ALGEBRA II

Prof. Dr. B. Pareigis

Sommer Semester 2003

Inhalt

1. Der Hauptsatz der Galoistheorie 2
2. Nullstellen von Polynomen 3
3. Konstruktionen mit Zirkel und Lineal 4
4. Elementare Gruppentheorie 4
5. Die Sylowschen Sätze 4
6. Elementare Theorie der kommutativen Ringe 5
7. Elementare Theorie der Körper und Polynome 6
8. Normale und separable Körpererweiterungen 7
9. Endliche Körper 8
10. Symmetrische Funktionen und allgemeine Polynome 8
11. Die Galoisgruppe von Polynomen niedrigen Grades 12
12. Kreisteilungskörper 16
13. Zyklische Erweiterungen und Kummererweiterungen 19
14. Radikalerweiterungen 22
15. Konstruktion regelmäßiger n-Ecke 26
16. Zahlen zur Basis p 27
17. Bewertungen 30
18. Cauchy-Folgen 33
19. Die p-adischen Zahlen 35

Wiederholung aus Algebra I

1. Der Hauptsatz der Galoistheorie

Hauptsatz 1.1 (über endlich erzeugte, abelsche Gruppen)**.** *Sei G eine endlich erzeugte abelsche Gruppe.*

(1) *Es gibt eindeutig bestimmte natürliche Zahlen s, t, $m_1, \ldots, m_s$* (Elementarteiler) *mit $m_i > 1$, m_i/m_{i+1} für alle $i = 1, \ldots, s-1$, so daß*

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_s\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{t-mal}. \tag{1}$$

(2) *Es gibt (bis auf die Reihenfolge) eindeutig bestimmte natürliche Zahlen n, t, $j_1, \ldots, j_n$ alle ≥ 1 und $p_1, \ldots, p_n$ alle prim mit*

$$G \cong \mathbb{Z}/p_1^{j_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_n^{j_n}\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{t-mal}. \tag{2}$$

Ist G endlich, so ist in beiden Darstellungen $t = 0$ und $|G| = \prod_{i=1}^{s} m_i = \prod_{i=1}^{n} p_i^{j_i}$.

Beispiele 1.2. (1) 6 läßt keine weitere Zerlegung nach (1) zu, aber die Zerlegung $6 = 2 \cdot 3$ nach (2). Also ist $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.
(2) Es gibt 6 nichtisomorphe endliche abelsche Gruppen der Ordnung 1500. Die Primzahlzerlegung nach (2) kann nämlich geschrieben werden als

$$1500 = 2^2 \cdot 3 \cdot 5^3 = 2 \cdot 2 \cdot 3 \cdot 5^3 = 2^2 \cdot 3 \cdot 5 \cdot 5^2 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5^2 = 2^2 \cdot 3 \cdot 5 \cdot 5 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 5.$$

Damit erhalten wir die folgenden Elementarteilerzerlegungen für G:

$$\mathbb{Z}_{1500} \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_{750} \ncong \mathbb{Z}_5 \oplus \mathbb{Z}_{300} \ncong \mathbb{Z}_{10} \oplus \mathbb{Z}_{150} \ncong \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{60} \ncong \mathbb{Z}_5 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{30}.$$

(3) Sei $G = \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54}$. Die Primteiler sind dann 2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2. Die Elementarteiler sind damit $15, 90, 2700$. Also ist

$$G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{2700}.$$

Definition 1.4. Eine Körpererweiterung $F : K$ heißt *galoissch*, wenn es eine endliche Untergruppe $G \subseteq \mathrm{Aut}(F/K)$ gibt mit $K = \mathrm{Fix}(F; G)$. Dann heißt G *Galoisgruppe von F über K*.

Satz 1.12 (Dedekind)**.** *Seien $\sigma_1, \ldots, \sigma_n$ paarweise verschiedene Charaktere von G in K ($\sigma_i : G \longrightarrow K^*$). Dann sind $\sigma_1, \ldots, \sigma_n \in \mathrm{Abb}(G, K)$ linear unabhängig über K.*

Satz 1.18 (Fortsetzungssatz)**.** *Sei $F : K$ galoissch mit Galoisgruppe G. Seien L_1, L_2 Zwischenkörper $K \subseteq L_i \subseteq F$ und $\varphi : L_1 \longrightarrow L_2$ ein K-Isomorphismus. Dann gibt es ein $g \in G$ mit $\forall a \in L : g(a) = \varphi(a)$.*

Definition 1.19. Zwei Untergruppen $U_1, U_2 \subseteq G$ heißen *konjugiert*, wenn es ein $g \in G$ gibt mit $gU_1g^{-1} = U_2$.

Definition 1.22. Sei $F : K$ galoissch. Zwei Zwischenkörper L_1, L_2 mit $K \subseteq L_i \subseteq F$ heißen *konjugiert*, wenn es einen K-Isomorphismus $\varphi : L_1 \cong L_2$ gibt.

Hauptsatz 1.21 (der Galoistheorie). *Sei $F : K$ eine galoissche Körpererweiterung mit Galoisgruppe $G \subseteq \mathrm{Aut}(F/K)$. Sei*

$$\mathcal{Z} := \{L | K \subseteq L \subseteq F \textit{ Zwischenkörper}\}$$

und

$$\mathcal{U} := \{U | U \subseteq G \textit{ Untergruppe}\}.$$

Dann gelten

(1) $\mathcal{Z} \ni L \mapsto \mathrm{Aut}(F/L) \in \mathcal{U}$ *und* $\mathcal{U} \ni U \mapsto \mathrm{Fix}(F;U) \in \mathcal{Z}$ *sind zueinander inverse Abbildungen.*
(2) $U_1 \subseteq U_2 \iff \mathrm{Fix}(F;U_1) \supseteq \mathrm{Fix}(F;U_2)$ *oder äquivalent* $L_1 \subseteq L_2 \iff \mathrm{Aut}(F/L_1) \supseteq \mathrm{Aut}(F/L_2)$.
(3) U_1 *konjugiert zu* U_2 *in* $G \iff \mathrm{Fix}(F;U_1)$ *konjugiert zu* $\mathrm{Fix}(F;U_2)$ *(mit demselben $g \in G$).*
(4) $U \subseteq G$ *normale Untergruppe* $\iff L = \mathrm{Fix}(F;U)$ *galoissch über K. In diesem Falle ist* $\mathrm{Aut}(L/K) \cong \mathrm{Aut}(F/K)/\mathrm{Aut}(F/L) = G/U$.
(5) *Für alle $L \in \mathcal{Z}$ ist F galoissch über L mit Galoisgruppe* $\mathrm{Aut}(F/L)$, *und es gilt* $|\mathrm{Aut}(F/L)| = [F : L]$.

2. Nullstellen von Polynomen

Definition 2.3. Sei $F : K$ eine Körpererweiterung. $u \in F$ heißt *algebraisch über K*, wenn es ein $f \in K[x] \setminus \{0\}$ gibt mit $f(u) = 0$. Ist $u \in F$ nicht algebraisch, so heißt *u transzendent*.

Definition 2.7 (vgl. 6.10). Sei $p \in K[x]$. p heißt *irreduzibel*, wenn

(1) $p \neq 0$ und p keine Einheit in $K[x]$.
(2) Wenn $p = q \cdot r$, dann ist q oder r eine Einheit in $K[x]$.

Satz 2.9 (vgl. 6.3). *Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring R. I ist genau dann ein maximales Ideal, wenn R/I ein Körper ist.*

Satz 2.10. *Sei $F : K$ eine Körpererweiterung, und sei $u \in F$ algebraisch über K. Dann ist*

(1) $K[u] = K(u)$ *(diese Bedingung ist äquivalent zur Bedingung u algebraisch über K).*
(2) $K[u] \cong K[x]/(p(x))$, *wobei $p(x)$ ein irreduzibles Polynom aus $K[x]$ mit höchstem Koeffizienten 1 vom Grad ≥ 1* (normiert) *ist, das eindeutig durch die Bedingung $p(u) = 0$ bestimmt wird und* Minimalpolynom *von u genannt wird. Weiter gilt:*

$$f(u) = 0 \iff \exists r(x) \in K[x] : f(x) = r(x) \cdot p(x).$$

(3) $n := [K(u) : K] = \mathrm{Grad}(p(x))$.
(4) $\{1, u, u^2, \ldots, u^{n-1}\}$ *ist eine K-Vektorraum-Basis von $K(u)$.*
(5) *Jedes Element von $K(u)$ hat eine eindeutige Darstellung der Form $\alpha_0 + \alpha_1 u + \ldots + \alpha_{n-1} u^{n-1}$ mit $\alpha_i \in K$.*

Satz 2.12 (über die Existenz von Nullstellen von Polynomen). *Sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad $n \geq 1$. Dann gibt es eine einfache Körpererweiterung $F = K(u)$ von K, so daß gelten*

(1) *u ist Nullstelle von $f(x)$, d.h. $f(u) = 0$.*
(2) *$[K(u) : K] \leq n$, wobei Gleichheit genau dann gilt, wenn $f(x)$ irreduzibel ist.*
(3) *Wenn $f(x)$ irreduzibel in $K[x]$ ist, dann ist $K(u)$ bis auf K-Isomorphie eindeutig bestimmt.*

Definition 2.13. Sei $f(x) \in K[x]$ irreduzibel. Dann ist $K(u) := K[x]/(f(x))$ der Körper, den man durch *Adjunktion einer Nullstelle* des Polynoms f an K erhält.
Beachte: Unter dieser Sicht sind alle Nullstellen eines irreduziblen Polynoms gleichwertig.

Folgerung 2.14. *Sei $f(x) \in K[x]$ vom Grad $n \geq 1$. Dann gibt es eine endliche Körpererweiterung $F : K$, so daß $f(x)$ in $F[x]$ vollständig in Linearfaktoren zerfällt.*

3. Konstruktionen mit Zirkel und Lineal

Hauptsatz 3.6. *Ein Punkt $(p, q) \in \mathbb{R}^2$ ist über K für einen Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ genau dann konstruierbar, wenn es eine endliche Folge von Körpern K_i mit*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{R}$$

gibt mit $p, q \in K_n$, wobei $K_i = K_{i-1}(\sqrt{a_i})$, $a_i \in K_{i-1}$, $a_i > 0$ für $i = 1, \ldots, n$.

4. Elementare Gruppentheorie

Satz 4.11. *Sei $U \subseteq G$ eine Untergruppe. Dann sind äquivalent:*
(1) *U ist Normalteiler in G.*
(2) *$G/U = U \backslash G$ ($\{gU | g \in G\} = \{Ug | g \in G\}$).*
(3) *$\Phi : G/U \times G/U \longrightarrow G/U$ mit $\Phi(aU, bU) := abU$ ist eine wohldefinierte Abbildung.*

Wenn (3) gilt, ist G/U mit dieser Multiplikation eine Gruppe (Restklassen-, Nebenklassen-, Faktor-, Quotienten-Gruppe).

Satz 4.13 (Lagrange)**.** *Sei G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe. Dann ist*

$$|G| = |U| \cdot |G : U|.$$

Folgerung 4.24 (Satz von Euler)**.** *Sei G eine endliche Gruppe und $g \in G$. Sei $n = |G|$ die Ordnung von G. Dann ist $g^n = e$.*

Definition 4.27. Eine Gruppe G heißt *einfach*, wenn Sie keinen nichttrivialen Normalteiler besitzt.

Beispiel 4.28. Die einfachen abelschen Gruppen sind die Gruppen $\mathbb{Z}/p\mathbb{Z}$ mit p prim bzw. $G = \{e\}$.

Satz 4.29. *Die alternierenden Gruppen A_n sind genau dann einfach, wenn $n \neq 4$ ist.*

5. Die Sylowschen Sätze

Satz 5.8 (Sylow I)**.** *Sei G eine Gruppe der Ordnung $n = p^r \cdot m$ mit $(m, p) = 1$. Dann besitzt G eine Untergruppe der Ordnung p^r.*

Folgerung 5.9 (Cauchy)**.** *Wenn $p/|G|$, dann gibt es in G ein Element g der Ordnung p.*

Definition 5.10. Wenn $|G| = p^r \cdot m$ mit $(m, p) = 1$ und $r \geq 1$, dann heißen die Untergruppen $H \subseteq G$ mit $|H| = p^r$ p-Sylow-Untergruppen von G.
Eine Gruppe der Ordnung p^i, $i \geq 1$ heißt eine p-Gruppe.

Satz 5.12. *Jede p-Gruppe $G \neq \{e\}$ besitzt ein Zentrum $Z(G) \neq \{e\}$.*

Satz 5.13. *Sei G eine p-Gruppe der Ordnung p^r. Dann gibt es eine Kette*

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_r = \{e\}$$

von Normalteilern H_i von G mit $|H_{i-1} : H_i| = p$, $i = 1, \ldots, r$.

Satz 5.14 (Sylow II). *Sei $K \subseteq G$ eine Untergruppe, deren Ordnung durch p teilbar ist und sei $H \subseteq G$ eine p-Sylow-Untergruppe. Dann gibt es eine konjugierte Untergruppe $H' = gHg^{-1}$, so daß $K \cap H'$ eine p-Sylow-Untergruppe von K ist.*

Satz 5.16 (Sylow III). *Sei $|G| = p^r \cdot m$ mit $(m,p) = 1$. Sei s die Anzahl der p-Sylow-Untergruppen von G. Dann gilt*

$$s/m \quad \textit{und} \quad s \equiv 1 \mod (p).$$

6. Elementare Theorie der kommutativen Ringe

Definition 6.1. Ein nullteilerfreier kommutativer Ring R heißt *Integritätsring*.

Definition 6.2. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ und wenn für alle Ideale $I, J \subseteq R$ gilt

$$I \cdot J \subseteq \mathfrak{p} \Longrightarrow I \subseteq \mathfrak{p} \text{ oder } J \subseteq \mathfrak{p}.$$

Beachte: Wenn $I = (m)$ und $J = (n)$ Hauptideale in R sind, so ist

$$I \subseteq J \iff n/m.$$

Lemma 6.3. *Sei R ein kommutativer Ring. Dann gelten*

(1) *$\mathfrak{p} \subseteq R$ Primideal $\iff$ $R/\mathfrak{p}$ Integritätsring.*
(2) *$\mathfrak{m} \subseteq R$ maximales Ideal $\iff$ $R/\mathfrak{m}$ Körper.*

Satz 6.5. *Jeder Ring $R \neq 0$ (mit Einselement) besitzt über jedem Ideal $I \subsetneqq R$ ein maximales Ideal.*

Definition 6.7. Ein Integritätsring R heißt *Hauptidealring*, wenn jedes Ideal ein Hauptideal ist.

Definition 6.8. Ein Integritätsring R heißt *euklidischer Ring*, wenn es eine Abbildung $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ gibt mit

(1) $\forall a, b \in R \setminus \{0\} : \varphi(ab) \geq \varphi(a)$.
(2) $\forall b \in R, a \in R \setminus \{0\} \exists q, r \in R : b = qa + r$ und ($r = 0$ oder $\varphi(r) < \varphi(a)$). (Divisionsalgorithmus)

Satz 6.9. *Jeder euklidische Ring ist ein Hauptidealring.*

Definition 6.10. (1) Ein Element $p \in R$ heißt *Primelement* oder *prim*, wenn
   (a) $p \neq 0$ und p ist keine Einheit;
   (b) $p/ab \Longrightarrow p/a$ oder p/b.
(2) Ein Element $p \in R$ heißt *irreduzibel*, wenn
   (a) $p \neq 0$ und p ist keine Einheit;
   (b) $p = ab \Longrightarrow a$ Einheit oder b Einheit.

Beachte: p Primelement $\Longrightarrow$ (p) Primideal. Aber ein Primideal darf 0 sein, während ein Primelement immer $p \neq 0$ erfüllt.

Satz 6.12. *Sei R ein Integritätsring.*

(1) *$\mathfrak{p} \subseteq R$ Primideal $\iff$*
   $R/\mathfrak{p}$ Integritätsring $\iff$
   $\forall a, b \in R : ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

(2) *$p \in R$ prim $\iff$ (p) Primideal und $p \neq 0$.*
(3) *$a \in R$ irreduzibel $\iff$ (a) maximal in der Menge der echten Hauptideale.*
(4) *Jedes Primelement ist irreduzibel: p prim $\implies$ p irreduzibel.*
(5) *R Hauptidealring $\implies$ (p prim $\iff$ p irreduzibel).*

Folgerung 6.13. *Sei K ein Körper. Für $p \in K[x]$ sind äquivalent:*
(1) *p ist irreduzibel.*
(2) *p ist prim.*
(3) *(p) ist ein maximales Ideal.*
(4) *(p) ist ein Primideal $\neq 0$.*

Satz 6.16 (Chinesischer Restsatz)**.** *Seien $A_1, \ldots, A_n \subseteq J \subseteq R$ Ideale. Dann gibt es einen Ringhomomorphismus (beachte hier: Ideale sind Ringe ohne 1-Element)*

$$\varphi : J/(A_1 \cap \ldots \cap A_n) \longrightarrow J/A_1 \times \ldots \times J/A_n.$$

Wenn $J^2 + A_i = J$ für alle i und $A_i + A_j = J$ für alle $i \neq j$, dann ist φ ein Isomorphismus.

Definition 6.18. Ein Integritätsring R heißt *Z.P.E. Ring* oder *faktorieller Ring*, wenn
(1) $\forall r \in R \setminus \{0\}$ keine Einheit $\exists p_1, \ldots, p_n \in R$ irreduzibel:

$$r = p_1 \cdot \ldots \cdot p_n.$$

(2) Sind p_i, q_i irreduzibel mit $p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_t$, so ist $s = t$, und es gibt ein $\sigma \in S_t$, so daß p_i assoziiert zu $q_{\sigma(i)}$ ist für alle $i = 1, \ldots, t$.

Satz 6.20. *Jeder Hauptidealring ist ein faktorieller Ring.*

7. Elementare Theorie der Körper und Polynome

Satz 7.3. *Sei K ein Körper mit $\chi(K) = p > 0$. Dann enthält K einen kleinsten Unterkörper K_0, und es ist $K_0 \cong \mathbb{Z}/p\mathbb{Z}$.*

Definition 7.5. $K(x) = Q(K[x]) := \{\frac{f}{g} | f, g \in K[x], g \neq 0\}$ heißt *Körper der rationalen Funktionen über K.*

Satz 7.6. *Sei K ein Körper mit $\chi(K) = 0$. Dann enthält K einen kleinsten Unterkörper K_0, und es ist $K_0 \cong \mathbb{Q}$.*

Definition 7.7. Die kleinsten möglichen Unterkörper $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Q}$ heißen *Primkörper.*

Satz 7.9. *Sei $F : K$ eine Körpererweiterung, $F = K(U)$ für $U \subseteq F$. Sei jedes $u \in U$ algebraisch. Dann ist $F : K$ algebraisch. Ist U zudem endlich, so ist $[F : K] < \infty$.*

Satz 7.11. *Sei $F : K$ ein Körpererweiterung und $L = \{a \in F | a$ algebraisch über $K\}$. Dann ist L der größte algebraische Zwischenkörper zwischen K ud F.*

Satz 7.12. *Sei $F : K$ ein Körpererweiterung und $u \in F \setminus \{0\}$. Dann sind äquivalent*
(1) *$u : K$ transzendent,*
(2) *$K[u] \subsetneqq K(u)$,*
(3) *$K(u) \cong K(x)$ = Funktionenkörper über K,*
(4) *$u^{-1} \notin K[u]$,*
(5) *$[K(u) : K] = \infty$.*

Satz 7.13. *Sei $\sigma : K \longrightarrow L$ ein Körperisomorphismus, u ein Element eines Erweiterungskörpers von K und v ein Element eines Erweiterungskörpers von L. Es gelte eine der beiden folgenden Bedingungen:*

(1) *u ist Nullstelle eines irreduziblen Polynoms $f \in K[x]$ und v ist Nullstelle von $\sigma(f) \in L[x]$.*
(2) *$u : K$ und $v : L$ sind transzendent.*

Dann gibt es einen Körperisomorphismus $\tau : K(u) \cong L(v)$ mit $\tau(u) = v$ und $(\tau|_K^L : K \longrightarrow L) = \sigma$.

Definition 7.15. Eine Körpererweiterung $F : K$ heißt *Zerfällungskörper* der Polynome $\{f_i | i \in I\}$, wenn alle f_i in $F[x]$ in Linearfaktoren zerfallen und F über K von den Nullstellen der f_i erzeugt wird.

Satz 7.17. *Sei $f \in K[x]$ nicht konstant. Dann existiert ein Zerfällungskörper F von f und es ist $[F : K] \leq \mathrm{Grad}(f)!$.*

Folgerung 7.19. *Je zwei Zerfällungskörper von f über K sind isomorph über K.*

Definition 7.20. Ein Körper L heißt *algebraisch abgeschlossen*, falls jedes (nicht-konstante) Polynom $f \in L[x]$ eine Nullstelle (und damit alle Nullstellen) in L besitzt, d.h. falls jedes über L algebraische Element schon in L liegt.

Satz 7.22 (Steinitz)**.** *Jeder Körper besitzt einen (bis auf Isomorphie) eindeutig bestimmten algebraischen Abschluß.*

8. Normale und separable Körpererweiterungen

Definition 8.1. Eine algebraische Körpererweiterung $F : K$ heißt *normal*, wenn jedes irreduzible Polynom $p \in K[x]$, das in F eine Nullstelle besitzt, in $F[x]$ in Linearfaktoren zerfällt.

Satz 8.2. *Sei $F : K$ ein endliche Körpererweiterung. Dann sind äquivalent:*

(1) *$F : K$ ist normal.*
(2) *F ist Zerfällungskörper eines Polynoms $f \in K[x]$.*

Definition 8.3. Sei $p \in K[x]$ irreduzibel. p heißt *separabel*, wenn p in einem Zerfällungskörper von p nur einfache Nullstellen hat.
Sei $F : K$ eine Körpererweiterung. Ein algebaisches Element $u \in F$ heißt *separabel*, wenn das Minimalpolynom von u separabel ist.
Sei $F : K$ eine algebraische Körpererweiterung. F heißt *separable Körpererweiterung* von K, wenn jedes Element von F über K separabel ist.
Ein Polynom $f \in K[x]$ heißt *separabel*, wenn alle irreduziblen Faktoren von f separabel sind.
Ist ein irreduzibles Polynom, ein algebraisches Element, eine algebraische Körpererweiterung, ein Polynom nicht separabel, so heißt es *inseparabel*.

