennen dieses ψ die kanonische Abbildung von R auf $\overline{R}$. Wieder sei hier an die analoge Konstruktion bei Faktorräumen von Vektorräumen hingewiesen.

DEFINITION. *Eine Teilmenge P von R (von G), in der je zwei Elemente inkongruent modulo $\mathfrak{a}$ (modulo N) sind, und die zu jedem $r \in R$ ($r \in G$) ein modulo $\mathfrak{a}$ (modulo N) kongruentes Element enthält, heißt ein vollständiges Repräsentantensystem modulo $\mathfrak{a}$ (modulo N).*

Als Beispiel wähle man etwa $P = \{0, 1, 2, \ldots, n-1\}$ für $\mathfrak{a} = \mathbb{Z} \cdot n = \{zn : z \in \mathbb{Z}\} \lhd \mathbb{Z}$ im Ring $\mathbb{Z}$ der ganzen Zahlen.

SATZ 1. *1. $\phi : R \to S$ sei ein Homomorphismus von Ringen mit Kern $\mathfrak{a}$. Dann faktorisiert ϕ durch $R/\mathfrak{a}$ über ψ:*

$$\phi_1\psi : R \xrightarrow{\psi} R/\mathfrak{a} \overset{\phi_1}{\rightarrowtail} S \text{ ist dasselbe wie } \phi\ .$$

Hierbei ist $\phi_1(\overline{r}) = \phi(r)$ ein durch ϕ allein bestimmter Monomorphismus.

2. $\phi : G \to H$ sei ein Homomorphismus von Gruppen mit Kern N. Dann faktorisiert ϕ durch G/N über ψ:

$$\phi_1\psi : G \xrightarrow{\psi} G/N \overset{\phi_1}{\rightarrowtail} H \text{ ist dasselbe wie } \phi\ .$$

Hierbei ist $\phi_1(\overline{g}) = \phi(g)$ ein durch ϕ allein bestimmter Monomorphismus.

SATZ 2. *1. Ist $\mathfrak{a}$ ein Ideal im Ring R und ψ der zugehörige kanonische Epimorphismus $R \twoheadrightarrow R/\mathfrak{a}$, so entsprechen die Ideale $\mathfrak{b}$ zwischen $\mathfrak{a}$ und R eineindeutig denen, I, von $R/\mathfrak{a}$:*

$$\mathfrak{b} \mapsto \{\psi(r) : r \in \mathfrak{b}\} = I \quad , \quad I \mapsto \{r \in R : \psi(r) \in I\} = \mathfrak{b}$$

ist eine umkehrbar eindeutige Korrespondenz mit $R/\mathfrak{b} \simeq \overline{R}/I$, $[r \bmod \mathfrak{b}] \mapsto [\overline{r} \bmod I]$, wenn $\mathfrak{b}$ und I wie oben zusammengehören.

2. Ist N ein Normalteiler der Gruppe G und ψ der zugehörige kanonische Epimorphismus $G \twoheadrightarrow G/N$, so entsprechen die Untergruppen U zwischen N und G eineindeutig denen, V, von G/N:

$$U \mapsto \{\psi(g) : g \in U\} = V \quad , \quad V \mapsto \{g \in G : \psi(g) \in V\} = U$$

ist eine umkehrbar eindeutige Korrespondenz, die Normalteiler in Normalteiler überführt und außerdem für solche $G/U \simeq \overline{G}/V$, $[g \bmod U] \mapsto [\overline{g} \bmod V]$ erfüllt, wenn U und V wie oben zusammengehören (und U also ein Normalteiler in G ist).

Wir werden später noch weitere Eigenschaften kennenlernen. Jetzt aber kehren wir erst einmal zurück zum Polynomring $K[x]$ und interessieren uns für dessen Ideale. Dank des Euklidischen Algorithmus haben wir

SATZ 3. *Die Ideale $\mathfrak{a}$ von $R = K[x]$ sind allesamt Hauptideale, d.h. von der Form $Rg = \{rg : r \in R\}$. Genauer: ist $\mathfrak{a} \neq 0$, so gilt $\mathfrak{a} = Rg$ mit dem normierten Polynom $g \in \mathfrak{a}$ von kleinstem Grad* [12]. *Ist $g \neq 0$, so gilt $[\, Rg = Rg_1 \iff g = \alpha \cdot g_1$ mit einem $0 \neq \alpha \in K\,]$. Der Faktorring $R/g \stackrel{\text{def}}{=} R/Rg$ besitzt in den Polynomen vom Grad $< \deg(g)$ ein vollständiges Repräsentantensystem. Er ist nullteilerfrei, genau wenn $g = 0$ oder g ein irreduzibles Polynom ist (also ein Polynom ohne Teiler vom Grad zwischen 1 und $\deg(g)$). Im letzteren Fall ist R/g ein Körper.*

In diesem Zusammenhang:

$K[x]$ ist ein ZPE-Ring [13], d.h. das jedes $0 \neq g \in K[x]$ bis auf Faktoren $\in K^\times$ (den konstanten Polynomen $\neq 0$) eindeutig als Produkt von irreduziblen Polynomen darstellbar ist. Die Einheiten in $K[x]$, das sind die invertieren Elemente dieses Ringes, sind genau die konstanten Polynome $\neq 0$. Schließlich: Sind $f, g \in K[x]$ teilerfremd zueinander, haben also nur konstante Polynome $\neq 0$ als gemeinsame Teiler, so existieren Polynome $s, t \in K[x]$ mit $sf + tg = 1$.

Der Ring $\mathbb{Z}$ hat die gleiche Eigenschaft: alle Ideale sind Hauptideale; $\mathbb{Z}/m$ ist nullteilerfrei $\iff$ $m = 0$ oder $m = p$, eine Primzahl; $\mathbb{Z}/p$ ist ein Körper (nämlich $= \mathbb{F}_p$). $\mathbb{Z}$ ist ZPE; die Einheiten in $\mathbb{Z}$ sind $\{\pm 1\}$.

Der Polynomring $\mathbb{Z}[x]$ ist kein Hauptidealring (z.B. ist $\{3g + xh : g, h \in \mathbb{Z}[x]\}$ ein Ideal, aber kein Hauptideal). Aber $\mathbb{Z}[x]$ ist noch ZPE, wie wir gelegentlich sehen werden.

Ideale $\mathfrak{a}$ eines Ringes R mit $R/\mathfrak{a}$ nullteilerfrei heißen Primideale und die, für die $R/\mathfrak{a}$ sogar ein Körper ist, sind genau die maximalen (bez. $\subset$) Ideale ($\neq R$) von R.

Für einen Erweiterungskörper L von K erhalten wir die natürliche Inklusion $K[x] \subset L[x]$. Sei nun $a \in L$ vorgegeben.

LEMMA. *Die Abbildung $K[x] \to L$, $g(x) = \sum_{j=0}^{d} \alpha_j x^j \mapsto g(a) = \sum_{j=0}^{d} \alpha_j a^j$ ist ein Homomorphismus von Ringen.*

Eine unmittelbare Folgerung daraus und dem Euklidischen Algorithmus ist

$$a \in L \text{ ist Nullstelle von } g(x) \in K[x] \iff x - a \mid g(x) \text{ in } L[x]$$

und

$$g(x) \text{ hat höchstens } \deg(g) \text{ verschiedene Nullstellen in } L\,.$$

DEFINITION. *Das Polynom $f(x) \in K[x]$ heißt separabel, wenn es keine mehrfache Nullstelle in beliebigen Erweiterungskörpern L von K besitzt.*

[12] normiert heißt, daß der höchste Koeffizient $=1$ ist

[13] ZPE steht für eindeutige Primfaktorzerlegung

Nun kennen wir längst nicht alle Erweiterungen L/K. Ein Separabilitätstest für f kann aber trotzdem durchgeführt werden.

LEMMA. *$f'(x)$ bezeichne die formale Ableitung von $f(x)$, also $f'(x) = \sum_{j=1}^{m} j\alpha_j x^{j-1}$ wenn $f(x) = \sum_{j=0}^{m} \alpha_j x^j$. Es gilt: f(x) ist separabel $\iff$ $\mathrm{ggT}(f, f') = 1$.*

Dabei ist der größte gemeinsame Teiler d zweier Polynome f, g so definiert:

$$d \mid f\,,\ d \mid g\,;\ \text{gilt auch } d_1 \mid f\,,\ d_1 \mid g \text{ für ein } d_1 \in K[x]\,,\ \text{so folgt } d_1 \mid d\,.$$

Man beachte, daß damit der größte gemeinsame Teiler nur bis auf Einheiten, also Elementen aus $K^\times$, bestimmt ist [14].

FOLGERUNG. *Irreduzible Polynome sind separabel, wenn $char(K) = 0$ oder wenn K ein endlicher Körper ist.*

Für endliches K mit Charakteristik p ist nämlich

$$K \to K\,,\ a \mapsto a^p$$

ein Automorphismus [15] und daher jedes Polynom in x^p schon p-te Potenz eines Polynoms in x.

Beispiel: Sei $K = \mathbb{F}_2(x)$ der rationale Funktionenkörper in der Variablen x über dem Körper $\mathbb{F}_2 = \mathbb{Z}/2$. Dann ist $f(X) = X^2 - x \in K[X]$ ein irreduzibles Polynom (in X), weil $\sqrt{x} \notin K$. Es ist inseparabel, weil es keine Vorzeichen in Charakteristik 2 gibt: $+1 = -1$.

Vielleicht ist das Ende dieses Kapitels ein guter Ort, wenigstens etwas darüber zu sagen, was Algebra ist und wo Algebra gebraucht wird.

Algebra ist zunächst die Lehre von den algebraischen Strukturen, also von Mengen mit Strukturen, die von $+$ und/oder $\cdot$ herrühren, z.B. Gruppen, Ringe oder Körper. Die Strukturen müssen dabei nicht unbedingt kommutativ sein. Besonders geht es dabei um das Studium von algebraischen Gleichungen, d.h. von Gleichungen, in denen Parameter und Unbekannte durch die vier Grundrechenarten $+, -, \cdot, /$ verknüpft sind. Einfachstes Beispiel sind Polynome in einer Variablen mit Koeffizienten aus einem Körper K. Gleichungen werden allerdings selten allein für sich betrachtet, sondern in aller Regel im Zusammenhang mit den durch sie erzeugten Strukturen, wie etwa die algebraischen Körpererweiterungen L/K im Kontext der Nullstellen von Polynomen einer Variablen und mit Koeffizienten aus K. Gruppen kommen dann automatisch mit in die Diskussion, indem man nämlich Symmetrieeigenschaften der zu studierenden Objekten beobachtet, wie z.B. die möglichen Beziehungen der Wurzeln eines irreduziblen Polynoms untereinander. Und Ringe bilden sozusagen die Bühne für alles: sie führen zu Körpern durch Restklassenbildung; sie erlauben ein intensives Studium von Gruppen (Stichwort *Gruppenringe*), indem deren Struktur gegen die bekannter Ringe (wie $\mathbb{Z}$) oder Körper (wie $\mathbb{C}$ oder $\mathbb{F}_p$) ausgespielt wird (*Darstellungstheorie*).

Die Algebra zerfällt in viele Spezialgebiete – so ist die *Gruppentheorie*, die unter anderem eine Klassifizierung aller möglichen endlichen Gruppen zum Ziel hat, ein eigenständiges Teilgebiet der Algebra.

[14] Analog zu einer Darstellung $sf + tg = 1$ der 1 im Falle *zueinander teilerfremder* Polynome f, g findet man im allgemeinen Fall: $\exists\, s, t \in K[x] : sf + tg = d = \mathrm{ggT}(f, g)$.

[15] denn:

1. $(a+b)^p = a^p + b^p$ weil ein Binomialkoeffizient $\binom{p}{i}$ für $0 < i < p$ durch p teilbar ist
2. $a^p = 0 \Longrightarrow a = 0$
3. $a \mapsto a^p$ ist injektiv, also surjektiv, auf dem endlichen K

Bedeutende andere sind die *Zahlentheorie*, deren Basisdaten algebraische Gleichungen mit rationalen oder gar ganzrationalen Koeffizienten sind, die *algebraische Geometrie*, in der geometrische Methoden zur Behandlung von algebraischen Gleichungen herangezogen werden, die *arithmetische Geometrie*, eine Kombination aus Zahlentheorie und algebraischer Geometrie, aus der übrigens die tiefsten zahlentheoretischen Resultate des letzten halben Jahrhunderts stammen (und dies wohl nicht zuletzt deshalb, weil in ihr algebraische Objekte mit analytischen, etwa L-Reihen und deren spezielle Werte, verglichen werden und es dabei zu ganz neuen Fragestellungen und Erkenntnissen kommt).

