Ergänzungen zur Algebra

gelesen von Joachim König
Sommersemester 2009
LaTeX von Maximilian Michel

8. Juli 2009

Inhaltsverzeichnis

1 Ergänzungen zur Körper- und Galois-Theorie **4**

1.1 Fundamentalsatz der Algebra 4
1.2 Endliche Körper 5
1.3 Spuren und Normen 6
1.4 Lineare Unabhängigkeit von Charakteren 8
1.5 Zyklische Erweiterungen 8
1.6 Einheitswurzeln und Kreisteilungspolynome 11
1.7 Auflösbarkeit durch Radikale 13
1.8 Zirkel- und Linealkonstruktion regulärer n-Ecke 15
1.9 Die Galoisgruppe von Xn-a 15
1.10 Symmetrische Polynome und die allgemeine Gleichung n-ten Grades 18
1.11 Diskriminanten 19
1.12 Bestimmung beliebiger Galoisgruppen und Reduktion modulo p 21

2 Auflösbare und nichtauflösbare Gruppentheorie **25**

2.1 Gruppen kleiner Ordnung 25
2.1.1 $|G|=pq$, $p<q$ Primzahlen 27
2.1.2 $|G|<16$ 27
2.1.3 $|G|=pgr$, $p<q<r$ Primzahlen 29
2.1.4 $p^a q^b$, $p < q$ Primzahlen, $ab, b \leq 2$ 30
2.1.5 Auflösbarkeit für $|G|<60$ 30
2.2 Der Satz von Jordan Hölder 30
2.3 Eine verallgemeinerung der Sylowsätze für auflösbare Gruppen 32

1 Ergänzungen zur Körper- und Galois-Theorie

1.1 Fundamentalsatz der Algebra

Der Fundamentalsatz der Algebra besagt, dass $\mathbb{C}$ algebraisch abgeschlossen ist.

Satz 1.1. ***Fundamentalsatz der Algebra****:*
Jedes nicht konstante Polynom $f \in \mathbb{C}[X]$ hat in $\mathbb{C}$ eine Nullstelle.

Es gibt verschiedene Beweismethoden, zum Beispiel in der Funktionentheorie mit dem **Satz von Liouville**. Wir beweisen den Satz Galoistheoretisch:

Lemma 1.2. *:*

(a) $\mathbb{R}$ hat keine echte Erweiterung ungeraden Grades

(b) $\mathbb{C}$ hat keine Grad 2 Erweiterung,

Beweis. (a) Sei $[E : \mathbb{R}]$ ungerade, $\alpha \in E$, Dann hat das Minimalpolynom von α über $\mathbb{R}$ auch ungeraden Grad, also eine reelle Nullstelle[1]. Da f irreduzibel über $\mathbb{R}$ ist, so muss schon $\operatorname{grad} f = 1$ sein, also $\alpha \in \mathbb{R}$

(b) Für $\operatorname{Char}(K) \neq 2$ gilt immer: $[K(\alpha) : K] = 2 \Rightarrow K(\alpha) = K(\sqrt{\beta})$ für ein $\beta \in K$. (Begründung: Lösungsformel für quadratische Gleichungen.)
Zu zeigen ist also nur, dass die Quadratwurzel komplexer Zahlen wieder in $\mathbb{C}$ liegen. Das folgt aus der Darstellung $\beta = r \cdot e^{i\varphi}$ $(r \in \mathbb{R}, \varphi \in [0, 2\pi))$ fÃ¼r alle $\beta \in \mathbb{C}$, denn

$$\sqrt{\beta} = \pm\sqrt{r} \cdot e^{i\frac{\varphi}{2}} \in \mathbb{C}.$$

□

Beweis. zu Satz 1.1 Sei $E|\mathbb{C}$ endlich. Dann ist auch $E|\mathbb{R}$ endlich und separabel. Sei L **Galoishülle** von $E|\mathbb{R}$ udn sei $G = \operatorname{Gal}(L|\mathbb{R})$. Sei P eine 2-Sylow-Gruppe von G

$$\Rightarrow \underbrace{[G : P]}_{\text{ungerade}} = [\operatorname{Fix}(P) : \mathbb{R}]$$