Satz 8.4 (Emil Artin)**.** *Sei $F : K$ eine Körpererweiterung. Dann sind äquivalent*

(1) *F ist galoissch über K.*
(2) *F ist separabel, normal und endlich über K.*
(3) *F ist Zerfällungskörper eines separablen Polynoms über K.*

Folgerung 8.5. *Sei $L : K$ eine endliche separable Körpererweiterung. Dann gibt es eine galoissche Körpererweiterung $F : K$ mit $F \supseteq L \supseteq K$.*

Definition 8.7. Ein Körper K heißt *perfekt (vollkommen)*, wenn jede algebraische Körpererweiterung $F : K$ separabel ist.

Satz 8.9. *Ein irreduzibles Polynom $p \in K[x]$ ist genau dann separabel, wenn$p' \neq 0$.*

Folgerung 8.11. *Jeder Körper der Charakteristik 0 ist perfekt.*

Folgerung 8.13. *Jeder endliche Körper ist perfekt.*

Satz 8.15. *Sei $F : K$ eine Körpererweiterung. Dann sind äquivalent*

(1) *F ist einfach und algebraisch über K, d.h. $F = K(u)$ und $u : K$ algebraisch.*
(2) *Es gibt nur endlich viele Zwischenkörper $K \subseteq L \subseteq F$.*

Satz 8.16 (Satz vom primitiven Element)**.** *Jede endliche, separable Körpererweiterung $F : K$ ist einfach: $F = K(u)$. (u heißt dann ein* primitives Element *für F.)*

Satz 8.17 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

9. Endliche Körper

Satz 9.1. *Jeder endliche Körper besitzt p^n Elemente für eine Primzahl $p \in \mathbb{N}$. Zu jeder Zahl p^n gibt es (bis auf Isomorphie) genau einen Körper $GF(p^n)$ mit p^n Elementen. $GF(p^n)$ ist Zerfällungskörper von $x^{p^n} - x \in \mathbb{F}_p[x]$ mit $\mathbb{F}_p = GF(p) = \mathbb{Z}/p\mathbb{Z}$. (GF steht für Galois-Feld.)*

Satz 9.3. *Seien $K \subseteq L$ endliche Körper. Dann ist $L : K$ galoissch, $|L| = p^n$, $|K| = p^m$ und m/n. Weiter ist $\mathrm{Aut}(L/K) = \{1, \Phi^m, (\Phi^m)^2, \ldots, (\Phi^m)^{n-1}\}$, wobei $\Phi : L \longrightarrow L$, $\Phi(a) = a^p$ der Frobenius-Homomorphismus ist.*

Folgerung 9.4. *Sei $L = GF(p^n)$. Dann gibt es zu jedem m mit m/n genau einen Unterkörper $K \subseteq L$ mit $|K| = p^m$. Das sind genau alle Unterkörper von L.*

Satz 9.5. *Sei K ein Körper beliebiger Charakteristik. Sei G eine endliche Untergruppe der multiplikativen Gruppe $K \setminus \{0\}$. Dann ist G zyklisch.*

Algebra II

10. Symmetrische Funktionen und allgemeine Polynome

Lemma 10.1. *Sei $K(x_1, x_2, \ldots, x_n) = K(x_1)(x_2)\ldots(x_n)$ der Körper der rationalen Funktionen in n Variablen $x_1, \ldots, x_n$. Die symmetrische Gruppe S_n operiert auf $K(x_1, \ldots, x_n)$ durch Körperautomorphismen mit*

$$\sigma\Big(\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}\Big) = \frac{f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})}{g(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})}.$$

Beweis. Durch einfaches Nachrechnen. □

Definition 10.2. Der Fixkörper L in $K(x_1, x_2, \ldots, x_n)$ unter der Operation von S_n heißt *Körper der symmetrischen rationalen Funktionen* in n Variablen über K. Die Polynome $f \in K[x_1, \ldots, x_n] \cap L$ heißen *symmetrische Polynome*.

Folgerung 10.3. *Der Körper der rationalen Funktionen in n Variablen $K(x_1, x_2, \ldots, x_n)$ ist galoissch über dem Körper der symmetrischen rationalen Funktionen in n Variablen mit der Galoisgruppe S_n. Der Körpergrad ist $[K(x_1, x_2, \ldots, x_n) : L] = n!$.*

Beweis. Definition der Galoiserweiterung und $n! = |S_n|$. □

Satz 10.4. *Sei G eine endliche Gruppe. Dann gibt es eine galoissche Körpererweiterung mit Galoisgruppe isomorph zu G.*

Beweis. Sei $n := |G|$. Nach Folgerung 10.3 ist $K(x_1, x_2, \ldots, x_n)$ galoissch über L mit Galoisgruppe S_n. Nach dem Satz von Cayley ist G isomorph zu einer Untergruppe G' von S_n. Sei L' der Fixkörper unter G' in $K(x_1, x_2, \ldots, x_n)$. Dann ist $K(x_1, x_2, \ldots, x_n)$ galoissch über L' mit Galoisgruppe G'. □

Bemerkung 10.5. Es ist ein offenes Problem, ob jede endliche Gruppe als Galoisgruppe einer Körpererweiterung $K/\mathbb{Q}$ auftritt.

Beispiele 10.6. Beispiele für symmetrische Funktionen:

(1) Potenzsummen $S_k = x_1^k + \ldots + x_n^k$.
(2) Wronskische Polynome $P_k = \sum_{i_1+\ldots+i_n=k} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$.
(3) Diskriminante $D = \prod_{1\le i<k\le n}(x_i - x_k)^2$.

Die *elementarsymmetrischen Polynome* oder *Funktionen* in den Variablen $x_1, \ldots, x_n$ sind

$$
\begin{aligned}
&C_1 := x_1 + x_2 + \ldots + x_n.\\
&C_2 := x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \textstyle\sum_{1\le i<k\le n} x_ix_k.\\
&C_3 := x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n = \textstyle\sum_{1\le i_1<i_2<i_3\le n} x_{i_1}x_{i_2}x_{i_3}.\\
&\vdots\\
&C_k := \textstyle\sum_{1\le i_1<i_2<\ldots<i_k\le n} x_{i_1}x_{i_2}\ldots x_{i_k}.\\
&\vdots\\
&C_n := x_1x_2\ldots x_n.
\end{aligned}
$$

Wir zeigen im folgenden Lemma, daß diese Polynome symmetrisch sind.
Die Ausdrücke $C_1, \ldots, C_n$ können auch gebildet werden, wenn die x_i nicht notwendig transzendent sind. Sie bilden die Koeffizienten des Polynoms, dessen Nullstellen vorgegebene $x_1, \ldots, x_n$ sind.

Lemma 10.7. *Seien $x_1, \ldots, x_n$ algebraische oder transzendente Elemente über K. Sei z eine Unbestimmte über $K(x_1, \ldots, x_n)$. Dann ist*

$$(z - x_1)(z - x_2)\ldots(z - x_n) = z^n - C_1z^{n-1} + C_2z^{n-2} - \ldots + (-1)^nC_n.$$

Beweis. Durch Ausmultiplizieren. Das zeigt dann auch, daß die elementarsymmetrischen Polynome symmetrisch, d.h. invariant unter der Orperation von S_n sind. □

Lemma 10.8. *Sei K ein Körper und seien $C_1, \ldots, C_n$ die elementarsymmetrischen Funktionen in n Variablen über K. Sei $1 \le k \le n-1$. Wenn $c_1, \ldots, c_k \in K[x_1, \ldots, x_n]$ die elementarsymmetrischen Funktionen in $x_1, \ldots, x_k$ sind, dann kann jedes c_i geschrieben werden als Polynom über K in den Variablen $C_1, \ldots, C_n$ und $x_{k+1}, \ldots, x_n$.*

Beweis. Die Aussage ist richtig für $k = n-1$, denn dann gilt $c_1 = C_1 - x_n$ und $c_i = C_i - c_{i-1}x_n$ für $i = 2, \ldots, n-1$. Wir führen nun einen Induktionsschluß für absteigende k durch. Gelte die Aussage für $k = r+1 \leq n-1$. Seien $t_1, \ldots, t_{r+1}$ die elementarsymmetrischen Funktionen in $x_1, \ldots, x_{r+1}$ und $c_1, \ldots, c_r$ die elementarsymmetrischen Funktionen in $x_1, \ldots, x_r$. Da $c_1 = t_1 - x_{r+1} = t_1(C_1, \ldots, C_n, x_{r+2}, \ldots, x_n) - x_{r+1}$ und $c_i = t_i - c_{i-1}x_{r+1} = t_i(C_1, \ldots, C_n, x_{r+2}, \ldots, x_n) - c_{i-1}(C_1, \ldots, C_n, x_{r+1}, \ldots, x_n)x_{r+1}$ folgt die Aussage für $k = r$. □

Satz 10.9. *Seien K ein Körper, L der Körper der symmetrischen rationalen Funktionen in $K(x_1, \ldots, x_n)$ und $C_1, \ldots C_n$ die elementarsymmetrischen Funktionen. Dann ist $L = K(C_1, \ldots, C_n)$.*

Beweis. Sei $M := K(C_1, \ldots, C_n) \subseteq K(x_1, \ldots, x_n)$. Wir haben Körpertürme

$$K \subseteq K(C_1, \ldots, C_n) = M \subseteq L \subseteq K(x_1, \ldots, x_n),$$
$$M \subseteq M(x_n) \subseteq M(x_{n-1}, x_n) \subseteq \ldots \subseteq M(x_2, \ldots, x_n) \subseteq M(x_1, \ldots, x_n) = K(x_1, \ldots, x_n).$$

Es genügt zu zeigen $[K(x_1, \ldots, x_n) : M] \leq n!$. Wir zeigen, daß x_k algebraisch über $M(x_{k+1}, \ldots, x_n)$ vom Grad $\leq k$ ist, d.h. daß der Grad des Minimalpolynoms $\leq k$ ist. Dann ist $[M(x_{k+1}, \ldots, x_n)(x_k) : M(x_{k+1}, \ldots, x_n)] = [M(x_k, \ldots, x_n) : M(x_{k+1}, \ldots, x_n)] \leq k$ und damit $[K(x_1, \ldots, x_n) : M] = [M(x_1, \ldots, x_n) : M] \leq n!$.
In $M[z]$ sei

$$g_n(z) := (z - x_1)(z - x_2) \ldots (z - x_n) = z^n - C_1 z^{n-1} + C_2 z^{n-2} - \ldots + (-1)^n C_n$$

Weiter sei

$$g_k(z) := (z - x_1)(z - x_2) \ldots (z - x_k) = g_n(z) / \big((z - x_{k+1})(z - x_2) \ldots (z - x_n)\big)$$

mit den Nullstellen $x_1, \ldots, x_k$.
Die Koeffizienten von $g_k(z)$ sind die elementarsymmetrischen Funktionen in $x_1, \ldots, x_k$ und damit nach Lemma 10.8 Polynome über K in den elementarsymmetrischen Funktionen $C_1, \ldots, C_n$ und den Variablen $x_{k+1}, \ldots, x_n$.
Also liegt $g_k(z)$ in $M(x_{k+1}, \ldots, x_n)[z]$. Das Element x_n hat als Nullstelle von $g_n(z)$ den Grad $\leq n$ über M und x_k als Nullstelle von $g_k(z)$ den Grad $\leq k$ über $M(x_{k+1}, \ldots, x_n)$. Die Behauptung ergibt sich dann aus dem zweiten oben angegebenen Körperturm. □

Folgerung 10.10. *Das Polynom*

$$g(z) = (z - x_1)(z - x_2) \ldots (z - x_n)$$

ist separabel und irreduzibel über dem Körper der rationalen Funktionen $K(x_1, \ldots, x_n)$.

Beweis. Wir haben im vorhergehenden Beweis sogar Gleichheit der einzelnen Grade bewiesen, also sind die Polynome $g_k(z)$ irreduzibel. Insbesondere ist $g(z) = g_n(z)$ irreduzibel. Es ist klar, daß $g(z)$ auch separabel ist, da es n verschiedene Nullstellen hat. □

Folgerung 10.11. *Sei K ein Körper und L der Körper der symmetrischen Funktionen im Körper der rationalen Funktionen $K(x_1, \ldots, x_n)$. Dann ist die Menge $X := \{x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} | 0 \leq i_k < k, k = 1, \ldots, n\}$ eine Basis von $K(x_1, \ldots, x_n)$ über L.*

Beweis. Wir beziehen uns auf den 2. Körperturm im vorhergehenden Beweis. $x_n, x_n^2, \ldots, x_n^{n-1}$ erzeugen $M(x_n)$ über M. $x_k, x_k^2, \ldots, x_k^{k-1}$ erzeugen $M(x_k, \ldots, x_n)$ über $M(x_{k+1}, \ldots, x_n)$. Also ist X eine Erzeugendenmenge von $K(x_1, \ldots, x_n)$ über L. Da $[K(x_1, \ldots, x_n) : L] = |S_n| = n! = |X|$, ist X eine Basis. □

Satz 10.12. *Sei K ein Körper und seien $C_1, \dots C_n$ die elementarsymmetrischen Funktionen in $K(x_1, \dots, x_n)$. Dann gelten*

(1) *Jedes Polynom in $K[x_1, \dots, x_n]$ läßt sich eindeutig als Linearkombination der $n!$ Elemente $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ mit $0 \le i_k < k, k = 1, \dots, n$ mit Koeffizienten in $K[C_1, \dots, C_n]$ schreiben.*

(2) *Jedes symmetrische Polynom in $K[x_1, \dots, x_n]$ liegt in $K[C_1, \dots, C_n]$.*

Beweis. (1) Wie im Beweis von Satz 10.9 sind die Koeffizienten von $g_k(z)$ die elementarsymmetrischen Funktionen in $x_1, \dots, x_k$ und damit nach Lemma 10.8 Polynome über K in den elementarsymmetrischen Funktionen $C_1, \dots, C_n$ und den Variablen $x_{k+1}, \dots, x_n$. Da g_k normiert ist und $g_k(x_k) = 0$ ist, kann x_k^k ausgedrückt werden als Polynom über K in $C_1, \dots, C_n, x_{k+1}, \dots, x_n$ und $x_k, x_k^2, \dots, x_k^{k-1}$.
Sei $h \in K[x_1, \dots, x_n]$. Wir setzen die zuvor bestimmten Polynome für x_k^k in h ein für $k = 1, \dots, n$ (bei $k = 1$ beginnend) und erhalten eine Darstellung von h als Polynom in $C_1, \dots, C_n, x_1, \dots, x_n$, bei dem die Exponenten i_k der x_k die Gleichung $i_k < k$ für $k = 1, \dots, n$ erfüllen. Damit ist h eine Linearkombinationen der $n!$ Elemente $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ mit $0 \le i_k < k, k = 1, \dots, n$ mit Koeffizienten in $K[C_1, \dots, C_n]$.Diese Koeffizienten sind eindeutig bestimmt, weil die $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ über $K(C_1, \dots, C_n)$ linear unabhängig sind.
(2) Tatsächlich haben wir auch gezeigt, daß ein Polynom $h \in K[x_1, \dots, x_n]$, das als Linearkombination der $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ mit Koeffizienten in $K(C_1, \dots, C_n)$ gegeben ist, seine Koeffizienten schon in $K[C_1, \dots, C_n]$ hat. Insbesondere gilt für ein symmetrisches Polynom $h \in K[x_1, \dots, x_n] \cap K(C_1, \dots, C_n)$ das Folgende: $h = h x_1^0 \dots x_n^0$, also ist $h \in K[C_1, \dots, C_n]$. □

Satz 10.13. *Sei K ein Körper und sei $K(x_1, \dots, x_n)$ der Körper der rationalen Funktionen in $x_1, \dots, x_n$. Das allgemeine Polynom*

$$f(z) = z^n - x_1 z^{n-1} + x_2 z^{n-2} - \dots + (-1)^n x_n$$

ist separabel und irreduzibel über $K(x_1, \dots, x_n)$. Die Galoisgruppe von $f(z)$ über $K(x_1, \dots, x_n)$ ist die symmetrische Gruppe S_n, die auf den Nullstellen von $f(z)$ durch Permutationen operiert.

Beweis. Seien $v_1, \dots, v_n$ die Nullstellen von $f(z)$ über $K(x_1, \dots, x_n)$, so daß $f(z) = (z - v_1)(z - v_2) \dots (z - v_n)$. Dann sind die x_i elementarsymmetrische Polynome in den v_i, also $x_1 = \sum_i v_i, x_2 = \sum_{i<k} v_i v_k, \dots, x_n = v_1 v_2 \dots v_n$. Insbesondere ist $K(x_1, \dots, x_n) \subseteq K(x_1, \dots, x_n)(v_1, \dots, v_n) = K(v_1, \dots, v_n)$.
Sei $K(y_1, \dots, y_n)$ der Körper der rationalen Funktionen in $y_1, \dots, y_n$ und seien die C_i die elementarsymmetrischen Polynome in den y_i. Wir definieren einen Ringhomomorphismus

$$K[x_1, \dots, x_n] \longrightarrow K[C_1, \dots, C_n] \subseteq K[y_1, \dots, y_n]$$

durch Einsetzen $x_i \mapsto C_i$. Diese Abbildung ist injektiv. Sei nämlich $p \in K[x_1, \dots, x_n]$ mit $p(C_1, \dots, C_n) = 0$ gegeben. Dann ist

$$p(\sum_i y_i, \sum_{i<k} y_i y_k, \dots, y_1 y_2 \dots y_n) = 0.$$

Da die y_i Unbestimmte sind, können wir die Nullstellen v_i für die y_i einsetzen und erhalten einen Ringhomomorphismus $K[y_1, \dots, y_n] \ni y_i \mapsto v_i \in K[v_1, \dots, v_n]$, also insgesamt einen Ringhomomorphismus

$$K[x_1, \dots, x_n] \longrightarrow K[C_1, \dots, C_n] \subseteq K[y_1, \dots, y_n] \longrightarrow K[v_1, \dots, v_n].$$

Dann gilt

$$p(x_1, \dots, x_n) = p(\sum_i v_i, \sum_{i<k} v_i v_k, \dots, v_1 v_2 \dots v_n) = 0.$$

Damit ist $K[x_1, \dots, x_n] \longrightarrow K[C_1, \dots, C_n]$ injektiv und nach Definition auch surjektiv. Dieses definiert einen Körperisomorphismus $\Phi : K(x_1, \dots, x_n) \cong K(C_1, \dots, C_n)$. Dabei ist $\Phi(f(z)) = g(z) = (z - y_1)(z - y_2) \dots (z - y_n)$. Damit sind auch die Zerfällungskörper $K(v_1, \dots, v_n) \cong K(y_1, \dots, y_n)$ mit einer Fortsetzung von Φ isomorph. Insbesondere ist mit g (nach Folgerung 10.10) auch f separabel und irreduzibel mit der Galoisgruppe S_n. □

Folgerung 10.14. *$\Phi : K[x_1, \dots, x_n] \longrightarrow K[C_1, \dots, C_n]$ mit $\Phi(x_i) = C_i$ ist ein Isomorphismus. Insbesondere sind die C_i transzendent über $K(C_1, \dots, C_{i-1})$.*

Definition 10.15. Sei $f \in K[x]$ ein Polynom vom Grad n mit n verschiedenen Nullstellen $u_1, \dots, u_n$ im Zerfällungskörper F. Sei die Charakteristik $\chi(K) \neq 2$. Sei

$$\Delta := \prod_{i<j} (u_i - u_j) = (u_1 - u_2) \cdot (u_1 - u_3) \cdot \ldots \cdot (u_{n-1} - u_n) \in F.$$

Die *Diskriminante* von f ist $D := \Delta^2$.

Folgerung 10.16. *Sei K ein Körper mit $\chi(K) \neq 2$. Dann ist die Galoisgruppe des allgemeinen Polynoms*

$$f(z) = z^n - x_1 z^{n-1} + x_2 z^{n-2} - \ldots + (-1)^n x_n$$

über dem Körper $K(x_1, \dots, x_n, \Delta)$ die alternierende Gruppe A_n.

Beweis. Der Ausdruck Δ bleibt fix unter allen geraden Permutationen, weil eine gerade Anzahl von Vorzeichenwechseln auftritt. Unter ungeraden Permutationen wechselt er das Vorzeichen. Also ist $K(x_1, \dots, x_n) \subsetneqq K(x_1, \dots, x_n, \Delta) \subsetneqq K(u_1, \dots, u_n)$, dem Zerfällungskörper von f und $K(x_1, \dots, x_n, \Delta)$ ist im Fixkörper von A_n enthalten, da die x_i elementarsymmetrische Polynome sind. Dann ist $(n!)/2 = |A_n| \leq [K(u_1, \dots, u_n) : K(x_1, \dots, x_n, \Delta)] < n!$, also $|A_n| = [K(u_1, \dots, u_n) : K(x_1, \dots, x_n, \Delta)]$, und damit ist $K(x_1, \dots, x_n, \Delta)$ Fixkörper von A_n. □

11. Die Galoisgruppe von Polynomen niedrigen Grades

Definition 11.1. Die *Galoisgruppe eines separablen Polynoms* $f \in K[x]$ ist $\mathrm{Aut}(F/K)$ für den Zerfällungskörper F von f über K.

Definition 11.2. Eine Untergruppe $U \subseteq S_n$ heißt *transitiv*, wenn für alle $i \neq j$, $1 \leq i, j \leq n$ ein $\sigma \in S_n$ mit $\sigma(i) = j$ existiert.

Satz 11.3. *Sei $f \in K[x]$ ein irreduzibles, separables Polynom vom Grad n mit Galoisgruppe G. Dann gilt $n/|G|$, und G ist eine transitive Untergruppe von S_n.*

Beweis. Seien $u_1, \dots, u_n$ die Nullstellen von f im Zerfällungskörper F von f. Sei $\sigma \in G$. Dann ist $\sigma(u_i)$ Nullstelle von f. Also induziert σ eine Permutation von $\{u_1, \dots, u_n\}$, und wir bekommen $G \longrightarrow S_n$. Es ist $F = K(u_1, \dots, u_n)$. Daher gibt es für $\sigma \neq \tau$ ein u_i mit $\sigma(u_i) \neq \tau(u_i)$. Damit ist $G \longrightarrow S_n$ injektiv und wir können G als Untergruppe von S_n betrachten. Damit ist $[K(u_1) : K] = \mathrm{Grad}(f) = n$ ein Teiler von $[F : K] = |G|$. Für $u_i \neq u_j$ gilt $K(u_i \cong K(u_j)$ über K. Es gibt eine Fortsetzung zu $\sigma : F \longrightarrow F$ mit $\sigma(u_i) = u_j$. Daher ist G transitiv. □

Satz 11.4. *Sei $f \in K[x]$ ein irreduzibles, separables Polynom vom Grad 2. Dann ist S_2 die Galoisgruppe von f.*

Beweis. klar. □

Satz 11.5. *Seien K, F, f und Δ wie in Definition 10.15. Dann gelten*

(1) $D \in K$,
(2) $\sigma \in G \subseteq S_n$ *ist genau dann gerade (ungerade), wenn* $\sigma(\Delta) = \Delta$ $(\sigma(\Delta) = -\Delta)$.