Da sich in der Mathematik das Arbeiten in und mit Strukturen bewährt hat, ist inzwischen Algebra ein wichtiger Bestandteil der gesamten Mathematik. Sie ist darüber hinaus wichtig für die Anwendungen geworden. So haben aufgrund der Suche nach sicher arbeitenden Verschlüsselungen etwa von Telekommunikationsdaten zahlentheoretische Ergebnisse Bedeutung erlangt: ihr entstammen die besten Algorithmen. Auch findet die Zahlentheorie Anwendung in der Schwingungslehre (Akustik). Gruppentheorie ist in der Physik im Zusammenhang mit der Beschreibung von Teilchenbewegungen nützlich und die Darstellungstheorie zum Beispiel für das Studium von Kristallen. Die Informatik baut gern abstrakte, wohlverstandene Strukturen in ihre Designtheorien ein – nicht bloß endliche Körper oder endliche Geometrien. Schon die wenigen hier aufgezählten Beispiele legen nahe, daß die Bedeutung der Algebra und ihrer Spezialgebiete für die Anwendungen in der Zukunft wohl weiter anwachsen wird. [16]

3. Galoistheorie

In diesem Kapitel ist ein Grundkörper K fixiert.

DEFINITION. 1. *Ist L/K eine Körpererweiterung und $\beta \in L$ ein über K algebraisches Element, so sei $f_\beta(x) \in K[x]$ das normierte Polynom kleinsten Grades in $K[x]$ mit Nullstelle β. Es wird das Minimalpolynom von β (über K) genannt.*

2. *Wir nennen ein Element $\beta \in L$ separabel über K, wenn es algebraisch über K mit separablem Minimalpolynom ist. L heißt algebraisch (bzw. separabel) über K, wenn jedes Element aus L algebraisch (bzw. separabel) über K ist.*

LEMMA. 1. *f_β ist irreduzibel und teilt jedes Polynom $g(x) \in K[x]$ mit Nullstelle β.*

2. *Sind $K \subset L_1 \subset L$ Körper und ist L/K algebraisch, so auch L/L_1 und L_1/K. Sind L_1/K und L/L_1 algebraisch, so auch L/K.*

3. *Ist L/K eine Körpererweiterung, so sind Summen, Differenzen, Produkte, Quotienten von über K algebraischen Elementen aus L algebraisch über K.*

Erinnerung: Ist $f(x) \in K[x]$ mit $\deg(f) > 0$ vorgegeben, so können wir wie folgt einen Erweiterungskörper L von K konstruieren, der von einer Wurzel (Nullstelle) von f über K erzeugt ist. Sei $p(x)$ ein (normierter) irreduzibler Teiler von f (insbesondere ist $\deg(p) > 0$). Jede Wurzel von p ist auch Wurzel von f. Bilde $K[x]/p(x)$. Dies ist ein Körper L, in dem wir K als Teilkörper über den Monomorphismus $K \rightarrowtail K[x] \to K[x]/p(x) = L$ auffassen. Offenbar ist $p(\overline{x}) = 0$ in L, wenn $\overline{x}$ das Bild von x in L ist, und also hat p, und damit f, eine Wurzel in L. Durch Iteration erhalten wir so Körper F/K, in denen alle Wurzeln von f liegen, so daß also $f(x)$ in $F[x]$ vollständig in Linearfaktoren zerfällt.

Im folgenden sei $f(x) \in K[x]$ irreduzibel und normiert [17]. Zu f bilden wir wie oben L: also $L = K(\omega)$ mit $f(\omega) = 0$. Des weiteren wählen wir irgendeine Körpererweiterung F/L, die alle

[16] Vergleiche z.B. Niederreiter/Xing, *Rational points on curves over finite fields: theory and applications*, LMS Lecture Note Series 285 (2001); Schroeder, *Number theory in science and communication*, Springer (1986); Brown/Bülow/Neubüser/Wondratschek/Zassenhaus, *Crystallographic groups of 4-dimensional space*, Wiley (1978)

[17] die Normiertheit ist tatsächlich keine Einschränkung

Wurzeln von f enthalte. Dann existieren K-Isomorphismen $\sigma : L \to F$, also Monomorphismen mit $\sigma(\alpha) = \alpha$ $(\forall \alpha \in K)$: denn ist $\tilde{\omega}$ eine Wurzel von f in F, so definiere einfach $\sigma(\omega) = \tilde{\omega}$, $\sigma(\alpha) = \alpha$. Das σ stiftet einen Isomorphismus $L = K(\omega) \simeq K(\tilde{\omega}) \subset F$ [18]. Wieviele solche σ gibt es? Wegen $f(\sigma(\omega)) = 0$, genauso viele, wie f verschiedene Wurzeln (in F) hat, also höchstens $\deg(f)$ viele und $= \deg(f)$ viele, nur wenn f separabel ist. Man beachte in dem Zusammenhang, daß die Vielfachheit ν einer Wurzel ω von f nicht von F abhängt:

$$K(\omega) \subset F \;\&\; f(x) = (x-\omega)^\nu g(x) \in K(\omega)[x]\,,\; g(\omega) \neq 0\,.$$

Nun sei L/K eine Körpererweiterung von endlichem Grad $[L : K] = n < \infty$. Dann gibt es Elemente $\omega_1, \ldots, \omega_r$ in L mit $L = K(\omega_1, \ldots, \omega_r) = K(\omega_1)(\omega_2, \ldots, \omega_r)$. Es seien $f_i(x) \in K[x]$ die Minimalpolynome der ω_i. Schließlich sei F/L eine Körpererweiterung, die alle Wurzeln aller f_i enthalte.

DEFINITION. *$I(L/K) = I_F(L/K) = \{\sigma : L \rightarrowtail F : \sigma(\alpha) = \alpha \;(\forall \alpha \in K)\}$ heißt die Isomorphismenmenge von L/K (bezüglich F).*

LEMMA. *1. Ist L_1 ein Zwischenkörper in L/K, also $K \subset L_1 \subset L$, so läßt sich jedes $\sigma_1 \in I(L_1/K)$ zu einem $\sigma \in I(L/K)$ fortsetzen, d.h. $\exists\, \sigma \in I(L/K) : \sigma_{|L_1} = \sigma_1$.*

2. $I(L/K)$ hat höchstens $[L : K]$ viele Elemente und genau $= [L : K]$ viele, wenn L/K separabel ist. Diese Aussage ist unabhängig von der speziellen Wahl von F.

Eine wichtige Folgerung ist diese

FOLGERUNG. *Sind $\beta_1, 0 \neq \beta_2 \in L$ separabel über K, so auch $\beta_1 \circ \beta_2$ mit $\circ = +, -, \cdot, /$. In der Situation $K \subset L_1 \subset L$ gilt: Ist L/K separabel, so auch L_1/K; sind L_1/K und L/L_1 separabel, so auch L/K.*

DEFINITION. *Die endliche Körpererweiterung L/K heißt galoissch, wenn sie separabel ist und wenn $\sigma(L) = L$ für alle $\sigma \in I(L/K)$ gilt. In diesem Fall ist $I(L/K)$ eine Gruppe der Ordnung $[L : K]$ [19], die mit $G_{L/K}$ bezeichnet wird.*

Dem nächsten Satz, dem sogenannten Hauptsatz der Galoistheorie, der allerdings erst durch seine vielen Folgerungen richtig lebendig werden wird, stellen wir noch ein technisches, aber sehr nützliches Lemma voran.

LEMMA. (Artin) *Ist L/K endlich, so sind die Elemente $\tau \in I(L/K)$ linear unabhängig über F, d.h. $\sum_{\tau \in I(L/K)} \gamma_\tau \tau(\lambda) = 0$ für alle $\lambda \in L$ und gewisse Koeffizienten $\gamma_\tau \in F$ impliziert, daß diese γ_τ alle $= 0$ sind.*

SATZ 4. *L/K sei galoissch mit Gruppe $G = G_{L/K}$. Die Zwischenkörper Z, $K \subset Z \subset L$, entsprechen eineindeutig den Untergruppen U von G, nämlich*

$$Z \leftrightarrow U \iff U = \{\tau \in G : \tau(z) = z \;(\forall z \in Z)\}\,,\; Z = \{\lambda \in L : \tau(\lambda) = \lambda \;(\forall \tau \in U)\}\,.$$

Insbesondere ist L galoissch über jedem Z und das zugehörige U ist $= G_{L/Z}$. Hinwiederum ist Z genau dann galoissch über K, wenn $U = G_{L/Z}$ ein Normalteiler in G ist; es gilt dann $G_{Z/K} \simeq G/G_{L/Z}$ (kanonisch). Und:

$$\begin{aligned} &Z_1 \subset Z_2 \iff G_{L/Z_1} \supset G_{L/Z_2} \\ &G_{L/Z_1 \cap Z_2} = \bigcap\{U \leq G : U \supset G_{L/Z_1}, G_{L/Z_2}\} \\ &U_1 \cap U_2 \text{ gehört zu } \bigcap\{Z : K \subset Z \subset L\,,\; Z \supset Z_1, Z_2\}\,. \end{aligned}$$

[18] $*_1 \simeq *_2$ ist kurz für: es gibt einen (surjektiven) Isomorphismus zwischen den Strukturen $*_1, *_2$

[19] die Ordnung $|G|$ einer Gruppe G ist die Anzahl der Elenente in G

Beachte, daß Satz 4 das i. allg. unendliche Datum L/K durch das endliche Datum $G_{L/K}$ beschreibt.

FOLGERUNG. *1. Ist L/K separabel* [20] *, so existiert ein $\lambda \in L$ mit $L = K(\lambda)$* ("Satz vom primitiven Element") *. Des weiteren: Es gibt eine bis auf K-Isomorphie eindeutig bestimmte galoissche Erweiterung $\tilde{L}/K$, die L enthält und die in jeder galoisschen Erweiterung L'/K mit $L \subset L'$ enthalten ist; sie heißt die galoissche Hülle von L über K.*

2. Ist L/K galoissch, so existiert ein $\lambda \in L$ so, daß $\{\tau(\lambda) : \tau \in G_{L/K}\}$ eine K-Basis von L ist ("Satz von der Normalbasis") *.*

3. L/K galoissch $\iff$ L ist von den Wurzeln eines separablen Polynoms $f(x) \in K[x]$ erzeugt und enthält alle Wurzeln von $f(x)$.

4. Ist L ein Körper und G eine endliche Gruppe von Automorphismen von L, so ist L galoissch mit Gruppe G über

$$K = L^G \stackrel{\text{def}}{=} \{\lambda \in L : \tau(\lambda) = \lambda \ (\forall \tau \in G)\} .$$

DEFINITION. *Ist L/K eine endliche Körpererweiterung und $f(x) \in K[x]$ so, daß $f(x) = \prod_{i=1}^{n}(x - \omega_i)$ mit $\omega_i \in L$ und $L = K(\omega_1, \ldots, \omega_n)$ gilt, so heißt L Zerfällungskörper von $f(x)$ über K.*

Beachte, daß dieser bis auf K-Isomorphie eindeutig durch K und f bestimmt ist. *Galoissche Erweiterungen L/K sind also genau die Zerfällungskörper der separablen Polynome aus $K[x]$.* Und: ist L/K separabel und etwa $L = K(\lambda)$, so ist (die galoissche Hülle von L über K) $\tilde{L}$ der Zerfällungskörper von $f_\lambda(x) \in K[x]$. Die Galoisgruppe $G_{\tilde{L}/K}$ besteht aus Permutationen der Wurzeln von f_λ und ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_d mit $d = \deg(f_\lambda)$.

Im folgenden seien L_1, L_2 zwei Erweiterungskörper von K von endlichem Grad, beide enthalten in einem Körper $\tilde{K}$. L_1L_2 bezeichne den kleinsten in $\tilde{K}$ gelegenen Körper, der L_1 und L_2 enthält.

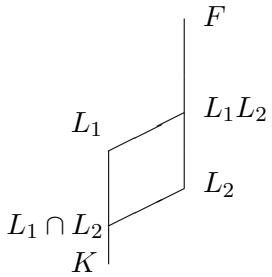
LEMMA. *1. Ist L_1/K separabel und gilt $L_1 = K(\lambda_1)$, so ist L_1L_2/L_2 auch separabel und $L_1L_2 = L_2(\lambda_1)$.*

2. (Translationssatz) *Ist L_1 galoissch über K mit Gruppe G_1, so ist L_1L_2/L_2 galoissch über L_2 und $G_{L_1L_2/L_2} \simeq G_{L_1/L_1\cap L_2}$. Der Isomorphismus wird von*

$$G_{L_1L_2/L_2} \ni \sigma \mapsto \sigma_{|L_1} \in G_{L_1/K}$$

vermittelt.

3. Sind L_1 und L_2 galoissch über K mit Gruppen G_1 bzw. G_2, so ist auch L_1L_2 galoissch über K und $G_{L_1L_2/K}$ ist (über die natürlichen Restriktionsabbildungen) kanonisch isomorph zu einer Untergruppe von $G_1 \times G_2$.



[20] Erinnerung: wir betrachten nur endlichen Grad $[L : K]$.

FOLGERUNG. *Unter der Voraussetzung 2. des obigen Lemmas gilt* $[L_1L_2 : L_2] \Big| [L_1 : K]$.