Beweis. Es ist $\operatorname{sgn}(\sigma) = \frac{\prod(u_i-u_j)}{\prod(\sigma(u_i)-\sigma(u_j))}$ (ähnlich wie $\operatorname{sgn}(\sigma) = \frac{\prod(i-j)}{\prod(\sigma(i)-\sigma(j))}$). Daraus folgt $\Delta = \operatorname{sgn}(\sigma)\sigma(\Delta)$ und damit (2). Weiter folgt $\sigma(\Delta^2) = \operatorname{sgn}(\sigma)^2\Delta^2 = \Delta^2$, also $\Delta^2 \in K$. □

Folgerung 11.6. $\operatorname{Aut}(F/K(\Delta)) = G \cap A_n$. *Insbesondere gilt*

$$G \subseteq A_n \iff \Delta \in K.$$

Beweis. $\sigma \in \operatorname{Aut}(F/K(\Delta))$ dann und nur dann, wenn $\sigma(\Delta) = \Delta$ dann und nur dann, wenn $\sigma \in A_n$. □

Folgerung 11.7. *Sei $f \in K[x]$ ein irreduzibles, separables Polynom vom Grad 3. Dann ist die Galoisgruppe von f entweder S_3 oder A_3.*
Wenn die Charakteristik $\chi(K) \neq 2$, dann ist die Galoisgruppe A_3 genau dann, wenn D in K ein Quadrat ist.

Satz 11.8. *(Reduzierung von Polynomen 3-ten Grades) Sei $\chi(K) \neq 2, 3$. Sei $f = x^3 + bx^2 + cx + d \in K[x]$ irreduzibel und separabel. Dann ist*

$$g(x) := f(x - \frac{b}{3}) = x^3 + px + q$$

irreduzibel und separabel und

$$D(f) = D(g) = -4p^3 - 27q^2$$

mit $p = -\frac{b^2}{3} + c$, $q = \frac{2b^3}{27} - \frac{bc}{3} + d$.

Beweis. Sei F der Zerfällungskörper von f. u ist eine Nullstelle von f genau dann, wenn $u + \frac{b}{3}$ eine Nullstelle von g ist. Also ist $D(f) = D(g)$. Es ist

$$\begin{aligned} g(x) &= (x - \tfrac{b}{3})^3 + b(x - \tfrac{b}{3})^2 + c(x - \tfrac{b}{3}) + d \\ &= x^3 - bx^2 + \tfrac{b^2}{3}x - \tfrac{b^3}{27} + bx^2 - 2\tfrac{b^2}{3}x + \tfrac{b^3}{9} + cx - \tfrac{bc}{3} + d \\ &= x^3 + (-\tfrac{b^2}{3} + c)x + (\tfrac{2b^3}{27} - \tfrac{bc}{3} + d) \\ &= x^3 + px + q. \end{aligned}$$

Seien v_1, v_2, v_3 Nullstellen von g in F. Dann ist $(x - v_1)(x - v_2)(x - v_3) = x^3 + px + q$, also $v_1 + v_2 + v_3 = 0$, $v_1v_2 + v_1v_3 + v_2v_3 = p$ und $-v_1v_2v_3 = q$. Aus der Nullstellen-Eigenschaft folgt $v_i^3 = -pv_i - q$, also durch mühevolles Nachrechnen $D(g) = \Delta^2 = -4p^3 - 27q^2$. □

Beispiele 11.9. (1) $x^3 - 3x + 1 \in \mathbb{Q}[x]$ ist irreduzibel, weil es keine Nullstelle in $\mathbb{Q}$ gibt. $D = +4 \cdot 27 - 27 \cdot 1 = 81 = 9^2$ in $\mathbb{Q}$. Also ist $\operatorname{Gal}(x^3 - 3x + 1) = A_3$.
(2) $x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x]$ ist irreduzibel, weil es keine Nullstelle in $\mathbb{Q}$ gibt. $g(x) = f(x - \frac{3}{3}) = (x - 1)^3 + 3(x - 1)^2 - (x - 1) - 1 = x^3 - 4x + 2$ ist ebenfalls irreduzibel (auch Eisenstein möglich). $D = 4 \cdot 64 - 27 \cdot 4 = 148$ ist kein Quadrat in $\mathbb{Q}$. Also ist $\operatorname{Gal}(x^3 - 3x + 1) = S_3$.

Wir studieren nun Polynome vom Grad 4.

Übung 11.10. Die Menge $V = \{(1), (12)(34), (13)(24), (14)(23)\} \subseteq S_4$ ist eine normale Untergruppe, die isomorph zur Kleinschen Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist. Ist $G \subseteq S_4$ eine Untergruppe, so ist $V \cap G$ eine normale Untergruppe von G.

Definition 11.11. Sei im folgenden K ein Körper, $f \in K[x]$ ein Polynom 4-ten Grades mit paarweise verschiedenen Nullstellen u_1, u_2, u_3, u_4 im Zerfällungskörper L von f und $G = \mathrm{Aut}(L/K)$. Dann ist $G \subseteq S_4$. Seien im folgenden

$$\begin{aligned} \alpha &:= u_1u_2 + u_3u_4, \\ \beta &:= u_1u_3 + u_2u_4, \\ \gamma &:= u_1u_4 + u_2u_3. \end{aligned}$$

Das Polynom $(x-\alpha)(x-\beta)(x-\gamma)$ wird *kubische Resovente* genannt.
Es liegt, wie wir in Lemma 11.13 sehen werden, in $K[x]$.

Lemma 11.12. *Seien K, f, L, u_i, V, α, β, γ und $G = \mathrm{Aut}(L/K)$ wie zuvor. Unter der Galois-Korrespondenz des Hauptsatzes der Galois-Theorie entspricht der Körper $K(\alpha, \beta, \gamma)$ der Untergruppe $V \cap G$. Insbesondere ist $K(\alpha, \beta, \gamma)$ galoissch über K mit der Galoisgruppe $\mathrm{Aut}(K(\alpha, \beta, \gamma)/K) \cong G/(V \cap G)$.*

Beweis. Jedes Element von $V \cap G$ läßt α, β, γ fest. Also wird $K(\alpha, \beta, \gamma)$ durch die Elemente von $V \cap G$ fest gelassen. Es bleibt zu zeigen, daß jedes Element außerhalb von V mindestens eines der α, β, γ nicht fest läßt. Wir zeigen das an dem Beispiel $\sigma = (12)$. Wenn $\sigma(\beta) = \beta$, dann ist $u_2u_3 + u_1u_4 = u_1u_3 + u_2u_4$, also ist $u_2(u_3 - u_4) = u_1(u_3 - u_4)$. Das kann nicht sein, da $u_1 \neq u_2$ und $u_3 \neq u_4$. Also ist $\sigma(\beta) \neq \beta$. Die anderen Fälle werden ähnlich behandelt. □

Lemma 11.13. *Sei $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$. Dann ist die kubische Resolvente von f das Polynom $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$.*

Beweis. f hat die Nullstellen u_1, u_2, u_3, u_4 in einem Zerfällungskörper L. Also ist $f = (x - u_1)(x - u_2)(x - u_3)(x - u_4) = x^4 - (u_1 + u_2 + u_3 + u_4)x^3 + (u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4)x^2 - (u_1u_2u_3 + u_1u_2u_4 + u_1u_3u_4 + u_2u_3u_4)x + u_1u_2u_3u_4$, also

$$\begin{aligned} b &= -(u_1 + u_2 + u_3 + u_4), \\ c &= u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4, \\ d &= -(u_1u_2u_3 + u_1u_2u_4 + u_1u_3u_4 + u_2u_3u_4), \\ e &= u_1u_2u_3u_4. \end{aligned}$$

Das Polynom $(x-\alpha)(x-\beta)(x-\gamma)$ hat dann die Form

$$\begin{aligned} &(x - u_1u_2 - u_3u_4)(x - u_1u_3 - u_2u_4)(x - u_1u_4 - u_2u_3) \\ &= x^3 - (u_1u_2 + u_3u_4 + u_1u_3 + u_2u_4 + u_1u_4 + u_2u_3)x^2 \\ &\quad +(u_1u_2u_1u_3 + u_1u_2u_2u_4 + u_3u_4u_1u_3 + u_3u_4u_2u_4 + u_1u_2u_1u_4 + u_1u_2u_2u_3 + u_3u_4u_1u_4 + u_3u_4u_2u_3 \\ &\qquad +u_1u_3u_1u_4 + u_1u_3u_2u_3 + u_2u_4u_1u_4 + u_2u_4u_2u_3)x \\ &\quad -(u_1u_2u_1u_3u_1u_4 + u_1u_2u_1u_3u_2u_3 + u_1u_2u_2u_4u_1u_4 + u_1u_2u_2u_4u_2u_3 \\ &\qquad +u_3u_4u_1u_3u_1u_4 + u_3u_4u_1u_3u_2u_3 + u_3u_4u_2u_4u_1u_4 + u_3u_4u_2u_4u_2u_3) \\ &= x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2. \end{aligned}$$

□

Bemerkung 11.14. Wir verwenden Satz 11.3. Wenn f vom Grad 4 ist, dann muß G die Ordnung 4, 8, 12 oder 24 haben. Die einzigen transitiven Untergruppen von S_4 der Ordnung 4, 12 und 24 sind $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und die zyklischen Untergruppen der Ordnung 4, die von

4-Zyklen erzeugt werden, A_4 und S_4. Eine Untergruppe der Ordnung 8 ist eine 2-Sylow-Untergruppe, also bis auf Isomorphie eindeutig bestimmt. Eine Untergruppe der Ordnung 8 wird von (1234) und (24) erzeugt und ist isomorph zur Diedergruppe D_4. Weil (1234) in der Gruppe liegt, ist sie transitiv. D_4 ist keine normale Untergruppe von S_4, also gibt es nach den Sylowschen Sätzen genau 3 zu D_4 isomorphe Untergruppen, alle von der Ordnung 8 und transitiv.

Wir wollen Kriterien für f angeben, wann diese Untergruppen als Galoisgruppen auftreten.

Satz 11.15. *Sei K ein Körper und $f \in K[x]$ ein irreduzibles separables Polynom 4-ten Grades mit Galoisgruppe $G(\subseteq S_4)$. Seien α, β, γ die Nullstellen der kubischen Resolvente und sei $m := [K(\alpha,\beta,\gamma) : K]$. Dann gelten*

(1) $m = 6 \iff G = S_4$;
(2) $m = 3 \iff G = A_4$;
(3) $m = 1 \iff G = V$;
(4) $m = 2 \iff G \cong D_4$ *oder* $G \cong \mathbb{Z}_4$. *In diesem Falle gilt:*
  (a) $G \cong D_4 \iff f$ *irreduzibel über* $K(\alpha,\beta,\gamma)$,
  (b) $G \cong \mathbb{Z}_4 \iff f$ *reduzibel über* $K(\alpha,\beta,\gamma)$.

Beweis. Da $K(\alpha,\beta,\gamma)$ Zerfällungskörper eines Polynoms dritten Grades ist, kommen nur $m = 1, 2, 3$ und 6 in Frage. Also genügt es jeweils die Richtung $\Leftarrow$ zu zeigen. Man beachte, daß $m = [K(\alpha,\beta,\gamma) : K] = |G/(G \cap V)|$.

Sei $G = S_4$. Dann ist $|S_4/V| = 6$.

Sei $G = A_4$. Dann ist $G \cap V = V$ und $m = |G/V| = 3$.

Sei $G = V$. Dann ist $G \cap V = G$ und $m = |G/G| = 1$.

Sei $G \cong D_4$. Dann ist $G \cap V = V$, weil V als normale Untergruppe in jeder 2-Sylow Untergruppe von S_4 enthalten ist. Also gilt $m = |G/V| = 2$.

Sei $G \cong \mathbb{Z}_4$. Dann wird G durch einen 4-Zyklus erzeugt. Das Quadrat muß in V liegen, so daß $|G \cap V| = 2$ ist. Also ist $m = |G/(G \cap V)| = 2$.

Sei $G \cong D_4$ und damit $G \cap V = V$. Seien u_1, u_2, u_3, u_4 die Nullstellen von f in einem Zerfällungskörper L. Da $V = G \cap V = \mathrm{Aut}(L/K(\alpha,\beta,\gamma))$ transitiv auf den Nullstellen operiert, gibt es für jedes $i \neq j$ ein $\sigma \in G \cap V$ mit $\sigma : K(\alpha,\beta,\gamma)(u_i) \cong K(\alpha,\beta,\gamma)(u_j)$ und $\sigma(u_i) = u_j$ und $K(\alpha,\beta,\gamma)$ fix unter der Operation von σ. Also sind u_i und u_j Nullstellen desselben Minimalpolynoms über $K(\alpha,\beta,\gamma)$. Damit ist f irreduzibel über $K(\alpha,\beta,\gamma)$.

Sei $G \cong \mathbb{Z}_4$. Dann hat $G \cap V = \mathrm{Aut}(L/K(\alpha,\beta,\gamma)$ die Ordnung 2 und ist nicht transitiv auf den Nullstellen von f. Also gibt es $i \neq j$, so daß es kein $\sigma \in G \cap V$ gibt mit $\sigma(u_i) = u_j$. Da L Zerfällungskörper von f über $K(\alpha,\beta,\gamma)(u_i)$ und auch über $K(\alpha,\beta,\gamma)(u_j)$ ist, würde ein Isomorphismus $K(\alpha,\beta,\gamma)(u_i) \cong K(\alpha,\beta,\gamma)(u_j)$, der auf $K(\alpha,\beta,\gamma)$ die Identität ist und u_i nach u_j abbildet, eine Fortsetzung zu einem Automorphismus aus $\mathrm{Aut}(L/K(\alpha,\beta,\gamma)) = G \cap V$ ergeben. Das ist nicht möglich. Also können u_i und u_j nicht Nullstellen desselben irreduziblen Polynoms in $K(\alpha,\beta,\gamma)[x]$ sein. Folglich ist f über $K(\alpha,\beta,\gamma)$ reduzibel. □

Beispiele 11.16. (1) Das Polynom $f = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$ ist separabel und nach Eisenstein irreduzibel. Die kubische Resolvente ist $x^3 - 4x^2 - 8x + 32 = (x-4)(x^2-8)$, so daß $\alpha = 4$, $\beta = \sqrt{8}$, $\gamma = -\sqrt{8}$. Weiter hat $\mathbb{Q}(\alpha,\beta,\gamma) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ den Körpergrad 2 über $\mathbb{Q}$. Also ist die Galoisgruppe D_4 oder $\mathbb{Z}_4$. Mit der Substitution $z := x^2$ ist $f = z^2 + 4z + 2$ mit den Nullstellen $z_{1,2} = -2 \pm \sqrt{2}$. Also sind die Nullstellen von f

$$x_{1,2,3,4} = \pm\sqrt{z_{1,2}} = \pm\sqrt{-2 \pm \sqrt{2}}.$$

Es folgt

$$\begin{aligned} f &= (x - \sqrt{-2+\sqrt{2}})(x + \sqrt{-2+\sqrt{2}})(x - \sqrt{-2-\sqrt{2}})(x + \sqrt{-2-\sqrt{2}}) \\ &= (x^2 - (-2+\sqrt{2}))(x^2 - (-2-\sqrt{2})) \in \mathbb{Q}(\sqrt{2})[x]. \end{aligned}$$

Also ist f über $\mathbb{Q}(\sqrt{2})[x]$ reduzibel. Damit ist $\mathbb{Z}_4$ die Galoisgruppe von f.

(2) Das Polynom $f = x^4 - 2 \in \mathbb{Q}[x]$ ist separabel und irreduzibel. Die kubische Resolvente ist $x^3 + 8x = x(x + 2\sqrt{2}i)(x - 2\sqrt{2}i)$ und $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2}i)$ hat den Grad 2 über $\mathbb{Q}$.

12. Kreisteilungskörper

Problem 12.1. Man zerfälle das Polynom $x^n - 1$. Die Nullstellen über $\mathbb{Q}$ liegen auf dem komplexen Einheitskreis $|z| = 1$ in $\mathbb{C}$: $z = r \cdot e^{i\varphi}$, $1 = z^n = r^n e^{in\varphi}$. Es folgt $r^n = 1$ und $r \in \mathbb{R}^+$, also $r = 1$ und daher $|z| = 1$. $x^n - 1$ ist offenbar reduzibel. Welches sind die irreduziblen Faktoren?

Betrachte $x^n - a = 0$ mit Nullstelle u. Dann ist $u^n = a$. Ist ζ Nullstelle von $x^n - 1$, so ist $(\zeta u)^n = a$, d.h. ζu ist weitere Nullstelle von $x^n - a = 0$.

Definition 12.2.
- Eine Nullstelle ζ (*im Zerfällungskörper* K_n) von $x^n - 1$ heißt eine *n-te Einheitswurzel*.
- Die n-ten Einheitswurzeln in K bilden *die Gruppe $E_n(K)$ der n-ten Einheitswurzeln in K*. Diese ist endlich und zyklisch (als endliche multiplikative Untergruppe von K). Sie hat höchstens die Ordnung n.
- Für $\chi(K) = p \nmid n$ sind $x^n - 1$ und nx^{n-1} teilerfremd, also hat $x^n - 1$ in K_n n verschiedene Nullstellen. Ein Erzeugendenelement von $E_n(K_n)$ hat in diesem Falle die Ordnung n.
- *Eine primitive n-te Einheitswurzel* ist eine n-te Einheitswurzel, die die Ordnung n hat. Sie ist ein Erzeugendenelement von $E_n(K)$, wenn sie in $E_n(K)$ liegt.
- Die Menge der primitiven n-ten Einheitswurzeln über K sei $PE_n(K)$.
- Sei $\chi(K) = p \nmid n$. Dann wird K_n, der Zerfällungskörper von $x^n - 1$ über K, von einer primitiven n-ten Einheitswurzel über K erzeugt: $K_n = K(\zeta)$ und heißt *n-ter Kreisteilungskörper* über K. Es gilt $PE_n(K) \subseteq E_n(K_n)$.
- Für $\chi(K) = p / n$ ist $x^n - 1 = x^{mp} - 1^p = (x^m - 1)^p$. Dann stimmen $E_m(K)$ und $E_n(K)$ überein.
- Wir setzen o.B.d.A. im folgenden voraus $p \nmid n$.

Definition 12.3. Für $n \in \mathbb{N}$ sei $\varphi(n)$ die Anzahl der natürlichen Zahlen $1 \leq m \leq n$, die zu n teilerfremd sind. $\varphi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$ heißt *Eulersche φ-Funktion.*

Satz 12.4. *(1) $\forall n \in \mathbb{Z} \setminus \{0\} : (\mathbb{Z}/n\mathbb{Z})^* = \{m + n\mathbb{Z} | (m,n) = 1\}$;*
(2) $\varphi(n) = \mathrm{Ord}(\mathbb{Z}/n\mathbb{Z})^*$;
(3) $(m,n) = 1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n)$;
(4) $n = p_1^{t_1} \cdot \ldots \cdot p_r^{t_r} \Longrightarrow \varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_r})$;
(5) $n = \sum_{d/n} \varphi(d)$.

Beweis. (1) $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^* \iff \exists m' : n/mm' - 1 \iff \exists m', n' : mm' + nn' = 1 \iff (m,n) = 1$.
(2) klar.

(3) $(m,n)=1 \Longrightarrow m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$ und $m\mathbb{Z}\cap n\mathbb{Z}=mn\mathbb{Z}$. Nach dem chinesischen Restsatz folgt $\mathbb{Z}/(mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, also $(\mathbb{Z}/(mn\mathbb{Z}))^* \cong (\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^*\times(\mathbb{Z}/n\mathbb{Z})^*$. Das ergibt die Behauptung.
(4) Für p^k ist p^{k-1} die Anzahl der Zahlen $\leq p^k$, die nicht teilerfremd zu p^k sind, nämlich $p, 2p, \ldots, p^{k-1}p$. Also ist $\varphi(p^k)=p^k-p^{k-1}=p^k(1-\frac{1}{p})$. Die Behauptung folgt durch Induktion.
(5) folgt aus 12.7. □

Folgerung 12.5. *Sei $n\in\mathbb{N}$ und $a\in\mathbb{Z}$ mit $(a,n)=1$. Dann ist*

$$a^{\varphi(n)} \equiv 1 \mod (n).$$

Beweis. Folgt unmittelbar aus Satz 12.4 (2) und dem Satz von Euler 4.24. □

Folgerung 12.6 (Kleiner Fermatscher Satz (1640))**.** *Sei p eine Primzahl und $p\nmid a\in\mathbb{Z}$. Dann ist*

$$a^{p-1}\equiv 1 \mod (p).$$

Für alle $a\in\mathbb{Z}$ ist

$$a^p \equiv a \mod (p).$$

Beweis. Es ist $\varphi(p)=p-1$. □

Bemerkung 12.7. *(über Einheitswurzeln):*

(1) Sei $\zeta\in PE_n(K)$ und $\chi(K)\not= n, m\in\mathbb{N}$. Dann gilt $\zeta^m\in PE_n(K) \iff (m,n)=1$.
(2) $\chi(K)\not= n \Longrightarrow |PE_n(K)|=\varphi(n)$.
(3) d/n, $d>0 \Longrightarrow E_d(K)\subseteq E_n(K)$ und $PE_d(K)=\{\zeta\in E_n(K)|\operatorname{Ord}(\zeta)=d\}$.
(4) Die Mengen $PE_d(K)$ mit d/n sind paarweise disjunkt und $E_n(K_n)=\dot\bigcup_{d/n}PE_d(K)$.
(5) $n=\sum_{d/n}\varphi(d)$.