Dies ist ohne 2. i. allg. allerdings falsch: $K = \mathbb{Q}$, $L_1 = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $L_2 = \mathbb{Q}(\alpha)$ mit einer nichtreellen Wurzel α von $x^3 - 2$; also $[L_1L_2 : L_2] = 2 \nmid 3 = [L_1 : \mathbb{Q}]$.

Wir fahren mit der Definition zweier Abbidungen zu einer endlichen Körpererweiterung L/K fort, der Spur und der Norm, welche sich im folgenden oft als wertvolle Werkzeuge erweisen werden und die im galoisschen Fall besonders leicht zu beschreiben sind.

DEFINITION. *L/K sei eine endliche Körpererweiterung und $\lambda \in L$. Die von λ vermittelte K-lineare Abbildung $L \to L$, $\alpha \mapsto \lambda\alpha$, heiße m_λ. Es sei*

$$\mathrm{Sp}(\lambda) = \mathrm{Sp}_{L/K}(\lambda) = \text{Spur der Abbildung } m_\lambda$$
$$\mathrm{N}(\lambda) = \mathrm{N}_{L/K}(\lambda) = \text{Determinante der Abbildung } m_\lambda .$$

LEMMA. *1.* $\mathrm{Sp}_{L/K} : L \to K$ *ist eine Linearform.*

2. $\mathrm{N}_{L/K}(\lambda) = 0 \iff \lambda = 0$; $\mathrm{N}_{L/K}(\lambda) = \lambda^{[L:K]}$ *für* $\lambda \in K$
$\mathrm{N}_{L/K} : L^\times \to K^\times$ *ist multiplikativ.*

3. Ist L_1 ein Zwischenkörper in L/K, so gilt

$$\mathrm{Sp}_{L/K} = \mathrm{Sp}_{L_1/K} \circ \mathrm{Sp}_{L/L_1} \quad \mathrm{N}_{L/K} = \mathrm{N}_{L_1/K} \circ \mathrm{N}_{L/L_1} .$$

4. $\mathrm{Sp}_{L/K}$ *ist genau dann die Nullabbildung, wenn L inseparabel über K ist.*

Die letzte Behauptung resultiert dabei so: Ist M/K die größte separable Teilerweiterung in L/K (i.e., M ist die Menge aller über K separablen Elemente von L), so gilt im Falle $L \neq M$, daß $\mathrm{char}(K) = p \neq 0$ und $[L : M]$ eine p-Potenz ist. Ist aber L/K separabel, so kann Artins Lemma zusammen mit $\mathrm{Sp}_{L/K}(\lambda) = \sum_{\sigma \in I(L/K)} \sigma(\lambda)$ angewandt werden [21].

FOLGERUNG. *a. Ist L/K galoissch mit Gruppe $G = G_{L/K}$, so gilt*

$$\mathrm{Sp}_{L/K}(\lambda) = \sum_{\sigma \in G} \sigma(\lambda) , \ \mathrm{N}_{L/K}(\lambda) = \prod_{\sigma \in G} \sigma(\lambda) \ \ (\forall \lambda \in L) .$$

b. Ist L/K separabel, so definiert

$$L \times L \to K , \ (\lambda_1, \lambda_2) \mapsto \mathrm{Sp}(\lambda_1\lambda_2)$$

eine nichtausgeartete K-Bilinearform auf L, die $G_{L/K}$-invariant im Falle einer galoisschen Erweiterung L/K ist: $(\sigma(\lambda_1), \sigma(\lambda_2)) = (\lambda_1, \lambda_2)$ $(\forall \sigma \in G_{L/K})$.

Der algebraische Abschluß K^{c} eines Körpers K :

SATZ 5. *Zu K existiert ein bis auf K-Isomorphie endeutig bestimmter Körper $K^{\mathrm{c}} \supset K$, der über K algebraisch ist und über dem jedes Polynom $\in K^{\mathrm{c}}[x]$ vollständig zerfällt. K^{c} heißt der algebraische Abschluß von K.*

[21] analog $\mathrm{N}_{L/K}(\lambda) = \prod_{\sigma \in I(L/K)} \sigma(\lambda)$

Das einfachste Beispiel ist $K = \mathbb{R}$, $K^c = \mathbb{C}$ – obwohl wir tatsächlich noch gar nicht wissen, daß $\mathbb{C}$ *algebraisch abgeschlossen* ist, daß also jedes Polynom $\in \mathbb{C}[x]$ über $\mathbb{C}$ vollständig zerfällt. Mit K^c läßt sich $I(L/K)$ eleganter so schreiben: $I(L/K) = \{\sigma \mid \sigma : L \to K^c\,,\, \sigma(\alpha) = \alpha\ (\forall \alpha \in K)\}$.

Der Beweis des Satzes benutzt ein Axiom, das sogenannte LEMMA VON ZORN, das hier zwar formuliert, dessen Zusammenhang mit anderen Axiomen aus der Mengenlehre, wie etwa dem Auswahlaxiom, aber nicht diskutiert werden soll (vgl. dazu etwa H. Kneser, Math. Z. **53** (1950), 110).

Es sei M eine nichtleere Menge. M heißt teilweise geordnet, wenn es eine Relation $\leq$ zwischen gewissen (nicht notwendig allen) Elementen von M gibt, die folgendes erfüllt:

$$\begin{array}{l} m_1 \leq m_2\ \&\ m_2 \leq m_1 \Longrightarrow m_1 = m_2 \\ m_1 \leq m_2\ \&\ m_2 \leq m_3 \Longrightarrow m_1 \leq m_3 \end{array} .$$

(Ein Beispiel ist $M = \mathbb{N} \setminus \{3^j : j \geq 2\}$ mit $m_1 \leq m_2 \iff m_1 \mid m_2$.) Sie heißt vollständig geordnet, wenn noch für je zwei Elemente $m_1, m_2 \in M$ gilt: $m_1 \leq m_2$ oder $m_2 \leq m_1$. Ein maximales Element in der teilweise geordneten Menge M ist ein Element $m_0 \in M$ mit $[\, m_0 \leq m_1 \in M \Longrightarrow m_0 = m_1\,]$ (im Beispiel etwa $m_0 = 3$). Eine Kette in M ist eine in der Teilordnung von M vollständig geordnete nichtleere Teilmenge N von M (wie im obigen Beispiel die Teilmenge $N_2 = \{2^i : i = 0, 1, 2, \ldots\}$). Das Zornsche Lemma besagt nun: *Ist $M \neq \emptyset$ teilweise geordnet und besitzt jede Kette N in M eine obere Schranke in M (d.h. $\exists m \in M : n \leq m\ (\forall n \in N)$), so gibt es maximale Elemente in M.* (Hätten wir im Beispiel $\mathbb{N}$ statt $\mathbb{N} \setminus \{3^j : j \geq 2\}$ genommen, so gäbe es da kein einziges maximales Element. Allerdings genügt auch $\mathbb{N} \setminus \{3^j : j \geq 2\}$ nicht der Zornschen Bedingung: N_2 besitzt keine obere Schranke.)

Warnung: mit zu sorglosem Umgang mit dem Zornschen Lemma kann aller möglicher Unsinn erreicht werden. Wichtig ist, daß, erstens, M eine wohldefinierte Menge und, zweitens, M nichtleer ist. Zum Beispiel gibt es nicht die Menge aller Mengen, noch die Menge aller algebraischen Erweiterungskörper von K, etc.

Die Standardanwendung betrifft eine Menge M, deren Elemente Teilmengen A einer vorgebenen Menge $\mathfrak{M}$ sind und deren Teilordnung durch $A_1 \leq A_2 \iff A_1 \subset A_2$ gegeben ist. Als obere Schranke einer Kette $N = \{A\}$ versucht man das Element $\bigcup_{A \in N} A$, das natürlich eine Teilmenge von $\mathfrak{M}$ ist, aber vielleicht nicht unbedingt in M liegt.

Wir schließen das Kapitel mit der Realisierung der symmetrischen Gruppe S_n (der Permutationsgruppe auf n Elementen [22]) als Galoisgruppe einer Erweiterung L/K.

k sei ein Körper und $L = k(x_1, x_2, \cdots, x_n)$ der Körper aller rationalen Funktionen in den unabhängigen Unbestimmten $x_1, \cdots, x_n$ und mit Koeffiozienten aus k (L entsteht also aus k durch sukzessive Adjunktion von transzendenten Elementen x_i $(1 \leq i \leq n)$). Auf L bewirken die Permutationen der x_i Körperautomorphismen und dadurch wird die S_n zu einer Gruppe von Automorphismen von L. Ist K der Fixkörper, so ist also L/K eine galoissche Erweiterung mit Gruppe $G(L/K) = S_n$.

DEFINITION.

$$a_{n-1} = -\sum_i x_i\,,\ a_{n-2} = \sum_{i \leq j} x_i x_j\,,\ \ldots\,,\ a_0 = (-1)^n \prod_i x_i$$

sind die elementar-symmetrischen Funktionen in den x_i.

[22] vergleiche den Anfang des nächsten Kapitels

Die sind alle sicher in K, mithin $k(a_0, a_1, \cdots, a_{n-1}) \subset K$ und

$$f(X) \stackrel{\text{def}}{=} X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in k(a_0, \cdots, a_{n-1})[X]\,, \quad f(X) = \prod_{i=1}^{n}(X - x_i) \text{ in } L[X]\,.$$

Das Polynom $f(X)$ ist separabel und hat über $k(a_0, \cdots, a_{n-1})$ den Zerfällungskörper

$$k(a_0, \cdots, a_{n-1})(x_1, \cdots, x_n) = k(x_1, \cdots, x_n) = L\,.$$

Insbesondere kann die zugehörige Galoisgruppe $G(L/k(a_0, \cdots, a_{n-1}))$ als Untergruppe der S_n angesehen werden. Es resultiert (aus Gradgründen) $K = k(a_0, \cdots, a_{n-1})$.

Gäbe es eine algebraische Relation zwischen den a_j $(0 \leq j \leq n-1)$, also ein von Null verschiedenes Polynom in n Unbestimmten mit Nullstelle $(a_0, \cdots, a_{n-1})$, so gäbe es auch ein solches mit Nullstelle $(x_1, \cdots, x_n)$, ein Widerspruch. So erscheint auch K als Körper aller rationalen Funktionen in n Unbestimmten (den $a_0, \cdots, a_{n-1}$) und mit Koeffizienten aus k. Das Polynom $f(X)$ ist übrigens irreduzibel in $K[X]$, weil es zu je zwei Wurzeln x_{i_1}, x_{i_2} ein $\pi \in S_n$ mit $\pi(x_{i_1}) = x_{i_2}$ gibt.

FOLGERUNG. *Die symmetrischen rationalen Funktionen in den x_i sind rationale Funktionen in den elementar-symmetrischen Funktionen a_j.*

Die Koeffizienten sind dabei natürlich immer im Grundkörper k. Tatsächlich kann man in der Folgerung 'rationale Funktionen' durch 'Polynome' ersetzen, vgl. etwa [van der Waerden, §33].

4. Gruppentheorie und Anwendungen in der Galoistheorie

Wir beginnen mit einem wichtigen Beispiel, der symmetrischen Gruppe S_n.

Zu $1 \leq n \in \mathbb{N}$ betrachte man alle Permutationen einer n-elementigen Menge M, also alle Bijektionen π von M auf sich (ohne Einschränkung kann man für M die Menge $\{1, 2, \cdots, n\}$ nehmen). Diese bilden über die Hintereinanderausführung eine Gruppe, die sogenannte symmetrische Gruppe S_n auf n Elementen (das Einselement ist die identische Abbildung von M auf sich; π^{-1} ist die Umkehrabbildung von π). Besondere Permutationen sind die k-Zykeln $\sigma \in S_n$:

> hier sind $2 \leq k \leq n$ und eine k-elementige Teilmenge $\{i_1, \cdots, i_k\}$ von M vorgegeben; der dazu gehörige k-Zykel σ ist dann wie folgt definiert: ist $j \in M \backslash \{i_1, \cdots, i_k\}$, so sei $\sigma(j) = j$, des weiteren sei $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots$, $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$.

Die Notation für ein solches σ ist auch $\sigma = (i_1 \ldots i_k)$. Ein 2-Zykel heißt Transposition; ein allgemeiner unspezifizierter Zykel ist ein k-Zykel für ein $2 \leq k \leq n$.

Beobachtungen:

1. Ist G eine endliche Gruppe mit n Elementen. so liefert $G \ni x \mapsto \pi_x \in S_n$, $\pi_x(y) = xy$ $(\forall\, y \in G =: M)$ einen Gruppenmonomorphismus von G in die S_n. M.a.W.: Bis auf Isomorphie sind die Untergruppen der symmetrischen Gruppen S_n, $n = 1, 2, \cdots$, die sämtlichen endlichen Gruppen.

2. S_n hat $n!$ Elemente; S_n ist für $n \geq 3$ nicht kommutativ.

3. k ist die kleinste natürliche Zahl > 0 mit $(i_1 \dots i_k)^k = 1$.