Definition 12.8. Sei $\chi(K)\not= n$. Für $\{\zeta_1,\ldots,\zeta_{\varphi(n)}\}=PE_n(K)$ heißt

$$\Phi_n(x) := (x-\zeta_1)\cdot\ldots\cdot(x-\zeta_{\varphi(n)})$$

das n*-te Kreisteilungspolynom.*

Satz 12.9. *Sei $\chi(K)\not= n$. Dann gelten:*

(1) *$\Phi_n(x)$ hat Koeffizienten in $\mathbb{Z}$ bzw. in $GF(p)=\mathbb{F}_p$.*
(2) *$x^n-1=\prod_{d/n}\Phi_d(x)$.*

Beweis. (2) folgt aus 12.7 (4).
(1) Induktion nach n:
$n=1$: $x^1-1=\Phi_1(x)\in R[x]$ mit $R=\mathbb{Z},\mathbb{F}_p$.
Gelte (1) für alle d/n, $d<n$, $\chi(K)\not= d$. Dann folgt $x^n-1=\Phi_n(x)\prod_{d/n,d<n}\Phi_d(x)$. $\prod_{d/n,d<n}\Phi_d(x)$ hat höchsten Koeffizienten 1. Damit ist Division mit Rest in $R[x]$ möglich:

$$\Phi_n(x)=(x^n-1):(\prod_{d/n,d<n}\Phi_d(x))\in R[x],$$

weil in $K_n[x]$ kein Rest bleibt. □

Beispiele 12.10. Sei $K = \mathbb{Q}$. Dann ist

$\Phi_1(x) = x - 1,$
$\Phi_2(x) = x + 1,$
$\Phi_3(x) = (x^3 - 1) : (x - 1) = x^2 + x + 1,$
$\Phi_4(x) = (x^4 - 1) : [(x - 1)(x + 1)] = x^2 + 1,$
$\Phi_5(x) = (x^5 - 1) : (x - 1) = x^4 + x^3 + x^2 + x + 1,$
$\Phi_6(x) = (x^6 - 1) : [(x - 1)(x + 1)(x^2 + x + 1)] = x^2 - x + 1,$
$\Phi_{12}(x) = (x^{12} - 1) : [(x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)] = x^4 - x^2 + 1.$

Definition 12.11. Eine galoissche Körpererweiterung heißt *abelsch*, wenn $\mathrm{Aut}(F/K)$ abelsch ist.
Eine galoissche Körpererweiterung heißt *zyklisch*, wenn $\mathrm{Aut}(F/K)$ zyklisch ist.

Satz 12.12. *Sei $\chi(K) \not| n$. Dann gibt es einen Monomorphismus*

$$\mathrm{Aut}(K_n/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

Insbesondere ist $\mathrm{Aut}(K_n/K)$ abelsch. Also ist K_n über K eine abelsche Körpererweiterung.

Beweis. Sei $\sigma \in \mathrm{Aut}(K_n/K)$. Dann gilt $\sigma(E_n(K_n)) = E_n(K_n)$. Damit ist $\sigma \in \mathrm{Gr\text{-}Aut}(E_n(K_n))$. Das definiert einen Homomorphismus $\mathrm{Aut}(K_n/K) \longrightarrow \mathrm{Gr\text{-}Aut}(E_n(K_n))$. Dieser Homomorphismus ist injektiv, weil $K_n = K(E_n(K_n))$. Nun ist $E_n(K_n) \cong \mathbb{Z}/n\mathbb{Z}$, also ist $\mathrm{Gr\text{-}Aut}(E_n(K_n)) \cong \mathrm{Gr\text{-}Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ eine abelsche Gruppe, denn $\tau : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ wird beschrieben durch $\tau(\overline{1}) = \overline{r}$ und ist bijektiv genau dann, wenn $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^*$. □

Folgerung 12.13. *Ist n prim und $n \neq \chi(K)$, so ist $\mathrm{Aut}(K_n/K)$ zyklisch. Also ist K_n über K eine zyklische Körpererweiterung.*

Beweis. $\mathrm{Aut}(K_n/K) \cong (\mathbb{Z}/n\mathbb{Z})^* \cong \mathbb{F}_n^*$ ist zyklisch. □

Satz 12.14. *Sei $\mathbb{Q}_n \supseteq \mathbb{Q}$ gegeben. Dann gelten:*
(1) *$\Phi_n(x)$ ist irreduzibel in $\mathbb{Q}[x]$.*
(2) *$[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.*
(3) *$\mathrm{Aut}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Beweis. (1) Sei $\zeta \in PE_n(\mathbb{Q})$ gegeben, und sei f das Minimalpolynom von ζ in $\mathbb{Q}[x]$.
Behauptung: $f(\zeta^p) = 0$ für alle p prim, $p \not| n$.
Beweis: Es ist $\zeta^n = 1$. Da f Minimalpolynom von ζ ist, folgt $x^n - 1 = f \cdot g$. Also gibt es (nach Satz 10.3) f^*, $g^* \in \mathbb{Z}[x]$ primitiv mit $x^n - 1 = r \cdot f^* \cdot g^* \in \mathbb{Z}[x]$ und $r \in \mathbb{Z}$. Der höchste Koeffizient von $x^n - 1$ ist 1, also ist $r = 1$ und damit $x^n - 1 = f^* \cdot g^*$ in $\mathbb{Z}[x]$. Weiterhin sind die höchsten Koeffizienten von f^* und g^* ebenfalls 1 und damit $f^* = f$ und $g^* = g$. *Angenommen:* $f(\zeta^p) \neq 0$. Dann ist $g(\zeta^p) = 0$, also ist ζ Nullstelle von $g(x^p)$. Da f Minimalpolynom von ζ ist, folgt $g(x^p) = f(x)h(x)$ in $\mathbb{Q}[x]$. Division mit Rest in $\mathbb{Z}[x]$ ergibt $g(x^p) = f(x)h_1(x) + r_1(x)$. Wegen der Eindeutigkeit der Division in $\mathbb{Q}[x]$ folgt $h_1(x) = h(x)$ und $r_1(x) = 0$. Also ist $h(x) \in \mathbb{Z}[x]$. Unter der kanonischen Abbildung $\mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x]$ gilt $\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$. Da $g = g^*$ primitiv in $\mathbb{Z}[x]$ ist, ist $\overline{g}(x) \neq 0$ in $\mathbb{F}_p[x]$. Weiter gilt $\overline{g}(x^p) = (\overline{g}(x))^p$ in $\mathbb{F}_p[x]$, da die Koeffizienten des Polynoms $\overline{g}(x)$ unter der p-ten Potenz (Frobeniushomomorphismus $\Phi : \mathbb{F}_p[x] \longrightarrow \mathbb{F}_p[x]$) fest bleiben. Also folgt $(\overline{g}(x))^p = \overline{f}(x)\overline{h}(x)$ in $\mathbb{F}_p[x]$. Damit haben $\overline{f}(x)$ und $\overline{g}(x)$ einen nicht trivialen gemeinsamen Teiler $(\overline{f}(x), \overline{g}(x)) \neq 1$ in $\mathbb{F}_p[x]$. Es folgt, daß $x^n - \overline{1} = \overline{f}(x)\overline{g}(x)$ mehrfache Nullstellen in einem Erweiterungskörper von $\mathbb{F}_p$ hat im Widerspruch zu $(x^n - \overline{1})' = \overline{n}x^{n-1} \neq 0$ wegen $p \not| n$.

Also gilt $f(\zeta^p) = 0$.
Behauptung: $\Phi_n(x)$ ist irreduzibel in $\mathbb{Z}[x]$.
Beweis: $\varepsilon \in PE_n(\mathbb{Q})$ genau dann, wenn es ein m gibt mit $\varepsilon = \zeta^n$, $(m,n) = 1$. Sei $m = p_1 \cdot \ldots \cdot p_r$, dann ist $(p_i, n) = 1$ für alle i, also ist $f(\zeta^{p_i}) = 0$. Daraus folgt $f(\zeta^{p_1 \cdots p_r}) = f((\zeta^{p_1})^{p_2 \cdots p_r}) = 0$, weil $\zeta^{p_1} \in PE_n(\mathbb{Q})$ und f Minimalpolynom von ζ^{p_1} ist. In der Tat ist f irreduzibel, normiert und $f(\zeta^{p_1}) = 0$. Durch Induktion folgt $f(\varepsilon) = f(\zeta^{p_1 \cdots p_r}) = 0$. Also hat das irreduzible, normierte Polynom f mindestens die $\varepsilon \in PE_n(\mathbb{Q})$ als Nullstellen und $\Phi_n(x)$ hat genau diese Nullstellen. Damit ist $\Phi_n = f$.
(2) Es ist $\mathbb{Q}_n = \mathbb{Q}(\zeta) = \mathbb{Q}(E_n(\mathbb{Q}_n))$. Daher ist $[\mathbb{Q}_n : \mathbb{Q}]$ gleich dem Grad des Minimalpolynoms von $\zeta = \mathrm{Grad}(\Phi_n) = \varphi(n)$.
(3) Daraus folgt $|\operatorname{Aut}(\mathbb{Q}_n/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ nach Satz 12.4 (2). Aus Satz 12.12 folgt nun die Behauptung. $\square$

13. Zyklische Erweiterungen und Kummererweiterungen

Definition 13.1. Sei $L : K$ eine galoissche Erweiterung mit Galoisgruppe $\operatorname{Aut}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$.
Die *Norm* eines Elements $\alpha \in L$ ist

$$N_K^L(\alpha) := \sigma_1(\alpha) \cdot \ldots \cdot \sigma_n(\alpha).$$

Die *Spur* eines Elements $\alpha \in L$ ist

$$T_K^L(\alpha) := \sigma_1(\alpha) + \ldots + \sigma_n(\alpha).$$

Offensichtlich gelten

$$N_K^L(\alpha\beta) = N_K^L(\alpha) N_K^L(\beta)$$

und

$$T_K^L(\alpha + \beta) = T_K^L(\alpha) + T_K^L(\beta).$$

Satz 13.2 (Hilberts Theorem 90)**.** *Sei L eine zyklische Erweiterung von K vom Grad n , sei σ ein Erzeugendenelement von* $\operatorname{Aut}(L/K)$*, und sei $\alpha \in L$. Dann sind äquivalent:*
1. $N_K^L(\alpha) = 1$.
2. *Es gibt ein $\beta \in L$ mit $\alpha = \beta\sigma(\beta)^{-1}$.*

Beweis. (1) $\Longrightarrow$ (2): $N_K^L(\alpha) = 1$ impliziert $\alpha \neq 0$. Da die $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ über L linear unabhängig sind (Satz von Dedekind 1.12), gibt es ein $\gamma \in L$ mit

$$\beta := \alpha\,\mathrm{id}(\gamma) + (\alpha\sigma(\alpha))\sigma(\gamma) + (\alpha\sigma(\alpha)\sigma^2(\alpha))\sigma^2(\gamma) + \ldots + (\alpha\sigma(\alpha)\ldots\sigma^{n-1}(\alpha))\sigma^{n-1}(\gamma) \neq 0.$$

Der letzte Summand ist $N_K^L(\alpha)\sigma^{n-1}(\gamma) = \sigma^{n-1}(\gamma)$. Daher ist

$$\sigma(\beta) = \sigma(\alpha)\sigma(\gamma) + \sigma(\alpha)\sigma^2(\alpha)\sigma^2(\gamma) + \ldots + \sigma(\alpha)\sigma^2(\alpha)\ldots\sigma^{n-1}(\alpha)\sigma^{n-1}(\gamma) + \sigma^n(\gamma) = \alpha^{-1}\beta.$$

Es folgt $\alpha = \beta\sigma(\beta)^{-1}$, weil $\beta \neq 0$ und daher $\sigma(\beta) \neq 0$.
(2) $\Longrightarrow$ (1): Sei $\alpha = \beta\sigma(\beta)^{-1}$. Es ist $\sigma^n(\beta^{-1}) = \beta^{-1}$, da σ die Ordnung n hat. Mit $\sigma^i(\beta\sigma(\beta)^{-1})) = \sigma^i(\beta)\sigma^{i+1}(\beta)^{-1}$ folgt:
$N_K^L(\alpha) = (\beta\sigma(\beta^{-1}))(\sigma(\beta)\sigma^2(\beta^{-1}))(\sigma^2(\beta)\sigma^3(\beta^{-1}))\ldots(\sigma^{n-1}(\beta)\sigma^n(\beta^{-1})) = 1$. $\square$

Bemerkung 13.3. Die moderne Ausdrucksweise für Hilberts Theorem 90 ist:

$$H^1(\operatorname{Aut}(L/K), L^*) = 1.$$

Satz 13.4. *Sei L eine zyklische Erweiterung von K vom Grad n, sei σ ein Erzeugendenelement von* $\operatorname{Aut}(L/K)$*, und sei $\alpha \in L$. Dann sind äquivalent:*

(1) $T_K^L(\alpha) = 0$.
(2) *Es gibt ein* $\beta \in L$ *mit* $\alpha = \beta - \sigma(\beta)$.

Beweis. (1) $\Longrightarrow$ (2): Da $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ über L linear unabhängig sind (Satz von Dedekind 1.12), gibt es ein $\gamma \in L$ mit

$$T_K^L(\gamma) := \mathrm{id}(\gamma) + \sigma(\gamma) + \sigma^2(\gamma) + \ldots + \sigma^{n-1}(\gamma) \neq 0.$$

Weiter ist $\sigma(T_K^L(\gamma)) = T_K^L(\gamma)$, also $T_K^L(\gamma) \in K$. Wir erhalten $\sigma(T_K^L(\gamma)^{-1}\gamma) = T_K^L(\gamma)^{-1}\sigma(\gamma)$. Für $\beta := T_K^L(\gamma)^{-1}\gamma$ ist dann

$$T_K^L(\beta) = T_K^L(\gamma)^{-1}\gamma + T_K^L(\gamma)^{-1}\sigma(\gamma) + \ldots + T_K^L(\gamma)^{-1}\sigma^{n-1}(\gamma) = T_K^L(\gamma)^{-1}T_K^L(\gamma) = 1.$$

Sei nun $T_K^L(\alpha) = 0$. Wir setzen

$$\delta := \alpha\beta + (\alpha + \sigma(\alpha))\sigma(\beta) + (\alpha + \sigma(\alpha) + \sigma^2(\alpha))\sigma^2(\beta) + \ldots + (\alpha + \sigma(\alpha) + \ldots + \sigma^{n-2}(\alpha))\sigma^{n-2}(\beta).$$

Aus $0 = T_K^L(\alpha) = \mathrm{id}(\alpha) + \sigma(\alpha) + \sigma^2(\alpha) + \ldots + \sigma^{n-1}(\alpha)$ folgt $\alpha = -(\sigma(\alpha) + \sigma^2(\alpha) + \ldots + \sigma^{n-1}(\alpha))$. Dann ist

$$\delta - \sigma(\delta) = \alpha\beta + \alpha\sigma(\beta) + \alpha\sigma^2(\beta) + \ldots + \alpha\sigma^{n-1}(\beta) = \alpha T_K^L(\beta) = \alpha.$$

(2) $\Longrightarrow$ (1): Sei $\alpha = \beta - \sigma(\beta)$. Dann ist $T_K^L(\beta - \sigma(\beta)) = T_K^L(\beta) - T_K^L(\sigma(\beta))$, also $T_K^L(\alpha) = T_K^L(\beta) - T_K^L(\sigma(\beta)) = \beta + \sigma(\beta) + \ldots + \sigma^{n-1}(\beta) - \sigma(\beta) - \sigma^2(\beta) - \ldots - \sigma^{n-1}(\beta) - \beta = 0$. □

Bemerkung 13.5. Die moderne Ausdrucksweise für Satz 13.4 ist:

$$H^1(\mathrm{Aut}(L/K), L^+) = 0.$$

Satz 13.6. *Sei* $\zeta \in K$ *eine primitive* n*-te Einheitswurzel, und sei* d *mit* d/n *gegeben. Dann gelten*

(1) $\eta := \zeta^{n/d}$ *eine* d*-te primitive Einheitswurzel.*
(2) *Sei* $a \in K$ *und* $\alpha \neq 0$ *eine Nullstelle von* $x^d - a$ *in einem Erweiterungskörper* L*. Dann sind* $\alpha, \eta\alpha, \ldots, \eta^{d-1}\alpha$ *paarweise verschiedene Nullstellen von* $x^d - a$ *in* L*. Weiterhin ist* $K(\alpha)$ *ein Zerfällungskörper von* $x^d - a$ *und* $K(\alpha) : K$ *galoissch.*

Beweis. (1) ζ erzeugt die zyklische Gruppe $E_n(K_n)$ der Ordnung n. Dann ist $(\zeta^{n/d})^d = \zeta^n = 1$. Offenbar hat $\zeta^{n/d}$ die Ordnung d. Also ist η eine primitive d-te Einheitswurzel, und alle $1, \eta, \eta^2, \ldots, \eta^{d-1}$ sind paarweise verschieden.
(2) Es sind $\alpha, \eta\alpha, \ldots, \eta^{d-1}\alpha$ genau alle Nullstellen von $x^d - a$. Also ist $K(\alpha)$ Zerfällungskörper von $x^d - a$. Weiter ist $x^d - a$ separabel, weil alle Nullstellen verschieden sind. Damit ist $K(\alpha) : K$ galoissch. □

Satz 13.7. *Sei* $\zeta \in K$ *eine primitive* n*-te Einheitswurzel* $(n \neq 1)$ *und* $L : K$ *ein Erweiterungskörper. Dann sind äquivalent:*

(1) $L : K$ *ist zyklisch vom Grad* d *mit* d/n*.*
(2) L *ist Zerfällungskörper eines Polynoms der Form* $x^n - a \in K[x]$*. Insbesondere ist* $L = K(\alpha)$ *für jede Nullstelle* α *von* $x^n - a$*.*
(3) L *ist Zerfällungskörper eines irreduziblen Polynoms der Form* $x^d - a \in K[x]$*, wobei* d/n*. Insbesondere ist* $L = K(\beta)$ *für jede Nullstelle* β *von* $x^d - a$*.*

Beweis. (1) $\Longrightarrow$ (3): $\mathrm{Aut}(L/K)$ ist zyklisch von der Ordnung $d = [L : K]$ mit d/n. Sei σ ein Erzeugendenelement von $\mathrm{Aut}(L/K)$. Sei η eine primitive d-te Einheitswurzel (in K). Dann ist $N_K^L(\eta) = \eta^d = 1$, also gibt es nach Hilberts Theorem 90 ein $\alpha \in L$ mit $\eta = \alpha^{-1}\sigma(\alpha)$. Es folgt $\sigma(\alpha) = \eta\alpha$ und $\sigma(\alpha^d) = (\eta\alpha)^d = \eta^d\alpha^d = \alpha^d$. Da $L : K$ galoissch ist, gilt $\alpha^d \in K$.

Damit ist α Nullstelle des Polynoms $x^d - a$ mit $a = \alpha^d$. Nach Satz 13.6 ist $K(\alpha)(\subseteq L)$ Zerfällungskörper von $x^d - a$. Weiter sind die $\sigma^i(\alpha) = \eta^i\alpha$ die paarweise verschiedenen Nullstellen von $x^d - a$, so daß $\sigma^i : K(\alpha) \cong K(\eta^i\alpha)$. Damit sind die $\sigma^i(\alpha)$ alle Nullstellen desselben Minimalpolynoms über K. $x^d - a$ muß dieses Minimalpolynom sein und ist daher irreduzibel und es gilt $[K(\alpha) : K] = d$.
(3) $\Longrightarrow$ (2): Sei $\alpha \in L$ eine Nullstelle von $x^d - a \in K[x]$. Dann ist $K(\alpha) = L$ Zerfällungskörper von $x^d - a$ nach Satz 13.6. Es ist $(\zeta\alpha)^n = (\alpha^d)^{n/d} = a^{n/d} =: b$ und damit $\zeta\alpha$ Nullstelle von $x^n - b$. Nach Satz 13.6 ist $K(\zeta\alpha)$ Zerfällungskörper von $x^n - b$. Es ist aber $K(\alpha) = \mathbb{K}(\zeta\alpha)$, und damit gilt (2).
(2) $\Longrightarrow$ (1): Sei α Nullstelle von $x^n - a$. Nach Satz 13.6 ist $L = K(\alpha)$ galoissch über K. Jedes $\sigma \in \mathrm{Aut}(L/K)$ ist vollständig bestimmt durch den Wert $\sigma(\alpha)$, was auch eine Nullstelle von $x^n - a$ ist. Als ist nach Satz 13.6 $\sigma(\alpha) = \zeta^i\alpha$ für ein geeignetes $i \in \{0, \dots, n-1\}$. Seien $\sigma, \tau \in \mathrm{Aut}(K(\alpha)/K)$. Dann ist $\sigma(\alpha) = \zeta^i\alpha$, $\tau(\alpha) = \zeta^j\alpha$, also $\sigma\tau(\alpha) = \sigma(\zeta^j\alpha) = \zeta^{i+j}\alpha$. Wir erhalten so einen Gruppenhomomorphismus $\varphi : \mathrm{Aut}(K(\alpha)/K) \ni \sigma \mapsto \bar{i} \in \mathbb{Z}/n\mathbb{Z}$. Da $\sigma \neq \tau$ impliziert $\bar{i} \neq \bar{j}$, ist φ injektiv. Also ist $\mathrm{Aut}(K(\alpha)/K) \subseteq \mathbb{Z}/n\mathbb{Z}$ und damit selbst zyklisch. Die Ordnung d muß die Ordnung n von $\mathbb{Z}/n\mathbb{Z}$ teilen. □

Folgerung 13.8 (Kummererweiterung I). *Sei p prim, $\chi(K) \neq p$ und $E_p(K) \subseteq K$. Sei $a \in K$ und $\alpha \notin K$ eine Nullstelle von $x^p - a$. Dann gelten*

(1) *$K(\alpha)$ ist galoissch über K,*
(2) *$[K(\alpha) : K] = p$.*

Beweis. K enthält eine primitive p Einheitswurzel $\zeta \in PE_p(K)$. Nach Satz 13.6 ist $K(\alpha)$ galoissch über K und Zerfällungskörper von $x^p - a$. Nach Satz 13.7 ist $[K(\alpha) : K]$ ein Teiler von p, also $[K(\alpha) : K] = p$. □

Folgerung 13.9 (Kummererweiterung II). *Sei p prim, $\chi(K) \neq p$ und $E_p(K) \subseteq K$. Sei $L : K$ galoissch und $[L : K] = p$. Dann gibt es ein $\alpha \in L$ mit $L = K(\alpha)$ und $\alpha^p \in K$. Weiter ist $x^p - \alpha^p$ irreduzibel.*

Beweis. K enthält eine primitive p-te Einheitswurzel, und die Gruppe $\mathrm{Aut}(L/K)$ hat die Ordnung p, ist also zyklisch. In Satz 13.7 verwenden wir $p = d = n$ und erhalten aus (3) die Behauptung. □

Satz 13.10 (Artin-Schreier). *Sei K ein Körper der Charakteristik $p \neq 0$ und L ein Erweiterungskörper von K. L ist genau dann eine zyklische Erweiterung von K vom Grade p, wenn L Zerfällungskörper eines irreduziblen Polynoms der Form $x^p - x - a \in K[x]$ ist. In diesem Falle ist $L = K(\alpha)$, wobei α eine Nullstelle von $x^p - x - a$ ist.*

Beweis. Sei $L : K$ zyklisch vom Grad p. Sei $\sigma \in \mathrm{Aut}(L/K)$ ein Erzeugendenelement. Dann ist $T_K^L(1) = [L : K]\cdot 1 = p\cdot 1 = 0$. Also gibt es nach Satz 13.4 ein $\alpha \in L$ mit $1 = -\alpha + \sigma(\alpha)$. Damit ist $\sigma(\alpha) = \alpha + 1 \neq \alpha$, also $\alpha \notin K$. Da $[L : K] = p$, gibt es keine echten Zwischenkörper, also ist $L = K(\alpha)$. Weiter ist $\sigma(\alpha^p) = (\alpha+1)^p = \alpha^p + 1$, also $\sigma(\alpha^p - \alpha) = (\alpha^p + 1) - (\alpha + 1) = \alpha^p - \alpha$ und damit $\alpha^p - \alpha =: a \in K$. Daher ist α eine Nullstelle von $x^p - x - a \in K[x]$. Dieses mußs das Minimalpolynom von α sein, weil der Grad des Minimalpolynoms gleich dem Körpergrad $[L : K] = p$ sein muß.
Die anderen Nullstellen von $x^p - x - a$ sind $\alpha + i \in K$, wobei $i = 1 + \ldots + 1 \in K$ im Primkörper liegt. Es ist nämlich $(\alpha + i)^p - (\alpha + i) - 1 = \alpha^p + i - \alpha - i - 1 = 0$. Also ist $K(\alpha)$ Zerfällungskörper von $x^p - x - a$.