4. Jedes $1 \neq \pi \in S_n$ ist eindeutig als Produkt von disjunkten [23] Zykeln darstellbar; die Faktoren vertauschen.

5. Jedes $\pi \in S_n$ ist ein Produkt von Transpositionen.

6. Es gilt

   (a) ist $\pi \in S_n$ und $(i_1 \dots i_k) \in S_n$ ein k-Zykel, so ist $\pi(i_1 \dots i_k)\pi^{-1} = (\pi(i_1) \dots \pi(i_k))$

   (b) $\pi_1, \pi_2 \in S_n \setminus \{1\}$ sind konjugiert in der S_n (i.e., es gibt ein $\tau \in S_n$ mit $\tau^{-1}\pi_1\tau = \pi_2$) genau wenn die Zykelzerlegungen von π_1 und π_2 (gemäß 4.) dieselben Zykellängen aufweisen.

7. Die Abbildung $\operatorname{sgn} : S_n \to \{\pm 1\}$, definiert durch

$$\prod_{1 \leq i < j \leq n} (i - j) = \operatorname{sgn}(\pi) \prod_{1 \leq i < j \leq n} (\pi(i) - \pi(j)) \,,$$

   ist ein surjektiver Gruppenhomomorphismus auf die 2-elementige Gruppe $\{\pm 1\}$. Ihr Kern $A_n = \{\pi \in S_n : \operatorname{sgn}(\pi) = 1\}$ heißt die alternierende Gruppe auf n Elementen. Es gilt

   (a) $\operatorname{sgn}((i_1 \dots i_k)) = (-1)^{k-1}$

   (b) $A_n \lhd S_n$

   (c) A_n hat $n!/2$ Elemente

   (d) A_n ist für $n \geq 3$ von den 3-Zykeln erzeugt (d.h. jedes $\pi \in A_n$ ist ein Produkt von 3-Zykeln).

Eine kleine *galoistheoretische Anwendung* ist diese: L sei der Zerfällungskörper des normierten separablen Polynoms $f(x) \in K[x]$ vom Grad n. Dann kann $G(L/K)$ kanonisch als eine Untergruppe der S_n aufgefaßt werden (Permutationen der Wurzeln $w_1, \cdots, w_n$ von f). Es gilt

$G(L/K)$ ist genau dann sogar Untergruppe der A_n, wenn die Diskriminante
$d_f \stackrel{\text{def}}{=} (-1)^{\binom{n}{2}} \prod_{i \neq j}(w_i - w_j) = \left(\prod_{i<j}(w_i - w_j)\right)^2$ ein Quadrat in K ist.

Man beachte, daß d_f invariant unter der Wirkung der S_n ist, also unter der von $G(L/K)$ festbleibt, und folglich in K liegt. Eine Wurzel ist $\prod_{i<j}(w_i - w_j)$, aber die ist nur unter der Wirkung von A_n invariant. Aus den früheren Überlegungen zu symmetrischen Funktionen resultiert, daß d_f ein Polynom in den Koeffizienten von $f(x)$ ist, z.B. für $f(x) = x^2 + ax + b$ ist $d_f = a^2 - 4b$ und für $f(x) = x^3 + bx + c$ ist $d_f = -4b^3 - 27c^2$ (letzteres ist etwas mühsam auszurechnen).

Weitere Beispiele endlicher Gruppen:

1. Zyklische Gruppen sind Gruppen, deren Elemente genau die Potenzen eines einzigen Elementes $a \in G$ sind,

$$G = \langle a \rangle = \{a^j : j \in \mathbb{Z}\} = \{1, a, a^2, \dots, a^{n-1}\} \,;$$

[23] die Zykeln $(i_1 \dots i_k)$ und $(j_1 \dots j_l)$ heißen disjunkt, wenn die Teilmengen $\{i_1, \cdots, i_k\}$ und $\{j_1, \cdots, j_l\}$ von M leeren Durchschnitt haben

beachte: da G endlich ist, existiert ein $1 \leq n \in \mathbb{N}$ mit $a^n = 1$, $a^i \neq 1$ für $1 \leq i \leq n-1$. Offenbar gilt $G \simeq \mathbb{Z}/n$, $a^j \mapsto j \bmod n$, insbesondere also $|G| = n$. Dieses n wird die Ordnung von a (bzw. von G) genannt; Notation $n = |a|$ (oder $n = |G|$). Des weiteren

(a) $a^s = 1 \iff n \mid s$

(b) $G = \langle a^k \rangle \iff \mathrm{ggT}(k,n) = 1\,; \quad |a^i| = \frac{n}{\mathrm{ggT}(n,i)}$

(c) Unter- und Faktorgruppen von G sind wieder zyklisch. Zu jedem Teiler d von $n = |G|$ gibt es sowohl genau eine Untergruppe U als auch eine Faktorgruppe $\overline{G}$ der Ordnung d.

2. Abelsche Gruppen sind Gruppen G mit $ab = ba$ $(\forall\, a, b \in G)$.

(a) Zyklische Gruppen sind abelsch. Untergruppen abelscher Gruppen sind Normalteiler.

(b) Unter- und Faktorguppen abelscher Gruppen sind ebenfalls abelsch.

(c) Zu jedem Teiler d von $|G|$ existiert eine Untergruppe der Ordnung d.

3. p-Gruppen sind Gruppen G mit $|G| = p$-Potenz (p ist immer eine Primzahl).

Beispiel: Ist G eine endliche *abelsche* Gruppe, so ist $G_p \stackrel{\text{def}}{=} \{x \in G : |x| = p\text{-Potenz}\}$ eine p-Untergruppe von G.

4. Das direkte Produkt endlicher vieler Gruppen G_i, $1 \leq i \leq m$, ist so erklärt

$$G = G_1 \times \cdots \times G_m = \{(a_1, \ldots, a_m) : a_i \in G_i\}$$

mit komponentenweiser Multiplikation. Es gilt

(a) Sind alle G_i abelsch, so auch G.

(b) $|G| = \prod_{i=1}^{m} |G_i|$

(c) $G_i \to G$, $a_i \mapsto \hat{a}_i \stackrel{\text{def}}{=} (1, \ldots, 1, a_i, 1, \ldots, 1)$ ist ein Monomorphismus mit Bild $\hat{G}_i \lhd G$; die $\hat{G}_i$ sind elementweise vertauschbar: $\hat{a}_i \hat{a}_j = \hat{a}_j \hat{a}_i$ für $i \neq j$; $G = \prod_i \hat{G}_i$. [24]

(d) Sind alle G_i zyklisch, so ist G zyklisch genau wenn die Ordnungen $|G_i|$ paarweise teilerfremd zueinander sind.

(e) Ist G abelsch und $|G| = p_1^{m_1} \cdots p_r^{m_r}$ mit verschiedenen Primzahlen p_i $(1 \leq i \leq r)$, so gilt (kanonisch)

$$G \simeq G_{p_1} \times \cdots \times G_{p_r} \quad \text{und} \quad |G_{p_i}| = p_i^{m_i}\,.$$

LEMMA. *Ist $U \leq G$, so gilt $|U| \,\Big|\, |G|$.*

FOLGERUNG. *Jedes $a \in G$ erfüllt $a^{|G|} = 1$.*

DEFINITION. *Ist $U \leq G$, so heißt $[G:U] = |G|/|U|$ der Index von U in G.*

Beachte

[24] In diesem Zusammenhang: Sind U_1, U_2 Untergruppen von G, so ist $U_1U_2 = \{u_1u_2 : u_1 \in U_1\,,\, u_2 \in U_2\}$ i.allg. keine Untergruppe; ist aber eine der beiden Untergruppen ein Normalteiler, so gilt $U_1U_2 \leq G$.

$[G:U] = |G/U|$ für Normalteiler $U \lhd G$

$[G:U]$ ist die Anzahl der verschiedenen Linksnebenklassen $aU = \{au : u \in U\} \subset G$ in G und auch die der verschiedenen Rechtsnebenklassen $Ua = \{ua : u \in U\} \subset G$. Zwei Links (Rechts) nebenklassen sind entweder gleich oder haben leeren Durchschnitt. Nur für $U \lhd G$ gilt $Ua = aU$ $(\forall a \in G)$.

Anwendung: Endliche Körper

Ist K ein endlicher Körper, so ist $|K| = q$ eine Potenz von $p = \mathrm{char}(K)$. Die multiplikative Gruppe $K^\times$ hat $q-1$ Elemente und folglich gilt $[\, a \in K,\, a \neq 0 \Longrightarrow a^{q-1} = 1\,]$ und $a^q = a$ $(\forall a \in K)$. Ist jetzt (und im folgenden) L/K eine Körpererweiterung vom Grad n, so ist $|L| = q^n$ und jedes $\lambda \in L$ Wurzel des separablen Polynoms $x^{q^n} - x \in \mathbb{F}_p[x] \subset K[x]$; insbesondere ist L der Zerfällungskörper von $x^{q^n} - x$ über K. Daraus folgt zweierlei:

1. Zu jeder Primzahlpotenz p^m gibt es genau einen Körper mit p^m Elementen. Diesen bezeichnen wir fortan mit $\mathbb{F}_{p^m}$; es gilt:

   a. $\mathbb{F}_{p^m}$ ist der Zerfällungskörper von $x^{p^m} - x \in \mathbb{F}_p[x]$.

   b. $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^k} \iff m \mid k$.

2. L ist galoissch über K mit zyklischer Galoisgruppe

$$G_{L/K} = \{1, \varphi_{L/K}, \varphi_{L/K}^2, \ldots, \varphi_{L/K}^{n-1}\}$$

   mit dem Erzeugenden $\varphi_{L/K}(\lambda) = \lambda^q$ $(\lambda \in L\,,\, q = |K|)$. $\varphi_{L/K}$ heißt der *Frobeniusautomorphismus* von L/K.

Es ist nun leicht zu sehen, daß es eine Normalbasis (und insbesondere ein primitives Element) in L gibt. Wegen Artins Lemma ist $x^n - 1$ das Minimalpolynom des K-linearen Endomorphismus $\varphi_{L/K}$ des K-Vektorraums L. Die Jordan Normalform von $\varphi_{L/K}$ ist deshalb

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots 0 & & 0 \\ & & & & \\ \vdots & & & & \vdots \\ & & & & \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix},$$

und mit dieser Basiswahl ist der erste Basisvektor Erzeuger einer Normalbasis (und auch ein primitives Element).

Schreibe $|K^\times| = q - 1 = \prod_i p_i^{m_i}$ als Produkt von Primzahlpotenzen und zerlege $G = K^\times$ in das Produkt der p_i-Untergruppen G_{p_i} der Ordnung $p_i^{m_i}$. Die Elemente in G_{p_i} lösen alle die Gleichung $x^{p_i^{m_i}} = 1$ und, wäre G_{p_i} nicht zyklisch, sogar $x^{p_i^{m_i-1}} = 1$. Die letzte Gleichung besitzt aber höchstens $p_i^{m_i-1}$ viele Wurzeln und also hätte $K^\times$ weniger als $q-1$ Elemente. Folglich sind die G_{p_i} alle zyklisch und daher auch $K^\times$. – Genauso zeigt man, daß jede endliche Untergruppe der multiplikativen Gruppe $K^\times$ eines beliebigen Körpers K zyklisch ist.

Zwei diesen Exkurs abschließende Bemerkungen:

1. Für jede ganze Zahl z gilt $z^p \equiv z \bmod p$ (bei vorgegebener Primzahl p). Diese Kongruenz wird oft auch als *kleiner Fermatscher Satz* bezeichnet.

2. $\mathbb{F}_p^\times$ ist zyklisch, also existiert eine ganze Zahl $w \not\equiv 0 \bmod p$ mit $\{1, w, w^2, \cdots, w^{p-2}\} = \mathbb{F}_p^\times$. Ein solches w heißt eine *Primitivwurzel modulo p*. Es gibt keine direkte Formel, wie ein w aus p abzuleiten wäre. Erste Beispiele

p	2	3	5	7
w	1	-1	2,3	-2,3

.

Zurück zur Gruppentheorie: Abelsche Gruppen; spezielle Untergruppen

SATZ. *Ist G abelsch, so ist G als direktes Produkt von zyklischen Untergruppen Z_i, $1 \le i \le r$, mit $|Z_i| \Big| |Z_{i+1}$ darstellbar. Die Zahlen $r, |Z_i|$ sind durch G eindeutig bestimmt.*

Dies ist der Satz von der Existenz und Eindeutigkeit der sogenannten Elementarteiler $|Z_i|$ einer abelschen Gruppe G. Er ist verwandt mit dem Satz über Jordanformen von Matrizen $A \in K_{n\times n}$ [25]. Das Hauptargument im Beweis ist: In einer abelschen p-Gruppe G sei a ein Element größter Ordnung. Des weiteren sei $\bar{b} \in G/\langle a\rangle$ ein Element in der Faktorgruppe von G nach $\langle a\rangle$. Dann existiert ein Urbild $b \in G$ von $\bar{b}$ mit $|b| = |\bar{b}|$.

DEFINITION. *a. Ist G eine endliche Gruppe und ist, für eine Primzahl p, p^n die größte in $|G|$ aufgehende p-Potenz, so heißt jede Untergruppe $P \le G$ mit $|P| = p^n$ eine p-Sylowuntergruppe von G.*

b. Zwei Untergruppen U, V von G heißen konjugiert (in G), wenn es ein $g \in G$ mit

$$U = V^g \stackrel{\text{def}}{=} g^{-1}Vg = \{g^{-1}vg : v \in V\}$$

gibt. Beachte, daß dies eine Äquivalenzrelation auf der Menge der Untergruppen von G definiert.

c. Das Zentrum einer Gruppe ist definiert als

$$Z(G) = \{z \in G : zg = gz \ (\forall g \in G)\},$$

die Kommutatorgruppe von G als

$$G' \stackrel{\text{def}}{=} \langle ghg^{-1}h^{-1} : g, h \in G\rangle .$$

Dabei bezeichnet $\langle g_1, \ldots, g_s\rangle$ die kleinste Untergruppe von G, die alle $g_i \in G$, $1 \le i \le s$ enthält (oder die, wie man auch sagt, von den g_i erzeugt ist).

SATZ. 1. *Für $V \le G$ und $N \lhd G$ sind VN/N und $V/V\cap N$ über $vn \bmod N \mapsto v \bmod V\cap N$, isomorph.*

2. *$G' \lhd G$; G/G' ist abelsch; G' ist in allen Normalteilern N von G mit abelscher Faktorgruppe G/N enthalten. Gilt $G' \le U \le G$, so ist $U \lhd G$ und G/U abelsch.*

3. *Zentrum und Kommutatorgruppe sind charakteristische Untergruppen von G, d.h. $\sigma(Z(G)) = Z(G)$, $\sigma(G') = G'$ für jeden Automorphismus σ von G.*

[25] Der Zusammenhang ist der: Dem Ring der ganzen Zahlen (denen die Ordnungen der Gruppe und ihrer Elemente angehören) entspricht der Polynomring $K[x]$ (wie $\mathbb{Z}$ ein Euklidischer Ring), der abelschen Gruppe G der Vektorraum $V = K^n$ und der Ordnung $|G|$ das Minimalpolynom von A, den Gruppenelementen $g \in G$ und ihren Ordnungen $|g|$ die Vektoren $v \in V$ sowie jeweils das normierte Polynom $m_v(x)$ kleinsten Grades mit $m_v(A) \cdot v = 0$.

4. *Die Anzahl der p-Sylowuntergruppen P in G ist $\equiv 1 \bmod p$ (insbesondere also ≥ 1) sowie ein Teiler von $|G|/|P|$.*
5. *Je zwei p-Sylowuntergruppen von G sind in G konjugiert.*
6. *Das Zentrum einer p-Gruppe $\neq 1$ schneidet jeden Normalteiler $\neq 1$ nichttrivial und ist insbesondere selbst $\neq 1$.*
7. *Gilt $p^m \Big| |G|$, so besitzt G eine Untergruppe der Ordnung p^m.*
8. *Gruppen G mit $|G| \Big| p^2$ sind abelsch.*
9. *Untergruppen vom Index p in p-Gruppen sind normal.*

Grundprinzip der Beweise für 4.-7. ist dieses:
M sei eine endliche Menge, auf der die Gruppe G wirke, d.h. es gebe eine Abbildung

$$G \times M \to M\,,\ (g,m) \mapsto gm \quad \text{mit} \quad 1m = m\,,\ g_1(g_2m) = (g_1g_2)m\,.$$

Die G-Wirkung prägt M eine Äquivalenzrelation durch $[\, m_1 \sim m_2 \iff \exists\, g \in G : gm_1 = m_2\,]$ auf. Definiere die *Standuntergruppe* oder den *Stabilisator* von $m_0 \in M$ durch $G_{m_0} = \{g \in G : gm_0 = m_0\}$ und die Äquivalenzklasse oder *Bahn* von m_0 durch $B_{m_0} = \{gm_0 : g \in G\}$. Dann ist $G_{m_0} \leq G$ und $|B_{m_0}| = [G : G_{m_0}] \mid |G|$. Zwei verschiedene Bahnen haben kein Element gemeinsam, also $|M| = \sum |B_m|$, wenn $\{m\}$ ein vollständiges Vertretersystem aller Äquivalenzklassen in M durchläuft.

Punkt 8. des Satzes ist Folge der allgemeineren Beobachtung: *Ist $G/Z(G)$ zyklisch, so ist G abelsch.* Nun verwende noch 6.; auch 8. folgt über Induktion aus 6.

Die Aussagen 1.-3. sind offenkundig. Man beachte noch zu 3., daß charakteristische Untergruppen stets normal sind, wie aus Anwendung der speziellen *inneren* Automorphismen $\sigma_g : x \mapsto x^g \stackrel{\text{def}}{=} g^{-1}xg\,, (x \in G)$ für $g \in G$ folgt (σ_g heißt die Konjugation mit g).

Anwendung auf Körper:

SATZ. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Betrachte dazu irgendeine nichttriviale galoissche Erweiterung $L/\mathbb{R}$. Die Gruppe sei G und P sei eine 2-Sylowuntergruppe mit Fixkörper Z. Dann ist $Z = \mathbb{R}(\alpha)$ und das Minimalpolynom von α über $\mathbb{R}$ hat ungeraden Grad. Aber jedes solche Polynom hat eine Nullstelle in $\mathbb{R}$ (Zwischenwertsatz), also ist $[Z : \mathbb{R}] = 1$ und G eine Gruppe der Ordnung 2^n. Ist $n = 1$, so ist $L = \mathbb{C}$. Eine Untergruppe der Ordnung 2^{n-1} gehört im anderen Fall zum Fixkörper $\mathbb{C}$. Aber $\mathbb{C}$ besitzt keine quadratische Erweiterung, also ist wieder $L = \mathbb{C}$.

Und wieder weiter mit Gruppentheorie: Zerfallende, nilpotente und auflösbare Gruppen

DEFINITION. 1. *G heißt nilpotent, wenn jede Sylowuntergruppe normal in G ist.*
2. *G heißt auflösbar, wenn es eine Kette*

$$G = G_0 \geq G_1 \geq G_2 \geq \ldots \geq G_r \geq G_{r+1} = 1$$

von Untergruppen G_i mit $G_i' \leq G_{i+1}$ für $0 \leq i \leq r$ gibt.
3. *G heißt einfach, wenn $\{1\}$ und G die einzigen Normalteiler in G sind.*

Beispiele nilpotenter Gruppen sind p-Gruppen; jede nilpotente Gruppe ist auflösbar; die einfachen abelschen Gruppen sind genau die zyklischen Gruppen von Primzahlordnung. Auflösbare Gruppen sind i.allg. nicht nilpotent (Beispiel S_3).

SATZ. *1. Genau dann ist G nilpotent, wenn G direktes Produkt von p-Gruppen ist.*

2. Sei $U \leq G$ und $N \lhd G$. Dann gilt

a. G nilpotent (bzw. auflösbar) $\Longrightarrow U$ und G/N nilpotent (bzw. auflösbar)

b. N und G/N auflösbar $\Longleftrightarrow G$ auflösbar.

3. G auflösbar $\Longleftrightarrow \exists$ Kette $G = G_0 \geq G_1 \geq \ldots \geq G_s \geq G_{s+1} = 1$ mit

$$G_{j+1} \lhd G_j \;\&\; G_j/G_{j+1} \text{ ist zyklisch von Primzahlordnung } (0 \leq j \leq s)\,.$$

SATZ. (Schur-Zassenhaus) *N sei ein Normalteiler von G mit* $\mathrm{ggT}(|N|, [G:N]) = 1$. *Dann zerfällt G über N, d.h. $\exists U \leq G : G = NU$, $N \cap U = 1$.*

Über die möglichen Komplemente U von N lassen sich im Falle, daß N oder G/N auflösbar ist, weitere Aussagen machen: sie sind alle konjugiert [26]. Der behauptete Zerfall ist unter anderem eine Folge des sogenannten *Frattiniarguments*:

ist $N \lhd G$ und P eine p-Sylowuntergruppe von N, so gilt $G = N \cdot N_G(P)$ mit $N_G(P) = \{x \in G : x^{-1}Px = P\}$, dem Normalisator von $P \leq G$ in G.

SATZ. *Die alternierende Gruppe A_n ist einfach für $n \geq 5$. Insbesondere ist die symmetrische Gruppe S_n für $n \geq 5$ nicht auflösbar.*

Beweisskizze: Weil die A_n von den 3-Zykeln erzeugt ist und je zwei solche für $n \geq 5$ in der A_n konjugiert sind, reicht es zu zeigen: ist $1 \neq N \lhd A_n$, so enthält N einen 3-Zykel. Sei dazu $1 \neq x \in N$ und es gelte entweder

1. daß die Zykelzerlegung von x einen Zykel $(abcd...)$ der Länge ≥ 4 enthalte, oder
2. keinen solchen, aber einen 3-Zykel (abc), und daß x einen Fixpunkt d habe, oder
3. wie zuvor, aber x habe keinen Fixpunkt (also etwa $x = (abc)(de\ldots)\ldots$), oder
4. daß die Zykelzerlegung von x nur Transpositionen enthalte, also, weil $\mathrm{sgn}(x) = 1$, $x = (ab)(cd)\ldots$.

Hier sind $a, b, c, d, e, \ldots$ die zu permutierenden Elemente.
Setze $y = (abc)$ im Fall 1., $y = (abd)$ in den Fällen 2. und 3., und $y = (ace)$ im Fall 4. Wir berechnen $yxy^{-1}x^{-1} \in N$:

1. $y^{-1} = (acb)$, $xy^{-1}x^{-1} = (dcb)$, $yxy^{-1}x^{-1} = (abd)$

2.,3. $y^{-1} = (adb)$, $xy^{-1}x^{-1} = (bec)$ mit $e =$ Bild von d bei x,

$$yxy^{-1}x^{-1} = \begin{cases} (ab)(cd) \text{ im Fall 2. } (d = e) \\ (abecd) \text{ im Fall 3. } (d \neq e)\,. \end{cases}$$

Damit führt Fall 2. hin zu Fall 4., Fall 3. zurück auf Fall 1.

[26] tatsächlich ist eine der beiden Gruppen, N oder G/N, stets auflösbar, nämlich aufgrund des Satzes von Feit und Thompson (1963): *Gruppen ungerader Ordnung sind auflösbar*. Dessen Beweis übersteigt unsere bisherigen Möglichkeiten einer gruppentheoretischen Diskussion allerdings bei weitem.

4. $y^{-1} = (aec)\,,\ xy^{-1}x^{-1} = (bfd)\,,$

$$xy^{-1}x^{-1} = \begin{cases} (ace)(bfd) \text{ falls das Bild } f \text{ von } e \text{ verschieden von } e \text{ ist} \\ (acedb) \text{ sonst .} \end{cases}$$

Hier führt der Fall $e \neq f$ zurück auf 3., der andere Fall, $e = f$, auf 1.

Insgesamt sieht man, daß spätestens dreimaliges Durchführen dieser Prozeduren beim Fall 1. landet, in welchem man direkt einen 3-Zykel in N sieht.

Wir beschreiben schließlich eine Konstruktion von neuen Gruppen aus schon bekannten, die besonders nützlich in der Galoistheorie ist.

DEFINITION. *Für eine Gruppe G bezeichne $AutG$ die Gruppe aller Automorphismen von G (die Hintereinanderausführung liefert die Multiplikation in $AutG$). Es liege eine zweite Gruppe H und ein Homomorphismus*

$$\eta : H \to \operatorname{Aut} G\,,\ h \mapsto \eta(h) = [\, g \mapsto g^h \,]$$

vor. Dann heißt

$$G \rtimes H = \{(g,h) : g \in G\,,\ h \in H\} \quad (g_1,h_1)(g_2,h_2) = (g_1 g_2^{h_1^{-1}}, h_1h_2)$$

das semidirekte Produkt aus G und H, η.

Offenbar gilt

$$G \simeq \hat{G} = \{(g,1)\} \lhd G \rtimes H\,,\ H \simeq \hat{H} = \{(1,h)\} \leq G \rtimes H\,,$$
$$\hat{G} \cap \hat{H} = 1\,,\ \hat{G} \cdot \hat{H} = G \rtimes H\,.$$

Fortan identifizieren wir G und $\hat{G}$ sowie H und $\hat{H}$ und schreiben statt (g,h) einfach gh. Beispiel: $S_3 = \mathbb{Z}/3 \rtimes \mathbb{Z}/2$ mit $\eta = \mathrm{id} : \mathbb{Z}/2 = \operatorname{Aut} \mathbb{Z}/3\,.$

Wenigstens für zyklische Gruppen G der Ordnung n soll nun $\operatorname{Aut} G$ bestimmt werden.