Sei umgekehrt L Zerfällungskörper von $x^p - x - a \in K[x]$. Sei α eine Nullstelle von $x^p - x - a$ in L. Dann enthält $K(\alpha)$ wie zuvor genau p verschiedene Nullstellen $\alpha + i$. Also ist $x^p - x - a$ separabel, $K(\alpha) = L$ ist Zerfällungskörper von $x^p - x - a$ und $L : K$ ist galoissch. Jedes $\sigma \in \mathrm{Aut}(L/K)$ ist vollständig bestimmt durch $\sigma(\alpha)$ und $\sigma(\alpha)$ ist Nullstelle von $x^p - x - a$. Daher ist $\sigma(\alpha) = \alpha + i$ für ein i im Primkörper von K. Wir erhalten durch $\sigma \mapsto i$ einen injektiven Homomorphismus $\varphi : \mathrm{Aut}(L/K) \longrightarrow \mathbb{Z}/p\mathbb{Z}$. Damit ergeben sich zwei Fälle:
(1) $\mathrm{Aut}(L/K) = 1$, $[L : K] = 1$ und $x^p - x - a$ zerfällt über K, oder
(2) $\mathrm{Aut}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$, $[L : K] = p$ und $x^p - x - a$ ist irreduzibel. □

Folgerung 13.11. *Sei K ein Körper der Charakteristik $\chi(K) = p \neq 0$. Das Polynom $x^p - x - a \in K[x]$ ist entweder irreduzibel oder es zerfällt in $K[x]$.*

Übung 13.12. (1) Hungerford Proposition 7.7

14. Radikalerweiterungen

Definition 14.1. Eine Körpererweiterung $L : K$ heißt eine *Radikalerweiterung*, wenn $L = K(u_1, \ldots, u_n)$ und wenn gelten

1. eine Potenz von u_1 liegt in K,
2. für alle $i \geq 2$ liegt eine Potenz von u_i in $K(u_1, \ldots, u_{i-1})$.

Wenn $u_1^m \in K$, dann ist u_1 Nullstelle von $x^m - (u_1^m) \in K[x]$. u_1 heißt dann ein *Radikal* über K.

Beachte: Radikalerweiterungen sind endliche Körpererweiterungen.

Definition 14.2. (1) Sei $f \in K[x]$. f heißt *durch Radikale auflösbar*, wenn es eine Radikalerweiterung $L : K$ gibt, die einen Zerfällungskörper F von f enthält: $L \supseteq F \supseteq K$.
(2) Eine Körpererweiterung $F : K$ heißt *durch Radikale auflösbar*, wenn es eine Radikalerweiterung $L : K$ gibt mit $L \supseteq F \supseteq K$.

Definition 14.3. $L : K$ heißt eine *irreduzible Radikalerweiterung*, wenn $L = K(u_1, \ldots, u_n)$ und das Minimalpolynom von u_i über $K(u_1, \ldots, u_{i-1})$ von folgender Form ist

$$x^m - v \in K(u_1, \ldots, u_{i-1})[x].$$

Beispiele 14.4. (1) $x^2 + ax + b = 0$ hat die Lösungen

$$x_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \qquad (\chi(K) \neq 2).$$

(2) *Cardanosche Formeln: (1545)* [vorher Scipio del Ferro, Tartaglia] Sei $\chi(K) \neq 2, 3$. Die kubische Gleichung $x^3 + ax^2 + bx + c = 0$ hat mit

$$p := b - \frac{a^2}{3},\ q := \frac{2a^3}{27} - \frac{ab}{3} + c$$

und

$$P := \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \text{ und } Q := \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

die Lösungen

$$P + Q - \frac{a}{3},$$
$$\omega P + \omega^2 Q - \frac{a}{3},$$
$$\omega^2 P + \omega Q - \frac{a}{3}$$

wobei ω eine 3-te primitive Einheitswurzel ist.

Definition 14.5. Eine Gruppe G heißt *auflösbar*, wenn es Untergruppen $\{e\} = G_r \subseteq G_{r-1} \subseteq \ldots \subseteq G_0 = G$ gibt mit G_{i+1} normal in G_i und G_i/G_{i+1} abelsch.

Bemerkung 14.6. (1) Abelsche Gruppen sind auflösbar.
(2) Jede Untergruppe U einer auflösbaren Gruppe ist auflösbar. Man schneide die *Auflösung* $\{e\} = G_r \subseteq G_{r-1} \subseteq \ldots \subseteq G_0 = G$ mit der Untergruppe U.
(3) *Übung:* Jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.

Lemma 14.7. *Seien $K \subseteq E \subseteq F$ galoissche Körpererweiterungen und seien* $\mathrm{Aut}(F/E)$ *und* $\mathrm{Aut}(E/K)$ *auflösbar. Dann ist auch* $\mathrm{Aut}(F/K)$ *auflösbar.*

Beweis. Es ist $\mathrm{Aut}(F/K)/\mathrm{Aut}(F/E) \cong \mathrm{Aut}(E/K) = U_0 \supseteq U_1 \supseteq \ldots \supseteq U_n = \{e\}$, wobei U_{i+1} in U_i normal und U_i/U_{i+1} abelsch sind. Wir identifizieren $\mathrm{Aut}(F/K)/\mathrm{Aut}(F/E)$ mit $\mathrm{Aut}(E/K)$ entlang des Isomorphismus. Die Restklassenabbildung $\nu : \mathrm{Aut}(F/K) \longrightarrow \mathrm{Aut}(E/K)$ ist surjektiv. Wir erhalten Untergruppen $V_i := \nu^{-1}(U_i)$ und eine Kette

$$\mathrm{Aut}(F/K) = V_0 \supseteq V_1 \supseteq \ldots \supseteq V_n = \mathrm{Aut}(F/E) \supseteq V_{n+1} \supseteq \ldots \supseteq V_m = \{e\}$$

mit V_{i+1} normal in V_i und V_i/V_{i+1} abelsch für alle $i = 0, \ldots, m$. Für $i = 0, \ldots, n-1$ gilt nämlich $V_i/V_{i+1} \cong (V_i/V_n)/(V_{i+1}/V_n) \cong U_i/U_{i+1}$. Damit sind alle Gruppen V_{i+1} in V_i normal und V_i/V_{i+1} abelsch. Folglich ist $\mathrm{Aut}(F/K)$ auflösbar. □

Natürlich ist dieses lediglich eine Aussage über Gruppen und hat mit Galoistheorie nichts zu tun. Wir werden aber die Aussage in dieser Form benötigen.

Satz 14.8. *Sei $\chi(K) = 0$ oder $\chi(K) = p > p_l$, wobei p_i die i-te Primzahl ist, und seien $\zeta_i \in PE_{p_i}(K)$ für alle $i \leq l$. Dann gelten:*
(1) *$L := K(\zeta_1, \ldots, \zeta_l)$ ist eine irreduzible Radikalerweiterung von K mit $L \supseteq E_{p_i}(K)$ für alle $i = 1, \ldots, l$.*
(2) *$L : K$ ist galoissch und* $\mathrm{Aut}(L/K)$ *ist auflösbar.*

Beweis. Wir konstruieren L durch vollständige Induktion nach l.
Induktionsanfang: $l = 1$ und $p_1 = 2$. Wegen $x^2 - 1 = (x-1)(x+1)$ ist $\zeta_1 = -1$. Dann ist $L := K_1 := K = K(-1) = K(\zeta_1) \supseteq K$ eine irreduzible Radikalerweiterung mit dem irreduziblen Polynom $x - 1$. Es ist $E_2(K) \subseteq K$ wegen $p > 2$ und $-1 = \zeta_1 \in K$. Schließlich ist $K : K$ galoissch mit auflösbarer Galoisgruppe $\mathrm{Aut}(K/K) = \{e\}$.
Induktionsannahme: Sei $K_{(l-1)} := K(\zeta_1, \ldots, \zeta_{l-1}) \supseteq K$ mit $K_{(l-1)} \supseteq E_{p_i}(K)$, $i < l$ eine irreduzible Radikalerweiterung und sei $K_{(l-1)} : K$ galoissch und $\mathrm{Aut}(K_{(l-1)}/K)$ auflösbar.
Induktionsschluß: Wir definieren $K_{(l)} := K_{(l-1)}(\zeta_l)$ als Zerfällungskörper von $x^{p_l} - 1$ über $K_{(l-1)}$. Dann ist $K_{(l)} : K_{(l-1)}$ galoissch, denn $(x^{p_l} - 1)' = p_l x^{p_l - 1}$ hat nur 0 als Nullstelle. Daher ist $x^{p_l} - 1$ separabel. Weiter ist $G := \mathrm{Aut}(K_{(l)}/K_{(l-1)})$ zyklisch nach Folgerung 12.13 und $|G| < p_l$ (Bezeichnung für unser $K_{(l)}$ in 12.13 ist K_{p_l}). Also gibt es Gruppen $\{e\} =$

$G_r \underset{\neq}{\subseteq} G_{r-1} \underset{\neq}{\subseteq} \ldots \underset{\neq}{\subseteq} G_0 = G$ mit $|G_i/G_{i+1}| = p_{j_i} < p_l(< p)$ für geeignete $j_i < l$ und die $G_i \subseteq G$ sind normale Untergruppen. Daraus erhalten wir Körpererweiterungen $K_{(l)} = L_r \underset{\neq}{\supseteq} \ldots \underset{\neq}{\supseteq} L_0 = K_{(l-1)}$ mit $[L_{i+1} : L_i] = p_{j_i}$. Also ist $L_{i+1} = L_i(\alpha_i)$, wobei α_i nach Satz 13.7 das Minimalpolynom $x^{p_j} - (\alpha_i^{p_j})$ hat. Damit ist $K_{(l)} : K_{(l-1)}$ eine irreduzible Radikalerweiterung. Nach Konstruktion gilt $K_{(l)} \supseteq E_{p_i}(K)$ für alle $i = 1, \ldots, l$. Es ist $\mathrm{Aut}(K_{(l)}/K_{(l-1)})$ abelsch und damit auflösbar. Da $K(l) = K(\zeta_1, \ldots, \zeta_l)$ Zerfällungskörper der Polynome -$^{p_i} - 1$, $i \leq 1$ über K ist, ist $K(l) : K$ galoissch. Es sind $\mathrm{Aut}(K_{(l)}/K_{(l-1)})$ und $\mathrm{Aut}(K_{(l-1)}/K)$ auflösbar. Die Auflösbarkeit von $\mathrm{Aut}(K_{(l)}/K)$ folgt aus Lemma 14.7. □

Lemma 14.9. *Sei $L : K$ eine Körpererweiterung. Sei $K(\alpha) : K$ eine galoissche Körpererweiterung. Dann ist auch $L(\alpha) : L$ eine galoissche Körpererweiterung. Weiter ist $\mathrm{Aut}(L(\alpha)/L) \subseteq \mathrm{Aut}(K(\alpha)/K)$.*

Beweis. Es gilt $L(\alpha) = K(\alpha)(L)$. Damit ist der Körper $L(\alpha)$ Zerfällungskörper des separablen (Minimal-)Polynoms $f \in K[x] \subseteq L[x]$ von α über L. Also ist $L(\alpha) : L$ eine galoissche Körpererweiterung.
Sei nun $\sigma \in \mathrm{Aut}(L(\alpha)/L)$. σ ist festgelegt durch die Permutation, die es auf den Nullstellen von f induziert. Also bildet σ den Körper $K(\alpha)$ in sich ab und läßt die Elemente von K fix. Diese Einschränkung von σ auf $K(\alpha)$ induziert offenbar einen Gruppenhomomorphismus $\mathrm{Aut}(L(\alpha)/L) \longrightarrow \mathrm{Aut}(K(\alpha)/K)$. Dieser ist injektiv, denn wenn σ auf $K(\alpha)$ die Identität ergibt, dann auch auf den Nullstellen von f und damit auch auf $L(\alpha)$. Folglich können wir identifizieren $\mathrm{Aut}(L(\alpha)/L) \subseteq \mathrm{Aut}(K(\alpha)/K)$. □

Definition 14.10. Sei $L : K$ eine Körpererweiterung und $\alpha \in L$. Der *Exponent* von α ist die kleinste natürliche Zahl m mit $\alpha^m \in K$ oder ∞.

Satz 14.11.
(1) *Sei $F : K$ eine galoissche Körpererweiterung und $\chi(K) = 0$ oder $\chi(K)$ größer als alle Primteiler von $[F : K]$. Sei $\mathrm{Aut}(F/K)$ eine auflösbare Gruppe. Dann ist F in einer Radikalerweiterung $L : K$ enthalten, d.h. durch Radikale auflösbar.*
(2) *Sei $F : K$ eine Körpererweiterung und sei $K(\alpha_1, \ldots, \alpha_n)$ eine Radikalerweiterung von K mit $F \subseteq K(\alpha_1, \ldots, \alpha_n)$. Sei $\chi(K) = 0$ oder $\chi(K)$ größer als alle Primteiler aller Exponenten der α_i. Dann besitzt die kleinste galoissche Körpererweiterung $L : K$ mit $L \supseteq F$ eine auflösbare Galoisgruppe.*

Beweis. (1) Sei p_l die größte Primzahl mit $p_l/[F : K]$. Wie in Satz 14.8 sei $K_{(l)} := K(\zeta_1, \ldots, \zeta_l)$. Da $F : K$ galoissch ist, ist $F := K(\alpha)$ (Satz vom primitiven Element). Damit ist $K_{(l)}(\alpha) : K_{(l)}$ galoissch und $F \subseteq K_{(l)}(\alpha)$. Also ist $G := \mathrm{Aut}(K_{(l)}(\alpha)/K_{(l)}) \subseteq \mathrm{Aut}(F/K)$ auflösbar. Folglich gibt es Untergruppen $\{e\} \subseteq H_1 \subseteq \ldots \subseteq H_s = G$ mit H_i/H_{i+1} abelsch und sogar $\cong \mathbb{Z}/p\mathbb{Z}$ (für geeignete Primzahlen p) nach dem Hauptsatz über endlich erzeugte abelsche Gruppen. Die entsprechende Kette der Fixkörper sei $K_{(l)} = L_s \subseteq \ldots \subseteq L_1 \subseteq K_{(l)}(\alpha)$ mit $L_i : L_{i+1}$ galoissch und $[L_i : L_{i+1}] = p \leq p_l$. Nach Folgerung 13.9 ist $L_i : L_{i+1}$ eine einfache irreduzible Radikalerweiterung und $K_{(l)}(\alpha) : K_{(l)}$ eine irreduzible Radikalerweiterung. Weiter ist $K_{(l)} : K$ eine irreduzible Radikalerweiterung und damit auch $K_{(l)}(\alpha) : K$. Da $F \subseteq K_{(l)}(\alpha)$, ist F durch Radikale auflösbar.
(2) Sei p_l die größte Primzahl mit $p_l/[F : K]$.
a) *Behauptung:* Es gibt Radikale β_i mit $K(\alpha_1, \ldots, \alpha_r) = K(\beta_1, \ldots, \beta_t)$, deren Exponenten Primzahlen $\leq p_l$ sind und die Teiler der Exponenten von einem der $\alpha_1, \ldots, \alpha_r$ sind.
Beweis: Sei α Nullstelle des Polynoms $x^m - a$ und sei $m = p_1 \cdot \ldots \cdot p_s$ die Primzahlzerlegung von m. Dann ist $K(\alpha) = K(\alpha^{p_2 \cdot \ldots \cdot p_s}, \alpha^{p_3 \cdot \ldots \cdot p_s}, \ldots, \alpha^{p_s}, \alpha)$, denn α ist Nullstelle von $x^{p_s} - \alpha^{p_s}$,

α^{p_s} ist Nullstelle von $x^{p_{s-1}} - \alpha^{p_{s-1} \cdot p_s}$, usw. Folglich ist

$$\alpha = \sqrt[p_s]{\sqrt[p_{s-1}]{\ldots \sqrt[p_1]{a}}} = \sqrt[m]{a}.$$

Man wähle also für die β_i geeignete Potenzen der α_j.
b) *Behauptung:* Sei $K_{(l)} := K(\zeta_1, \ldots, \zeta_l)$ wie in Satz 14.8. Für $K_{(l)}(\beta_1, \ldots, \beta_t)$ gibt es eine Körpererweiterung $L_t \supseteq K_{(l)}(\beta_1, \ldots, \beta_t)$ mit

i) $L_t : K$ ist galoissch.
ii) $L_t = K_{(l)}(\gamma_1, \ldots, \gamma_s)$, wobei die γ_i Radikale mit Primzahlexponent $\leq p_l$ sind und die $K_{(l)}(\gamma_1, \ldots, \gamma_{i+1}) : K_{(l)}(\gamma_1, \ldots, \gamma_i)$ galoissch vom Grad $p \leq p_l$ für Primzahlen p sind.

Beweis von i) durch Induktion nach t: Der Fall $t = 0$ ist trivial.
Induktionsschluß von $t-1$ auf t. Sei β_t Nullstelle von $x^p - b$ mit $b \in L_{t-1}$ und $p \leq p_l$. Seien $b = b^{(1)}, b^{(2)}, \ldots, b^{(r)}$ die Konjugierten von b in L_{t-1} über K (d.h. $b^{(i)} = \sigma_i(b)$, $\sigma_i \in \mathrm{Aut}(L_{t-1}/K)$). Seien $\beta_t = \beta^{(1)}, \ldots, \beta^{(n)}$ alle Nullstellen aller Polynome $x^p - b^{(i)}$. Definiere $L_t := L_{t-1}(\beta^{(1)}, \ldots, \beta^{(n)})$.
Sei $N : K$ eine galoissche Körpererweiterung mit $N \supseteq L_t$. Sei $\sigma : L_t \longrightarrow N$ ein K-(Körper-) Homomorphismus. Dann läßt sich σ auf N fortsetzen, und es gilt $\sigma(L_{t-1}) \subseteq L_{t-1}$, weil $L_{t-1} : K$ galoissch ist.
Wir berechnen die $\sigma(\beta^{(i)})$ wie folgt. $\beta^{(i)p} = b^{(j)}$, also $\sigma(\beta^{(i)})^p = \sigma(b^{(j)}) \in \{b^{(1)}, \ldots, b^{(r)}\}$. Damit ist $\sigma(\beta^{(i)}) \in \{\beta^{(1)}, \ldots, \beta^{(n)}\}$ und $\sigma(L_t) \subseteq L_t$. Daraus folgt, daß $L_t : K$ galoissch ist, also Aussage i).
Beweis von ii) durch Induktion nach $j \leq n$: Es sind ineinander enthalten:

$$K \subseteq L_{t-1}(\ni b^{(1)}, \ldots, b^{(r)}) \subseteq L_t(\ni \beta^{(1)}, \ldots, \beta^{(n)}) \subseteq N$$

Induktionsanfang $i = 1$:
1. Fall: $\beta^{(1)} \in L_{t-1}$. Dann ist kein γ zu L_{t-1} hinzuzufügen.
2. Fall: $\beta^{(1)} \notin L_{t-1}$. Dann ist $L_{t-1}(\beta^{(1)}) : L_{t-1}$ galoissch und $[L_{t-1}(\beta^{(1)}) : L_{t-1}]$ ist eine Primzahl $\leq p_l$. Nach Folgerung 13.8 setzen wir $\gamma_1 := \beta^{(1)}$.
Induktionsschluß von $j-1$ auf j:
1. Fall: $\beta^{(j)} \in L_{t-1}(\beta^{(1)}, \ldots, \beta^{(j-1)}) = L_{t-1}(\gamma_1, \ldots, \gamma_m) = K_{(l)}(\gamma_1, \ldots, \gamma_m)$. Dann ist kein γ hinzuzufügen.
2. Fall: $\beta^{(j)} \notin L_{t-1}(\beta^{(1)}, \ldots, \beta^{(j-1)})$. Wie zuvor setzen wir $\gamma_{m+1} := \beta^{(j)}$.
c) *Behauptung:* Die Galoisgruppe von $L_t : K$ ist auflösbar, also auch die Galoisgruppe der kleinsten Galoiserweiterung L von K, die F enthält.
Beweis: Nach Satz 14.8 ist $K_{(l)} : K$ galoissch mit auflösbarer Galoisgruppe. Wir haben $K \subseteq K_{(l)} \subseteq K_{(l)}(\gamma_1) \subseteq \ldots \subseteq K_{(l)}(\gamma_1, \ldots, \gamma_s) = L_t$. Dabei ist $L_t : K$ galoissch mit Galoisgruppe G. Die zugehörige Kette von Untergruppen ist $G \supseteq U_0 \supseteq \ldots \supseteq U_s = \{e\}$. Dabei ist $G/U_0 = \mathrm{Aut}(K_{(l)}/K)$ auflösbar, $U_i/U_{i+1} = \mathrm{Aut}(K_{(l)}(\gamma_1, \ldots, \gamma_{i+1})/K_{(l)}(\gamma_1, \ldots, \gamma_i))$ hat die Ordnung $p \leq p_l$ nach Behauptung b). Mit U_{i+1} und U_i/U_{i+1} ist nach Lemma 14.7 auch U_i auflösbar. Mit U_0 und G/U_0 ist auch G auflösbar. $\square$

Folgerung 14.12. *Sei $\chi(K) = 0$ oder $\chi(K) > 3$. Dann ist jedes Polynom $f \in K[x]$ vom Grad ≤ 4 durch Radikale auflösbar.*

Beweis. Sei L Zerfällungskörper von f. Das Polynom f hat ≤ 4 Nullstellen in L. $\mathrm{Aut}(L/K)$ permutiert diese Nullstellen, also ist $\mathrm{Aut}(L/K) \subseteq S_4$. S_4 ist auflösbar, denn wir haben $S_4 \supseteq A_4 \supseteq V_4 \supseteq \{e\}$, alle Untergruppen sind normal in der nächst größeren Untergruppe und die Restklassengruppen sind $S_4/A_4 \cong \mathbb{Z}_2$, $A_4/V_4 \cong \mathbb{Z}_3$ und V_4, also abelsch. Also ist $\mathrm{Aut}(L/K) \supseteq (\mathrm{Aut}(L/K \cap A_4) \supseteq (\mathrm{Aut}(L/K) \cap V_4) \supseteq 0$ eine Auflösung von $\mathrm{Aut}(L/K)$. □

Hauptsatz 14.13 (über Auflösung durch Radikale)**.** *Sei $F : K$ eine Galoiserweiterung und $\chi(K) = 0$ oder $\chi(K) = p$, wobei p größer als alle Primteiler von $[F : K]$ ist. Dann sind äquivalent:*

(1) $\mathrm{Aut}(F/K)$ *ist auflösbar;*
(2) $F : K$ *ist durch Radikale auflösbar.*

Satz 14.14 (von Abel (1824))**.** *Sei $\chi(K) = 0$ oder $\chi(K) = p$, wobei p größer als alle Primteiler von n ist. Sei*

$$f(x) = x^n - a_1 x^{n-1} + \ldots + (-1)^n a_n \in K(a_1, \ldots, a_n)[x]$$

die allgemeine Gleichung n-ten Grades*. Die a_i seien transzendent über $K(a_1, \ldots, a_{i-1})$ für alle $i = 1, \ldots, n$. Das Polynom $f(x)$ ist genau dann durch Radikale auflösbar, wenn $n \leq 4$.*

Beweis. Die Galoisgruppe von f ist S_n nach Satz 10.13. Die Gruppe S_n enthält A_n als Normalteiler. A_n ist nach Satz 4.29 genau dann einfach, wenn $n \neq 4$. Da A_n für $n > 4$ nicht abelsch ist, ist S_n für $n > 4$ nicht auflösbar. Da $A_2 = \{e\}$ und $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, sind S_2, S_3, und S_4 auflösbar. □

15. Konstruktion regelmässiger n-Ecke

Bemerkung 15.1. Das regelmäßige n-Eck ist genau dann konstruierbar, wenn eine primitive n-te Einheitswurzel $\zeta = \alpha + i\beta \in \mathbb{C}$ konstruierbar ist.