SATZ. *Ist $G = \langle a \rangle$ zyklisch von der Ordnung n, also $G \simeq \mathbb{Z}/n\,,\ a \mapsto 1$, so ist*

$$\operatorname{Aut} G \simeq (\mathbb{Z}/n)^\times = \{s \in \mathbb{Z} \bmod n\,,\ \mathrm{ggT}(s,n) = 1\}$$

vermöge $AutG \ni \sigma \mapsto s \bmod n \iff \sigma(a) = a^s$. Insbesondere ist $AutG$ abelsch. Im Falle, daß $n = p^k$ eine Primzahlpotenz ist, ist

1. *$AutG$ für ungerades p zyklisch, erzeugt von $w_p^{p^{k-1}}(1+p) \bmod p^k$, mit $\langle w_p \bmod p\rangle = (\mathbb{Z}/p)^\times$*
2. *$AutG \simeq \mathbb{Z}/2 \times \mathbb{Z}/2^{k-2} = \langle -1 \bmod 2^k\rangle \times \langle 5 \bmod 2^k\rangle$ für $p = 2$.*

Des weiteren $|\operatorname{Aut} G| = \phi(n) = \prod_{p|n}(p-1)p^{k_p-1}$, wenn $|G| = n = \prod_{p|n} p^{k_p}$.

Die Funktion ϕ heißt die Eulersche ϕ-Funktion; $\phi(n)$ zählt die zu n teilerfremden Zahlen zwischen 1 und n. Sie ist multiplikativ in dem eingeschränkten Sinne

$$\mathrm{ggT}(n_1, n_2) = 1 \Longrightarrow \phi(n_1 n_2) = \phi(n_1)\phi(n_2)$$

und erfüllt $\phi(p^k) = (p-1)p^{k-1}$.

In diesem Zusammenhang ist es vielleicht hilfreich, gruppentheoretische Literatur zu nennen, z.B. B. Huppert, *Endliche Gruppen 1* (Springer Grundlehren Bd. 134) Kapitel I, §§9,18 und V, §5, oder H. Kurzweil *Endliche Gruppen* (Springer Hochschultext, 1977) Kapitel III, §5, IV, §3 und VI, §2.

Beispiele :

1. Es gelte $|G| = pq$ mit Primzahlen p und q. Falls $p = q$, also $|G| = p^2$ ist, so ist G abelsch und von einem der beiden Isomorphietypen $G \simeq \mathbb{Z}/p^2$ oder $G \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. Im Fall $p < q$ und $q \not\equiv 1 \bmod p$ existiert nur die zyklische Gruppe $G \simeq \mathbb{Z}/pq$, denn die Anzahlen a_p, a_q der p- bzw. q-Sylowuntergruppen erfüllen $a_p | q$, $a_p \equiv 1 \bmod p$, $\quad a_q | p$, $a_q \equiv 1 \bmod q$ und sind damit beide $= 1$. Ist aber $q \equiv 1 \bmod p$, dann gibt es außer der zyklischen Gruppe $G \simeq \mathbb{Z}/pq$ noch die nichtabelsche Gruppe $G = \mathbb{Z}/q \rtimes \mathbb{Z}/p$, wobei $\mathbb{Z}/p$ auf $\mathbb{Z}/q$ über die Identifizierung von $\mathbb{Z}/p$ mit der Untergruppe der Ordnung p von $\mathrm{Aut}(\mathbb{Z}/q) = (\mathbb{Z}/q)^\times$ wirkt; dies ist eine Konsequenz aus dem Satz von Schur-Zassenhaus.

2. Gleichbedeutend mit " *zu der Gruppenordnung n existiert allein die zyklische Gruppe* $G \simeq \mathbb{Z}/n$" ist " $(n, \phi(n)) = 1$ " .

   Denn für $n = p^r s$ mit $r \geq 2, p \nmid s$ sehen wir wenigstens die beiden Gruppen $\mathbb{Z}/p^r \times \mathbb{Z}/s$ und $\mathbb{Z}/p \times \mathbb{Z}/p^{r-1} \times \mathbb{Z}/s$. Folglich muß n quadratfrei sein. Ist n keine Pmzahl, also $n = pqt$ mit verschiedenen Primzalen p und q, die beide t nicht teilen, so sehen wir im Fall $q \equiv 1 \bmod p$ die beiden Gruppen $\mathbb{Z}/pqt$ und $(\mathbb{Z}/q \rtimes \mathbb{Z}/p) \times \mathbb{Z}/t$ mit der durch $\mathbb{Z}/p \leq (\mathbb{Z}/q)^\times$ induzierten Wirkung. Daher ist die Bedingung $(n, \phi(n)) = 1$ notwendig.

   Für die Umkehrung setzen wir zusätzlich voraus, daß G auflösbar sei (was aber wegen des Satzes von Feit-Thompson unnötig ist, da n ungerade sein muß). Es gilt dann $G' < G$. Nun impliziert $(n, \phi(n) = 1)$ sicher $(|G'|, [G : G']) = 1$ und dann der Satz von Schur-Zassenhaus die Existenz einer Untergruppe $U \leq G$ mit $U \cap G' = 1$, $G = G'U$. Die Voraussetzung $(|G|, \phi(|G|)) = 1)$ vererbt sich auf G' und U ; aufgrund einer Induktion nach der Gruppenordnung sind deshalb diese beiden Gruppen zyklisch. Aber die Automorphismengruppe der zyklischen Gruppe G' enthält kein Element $\neq 1$ mit einer $|U|$ teilenden Ordnung, weshalb G abelsch und damit zyklisch ist.

5. Galoissche Theorie: Vertiefungen

Irreduzibilitätskriterien etc.

Definition. *Ist R ein kommutativer nullteilerfreier Ring, so heißt*

$$\begin{aligned} &K = \{(a,b) : a, b \in R\,,\ b \neq 0\} \\ &(a_1, b_1) = (a_2, b_2) \iff a_1 b_2 = a_2 b_1 \\ &(a_1, b_1) + (a_2, b_2) = (a_1 b_2 + a_2 b_1, b_1 b_2) \\ &(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) \end{aligned}$$

der Quotientenkörper von R.

Die Gleichheit in K legt die Vorstellung von (a,b) als den Bruch a/b, mit Zähler und Nenner ($\neq 0$) in R, nahe. Im folgenden benützen wir deshalb meistens diese Schreibweise. Die Abbildung $a \mapsto a/1$ ist ein Ringmonomorphismus von R in K, über den wir fortan R als Teilmenge in K identifizieren. Natürlich ist K ein Körper: $(a,b)^{-1} = (b,a)$, vorausgesetzt daß $(a,b) \neq 0$, also $a \neq 0$ ist.

LEMMA. (Gauß) *R sei ein ZPE-Ring, also ein kommutativer nullteilerfreier Ring mit eindeutiger Primfaktorzerlegung, und K sei sein Quotientenkörper. Ist dann $f(x) \in R[x]$ irreduzibel in $R[x]$, so auch in $K[x]$.*

Als Beispiel dient vor allem $R = \mathbb{Z}$. Der Beweis des Lemmas beruht auf folgender Tatsache: Sind $g(x) = \sum_i a_i x^i$ und $h(x) = \sum_j b_j x^j$ zwei Polynome $\in R[x]$ mit $\mathrm{ggT}(a_i) = 1 = \mathrm{ggT}(b_j)$, so gilt $\mathrm{ggT}(c_k) = 1$ für $g(x)h(x) = \sum_k c_k x^k$. Das Lemma impliziert, daß sich die ZPE-Eigenschaft von $K[x]$ auf $R[x]$ vererbt, i.e., R ZPE $\Longrightarrow R[x]$ ZPE .

Anwendungen :

1. Symmetrische rationale Funktionen in n Variablen $x_1, \ldots, x_n$ sind Quotienten symmetrischer Polynome in diesen Variablen.

2. *Eisenstein :* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \in R[x]$ habe die Eigenschaft, daß es ein Primelement $p \in R$ mit

$$p \nmid a_n \ , \ p \mid a_i \ (0 \leq i \leq n-1) \ , \ p^2 \nmid a_0$$

   gebe. Dann ist $f(x)$ in $K[x]$ irreduzibel.

3. Ist $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ ein Polynom, das irreduzibel modulo einer Primzahl p ist und $p \nmid a_n$ erfüllt, so ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$.

Man beachte, daß das Eisenstein-Kriterium sozusagen konträr zu 3. ist: dort ist nämlich $f(x) \equiv \overline{a}_n x^n \bmod p$. Es gibt übrigens normierte irreduzible Polynome $f(x) \in \mathbb{Z}[x]$, die reduzibel modulo jeder Primzahl sind, so etwa das irreduzible Polynom $x^4 - 10x^2 + 1$ von $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$ [27].

LEMMA. *Im Fall $\mathrm{char}(K) = p \neq 0$ ist ein Artin-Schreier-Polynom $x^p - x + \alpha \in K[x]$ entweder irreduzibel oder zerfällt vollständig über K.*

Solche Polynome sind natürlich separabel.

Einheitswurzeln

DEFINITION. *K sei ein Körper der Charakteristik $p \geq 0$ und n eine nicht durch p teilbare natürliche Zahl. Dann heißt $\zeta_n \in K^{\mathrm{c}}$ eine primitive n-te Einheitswurzel, wenn ζ_n Wurzel des Polynoms $x^n - 1 \in K[x]$, aber keine Wurzel von $x^m - 1 \in K[x]$ für $m < n$ ist.*

Beachte, daß im Falle $\mathrm{char}(K) \nmid n$ das Polynom $x^n - 1$ separabel ist und seine Wurzeln in $(K^{\mathrm{c}})^\times$ eine Gruppe der Ordnung n bilden. Diese ist zyklisch, $\simeq \mathbb{Z}/n$, und die primitiven n-ten Einheitswurzeln sind genau die Erzeugenden. Des weiteren ist $K(\zeta_n)/K$ als Zerfällungskörper von $x^n - 1$ galoissch und die Galoisgruppe $G_{K(\zeta_n/K)}$ eine Untergruppe von Aut $\langle \zeta_n \rangle$:

$$G_{K(\zeta_n)/K} \ni \sigma \leftrightarrow s \bmod n \iff \sigma(\zeta_n) = \zeta_n^s \quad (\mathrm{ggT}(s,n) = 1) \, .$$

[27] dazu mehr im kommenden Semester

Daher gilt : $G_{K(\zeta_n/K)}$ *ist abelsch und sogar zyklisch, wenn* n *Potenz einer ungeraden Primzahl ist.* Welche zu n teilerfremden Zahlen s zwischen 1 und n als Automorphismen σ vorkommen, hängt von K ab; z.B. nur $s = 1$, wenn $\zeta_n \in K$, jedoch alle s, wenn $K = \mathbb{Q}$, wie aus dem nächsten Kapitel folgt.

Im Falle $\mathrm{char}(K) \mid n$ gilt $x^n - 1 = (x^{n/p} - 1)^p$; es kann dann also gar keine primitiven n-ten Einheitswurzeln geben.

SATZ. *Die irreduzible Gleichung* $f_{(n)}(x)$ *von* ζ_n *über* $\mathbb{Q}$ *ist ganzzahlig und vom Grad* $\phi(n)$*. Es gilt*

$$f_{(n)}(x) = (x^n - 1) \Big/ \prod_{\substack{d \mid n \\ d \neq n}} f_{(d)}(x)$$

und insbesondere für eine Primzahlpotenz $n = p^r$

$$f_{(p^r)}(x) = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots x^{p^{r-1}} + 1 \ .$$

Auflösbare Galoisgruppen

DEFINITION. *Die Gruppe* $G_{L/K}$ *des Zerfällungskörpers* L *eines separablen Polynoms* $f(x) \in K[x]$ *heißt die Gruppe von* f*; Bezeichnung:* $G_f = G_{L/K}$ *und* $L_f = L$*.*

SATZ. *Es sei* $f(x) \in K[x]$ *separabel. Dann ist* G_f *genau dann auflösbar, wenn es eine galoissche Erweiterung* L/K *mit auflösbarer Galoisgruppe* $G_{L/K}$ *gibt, die* L_f *enthält.*

Genau im Fall, wenn G_f auflösbar ist, existiert also ein Körperturm

$$L = L_0 \supset L_1 \supset L_2 \supset \ldots \supset L_r \supset L_{r+1} = K$$

mit

$L \supset L_f$

L/K ist galoissch

L_i/L_{i+1} ist zyklisch von Primzahlordnung.

Sei nun $\mathrm{char}(K) = 0$ und $n = [L : K]$ (mit obigem L). Die Adjunktion einer primitiven n-ten Einheitswurzel ζ_n an K liefert

$$K \subset K(\zeta_n) = L_{r+1}(\zeta_n) \subset \ldots \subset L_0(\zeta_n) = L(\zeta_n) \, .$$

Wieder ist $L(\zeta_n)/K$ galoissch auflösbar, weil $K(\zeta_n)/K$ abelsch sowie $L_i(\zeta_n)/L_{i+1}(\zeta_n)$ zyklisch von Primzahlgrad $|n$ ist.