Satz 15.2. *Das regelmäßige n-Eck ist genau dann konstruierbar, wenn die Eulersche φ-Funktion $\varphi(n)$ eine Zweierpotenz ist.*

Beweis. Die primitive Einheitswurzel $\zeta = \alpha + i\beta \in \mathbb{C}$ ist genau dann konstruierbar (über $\mathbb{Q}$), wenn α und β konstruierbar sind, d.h. daß es nach Satz 3.6 $\alpha, \beta \in L \subseteq \mathbb{R}$ gibt mit $[L : \mathbb{Q}] = 2^n$. Da $i \in \mathbb{Q}(i)$ mit $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, ist $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^m$ äequivalent zu $[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = [\mathbb{Q}(\zeta, i) : \mathbb{Q}] = 2^{m+1}$. Tatsächlich ist $\frac{1}{2}(\zeta + \overline{\zeta}) = \alpha$ mit $\overline{\zeta} = \zeta^{n-1}$ und $\frac{1}{2i}(\zeta - \overline{\zeta}) = \alpha$. Das ist wiederum äquivalent zu $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}_n : \mathcal{Q}_n) = 2^r$ für geeignetes r. Nach Satz 12.14 (2) ist das äquivalent zu $\varphi(n) = 2^r$. □

Definition 15.3. Ein Primzahl p heißt *Fermatsche Primzahl*, wenn p geschrieben werden kann als

$$p = 2^{2^m} + 1.$$

Lemma 15.4. *Sei p eine Primzahl der Form $p = 2^N + 1$. Dann ist p eine Fermatsche Primzahl.*

Beweis. Sei a ein Teiler von N. Dann ist die Primzahl

$$p = (2^b)^a + 1 = (2^b + 1)((2^b)^{a-1} - (2^b)^{a-2} + \ldots + 1),$$

also $a = 1$ und damit $N = 2^m$. Damit ist p eine Fermatsche Primzahl. □

Bemerkung 15.5. Die einzigen bekannten Fermatschen Primzahlen sind

$$3 = 2^{2^0} + 1,\ 5 = 2^{2^1} + 1,\ 17 = 2^{2^2} + 1,\ 257 = 2^{2^3} + 1,\ 65537 = 2^{2^4} + 1.$$

Es ist sicher, daß die Zahlen $2^{2^m} + 1$ für $m = 5, \ldots, 19$ keine Primzahlen sind. So ist etwa

$$F_5 = 2^{2^5} + 1 = 641 \cdot 6700417.$$

Satz 15.6. *Das regelmäßige n-Eck läßt sich genau dann mit Zirkel und Lineal konstruieren, wenn n ein Produkt einer Zweierpotenz mit paarweise verschiedenen Fermatschen Primzahlen ist*

$$n = 2^r p_2 \dots p_m.$$

Beweis. n werde als Produkt von Primzahlpotenzen geschrieben $n = 2^{i_1} p_2^{i_2} \dots p_m^{i_m}$. Nach Satz 12.4 ist dann $\varphi(n) = \varphi(2^{i_1})\varphi(p_2^{i_2}) \dots \varphi(p_m^{i_m})$ ebenfalls ein entsprechendes Produkt. Jeder Faktor ist eine Zweierpotenz genau dann, wenn das regelmäßige n-Eck konstruierbar ist.
Es ist $\varphi(2^i) = 2^i \cdot (1 - \frac{1}{2})$ immer eine Zweierpotenz. Weiter ist $\varphi(p^i) = p^i - p^{i-1}$ durch p^{i-1} teilbar, also nur dann eine Zweierpotenz, wenn $i = 1$ ist. In diesem Falle ist $\varphi(p) = p - 1$ eine Zweierpotenz genau dann, wenn $p = 2^N + 1$. □

Bemerkung 15.7. Konstruktionen des regelmäßigen n-Ecks für $n = 3, 5, 15$ und $n = 2^m \cdot 3, 2^m \cdot 5, 2^m \cdot 15$ sind aus dem Altertum bekannt. Das 7-Eck und das 9-Eck sind nicht konstruierbar. Die Konstruktion des 5-Ecks hängt eng mit dem goldenen Schnitt zusammen. C.F.Gauß (1777–1855) hat 1796 als erster die Konstruktion des regelmäßigen 17-Ecks angegeben. Eine mögliche Konstruktion des regelmäßigen 17-Ecks geht auf F.J.Richelot (1808–1875) zurück (1832). In den Archiven des Göttinger Mathematischen Seminars liegt ein Koffer mit einer unter Gauß entstandene Dissertation über die Konstruktion des regelmäßigen 65537-Ecks.

16. Zahlen zur Basis p

Bemerkung 16.1. Sei $p > 1$ eine natürliche Zahl. Jede natürliche Zahl $r \in \mathbb{N}$ läßt sich eindeutig in der Darstellung zur Basis p

$$r = a_n p^n + a_{n-1} p^{n-1} + \dots + a_1 p^1 + a_0 p^0 = (a_n a_{n-1} \dots a_1 a_0)_p$$

mit $0 \le a_i < p$ und $0 < a_n$ darstellen. Die Addition von natürlichen Zahlen in der Darstellung zur Basis p erfolgt wie folgt:

$$\begin{aligned} r &= (a_n a_{n-1} \dots a_1 a_0)_p \\ s &= (b_n b_{n-1} \dots b_1 b_0)_p \\ r + s &= (c_{n+1} c_n \dots c_1 c_0)_p \\ c_i &= \begin{cases} a_i + b_i + d_{i-1}, \\ a_i + b_i + d_{i-1} - p, \end{cases} \qquad d_i = \begin{cases} 0, & \text{falls } a_i + b_i + d_{i-1} < p, \\ 1, & \text{falls } a_i + b_i + d_{i-1} \ge p, \end{cases} \end{aligned}$$

Die Multiplikation hat eine ähnliche Beschreibung des "Übertragens" auf andere Stellen.

Bemerkung 16.2 (Zur Bestimmung der Ziffern in der Darstellung zur Basis p.)**.** Wir schreiben die Elemente von $\mathbb{Z}/p^n\mathbb{Z}$ als $\{\overline{0}, \overline{1}, \dots, \overline{a}, \dots, \overline{p^n - 1}\}$ mit den von nun an festgelegten Repräsentanten $0 \le a < p^n$.
Sei

$$\nu_{n-1} : \mathbb{Z}/p^n\mathbb{Z} \ni \overline{a} \mapsto \overline{a} \in \mathbb{Z}/p^{n-1}\mathbb{Z}$$

der Restklassenhomomorphismus. Sei weiter

$$\iota_{n-1} : \mathbb{Z}/p^{n-1}\mathbb{Z} \ni \overline{a} \mapsto \overline{a} \in \mathbb{Z}/p^n\mathbb{Z}$$

die mit den oben definierten Repräsentanten gebildete Abbildung

$$\mathbb{Z}/p^{n-1}\mathbb{Z} \cong \{0, 1, \dots, a, \dots, p^{n-1} - 1\} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

Beachte, daß durch die eindeutige Festlegung der Repräsentanten keine Wohldefiniertheit geprüft werden muß und daß ι_{n-1} kein Homomorphismus ist. Es ist jedoch

$$\nu_{n-1}\iota_{n-1} = \mathrm{id}_{\mathbb{Z}/p^{n-1}\mathbb{Z}} : \mathbb{Z}/p^{n-1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

Weiter ist $\alpha_{n-1} := \mathrm{id}_{\mathbb{Z}/p^n\mathbb{Z}} - \iota_{n-1}\nu_{n-1} : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ eine Abbildung mit $\mathrm{Bi}(\alpha_{n-1}) = p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$, denn $\nu_{n-1}\alpha_{n-1} : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}$ ist die Nullabbildung. Die Elemente aus $\mathrm{Bi}(\alpha_{n-1}) = p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$ haben dann die Darstellung $\overline{ap^{n-1}}$ mit einem eindeutig bestimmten a mit $0 \leq a < p$.
Unter dem kanonischen Isomorphismus $\gamma_{n-1} : p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \cong \{0, 1, \ldots, p-1\}$ wird dann jedes Element $\overline{ap^{n-1}}$ abgebildet auf $a \in \{0, 1, \ldots, p-1\}$. Es sei $\beta_{n-1} = \gamma_{n-1}\alpha_{n-1}$.
Die Zahl

$$\overline{r} = \overline{(a_np^n + a_{n-1}p^{n-1} + \ldots + a_1p^1 + a_0p^0)} = \overline{(a_na_{n-1}\ldots a_1a_0)_p}$$

wird durch β_i dann abgebildet auf a_i. Damit erhalten wir die oben angebene Darstellung $r = (a_na_{n-1}\ldots a_1a_0)_p$ und die zu bestimmenden Koeffizienten. Die Addition und Multiplikation von zwei Zahlen zur Basis p kann man also in $\mathbb{N}$ vornehmen und dann die β_i auf die Ergebnisse anwenden.
Da die Stellen in der Darstellung zur Basis p mit Hilfe von Abbildungen β_i erhalten werden, ist die Darstellung von natürlichen Zahlen in der Form $r = (a_na_{n-1}\ldots a_1a_0)_p = (\beta_n(\overline{r})\beta_{n-1}(\overline{r})\ldots\beta_1(\overline{r})\beta_0(\overline{r}))_p$ eindeutig.
Beachte: $(a_na_{n-1}\ldots a_1a_0)_p + (b_nb_{n-1}\ldots b_1b_0)_p \equiv (a_{n-1}\ldots a_1a_0)_p + (b_{n-1}\ldots b_1b_0)_p \mod p^n$ und analog $(a_na_{n-1}\ldots a_1a_0)_p \cdot (b_nb_{n-1}\ldots b_1b_0)_p \equiv (a_{n-1}\ldots a_1a_0)_p \cdot (b_{n-1}\ldots b_1b_0)_p \mod p^n$, weil beide Operationen in $\mathbb{Z}/p^n\mathbb{Z}$ bzw. $\mathbb{Z}/p^{n-1}\mathbb{Z}$ durchgeführt werden.

Beispiel 16.3. (1) Es ist $\overline{0}$ das neutrale Element der Addition in $\mathbb{Z}/p^n\mathbb{Z}$, also ist $(0\ldots0)_p$ das neutrale Element für die Addition der Zahlen zur Basis p.
(2) Sei $\overline{r} = \overline{\sum_{i=0}^n (p-1)p^i} = \overline{((p-1)(p-1)\ldots(p-1)(p-1))_p}$. Dann ist $\overline{1} + \overline{r} = \overline{(1)_p} + \overline{((p-1)(p-1)\ldots(p-1)(p-1))_p} = \overline{0}$ also

$$\overline{-1} = \overline{((p-1)(p-1)\ldots(p-1)(p-1))_p}$$

oder

$$-1 \equiv ((p-1)(p-1)\ldots(p-1)(p-1))_p \mod (p^n).$$

Definition 16.4. Sei

$$(a_i|i = 0, 1, \ldots, \infty)$$

eine Folge von natürlichen Zahlen mit $0 \leq a_i < p$. Wir betrachten die Folge der Teilsummen

$$(b_n) := (\sum_{k=0}^n a_kp^k|i \in \mathbb{N}) = (a_na_{n-1}\ldots a_1a_0)_p \tag{1}$$

Die Reihe

$$\sum_{k=0}^\infty a_kp^k = (\ldots a_3a_2a_1a_0)_p$$

sei eine Abkürzung für die Folge der Teilsummen (b_i) und heißt eine *p-adische ganze Zahl.* Die Menge der p-adischen ganzen Zahlen werde mit $\mathbb{Z}_p$ bezeichnet.
Beachte, daß die Folge der Teilsummen nicht konvergiert und daß damit (zunächst) $\sum_{k=0}^\infty a_kp^k = (\ldots a_3a_2a_1a_0)_p$ kein Element darstellen kann, gegen daß die Folge der endlichen Teilsummen konvergieren könnte.

Bemerkung 16.5. Die p-adischen ganzen Zahlen haben eine Addition und eine Multiplikation, indem man die Teilsummen (oder Teilfolgen zur Basis p) addiert bzw. multipliziert. Die p-adischen ganzen Zahlen sind damit ein kommutativer Ring und der Ring $\mathbb{Z}$ kann mit dem Unterring der abbrechenden Reihen ($a_n = 0$ für genügend große n) identifiziert werden.

Beispiel 16.6. Sei $r \in \mathbb{N}$. Dann hat r eine eindeutige Darstellung zur Basis p in der Form $r = \sum_{k=0}^{\infty} a_k p^k$ (Zifferndarstellung) in $\mathbb{Z}_p$, wobei ein n_0 existiert, sodaß die $a_n = 0$ für alle $n > n_0$.
Für $-1 \in \mathbb{Z}$ hat $(\ldots 00(-1))_p$ die Darstellung

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \ldots = \sum_{k=0}^{\infty} (p-1)p^k,$$

denn die Summe ist

$$\begin{aligned} p + (p-1)p + (p-1)p^2 + \ldots &= 0 + p \cdot p + (p-1)p^2 + \ldots \\ &= 0 + 0 + p \cdot p^2 + \ldots \\ &= 0 + 0 + 0 + \ldots = 0. \end{aligned}$$

Man darf bis zum n-ten Glied rechnen, da die Terme in $\mathbb{Z}/p^n\mathbb{Z}$ betrachtet werden.
In ähnlicher Weise haben alle negativen ganzen Zahlen Darstellungen durch (1).
Die rationale Zahl $\frac{1}{2}$ läßt sich für $p = 3$ darstellen als

$$\frac{1}{2} = 2 + 1 \cdot p + 1 \cdot p^2 + \ldots = (\ldots 1112)_3,$$

denn bei Multiplikation mit 2 ergibt sich

$$\begin{aligned} 1 &= (\ldots 1112)_3 \cdot (\ldots 0002)_3 \\ &= (2 \cdot 2) \cdot 3^0 + 2 \cdot 3 + 2 \cdot 3^2 + \ldots \\ &= 1 + 3 \cdot 3 + 2 \cdot 3^2 + \ldots \\ &= 1 + 0 + 3 \cdot 3^2 + \ldots \\ &= 1 + 0 + 0 + \ldots \end{aligned}$$

oder

$$\begin{array}{r} \ldots 1112 \cdot \ldots 0002 \\ \hline \ldots 0011 \\ \ldots 0002 \\ \ldots 0002 \\ \ldots 0002 \\ \hline \ldots 0001 \end{array}$$

Ein weiteres interessantes Element mit der Darstellung (1) ist

$$\sqrt{7} = 1 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + \ldots = (\ldots 20020111)_3,$$

denn durch Quadrieren der Zahlen zur Basis 3 erhält man

$$\begin{array}{r} \ldots 20020111 \cdot \ldots 20020111 \\ \hline \ldots 20020111 \\ \ldots 20020111 \\ \ldots 20020111 \\ \ldots 110110222 \\ \ldots 110110222 \\ \hline 7 = \quad \ldots 00000021 \end{array}$$

Bemerkung 16.7 (Die p-adischen Zahlen als Limes der Restklassen modulo p^n)**.** Sei $\nu_i^k : \mathbb{Z}/p^k\mathbb{Z} \ni \overline{a} \longrightarrow \overline{a} \in \mathbb{Z}/p^i\mathbb{Z}$ der kanonische Restklassenhomomorphismus für alle $i < n$. Wir definieren

$$\mathbb{Z}_p^{(n)} := \left\{ (\overline{b_n}, \ldots, \overline{b_2}, \overline{b_1}) \in \mathbb{Z}/p^n\mathbb{Z} \times \ldots \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \middle| \nu_i^k(\overline{b_k}) = \overline{b_i} \right\}.$$

Offenbar ist $\mathbb{Z}_p^{(n)} \subseteq \mathbb{Z}/p^n\mathbb{Z} \times \ldots \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ein Unterring. Weiter ist $\mathbb{Z}_p^{(n)} \cong \mathbb{Z}/p^n\mathbb{Z}$. Die Elemente $(\overline{b_n}, \ldots, \overline{b_2}, \overline{b_1}) \in \mathbb{Z}/p^n\mathbb{Z} \times \ldots \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ lassen sich wie oben in Zifferndarstellung zur Basis p darstellen. Dabei folgt aus $(a_{k-1} \ldots a_1 a_0)_p = (\overline{b_k}, \ldots, \overline{b_2}, \overline{b_1})$ die Gleichung $(a_{i-1} \ldots a_1 a_0)_p = (\overline{b_i}, \ldots, \overline{b_2}, \overline{b_1})$ für alle $i < k$.
Damit sind Addition, Subtraktion und Multiplikation der ersten i-Stellen der Darstellung zur Basis p unabhängig von dem Ergebniss bei den höheren Stellen. Die höheren Stellen können bei Rechnungen zunächst „vernachlässigt“ werden.
Aus diesen Überlegungen erhalten wir eine neue Definition von $\mathbb{Z}_p$ als

$$\mathbb{Z}_p := \left\{ (\ldots, \overline{b_2}, \overline{b_1}) \in \ldots \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \middle| \nu_i^k(\overline{b_k}) = \overline{b_i} \right\}.$$

Offenbar ist $\mathbb{Z}_p \subseteq \ldots \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$ ein Unterring. Die Elemente $(\ldots, \overline{b_2}, \overline{b_1}) \in \ldots \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ lassen sich wie oben in Zifferndarstellung zur Basis p darstellen. Dabei folgt aus $(\ldots a_1 a_0)_p = (\ldots, \overline{b_2}, \overline{b_1})$ die Gleichung $(a_{i-1} \ldots a_1 a_0)_p = (\overline{b_i}, \ldots, \overline{b_2}, \overline{b_1})$ für alle i.
Damit sind Addition, Subtraktion und Multiplikation der ersten i-Stellen der Darstellung zur Basis p unabhängig von dem Ergebniss bei den höheren Stellen. Die höheren Stellen können bei Rechnungen zunächst „vernachlässigt“ werden.
Allerdings ist $\mathbb{Z}_p$ nicht isomorph zu einem der Faktoren im Produkt.

17. Bewertungen

Definition 17.1. Sei R ein Integritätsring. Eine *Bewertung von R* ist eine Funktion $\varphi : R \longrightarrow \mathbb{R}$ mit

1. $\forall a \in R : \varphi(a) \geq 0$ und $\varphi(a) = 0$ dann und nur dann, wenn $a = 0$.
2. $\forall a, b \in R : \varphi(ab) = \varphi(a)\varphi(b)$.
3. $\forall a, b \in R : \varphi(a + b) \leq \varphi(a) + \varphi(b)$ (Dreiecksungleichung).

Eine Funktion $\varphi : R \longrightarrow \mathbb{R}$ heißt *nicht archimedische Bewertung* oder *Ultranorm*, wenn

1. $\forall a \in R : \varphi(a) \geq 0$ und $\varphi(a) = 0$ dann und nur dann, wenn $a = 0$.
2. $\forall a, b \in R : \varphi(ab) = \varphi(a)\varphi(b)$.
3. $\forall a, b \in R : \varphi(a + b) \leq \max(\varphi(a), \varphi(b))$.

Wenn eine Bewertung keine Ultranorm ist, dann heißt sie *archimedisch*.

Beachte: $\max(\varphi(a), \varphi(b)) \leq \varphi(a) + \varphi(b)$, weil $\varphi(a), \varphi(b) \in \mathbb{R}_0^+$.

Lemma 17.2. *Sei φ eine Bewertung von R. Dann gelten*

1. *$\varphi(1) = 1$.*
2. *$\varphi(-1) = 1$.*
3. *$\forall a \in R : \varphi(-a) = \varphi(a)$.*
4. *$\forall a, b \in R : |\varphi(a) - \varphi(b)| \leq \varphi(a - b)$.*

Beweis. (1) Nach Definition 17.1 (2) ist $\varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1)$, also $\varphi(1) = 1$.
(2) Nach Definition 17.1 (2) ist $1 = \varphi(1) = \varphi((-1)(-1)) = \varphi(-1)\varphi(-1)$. Wegen Definition 17.1 (1) ist $\varphi(-1) > 0$, also folgt $\varphi(-1) = 1$.
(3) Es ist $\varphi(-a) = \varphi(a \cdot (-1)) = \varphi(a)\varphi(-1) = \varphi(a)$.

(4) Es ist $\varphi(a) = \varphi(b + a - b) \leq \varphi(b) + \varphi(a - b)$, also $\varphi(a) - \varphi(b) \leq \varphi(a - b)$. Entsprechend ist $\varphi(b) - \varphi(a) \leq \varphi(b - a) = \varphi(a - b)$. Daraus folgt die Behauptung. □

Beispiele 17.3. (1) Sei $R \subseteq \mathbb{C}$. Dann ist $|.| : R \longrightarrow \mathbb{R}$ eine archimedische Bewertung.

(2) Sei R ein Integritätsring und $\varphi(a) = 1$ für $a \neq 0$ und $\varphi(0) = 0$. Dann ist φ eine Bewertung, die *triviale Bewertung*.

(3) Sei $R = \mathbb{Z}$ und p eine Primzahl. Jedes $a \in \mathbb{Z} \setminus \{0\}$ hat eine eindeutige Darstellung $a = p^k a'$ mit $p \nmid a'$ und $k \geq 0$. Dann ist $\varphi_p(a) := p^{-k}$ zusammen mit $\varphi_p(0) := 0$ eine nicht archimedische Bewertung von R, denn

(1) ist klar.

(2) folgt aus $a = p^k a'$, $b = p^l b' \Longrightarrow ab = p^{k+l} a'b' \Longrightarrow \varphi_p(ab) = p^{-(k+l)} = p^{-k}p^{-l} = \varphi_p(a)\varphi_p(b)$.

(3) Sei $a = p^k a'$, $b = p^l b'$ mit $k \leq l$. Dann ist $a+b = p^k(a'+p^{l-k}b')$ und $p \nmid a'+p^{l-k}b'$. Also folgt $\varphi_p(a + b) = p^{-k} = \varphi_p(a) = \max(\varphi_p(a), \varphi_p(b))$.

(4) Sei K ein Körper und p ein irreduzibles Polynom in $K[x]$. Dann induziert p eine nicht archimedische Bewertung von $K[x]$ wie in (3). Die induzierte Bewertung von K ist die triviale Bewertung.

Übung. Sei K ein Körper und sei $c \in K \setminus \{0\}$. Für ein Polynom $f \in K[x]$ vom Grad n definieren wir $\varphi(f) := c^{-n}$. Zeige, daß dieses eine Bewertung ist. Ist sie archimedisch?

Satz 17.4. *Sei R ein Integritätsring mit Quotientenkörper $Q(R)$. Sei $\varphi : R \longrightarrow \mathbb{R}$ eine Bewertung von R. Dann gibt es genau eine Fortsetzung von φ zu einer Bewertung $\psi : Q(R) \longrightarrow \mathbb{R}$. Ist φ nicht archimedisch, so ist auch ψ nicht archimedisch.*

Beweis. Sei ψ eine Fortsetzung von φ. Dann gilt $\psi(\frac{a}{b})\varphi(b) = \psi(\frac{a}{b})\psi(b) = \psi(\frac{a}{b}b) = \psi(a) = \varphi(a)$, also

$$\psi(\frac{a}{b}) = \frac{\varphi(a)}{\varphi(b)}.$$

Es bleibt zu zeigen, daß die Funktion $\psi(\frac{a}{b}) := \frac{\varphi(a)}{\varphi(b)}$ tatsächlich immer eine Bewertung ist. (1) und (2) sind klar. Zu (3) gilt

$$\begin{aligned} \psi(\frac{a}{b} + \frac{c}{d}) = \psi(\frac{ad + bc}{bd}) = \frac{\varphi(ad + bc)}{\varphi(bc)} &\leq \frac{\varphi(ad) + \varphi(bc)}{\varphi(bc)} \\ = \psi(\frac{ad}{bd}) + \psi(\frac{bc}{bd}) = \psi(\frac{a}{b}) + \psi(\frac{c}{d}). \end{aligned}$$

Sei nun φ nicht archimdisch. Dann haben wir

$$\begin{aligned} \psi(\frac{a}{b} + \frac{c}{d}) = \psi(\frac{ad + bc}{bd}) = \frac{\varphi(ad + bc)}{\varphi(bc)} \leq \frac{\max(\varphi(ad), \varphi(bc))}{\varphi(bc)} \\ = \max(\frac{\varphi(ad)}{\varphi(bd)}, \frac{\varphi(bc)}{\varphi(bd)}) = \max(\psi(\frac{ad}{bd}), \psi(\frac{bc}{bd})) = \max(\psi(\frac{a}{b}), \psi(\frac{c}{d})). \end{aligned}$$

□

Definition 17.5. Die Bewertung $\varphi_p : \mathbb{Z} \longrightarrow \mathbb{R}$ aus Beispiel 17.3 (3) ist eine nicht archimedische Bewertung und die Fortsetzung $\varphi_p : \mathbb{Q} \longrightarrow \mathbb{R}$ ist ebenfalls nicht archimedisch. Diese Bewertungen heißen *p-adische Bewertungen*. Wir schreiben $|a|_p := \varphi_p(a)$.

Beispiel 17.6. Die Fortsetzung der p-adischen Bewertung $\varphi_p : \mathbb{Q} \longrightarrow \mathbb{R}$ kann wie folgt beschrieben werden. Für eine rationale Zahl $\frac{a}{b} \in \mathbb{Q}$ nehmen wir $(a, b) = 1$ an. Dann ist $a = p^i a'$ mit $(p, a') = 1$, $(p, b) = 1$ und $i \geq 1$ oder es ist $b = p^{-i} b'$ mit $(p, b') = 1$, $(p, a) = 1$ und $i < 0$. Die p-adische Norm ist dann

$$|\frac{a}{b}|_p = p^{-i}.$$

Satz 17.7. *Eine Bewertung $\varphi : R \longrightarrow \mathbb{R}$ ist genau dann archimedisch, wenn es Zahl $n \in \mathbb{N}$ gibt mit $\varphi(n \cdot 1) > 1$.*

Beweis. Sei φ nicht archimedisch. Dann ist $\varphi(n \cdot 1) = \varphi(1 + \ldots + 1) \leq \max(\varphi(1), \ldots, \varphi(1)) = \varphi(1) = 1$.
Sei $\varphi(n \cdot 1) \leq 1$ für alle n. Dann ist $\varphi(n \cdot c) = \varphi(n \cdot 1)\varphi(c) \leq \varphi(c)$. Daraus folgt

$$\begin{aligned}
\varphi(a+b)^n &= \varphi((a+b)^n) \\
&= \varphi\left(a^n + \tbinom{n}{1} a^{n-1} b + \ldots + \tbinom{n}{n-1} a b^{n-1} + b^n\right) \\
&\leq \varphi(a^n) + \varphi(\tbinom{n}{1} a^{n-1} b) + \ldots + \varphi(\tbinom{n}{n-1} a b^{n-1}) + \varphi(b^n) \\
&\leq \varphi(a^n) + \varphi(a^{n-1} b) + \ldots + \varphi(a b^{n-1}) + \varphi(b^n) \\
&\leq (n+1) \max(\varphi(a), \varphi(b))^n,
\end{aligned}$$

oder $\varphi(a + b) \leq \sqrt[n]{n+1} \max(\varphi(a), \varphi(b))$. Da $\lim_{n \longrightarrow \infty} \sqrt[n]{n+1} = 1$, ergibt sich $\varphi(a + b) \leq \max(\varphi(a), \varphi(b))$. Also ist φ nicht archimedisch. □

Bemerkung 17.8. Bei einer archimedischen Bewertung gibt es natürliche Zahlen m mit beliebig großer Bewertung $\varphi(m)$, weil für $\varphi(n) = 1 + \delta$ gilt $\varphi(n^t) = \varphi(n)^t \geq 1 + t \cdot \delta$. Dieses ist das archimedische Axiom in der Elementargeometrie.

Satz 17.9. *Sei K ein endlicher Körper. Jede Bewertung von K ist trivial.*

Beweis. Sei $a \in K$, $a \neq 0$. Da $K^\times$ eine endliche Gruppe ist, gibt es ein m mit $a^m = 1$. Dann ist $\varphi(a)^m = \varphi(a^m) = \varphi(1) = 1$ in $\mathbb{R}_0^+$, also $\varphi(a) = 1$. □

Bemerkung 17.10. Die Dreiecksungleichung im p-adischen Fall ist $|a+b|_p \leq \max(|a|_p, |b|_p)$. Sie bedeutet im Falle $|a|_p \neq |b|_p$ folgendes. O.E.d.A. sei $|a|_p < |b|_p$. Dann ist $|a + b|_p \leq |b|_p$. Weiter ist $|b|_p = |(a+b) - a|_p \leq \max(|a+b|_p, |a|_p)$. Wegen $|b|_p > |a|_p$ ist dann $|b|_p \leq |a+b|_p$, also folgt $|b|_p = |a + b|_p$. Wir haben gezeigt: Jedes Dreieck mit den Seiten a, b, $a + b$ ist im p-adischen Fall gleichschenklig.

Bemerkung 17.11. Sei $r \in \mathbb{R}^+$ und $a \in R$. Der Ring R sei nicht-archimedisch bewertet mit $||a|| := \varphi(a)$. Die *offene Kreisscheibe* um a mit dem Radius r sei

$$D(a, r) := \{x \in R \mid ||x - a|| < r\}.$$

Sei nun $b \in D(a, r)$. Dann folgt

$$\begin{aligned}
&x \in D(a, r) \Rightarrow ||x - a|| < r \Rightarrow \\
&||x - b|| = ||(x - a) + (a - b)|| \leq \max(||x - a||, ||a - b||) < r \Rightarrow \\
&x \in D(b, r).
\end{aligned}$$

Analog zeigt man $D(b, r) \subseteq D(a, r)$, also $D(a, r) = D(b, r)$. Die offene Kreisscheibe mit Radius r um jeden Punkt $b \in D(a, r)$ ist genau $D(a, r)$.

18. Cauchy-Folgen

Definition 18.1. Sei $\varphi = ||.|| : R \longrightarrow \mathbb{R}$ eine Bewertung. Eine *Cauchy-Folge* bzgl. φ ist eine Folge $(a_i)_{i\in\mathbb{N}}$ mit der Eigenschaft:

zu jedem $\varepsilon > 0$ in $\mathbb{R}$ gibt es ein $n_0 \in \mathbb{N}$, so daß für alle $i, j > n_0$ gilt $||a_i - a_j|| < \varepsilon$,
$\forall \varepsilon > 0, \varepsilon \in \mathbb{R}\ \exists n_0 \in \mathbb{N}\ \forall i, j > n_0 : ||a_i - a_j|| < \varepsilon.$

Die Menge der Cauchyfolgen werde mit Ω_φ bezeichnet.

Definition 18.2. Zwei Bewertungen $\varphi : R \longrightarrow \mathbb{R}$ und $\varphi' : R \longrightarrow \mathbb{R}$ heißen *äquivalent*, wenn jede Folge $(a_i)_{i\in\mathbb{N}}$ genau dann bzgl. φ eine Cauchy-Folge ist, wenn sie bzgl. φ' eine Cauchy-Folge ist

Satz 18.3 (Ostrowski)**.** *Jede nicht-triviale Bewertung $||.||$ auf $\mathbb{Q}$ ist äquivalent zur Ultranorm $|.|_p$ für eine Primzahl p oder zur gewöhnlichen Norm $|.|_\infty := |.|$ auf $\mathbb{Q}$.*

Beweis. Fall 1: Sei $\varphi = ||.||$ eine archimedische Bewertung. Dann existiert eine natürliche Zahl n mit $||n|| > 1$. Sei n_0 die kleinste natürliche Zahl mit $||n_0|| > 1$. Beachte: $n_0 > 1$. Daher existiert eine positive reelle Zahl α mit $||n_0|| = n_0^\alpha$. Wir drücken jede natürliche Zahl in ihrer n_0-adischen Zifferndarstellung aus:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_s n_0^s \text{ mit } 0 \le a_i < n_0,$$

kurz

$$n = (a_s \ldots a_1 a_0)_{n_0}.$$

Dann ist

$$\begin{aligned} ||n|| &\le ||a_0|| + ||a_1 n_0|| + ||a_2 n_0^2|| + \ldots + ||a_s n_0^s|| \\ &= ||a_0|| + ||a_1|| n_0^\alpha + ||a_2|| n_0^{2\alpha} + \ldots + ||a_s|| n_0^{s\alpha} \end{aligned}$$

Da $a_i < n_0$, ist $||a_i|| \le 1$, also ist

$$\begin{aligned} ||n|| &\le 1 + n_0^\alpha + n_0^{2\alpha} + \ldots + n_0^{s\alpha} \\ &= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \ldots + n_0^{-s\alpha}) \\ &\le n^\alpha \left(\textstyle\sum_{i=0}^\infty (1/n_0^\alpha)^i\right), \end{aligned}$$

da $n \ge n_0^s$. Da $\sum_{i=0}^\infty (1/n_0^\alpha)^i$ konvergiert und unabhängig von n ist, gibt es eine Konstante C mit

$$||n|| \le C n^\alpha$$

für alle $n \in \mathbb{N}$. Insbesondere ist

$$||n||^N = ||n^N|| \le C(n^N)^\alpha = C(n^\alpha)^N$$

oder

$$||n|| \le \sqrt[N]{C} n^\alpha.$$

Wir bilden den Limes für $N \longrightarrow \infty$ und erhalten

$$||n|| \le n^\alpha.$$

Es gilt aber auch die umgekehrte Ungleichung. Wie zuvor schreiben wir $n = (a_s \ldots a_1 a_0)_{n_0}$. Dann gilt $n_0^{s+1} > n \ge n_0^s$. Da $||n_0^{s+1}|| = ||n + n_0^{s+1} - n|| \le ||n|| + ||n_0^{s+1} - n||$, erhalten wir

$$||n|| \ge ||n_0^{s+1}|| - ||n_0^{s+1} - n|| \ge n_0^{(s+1)\alpha} - (n_0^{n+1} - n)^\alpha,$$

denn $||n_0^{s+1}|| = n_0^{(s+1)\alpha}$ und nach der ersten Ungleichung gilt $||n_0^{s+1} - n|| \leq (n_0^{n+1} - n)^\alpha$. Daraus erhalten wir

$$\begin{aligned} ||n|| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha \text{ (da } n \geq n_0^s) \\ &= n_0^{(s+1)\alpha}\left[1 - \left(1 - \tfrac{1}{n_0}\right)^\alpha\right] \\ &\geq C' n^\alpha \end{aligned}$$

mit einer Konstanten C', die von α und n_0 abhängt, jedoch nicht von n. Insbesondere ist

$$||n||^N = ||n^N|| \geq C'(n^N)^\alpha = C'(n^\alpha)^N$$

oder

$$||n|| \geq \sqrt[N]{C'} n^\alpha.$$

Wir bilden den Limes für $N \longrightarrow \infty$ und erhalten $||n|| \geq n^\alpha$, also

$$||n|| = n^\alpha.$$

Wegen der Verträglichkeit mit Produkten erhalten wir $||\frac{r}{s}|| = |\frac{r}{s}|^\alpha$ für alle rationalen Zahlen $\frac{r}{s} \in \mathbb{Q}$.

Wir zeigen jetzt, daß die gewöhnliche Norm $|x|$ äquivalent ist zur gegebenen Norm $||x||$. Dazu betrachten wir $a_i - a_j$ und untersuchen die Cauchyfolgenbedingung. Da $\alpha > 0$ und damit die Funktion $\mathbb{R}_+ \ni x \mapsto x^\alpha \in \mathbb{R}_+$ streng monoton wachsend ist, ist

$$|a_i - a_j| < \varepsilon \iff |a_i - a_j|^\alpha < \varepsilon^\alpha.$$

Damit ist (a_i) genau dann eine Cauchyfolge bzgl. $|.|$, wenn es eine Cauchyfolge bzgl. $||.||$ ist. Die beiden Normen sind also äquivalent.

Fall 2: Sei $\varphi = ||.||$ eine nicht archimedische Bewertung. Dann gilt für jede natürliche Zahl n die Gleichung $||n|| \leq 1$. Sei n_0 die kleinste natürliche Zahl mit $||n_0|| < 1$. Ein solches n_0 existiert, weil die Bewertung nicht trivial ist.

Wir zeigen, daß n_0 eine Primzahl ist. Sei $n_0 = n_1 \cdot n_2$ mit $n_1, n_2 < n_0$. Dann ist $||n_1|| = ||n_2|| = 1$ und damit $||n_0|| = ||n_1|| \cdot ||n_2|| = 1$. Also kann n_0 nur eine Primzahl $p := n_0$ sein.

Sei $q \neq p$ eine weitere Primzahl in $\mathbb{N}$. Angenommen $||q|| < 1$. Dann gibt es ein N mit $||q^N|| = ||q||^N < \frac{1}{2}$. Weiter gibt es ein M mit $||q^M|| = ||q||^M < \frac{1}{2}$. Da p^M und q^N teilerfremd sind, gibt es ganze Zahlen m und n mit $mp^M + nq^N = 1$. Es folgt

$$1 = ||1|| = ||mp^M + nq^N|| \leq ||mp^M|| + ||nq^N|| = ||m||\ ||p^M|| + ||n||\ ||q^N||.$$

Wegen $||m||, ||n|| \leq 1$ folgt

$$1 \leq ||p^M|| + ||q^N|| < \frac{1}{2} + \frac{1}{2} = 1.$$

Also muß $||q|| = 1$ für jede Primzahl $q \neq p$ sein.

Für jede natürliche Zahl $a = p_1^{i_1} p_2^{i_2} \ldots p_r^{i_r} \in \mathbb{N}$ erhalten wir

$$||a|| = ||p_1^{i_1} p_2^{i_2} \ldots p_r^{i_r}|| = ||p_1||^{i_1} ||p_2||^{i_2} \ldots ||p_r||^{i_r} = ||p||^i,$$

wobei $a = p^i b$ mit $(p, b) = 1$.

Wegen der Verträglichkeit mit Produkten können wir die Norm auf $\mathbb{Q}$ für einen gekürzten Bruch $\frac{a}{b} \in \mathbb{Q}$ wie folgt ausdrücken:

$$||\frac{a}{b}|| = \frac{||a||}{||b||} = ||p||^i$$

mit dem eindeutig bestimmten $i \in \mathbb{Z}$ mit $a = p^i a'$ oder $b = p^{-i} b'$ und $(p, a') = (p, b') = 1$.

Sei $q := ||p||^{-1}$. Dann gilt für $a = p^i b$ mit $b = \frac{c}{d} \in \mathbb{Q}$ und c und d nicht teilbar durch p:

$$||a|| = q^{-i} \text{ und } |a|_p = p^{-i}.$$

Es ist $p^k < \varepsilon$ genau dann, wenn $p < \sqrt[k]{\varepsilon}$ genau dann, wenn $q < \frac{q}{p}\sqrt[k]{\varepsilon}$. Daher ist eine Folge genau dann Cauchyfolge bzgl. der gegebenen Norm $||a||$, wenn sie Cauchyfolge bzgl. der p-adischen Norm $|a|_p$ ist. Die beiden Normen sind also äquivalent. □

19. Die p-adischen Zahlen

Definition 19.1. Sei $\varphi = |.|_p : \mathbb{Q} \longrightarrow \mathbb{R}$ die p-adische Bewertung und Ω_φ die Menge der Cauchyfolgen.
Auf Ω_φ sei die Relation $(a_i) \sim (b_i)$ definiert durch die Bedingung

$$\forall \varepsilon > 0 \; \exists n \in \mathbb{N} \; \forall i > n : \varphi(a_i - b_i) < \varepsilon.$$

Bemerkung 19.2. Sei (a_i) eine Cauchy-Folge in $\mathbb{Q}$ bezüglich der p-adischen Bewertung $|.|_p$. Dann gibt es zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$, so daß für alle $i, j > n_0$ gilt $|a_i - a_j|_p = (1/p)^k < \varepsilon$ oder $\frac{1}{\sqrt[k]{\varepsilon}} < p$, wobei p^kdie größte p Potenz ist, die $a_i - a_j$ teilt. Beachte: für rationale a_i kann k auch negativ sein:

$$a = \frac{r}{s} = \frac{p^u r'}{p^v s'} = p^{u-v}\frac{r'}{s'}$$

mit $(p, r') = (p, s') = 1$. Man sieht so auch, daß die Werte, die $|.|_p$ annehmen kann, von der Form $p^k, k \in \mathbb{Z}$ oder 0 sind.
Sei $r = \frac{a}{b} \in \mathbb{Q}$ und $r = p^i \frac{a'}{b'}$ mit $(p, a') = (p, b') = 1$. Dann ist $|r|_p < \varepsilon$ genau dann, wenn $p^{-i} < \varepsilon$ genau dann, wenn $\frac{1}{\varepsilon} < p^i$. Für kleine ε ist damit p^i und ebenso r „groß“, genauer ein Vielfaches einer großen Potenz von p. Für ganze Zahlen $a \in \mathbb{Z}$ ist damit

$$|a|_p \leq p^{-i} \iff p^i / a.$$

Satz 19.3. *Sei φ die p-adische Bewertung von $\mathbb{Q}$. Die Relation der vorangehenden Definition ist eine Äquivalenzrelation. Die Menge der Äquivalenzklassen*

$$\mathbb{Q}_p := \Omega_\varphi / \sim$$

ist ein Körper der Charakteristik 0 mit

$$\overline{(a_i)} + \overline{(b_i)} := \overline{(a_i + b_i)}$$
$$\overline{(a_i)} \cdot \overline{(b_i)} := \overline{(a_i \cdot b_i)}.$$

Der Körper $\mathbb{Q}_p$ enthält $\mathbb{Q}$ als Unterkörper. Es existiert eine Fortsetzung der p-adischen Bewertung von $\mathbb{Q}$ auf $\mathbb{Q}_p$, und $\mathbb{Q}_p$ ist vollständig bezüglich dieser Bewertungsfortsetzung, d.h. jede Cauchyfolge in $\mathbb{Q}_p$ hat einen Grenzwert in $\mathbb{Q}_p$.