SATZ. *Sei* $\zeta_n \in K$*. Ist dann* M/K *zyklisch vom Grad* $|n$*, so existiert ein* $a \in K$ *mit* $M = K(\sqrt[n]{a})$*. Umgekehrt ist jede Erweiterung* $K(\sqrt[n]{a})/K$ *zyklisch vom Grad* $|n$*.*

Hauptbestandteil des Beweises ist der wichtige, sogenannte *Hilbert Satz 90*:

Ist M/K *zyklisch vom Grad* n *und* $\langle\sigma\rangle = G_{M/K}$*, so gilt für* $\alpha \in M$

$$\mathrm{N}_{M/K}(\alpha) = 1 \iff \exists\, 0 \neq \beta \in L : \alpha = \beta/\sigma(\beta) \ .$$

Wegen Artins Satz über die lineare Unabhängigkeit von Automorphismen existiert nämlich ein $\gamma \in M$ mit

$$\beta \stackrel{\text{def}}{=} \gamma + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \prod_{i=0}^{n-2} \sigma^i(\alpha) \cdot \sigma^{n-1}(\gamma)\,,$$

und dieses β tut das Verlangte.

FOLGERUNG. *Die Wurzeln einer separablen Gleichung $f(x) \in K[x]$ lassen sich genau dann durch Radikale ausdrücken (d.h. sie liegen in einer Erweiterung*

$$L = K(\zeta_n,\ \sqrt[n_1]{a_1}, \ldots,\ \sqrt[n_r]{a_r}) \text{ mit } a_i \in K(\zeta_n,\ \sqrt[n_1]{a_1}, \ldots,\ \sqrt[n_{i-1}]{a_{i-1}})\,)\,,$$

wenn f auflösbar (d.h. G_f auflösbar) ist. Insbesondere lassen sich die Wurzeln eines Polynoms vom Grad ≥ 5 im allgemeinen nicht durch Radikale ausdrücken.

Denn die S_n kommt als Galoisgruppe einer geeigneten Erweiterung L/K vor und ist für $n \geq 5$ nicht auflösbar, weil sie die einfache Gruppe A_n enthält. Ist allerdings $f(x) \in K[x]$ separabel und vom Grad ≤ 4, so ist f durch Radikale auflösbar, weil $G_f \leq S_4$ Untergruppe der auflösbaren Gruppe S_4 und somit selbst auflösbar ist.

Eine weitere Folgerung aus Hilberts Satz 90 ist diese

Im Falle $char(K) = 0$ impliziert $[K^c : K] < \infty$, daß dieser Grad $= 1$ oder 2 ist und im zweiten Fall noch $K^c = K(i)$ mit $i^2 = -1$ [28].

Als Anwendung leiten wir die Cardanoschen Formeln für die Wurzeln des allgemeinen Polynoms dritten Grades her.

Ist $f(x) = x^3 + a_1x^2 + a_2x + a_3$ und $6 \neq 0$ in K, so führt die Substitution $x \rightsquigarrow x - a_1/3$ auf das neue Polynom $f(x) = x^3 + ax + b = \prod_{i=1}^{3}(x - w_i)$ mit Diskriminante

$$\sqrt{d_f} = (w_1 - w_2)(w_1 - w_3)(w_2 - w_3) = \sqrt{-4a^3 - 27b^2}\,.$$ [29]

Wir setzen $a \neq 0$ voraus (sonst folgt mit geeigneter Numerierung $w_j = \zeta^j \sqrt[3]{-b}$ und es bleibt nichts zu tun). Die Gruppe G_f ist die S_3 mit dem zyklischen Normalteiler $A_3 \simeq \mathbb{Z}/3$ und Faktorgruppe $\mathbb{Z}/2$ (weil wir im allgemeinen Fall sind [30]). Adjunktion von $\sqrt{d_f}$ und $\zeta \stackrel{\text{def}}{=} \zeta_3 = -1/2 + 1/2\sqrt{-3}$ führt zu der zyklischen Erweiterung $L_f(\zeta)/K(\sqrt{d_f}, \zeta)$ vom Grad 3. Sie ist sowohl von w_1 als auch von der *Lagrangeschen Resolvente* $\rho \stackrel{\text{def}}{=} w_1 + \zeta w_2 + \zeta^2 w_3$

[28] Die Charakteristik-Voraussetzung ist tatsächlich unnötig; darüber hinaus kann man noch zeigen, daß K ähnlich wie $\mathbb{R}$ aussehen muß ('reel abgeschlossen').

[29] Ist $f(x) \in K[x]$ normiert, irreduzibel und separabel mit den Wurzeln $\theta_1, \ldots, \theta_n$ in K^c, so rechnet man leicht

$$f'(\theta_i) = \prod_{j \neq i}(\theta_i - \theta_j))\,, \quad N_{K(\theta_1)/K}(f'(\theta_1)) = \prod_{i=1}^{n} f'(\theta_i) = (-1)^{\binom{n}{2}} d_f$$

nach, also, angewendet auf unser $f(x) = x^3 + ax + b$, $-d_f = N(\frac{3w_1^3 + aw_1}{w_1}) = 4a^3 + 27b^2$.

[30] Im anderen Fall ist $G_f = A_3$ und $\sqrt{d_f} \in K$. Ansonsten ändert sich nichts im weiterten Verlauf der Diskussion.

erzeugt (denn $\rho \neq 0$ [31]). Letztere erfüllt $\rho^3 \in K(\sqrt{d_f}, \zeta)$. Wir führen zuerst folgende Rechnungen durch

$$\rho^3 = w_1^3 + w_2^3 + w_3^3 + 3\zeta(w_1^2 w_2 + w_2^2 w_3 + w_3^2 w_1) + 3\zeta^2(w_1 w_2^2 + w_2 w_3^2 + w_3 w_1^2) + 6 w_1 w_2 w_3$$
$$\sqrt{d_f} = w_1^2 w_2 + w_2^2 w_3 + w_3^2 w_1 - w_1 w_2^2 - w_2 w_3^2 - w_3 w_1^2$$
$$\Longrightarrow \rho^3 = w_1^3 + w_2^3 + w_3^3 - \tfrac{3}{2}(w_1^2 w_2 + w_2^2 w_3 + w_3^2 w_1 + w_1 w_2^2 + w_2 w_3^2 + w_3 w_1^2) + 6 w_1 w_2 w_3 - \tfrac{3}{2}\sqrt{-3}\sqrt{d_f}\ ,$$

und drücken sodann die symmetrischen Funktionen in den w_i durch die elementar-symmetrischen Funktionen $0 = w_1 + w_2 + w_3$, $a = w_1 w_2 + w_1 w_3 + w_2 w_3$, $b = -w_1 w_2 w_3$ in den w_i aus und erhalten

$$w_1^3 + w_2^3 + w_3^3 + 3(w_1^2 w_2 + w_2^2 w_3 + w_3^2 w_1 + w_1 w_2^2 + w_2 w_3^2 + w_3 w_1^2) + 6 w_1 w_2 w_3 = 0\,(= 0^3\,)$$
$$\tfrac{9}{2}(w_1^2 w_2 + w_2^2 w_3 + w_3^2 w_1 + w_1 w_2^2 + w_2 w_3^2 + w_3 w_1^2) + \tfrac{27}{2} w_1 w_2 w_3 = 0\,(= \tfrac{9}{2} 0 a\,)$$
$$\tfrac{27}{2} w_1 w_2 w_3 = -\tfrac{27}{2} b$$
$$\Longrightarrow \rho^3 = -\tfrac{27}{2} b + \tfrac{3}{2}\sqrt{-3}\sqrt{d_f}$$

Setze $\rho_0 = w_1 + w_2 + w_3 = 0$, $\rho_1 = \rho$ und $\rho_2 = w_1 + \zeta^2 w_2 + \zeta w_3$; dann ist

$$3w_1 = \rho_0 + \rho_1 + \rho_2 = \sqrt[3]{-\frac{27}{2} b + \frac{3}{2}\sqrt{-3 d_f}} + \sqrt[3]{-\frac{27}{2} b - \frac{3}{2}\sqrt{-3 d_f}}$$

und entsprechend bekommt man w_2, w_3. Die dritten Wurzeln $\sqrt[3]{}$ sind so zu wählen, daß die Gleichung $\rho_1 \rho_2 = w_1^2 + w_2^2 + w_3^2 - w_1 w_2 - w_1 w_3 - w_2 w_3 = -3a$ erfüllt ist.

Konstruktionen mit Zirkel und Lineal aus gegegenen Größen führen auf lineare und quadratische Gleichungen. Dabei arbeiten wir in jedem Schritt in der komlexen Ebene $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ und erlauben

die Wahl endlich vieler Hilfspunkte

die Zeichnung der Verbindungsgeraden durch zwei gewählte oder schon konstruierte Punkte

die Zeichnung des Kreises mit gewähltem oder konstruiertem Mittelpunkt und einem solchem auf seiner Peripherie

den Schnitt zweier schon konstruierter Geraden oder Kreise, oder einer Geraden mit einem Kreis.

Der Koordinatenkörper kann sich bei jedem Schritt ändern, aber natürlich nicht bei den beiden erstgenannten. Die Addition, Substraktion, Multiplikation und Division in $\mathbb{C}$ spiegelt sich geometrisch in Parallelogrammen (für + und -) und im Strahlensatz (für $\times$ und : [mit der Hilfsgröße 1]) wider.

Beim dritten und vierten treten quadratische Gleichungen für die zu bestimmenden Koordinaten auf: diese führen also auf quadratische Erweiterungen des Koordinatenkörpers. Man beachte, daß auch der Schnitt zweier Kreise nur lineare und quadratische Gleichungen liefert. Man legt nämlich das Koordinatensystem so, daß ein Kreis den Urprung als Mittelpunkt hat – dies ist eine lineare Umformung und führt auf

$$x^2 + y^2 = r\,,\ (x - x_0)^2 + (y - y_0)^2 = s \Longrightarrow 2x_0 x + 2y_0 y = r - s + x_0^2 + y_0^2\,,\ x = \pm\sqrt{r - y^2}.$$

[31] ρ resultiert aus Hiberts Satz 90 angewendet auf $\alpha = \zeta$. Dasselbe mit ζ ersetzt durch 1 bzw. ζ^{-1} liefert ein $\rho_0 = 0$ bzw. ein ρ_2. Wegen $\rho_0 + \rho + \rho_2 = 3w_1$ und $\rho \cdot \rho_2 = -3a$ ist also tatsächlich $\rho \neq 0$.

Eine quadratische Gleichung (in einer komplexen Variablen) kann in $x^2 = d = r(\cos\varphi + i\sin\varphi)$ substituiert werden. Um $\sqrt{d}$ zu konstruieren, zeichnet man die Strecke $[0, r+1]$ und darüber den Thaleskreis; nach dem Höhensatz ist $\sqrt{r}$ der Abstand vom Kreis zur Strecke bei 1; außerdem muß natürlich noch der Winkel φ halbiert werden. Wir sehen damit

> *Aus den Anfangsdaten $\alpha_1, \ldots, \alpha_n$ ist die Größe β mit Zirkel und Lineal genau dann konstruierbar, wenn β algebraisch über $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ ist und die galoissche Hülle von $K(\beta)$ über K 2-Potenzgrad hat.*

In der Tat ist die angegebene Bedingung äquivalent zur Existenz eines Körperturms

$$K(\beta) \subset K_r \supset K_{r-1} \supset \ldots \supset K_1 \supset K_0 = K$$

mit $[K_{i+1} : K_i] = 2$. Somit ist z.B. die Quadratur des Kreises ($\pi r^2 = a^2$) unmöglich [32], weil π über $\mathbb{Q}$ transdendent ist (für den Transzendenzbeweis von π vgl. etwa Langs Buch). Auch die Dreiteilung des Winkels ist mit Zirkel und Lineal i.allg. nicht durchführbar, sonst käme man etwa von 120^0 zu 40^0, also von ζ_3 zu ζ_9 im Widerspruch zu $[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\zeta_3)] = 3$. Und welche regelmäßigen n-Ecke konstruierbar sind, hängt allein vom Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ ab.

SATZ. *Das regelmäßige n-Eck ist genau dann konstruierbar, wenn*

$$n = 2^r \prod_i (1 + 2^{2^{r_i}})$$

mit verschiedenen Primzahlen $1 + 2^{2^{r_i}}$ gilt.

Eine Zahl $1 + 2^n$ kann nur prim sein, wenn n eine Potenz von 2 ist. Die Zahlen $1 + 2^{2^r}$ heißen Fermatzahlen; diese sind für $r = 0, 1, 2, 3, 4$ prim; aber $641 \mid 1 + 2^{32}$. Außer den 5 angegebenen Fermat-Primzahlen kennt man heute keine weitere.

Die Konstruktion des regelmäßigen p-Ecks, p eine Fermat-Primzahl, erfordert die explizite Konstruktion sukzessiver Quadratwurzeln, um den Körperturm

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_r \subset K_{r+1} = \mathbb{Q}(\zeta_p)$$

in Schritten $[K_i : K_{i-1}] = 2$ aufbauen zu können.
Dazu sehen wir uns zunächst eine allgemeine galoissche Körpererweiterung L/K mit Gruppe G an; $\alpha \in L$ erzeuge eine Normalbasis. Ist nun $U \leq G$ und $F = L^U$ der zugehörige Fixkörper, so gilt

1. α erzeugt auch eine Normalbasis für L/F.
2. $\{\mathrm{Sp}_{L/F}(\tau(\alpha)) = \sum_{\sigma \in U} \sigma\tau(\alpha) : G = \bigcup_\tau U\tau\}_\tau$ ist eine Basis von F/K, falls $G = \bigcup_\tau U\tau$ eine disjunkte Zerlegung von G in Rechtsnebenklassen $U\tau$, $\tau \in G$, von U ist.
3. Ist $U \lhd G$, also F/K galoissch, so erzeugt $\mathrm{Sp}_{L/F}(\alpha)$ den Körper F über K.

Einheitswurzelkörper $\mathbb{Q}(\zeta_p)$ haben offenbar in $\alpha = \zeta_p$ ein Normalbasiserzeugendes:

$$\{\sigma(\zeta_p) : \sigma \in G_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\} = \{\zeta_p^i : 1 \leq i \leq p-1\}\,,$$

[32] unsere Anfangsdaten α_j seien im folgenden stets 0,1 , und $K = \mathbb{Q}$

und letztere Menge besteht aus über $\mathbb{Q}$ linear unabhängigen Elementen, weil $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ zufolge der Irreduzibilität des p-ten Kreisteilungspolnoms über $\mathbb{Q}$ unabhängig ist [33].

Nützen wir das für $p = 17$ aus. Unser Körperturm ist $\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset \mathbb{Q}(\zeta)$ mit $\zeta = \zeta_{17}$. Die Gruppe $G = G_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ ist zyklisch, erzeugt etwa von

$$\sigma\,,\ \sigma(\zeta) = \zeta^3\,,$$

(denn 3 ist eine Primitivwurzel modulo 17). Die Untergruppe der Ordnung 8 von G ist von σ^2 erzeugt, K_1 also von

$$a_1 = \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2\,.$$

Das dazu konjugierte Element in K_1 ist

$$a_2 = \sigma(a_1) = \zeta^3 + \zeta^{-7} + \zeta^5 + \zeta^{-6} + \zeta^{-3} + \zeta^7 + \zeta^{-5} + \zeta^6\,.$$

Wegen $\sum_{i=0}^{16} \zeta^i = 0$ gilt $a_1 + a_2 = -1$, und man rechnet direkt $a_1 a_2 = -4$ nach. Deshalb, und weil $a_1 > a_2$, ist $a_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{17}$.
Die Untergruppe der Ordnung 4 von G ist von σ^4 erzeugt, K_2 also von $b_1 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4$ mit Konjugiertem (über K_1) $b_2 = \sigma^2(b_1) = \zeta^{-8} + \zeta^{-2} + \zeta^2 + \zeta^8$. Wieder rechnet man $b_1 + b_2 = a_1$, $b_1 b_2 = -1$, $b_1 > b_2$ nach; es folgt, daß hier die Lösungen von $x^2 - a_1 x - 1 = 0$ vorliegen. σ^8 erzeugt die Untergruppe der Ordnung 2 von G und deshalb $c_1 = \zeta + \zeta^{-1}$ den Körper K_3; $c_2 = \sigma^4(c_1) = \zeta^{-4} + \zeta^4$ ist das Konjugierte von c_1 über K_2. Wir haben $c_1 + c_2 = b_1$, $c_1 c_2 = \zeta^3 + \zeta^5 + \zeta^{-3} + \zeta^{-5} = \sigma(b_1)$, $c_1 > c_2$; somit sind c_1, c_2 die Lösungen von $x^2 - b_1 x + \sigma(b_1)$. Wie kommen wir an $\sigma(b_1)$? So: $\sigma(b_1)$ und $\sigma^3(b_1)$ lösen $x^2 - a_2 x - 1 = 0$ und $\sigma(b_1) > \sigma^3(b_1)$. Endlich ist noch ζ eine Lösung von $x^2 - c_1 x + 1 = 0$, und jede solche erzeugt das regelmäßige 17-Eck.

In diesem Zusammenhang [34] sei folgendes beobachtet:

> *Die Körpererweiterung $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ ist zyklisch von der Ordnung $p-1$ und enthält deshalb für $p \geq 3$ genau einen Teilkörper vom Index 2, nämlich $K_o = \mathbb{Q}(\zeta_p) \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, und einen vom Grad 2 über $\mathbb{Q}$, nämlich $K_u = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p})$. Die irreduzible Gleichung für ζ_p über K_o ist $x^2 - (\zeta_p + \zeta_p^{-1})x + 1$.*

Spezielle abelsche Erweiterungen spezieller Körper (Kummertheorie)

Die Körper K sind dadurch ausgezeichnet, daß sie eine gegebene primitive Einheitswurzel $\zeta = \zeta_n$ enthalten; die Erweiterungen L/K sind alle galoissch abelschen Erweiterungen mit $[\sigma \in G(L/K) \Longrightarrow \sigma^n = 1]$. Diese werden im folgenden allein durch "innere Daten" von K beschrieben. Es handelt sich dabei um eine Fortsetzung der Diskussion, die mit dem dritten Satz auf S. 24

> *Sei $\zeta_n \in K$. Ist dann M/K zyklisch vom Grad $|n$, so existiert ein $a \in K$ mit $M = K(\sqrt[n]{a})$. Umgekehrt ist jede Erweiterung $K(\sqrt[n]{a})/K$ zyklisch vom Grad $|n$.*

eingeleitet wurde.

[33] Das zeigt zugleich, daß ζ_{p^t} für $t > 1$ *keine* Normalbasis in $\mathbb{Q}(\zeta_{p^t})/\mathbb{Q}$ erzeugt!
[34] Auch dazu mehr im kommenden Semester.

DEFINITION. *1. Ist G eine endliche Gruppe, so ist der Exponent von G durch $exp(G) = \min\{t \in \mathbb{N} : g^t = 1 \ (\forall\, g \in G)\}$ definiert; insbesondere gilt also $\exp(G) \mid |G|$ und $[\, G \text{ zyklisch} \Longrightarrow \exp(G) = |G|\,]$ (aber $\exp(S_3) = 6$).*

2. Ist $n \in \mathbb{N}$ und L/K galoissch, so heißt L/K vom Exponenten $|n$, falls $\exp(G_{L/K}) \mid n$.

Ab jetzt sei also $n \in \mathbb{N}$ vorgegeben und K ein gegebener Körper mit $\mathrm{char}(K) \nmid n$ und $\zeta_n \in K$. Es bezeichne $(K^\times)^n$ die Untergruppe von $K^\times$, die aus allen n-ten Potenzen der Elemente $0 \neq a \in K$ besteht; des weiteren $\overline{U}$ eine endliche Untergruppe von $K^\times/(K^\times)^n$ und $U \geq (K^\times)^n$ ihr volles Urbild in $K^\times$.

LEMMA. *1. Ist L/K galoissch abelsch vom Exponenten $|n$, so gilt $L = K(\alpha_1, \ldots, \alpha_r)$ mit $\alpha_i^n = a_i \in K^\times$ $(1 \leq i \leq r)$.*

2. Jede Erweiterung $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ von K ist galoissch abelsch vom Exponenten $|n$.

3. Es sei L wie oben, $U_L = \langle a_1, \ldots, a_r, (K^\times)^n \rangle \leq K^\times$ und $\overline{U}_L = U_L/(K^\times)^n$. Dann ist durch

$$G_{L/K} \times \overline{U}_L \to \langle \zeta_n \rangle \ : \quad (\sigma, \overline{a}) \mapsto \sigma(\alpha)/\alpha \quad , \quad \alpha^n = a$$

eine in beiden Arumenten multiplikative Funktion erklärt (eine Bilinearform*), die nichtausgeartet im folgenden Sinne ist:*

$$(\sigma, \overline{a}) = 1 \begin{cases} \forall\, \sigma \in G_{L/K} \\ \forall\, a \in U_L \end{cases} \Longrightarrow \begin{cases} a \in (K^\times)^n \\ \sigma = 1 \end{cases} .$$

Man beachte, daß obige Bilinearform wohldefiniert ist, also nicht von der Wahl einer speziellen n-ten Wurzel $\alpha = \sqrt[n]{a}$ abhängt: zwei solche unterscheiden sich nämlich um eine Potenz von ζ_n und $\zeta_n \in K$.

DEFINITION. *Ist G eine endliche abelsche Gruppe, so heißt $G^* \stackrel{\text{def}}{=} \mathrm{Hom}(G, \mathbb{C}^\times)$ die Charaktergruppe von G.*

Elemente $\chi, \psi \in G^*$, also *Charaktere von G*, werden so multipliziert: $(\chi \cdot \psi)(g) = \chi(g) \cdot \psi(g)$, ε mit $\varepsilon(g) = 1$ $(\forall\, g \in G)$ ist also das Einselement in G^*.
In unserer Situation ($G = G(L/K)$, $\zeta_n \in K$, $\exp(G) \mid n$) hat man übrigens über

$$\mathbb{Z}/n \overset{1 \leftrightarrow \zeta_n}{\simeq} \langle \zeta_n \rangle \overset{\zeta_n \mapsto e^{2\pi i/n}}{\leq} \mathbb{C}^\times$$

natürliche Identifizierungen $\mathrm{Hom}(G, \mathbb{Z}/n) = \mathrm{Hom}(G, \langle \zeta_n \rangle) = G^*$.

LEMMA. $|G| = |G^*|$

FOLGERUNG. *1.* $[L : K] = [U_L : (K^\times)^n]$.

2. Die Korrespondenz

(a) L/K, L/K ist abelsch vom Exponenten $|n$, und
(b) $(K^\times)^n \leq U_L \leq K^\times$, $[U_L : (K^\times)^n] < \infty$

ist eineindeutig und $L = K(\sqrt[n]{U_L})$.

Das letzte Lemma sagt nicht die volle Wahrheit. Es gilt nämlich über $|G| = |G^*|$ hinaus

LEMMA. *G und G^* sind (unkanonisch) isomorph. G und $(G^*)^*$ sind jedoch kanonisch isormorph:*

$$(G^*)^* \simeq G \quad \text{durch} \quad (G^*)^* \ni \gamma \leftrightarrow g \in G : \gamma(\chi) = \chi(g)\,.$$

Und (mit den Bezeichnungen aus der Folgerung): $G(L/K) \simeq (\overline{U}_L)^*$.

Anwendung:

1. Die abelschen Erweiterungen vom Exponenten 2 von $\mathbb{Q}$ sind genau die Körper

   $$\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r}) \text{ mit ganzen Zahlen } a_i \text{ ohne quadratische Teiler}\,.$$

   Die zugehörige Galoisgruppe ist isomorph zu $\mathrm{Hom}(\langle a_1, \ldots, a_r, (\mathbb{Q}^\times)^2\rangle, \mathbb{F}_2)$ und hat die Ordnung $[\langle a_1, \ldots, a_r, (\mathbb{Q}^\times)^2\rangle : (\mathbb{Q}^\times)^2]$. Sind die $a_1, \ldots, a_r$ zueinander teilerfremde ganze Zahlen, so ist diese Ordnung $= 2^r$. Insbesondere sind die Wurzeln aus r verschiedenen Primzahlen linear unabhängig über $\mathbb{Q}$ (im $\mathbb{Q}$-Vektorraum $\mathbb{R}$).

2. Ist $[\langle a_1, \ldots, a_r, (\mathbb{Q}^\times)^2\rangle : (\mathbb{Q}^\times)^2] = 2^r$, so sind die $\mathbb{Q}(\sqrt{a_{i_1} \cdots a_{i_s}})$ mit $i_{j_1} \neq i_{j_2}$ für $j_1 \neq j_2$ und $1 \leq s \leq r$ die sämtlichen über $\mathbb{Q}$ quadratischen Teilkörper von $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r})$.

Wir hängen in diesem Zusammenhang noch ein paar Beobachtungen über abelsche Gruppen G an (*Dualitätstheorie*).

LEMMA. *1.* $\displaystyle\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \varepsilon \\ |G| & \text{if } \chi = \varepsilon \end{cases} \quad ; \quad \sum_{\chi \in G^*} \chi(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1 \end{cases}$

2. Jeder Charakter einer Untergruppe von G läßt sich zu einem Charakter von G fortsetzen.

3. Für Untergruppen $V \leq G$ gilt $V^* \simeq G^*/V^\perp$ mit

$$V^\perp = \{\varphi \in G^* : \varphi(v) = 1 \ (\forall\, v \in V)\} \leq G^*\,,$$

nämlich vermöge der Restriktionsabbildung $G^* \to V^*$; insbesondere $|V| \cdot |V^\perp| = |G|$.

Man beachte die Analogie *Charakter* $\leftrightarrow$ *Linearform* in der Dualitätstheorie endlich dimensionaler Vektorräume.