Beweis. Es ist klar, daß die Relation zwischen Cauchyfolgen reflexiv und symmetrisch ist. Sind (a_i), (b_i) und (c_i) Cauchyfolgen mit $(a_i) \sim (b_i)$ und $(b_i) \sim (c_i)$. Sei dann $\varepsilon > 0$ gegeben mit $n_1 \in \mathbb{N}$, so daß für alle $i > n_1$ gilt $|a_i - b_i|_p < \varepsilon$, und mit $n_2 \in \mathbb{N}$, so daß für alle $i > n_2$ gilt $|b_i - c_i|_p < \varepsilon$, so ist $|a_i - c_i|_p = |(a_i - b_i) + (b_i - c_i)|_p \leq \max(|a_i - b_i|_p, |b_i - c_i|_p) < \varepsilon$ für alle $i > \max(n_1, n_2)$, also $(a_i) \sim (c_i)$.
Wir definieren zunächst die Einbettung von $\mathbb{Q}$ in $\mathbb{Q}_p$. Jedem Element $r \in \mathbb{Q}$ ordenen wir zu die Äquivalenzklasse der konstanten Cauchyfolge (r). Diese Abbildung ist injektiv, denn wenn $\overline{(r)} = \overline{(s)}$ gilt, so sind (r) und (s) äquivalent. Sei $r \neq s$ und $0 < \varepsilon < |r - s|_p$. Dann gibt es ein n, so daß für alle $i > n$ gilt $|r - s| < \varepsilon$, ein Widerspruch. Also gilt $r = s$.

Wir bezeichnen die konstante Folge (r) mit r und identifizieren so $\mathbb{Q}$ mit einer Teilmenge von $\mathbb{Q}_p$.
Wir benötigen für unsere Rechnungen, daß die Cauchyfolgen „beschränkt“ sind. Sei (a_i) eine Cauchyfolge. Für $\varepsilon = 1$ sei $|a_i - a_j| < 1$ für alle $i, j \geq n$. Dann ist offenbar $|a_k|_p \leq \max(1, |a_1|_p, \ldots, |a_n|_p)$ für $k \leq n$. Es ist aber auch für $i > n$

$$|a_i|_p = |(a_i - a_n) + a_n|_p \leq \max(|a_i - a_n|_p, |a_n|_p) \leq \max(1, |a_1|_p, \ldots, |a_n|_p).$$

Seien nun $a, b \in \mathbb{Q}_p$ mit $a = \overline{(a_i)}$ und $b = \overline{(b_i)}$. Wir definieren $a + b$ als die Äquivalenzklasse, die von $(a_i + b_i)$ repräsentiert wird. Das ist eine Cauchyfolge, denn

$$|a_i + b_i - a_j - b_j|_p \leq \max(|a_i - a_j|_p, |b_i - b_j|_p) < \varepsilon$$

für $i, j > \max(n_a, n_b)$.
Wenn andere Repräsentanten gegeben sind: $a = \overline{(a'_i)}$ und $b = \overline{(b'_i)}$, so ist

$$|a'_i + b'_i - a_i - b_i|_p = |(a'_i - a_i) + (b'_i - b_i)|_p \leq \max(|a'_i - a_i|_p, |b'_i - b_i|_p) < \varepsilon$$

für $i > \max(n_a, n_b)$.
Seien $a, b \in \mathbb{Q}_p$ mit $a = \overline{(a_i)}$ und $b = \overline{(b_i)}$. Wir definieren $a \cdot b$ als die Äquivalenzklasse, die von $(a_i \cdot b_i)$ repräsentiert wird. Das ist eine Cauchyfolge, denn

$$|a_i \cdot b_i - a_j \cdot b_j|_p = |a_i(b_i - b_j) + (a_i - a_j)b_j|_p \leq \max(|a_i|_p|b_i - b_j|_p, |a_i - a_j|_p|b_j|_p) < \varepsilon$$

für $i, j > \max(n_a, n_b)$, wobei $|a_i - a_j|_p < \varepsilon / \sup(1, |b_i|_p)$ und $|b_i - b_j|_p < \varepsilon / \sup(1, |a_i|_p)$ für alle $i, j > \max(n_a, n_b)$.
Wenn andere Repräsentanten gegeben sind: $a = \overline{(a'_i)}$ und $b = \overline{(b'_i)}$, so ist

$$|a'_i \cdot b'_i - a_i \cdot b_i|_p = |a'_i(b'_i - b_i) + b_i(a'_i - a_i)|_p \leq \max(|a'_i|_p|b'_i - b_i|_p, |b_i|_p|a'_i - a_i|_p) < \varepsilon$$

für $i > \max(n_a, n_b)$.
Das additive Inverse von $\overline{(a_i)}$ ist $\overline{(-a_i)}$. Da alle Operationen „komponentenweise“definiert sind, wird $\mathbb{Q}_p$ damit ein kommutativer Ring.
Um das multiplikative Inverse von $\overline{(a_i)} \neq 0$ zu bilden, ändern wir (a_i) ab zu der Folge (b_i), die durch Fortlasen aller Nullen entsteht. Offenbar ist dann $|a_i - b_i|_p = |a_i - a_j|_p < \varepsilon$ für genügend große $i < j$. Dann bilden wir $\overline{(a_i)}^{-1} = \overline{(b_i^{-1})}$. Man zeigt leicht, daß dieses eine Cauchyfolge ergibt, deren Äquivalenzklasse invers zu $\overline{(a_i)}$ ist. Ebenso zeigt man leicht, daß diese Konstruktion nicht von der Wahl des Repräsentanten für $\overline{(a_i)}$ abhängt. Damit wird $\mathbb{Q}_p$ ein Körper, und $\mathbb{Q}$ ist offenbar vermöge der Identifizierung ein Unterkörper.
Wir definieren nun eine Fortsetzung der p-adischen Bewertung auf $\mathbb{Q}_p$. Sei $a = \overline{(a_i)}$. Wir definieren

$$|a|_p := \lim_{i \longrightarrow \infty} |a_i|_p.$$

Wenn $a = 0$, dann ist (a_i) eine Nullfolge, also ist $|a_i|_p = |a_i - 0|_p < \varepsilon$ für $i > n$. Damit ist $|a|_p = \lim_{i \longrightarrow \infty} |a_i|_p = 0$.
Wenn $a \neq 0$, dann gibt es ein $\varepsilon > 0$, so daß für jedes n ein $i_n > n$ existiert mit $|a_{i_n}|_p > \varepsilon$. Das ist die Negation der Definition einer Nullfolge. Wählen wir nun n so groß, daß $|a_i - a_j|_p < \varepsilon$ für alle $i, j > n$, dann ist insbesondere $|a_i - a_{i_n}|_p < \varepsilon$. Da $|a_{i_n}|_p > \varepsilon$, folgt aus Bemerkung 17.10 $|a_i|_p = |a_{i_n}|_p$ für alle $i > n$. Also ist $\lim_{i \longrightarrow \infty} |a_i|_p = |a_{i_n}|_p$.
Dieses merkwürdige Verhalten liegt an der Tatsache, daß die Werte von $|.|_p$ nach Bemerkung 19.2 von der Form $p^k, k \in \mathbb{Z}$ oder 0 sind.

Seien $a = \overline{(a_i)}$ und $b = \overline{(b_i)}$ in $\mathbb{Q}_p$ gegeben. Dann ist $|a+b|_p = \lim_{i\longrightarrow\infty} |a_i + b_i|_p \leq \lim_{i\longrightarrow\infty} \max(|a_i|_p, |b_i|_p) = \max(\lim_{i\longrightarrow\infty} |a_i|_p, \lim_{i\longrightarrow\infty} |b_i|_p)$. Ebenso ist $|a \cdot b|_p = \lim_{i\longrightarrow\infty} |a_i \cdot b_i|_p = \lim_{i\longrightarrow\infty}(|a_i|_p \cdot |b_i|_p) = \lim_{i\longrightarrow\infty} |a_i|_p \cdot \lim_{i\longrightarrow\infty} |b_i|_p = |a|_p |b|_p$. Also ist $|.|_p$ eine Ultranorm auf $\mathbb{Q}_p$.
Als Letztes bleibt zu zeigen, daß $\mathbb{Q}_p$ vollständig ist. Sei $(a_j|j \in \mathbb{N})$ eine Cauchyfolge in $\mathbb{Q}_p$. Für die Äquivalenzklassen a_j seien Repräsentanten $(a_{ji}|i \in \mathbb{N})$ ausgewählt, also $a_j = \overline{(a_{ji})_i}$. Wir bestimmen Zahlen $n_j \in \mathbb{N}$ so, daß

$$|a_{ji} - a_{jk}|_p < p^{-j} \text{ für alle } i, k \geq n_j.$$

Weiter wählen wir die Zahlen n_j aufsteigend, so daß $i < j$ impliziert $n_i < n_j$. Insbesondere sind dann $i \leq n_i$. Dann bilden wir die Folge $(a_{jn_j}|j \in \mathbb{N})$. Dieses ist eine Cauchyfolge, denn für $\varepsilon > 0$ folgt aus $|a_j - a_k| < \varepsilon/2$ die Ungleichung $\lim_{i\longrightarrow\infty} |a_{ji} - a_{ki}|_p < \varepsilon/2$. Damit ist $|a_{ji} - a_{ki}| < \varepsilon$ für genügend große i, j, k. Es folgt für $j > l$

$$|a_{jn_j} - a_{ln_l}|_p = |a_{jn_j} - a_{ln_j} + a_{ln_j} - a_{ln_l}|_p \leq \max(|a_{jn_j} - a_{ln_j}|_p, p^{-j}) < \varepsilon$$

für genügend große j und l und damit n_j und n_l. Weiter ist $\overline{(a_{jn_j})}$ der Limes der Folge (a_j) wegen $|a_{ji} - a_{jn_j}|_p < p^{-j}$ für alle j und genügend große i. □

Definition 19.4. Sei φ_p die p-adische Bewertung auf $\mathbb{Q}$. Der Körper

$$\mathbb{Q}_p := \Omega_p / \sim,$$

heißt *Körper der p-adischen Zahlen.*

Lemma 19.5. *Die Menge*

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \middle| |x|_p \leq 1 \right\}$$

ist ein Integritätsring und heißt Ring der p-adischen ganzen Zahlen.

Beweis. Wenn $x, y \in \mathbb{Z}_p$, dann ist $\varphi_p(xy) = \varphi_p(x)\varphi_p(y) \leq 1$ und $\varphi_p(x+y) \leq \max(\varphi_p(x), \varphi_p(y)) \leq 1$. Damit ist $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ ein Unterring. □

Lemma 19.6. *Sei $a \in \mathbb{Q}$ mit $|a|_p \leq 1$. Dann gibt es zu jedem i eine ganze Zahl $r \in \mathbb{Z}$, so daß $|r - a|_p \leq p^{-i}$. Die Zahl r kann aus der Menge $\{0, 1, 2, \ldots, p^i - 1\}$ gewählt werden.*

Beweis. Sei $a = \frac{b}{c}$ mit $(b, c) = 1$ gekürzt. Da $|a|_p \leq 1$, ist c nicht durch p teilbar, also ist $(p^i, c) = 1$. Es gibt $m, n \in \mathbb{Z}$ mit $mc + np^i = 1$.
Wir betrachten m als Approximation des Inversen von c, denn $mc \equiv 1 \mod p^i$ und $p^i / mc - 1$ impliziert $|mc - 1|_p \leq p^{-i}$.
Sei $r := bm$. Dann sollte r eine gute Approximation von $\frac{b}{c}$ sein. Tatsächlich ist

$$|r - a|_p = |bm - \frac{b}{c}|_p = |\frac{b}{c}|_p |mc - 1|_p \leq |mc - 1|_p = |np^i|_p = |n|_p p^{-i} \leq p^{-i}.$$

Schließlich können wir Vielfache von p^i zu r addieren, um eine ganze Zahl zwischen 0 und $p^i - 1$ zu erhalten, die weiterhin $|r - a|_p \leq p^{-i}$ erfüllt. □

Satz 19.7. *Jedes Element a in $\mathbb{Z}_p$ besitzt genau eine Cauchyfolge $(a_i|i \in \mathbb{N}_0)$ als Repräsentanten, für die gilt:*

(1) $0 \leq a_i < p^{i+1}$ *für* $i = 0, 1, 2, 3, \ldots$*;*
(2) $a_i \equiv a_{i+1} \mod p^{i+1}$ *für* $i = 0, 1, 2, 3, \ldots$*.*

Beweis. Eindeutigkeit: Sei (b_i) eine weitere Folge, die (1) und (2) erfüllt. Sei $a_{i_0} \neq b_{i_0}$. Dann ist auch $a_{i_0} \not\equiv b_{i_0} \mod p^{i_0}$, weil beide Terme zwischen 0 und p^{i_0} liegen. Für alle $i \geq i_0$ gilt dann wegen (2)

$$a_i \equiv a_{i_0} \not\equiv b_{i_0} \equiv b_i \mod p^{i_0}$$

also $a_i \not\equiv b_i \mod p^{i_0}$. Damit ist

$$|a_i - b_i|_p > p^{-i_0}$$

für alle $i \geq i_0$, also $(a_i) \not\sim (b_i)$.

Sei nun eine beliebige Cauchyfolge (b_i) gegeben $(a = \overline{(b_i)})$. Wir suchen eine dazu äquivalente Folge (a_i), die (1) und (2) erfüllt. Für alle $j = 1, 2, 3, \ldots$ sei n_j die natürliche Zahl, so daß $|b_i - b_k|_p \leq p^j$ für alle $i, k \geq n_j$. Wir wählen die n_j streng monoton wachsend, also insbesondere $n_j \geq j$.

Wir haben $|b_i|_p \leq 1$ für alle $i \geq n_1$, denn für alle $k \geq n_1$ gilt

$$|b_i|_p \leq \max(|b_k|_p, |b_i - b_k|_p) \leq \max(|b_k|_p, p^{-1}),$$

und $|b_k|_p \longrightarrow |a|_p \leq 1$ mit $k \longrightarrow \infty$.

Wir können daher Lemma 19.6 anwenden und konstruieren ganze Zahlen a_i mit $0 \leq a_i < p^i$, so daß

$$|a_i - b_{n_i}|_p \leq p^{-i}.$$

Wir zeigen, daß (a_i) die gewünschten Eigenschaften hat. Es ist nämlich

$$\begin{aligned} |a_{i+1} - a_i|_p &= |a_{i+1} - b_{n_{i+1}} + b_{n_{i+1}} - b_{n_i} - (a_i - b_{n_i})|_p \\ &\leq \max(|a_{i+1} - b_{n_{i+1}}|_p, |b_{n_{i+1}} - b_{n_i}|_p, |a_i - b_{n_i})|_p) \\ &\leq \max(p^{-(i+1)}, p^{-i}, p^{-i}) \\ &= p^{-i}. \end{aligned}$$

Damit ist $a_{i+1} \equiv a_i \mod p^{-i}$.

Weiter sei i gegeben und $k \geq n_i$. Dann ist

$$\begin{aligned} |a_k - b_k|_p &= |a_k - a_i + a_i - b_{n_i} - (b_k - b_{n_i})|_p \\ &\leq \max(|a_k - a_i|_p, |a_i - b_{n_i}|_p, |b_k - b_{n_i}|_p) \\ &\leq \max(p^{-i}, p^{-i}, p^{-i}) \\ &\leq p^{-i}. \end{aligned}$$

Folglich ist $\lim_{i \longrightarrow \infty} |a_i - b_i|_p = 0$ und damit $(b_i) \sim (a_i)$. □

Folgerung 19.8 (Die Darstellung von p-adischen ganzen Zahlen)**.** *Jedes Element a in $\mathbb{Z}_p$ besitzt genau eine Darstellung*

$$a = \sum_{i=0}^{\infty} a_i p^i = (\ldots a_2 a_1 a_0)_p$$

zur Basis p, für die gilt: $0 \leq a_i < p$ für alle $i \in \mathbb{N}_0$, und jede so definierte Folge von natürlichen Zahlen stellt ein Element a in $\mathbb{Z}_p$ dar.

Beweis. Wie in Definition 16.4 schreiben wir die Folge (b_i), die wir gemäß Satz 19.7 zu a bilden, in einer Darstellung zur Basis p

$$b_n := \sum_{k=0}^{n} a_k p^k = (a_n a_{n-1} \ldots a_1 a_0)_p.$$

Wegen (2) $b_{n-1} \equiv b_n \mod p^n$ unterscheiden sich b_{n-1} und b_n um ein Vielfaches von p^n, so daß bei der Darstellung von b_n dieselben Ziffern $a_{n-1} \dots a_1 a_0$ verwendet werden, wie bei der Darstellung von b_{n-1}. Da gilt (1) $0 \leq b_n < p^{n+1}$, folgt für den Faktor a_n die Ungleichung $0 \leq a_n < p$.
Umgekehrt erfüllt jede Folge $(b_n) = (\sum_{k=0}^{n} a_k p^k)$ von Teilsummen mit $0 \leq a_i < p$ die Bedingungen (1) und (2) aus dem Satz 19.7 und ist damit insbesondere eine Cauchyfolge. Offenbar ist $|\overline{(b_i)}|_p = \lim_{i \longrightarrow \infty} |b_i|_p = \lim_{i \longrightarrow \infty} p^{-k} = p^{-k} \leq 1$, wobei k bestimmt ist durch die Bedingung $a_0 = \ldots = a_{k-1} = 0$. Also ist $\overline{(b_i)}$ in $\mathbb{Z}_p$.
Damit können wir die p-adischen ganzen Zahlen aus $\mathbb{Z}_p$ eindeutig darstellen als

$$a = (\dots a_2 a_1 a_0)_p.$$

□

Bemerkung 19.9 (Die Darstellung von p-adischen Zahlen)**.** Wenn a eine p-adische Zahl in $\mathbb{Q}_p \setminus \mathbb{Z}_p$ ist, dann ist $|a|_p = p^n$ für ein $n > 0$. Wir multiplizieren a mit p^n und erhalten $b = p^n a$ mit $|b|_p \leq 1$. Dann läßt sich b schreiben als $b = (\dots a_2 a_1 a_0)_p$ oder als Äquivalenzklasse der Teilsummenfolge $(\sum_{k=0}^{m} a_k p^k)$. Dann läßt sich a schreiben als Äquivalenzklasse der Teilsummenfolge $(\sum_{k=0}^{m} (a_k \cdot p^{-n}) p^k) = (\sum_{k=-n}^{m} a_{k+n} p^k) = (\sum_{k=-n}^{m} a'_k p^k)$ mit $a'_k := a_{k+n}$ für alle $k \geq -n$. Die p-adische Zahl a hat damit eine eindeutige p-adische Darstellung

$$a = (\dots a_2 a_1 a_0,\ a_{-1} a_{-2} \dots a_{-n})_p.$$

Sie kann mit einem unendlichen Dezimalbruch verglichen werden. Die „kleinen“ Terme stehen in dieser Darstellung jedoch links mit der Bedeutung $a_n p^n$ und der Norm p^{-n}.

Folgerung 19.10 (Die p-adischen Einheiten)**.** *Sei $a \in \mathbb{Z}_p$ eine p-adische ganze Zahl. Dann sind äquivalent:*

(1) *a ist in $\mathbb{Z}_p$ invertierbar.*
(2) $|a|_p = 1$.
(3) *a hat die p-adische Darstellung $a = (\dots a_2 a_1 a_0)_p$ mit $a_0 \neq 0$.*
(4) *a ist per Definition eine* p-adische Einheit.

Beweis. Sei $a \in \mathbb{Z}_p$. Die Zahl a ist invertierbar in $\mathbb{Z}_p$ genau dann, wenn ein $b \in \mathbb{Z}_p$ existiert mit $ab = 1$. Daraus folgt $|ab|_p = |a|_p |b|_p = |1|_p = 1$, also muß gelten $|a|_p = 1$. Ist umgekehrt $|a|_p = 1$ also insbesondere $a \neq 0$, so gilt für das Inverse $b \in \mathbb{Q}_p$ von a die Gleichung $|a|_p |b|_p = |ab|_p = |1|_p = 1$, also $|b|_p = 1$. Damit ist nach Definition $b \in \mathbb{Z}_p$, also a in $\mathbb{Z}_p$ invertierbar. Mit der p-adischen Darstellung von $a = (\dots a_2 a_1 a_0)_p$ gilt $|a|_p = p^{-k}$, wenn $a_0 = a_1 = \ldots = a_{k-1} = 0$. Damit folgt auch die Äquivalenz (2) $\iff$ (3). □

Bemerkung 19.11 (Diverse Resultate)**.**

(1) Die Körper $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$ (für alle Primzahlen p) sind paarweise nicht isomorphe Erweiterungen von $\mathbb{Q}$, also alle von Charakteristik 0. Insbesondere sind alle Polynome über diesen Körpern und allen Unterkörpern separabel.
(2) Eine p-adische Darstellung

$$a = (\dots a_2 a_1 a_0, a_{-1} a_{-2} \dots a_{-n})_p$$

bricht genau dann ab ($a_i = 0$ für alle $i > n$), wenn a eine eine positive rationale Zahl ist, deren Nenner eine Potenz von p ist.
(3) Ein p-adische Darstellung von a ist periodisch genau dann, wenn $a \in \mathbb{Q}$.

(4) („Fermat“) Die Gleichung $x^p - x = 0$ hat p verschiedene Nullstellen $a_0, \dots, a_{p-1}$ in $\mathbb{Q}_p$ (Teichmüller Ziffern). Diese erfüllen $a_i \equiv i \mod p$.
(5) („Eisensteinkriterium“) Sei $f(x) = \sum_{k=0}^n a_k x^k$ ein Polynom in $\mathbb{Z}_p[x]$. Wenn $a_i \equiv 0 \mod p$ für $i = 0, \dots, n-1$, $a_n \not\equiv 0 \mod p$ und wenn $a_0 \not\equiv 0 \mod p^2$, dann ist $f(x)$ irreduzibel in $\mathbb{Q}_p$.
(6) Eine Reihe $\sum_{i=0}^\infty c_i$ mit c_i in $\mathbb{Q}_p$ konvergiert genau dann, wenn (c_i) eine Nullfolge bilden.
(7) $\mathbb{Z}_p$ ist folgenkompakt, d.h. jede Folge in $\mathbb{Z}_p$ hat eine konvergente Teilfolge.
(8) Der algebraische Abschluß $\overline{\mathbb{Q}_p}$ von $\mathbb{Q}_p$ ist nicht vollständig, trägt jedoch eine p-adische Topologie. Die Vervollständigung Ω von $\overline{\mathbb{Q}_p}$ ist algebraisch abgeschlossen. Ω ist das beste nicht archimedische Analogon zu den komplexen Zahlen $\mathbb{C}$.