[1] Klar, wegen Zwischenwertsatz und

$$\lim_{x\to\infty} f(x) = \infty, \text{ und } \lim_{x\to-\infty} = -\infty.$$

Nach Lemma 1.2 ist dann $\mathrm{Fix}(P) = \mathbb{R}$, das heißt $P = G$ ist eine 2-Gruppe. Damit ist auch $\mathrm{Gal}(L|\mathbb{C}) \leq G$ eine 2-Gruppe, das heißt $[L : \mathbb{C}] = 2^k$, Falls $k \geq 1$, dann hat $\mathrm{Gal}(L|\mathbb{C})$ eine Untergruppe U vom Index 2. (Satz 2.56 Wintersemester). Dann ist $[\mathrm{Fix}(U) : \mathbb{C}] = [\mathrm{Gal}(L|\mathbb{C}) : U] = 2$, was nach Lemma 1.2 nicht sein kann. Also $[L : \mathbb{C}] = 1$, insbesondere $E = \mathbb{C}$, und $\mathbb{C}$ ist algebraisch abgeschlossen. □

1.2 Endliche Körper

Wir sammeln einige grundlegende Aussagen über endliche Körper.

Lemma 1.3. *Sei K endlicher Körper ($|K| < \infty$). Dann gilt:*

(a) $\mathrm{Char}\, K = p \in \mathbb{P}$

(b) $|K| = p^n,\ n \in \mathbb{N}$.

(c) $\forall_{a \in K} :\ a^q - a = 0$, *wobei* $q := |K|$

(d) K ist Zerfällungskörper von $X^q - X \in P[X]$, P ist hierbei der Primkörper von K

*(e) Zwei endliche Körper gleicher Mächtigkeit sind **isomorph**.*

(f) zu jeder Primpotenz p^n existiert ein Körper mit p^n Elementen.

(g) $[\bar{K} : K] = \infty$ *wobei $\bar{K}$ algebraisch Abschluss von K sei.*

Beweis. (a) $\mathrm{Char}(K) > 0$, da K endlich und wäre $\mathrm{Char}(K) = p \cdot q$ reduzibel, dann wären p, q nichttriviale Nullteiler in K

(b) K ist eine endliche Erweiterung seines Primkörpers $P = \{0, 1, 1+1, \ldots\}$ mit $|P| = p$. Da K P-Vektorraum ist, folgt $|K| = p^n$.

(c) Siehe Übung im Wintersemester ($(K^\times, \cdot)$ ist zyklisch der Ordnung $q - 1$, das heißt $a^{q-1} = 1\ \forall_{a \in K^\times}$)

(d) Alle $\underbrace{a \in K}_{q \text{ Elemente}}$ sind Nullstellen von $X^q - X$. Aus Gradgründen sind das schon alle Nullstellen also ist K **Zerfällungskörper** von $X^q - X$-

(e) Das war Aussage 4.17 im Wintersemester („Zwei Zerfällungskörper des gleichen Polynoms über den gleichen Grundkörper sind isomorph“)

(f) Sei $q = p^n$, E die Menge aller Nullstellen von $f = X^q - X$ [2]. Man sieht leicht, dass E sogar ein Körper ist[3]. Also ist $|E| = p^n$, E ein Körper wie gewünscht.

(g) $\left|\bar{K}\right| = \infty$, denn Übung 12 aus dem Wintersemester zeigte: endliche Körper sind **nie** algebraisch abgschlossen.

□

[2]Das Polynom ist **separabel**, denn $f' = \underbrace{q \cdot X^{q-1}}_{=0} - 1$; hat also genau q Nullstellen.

[3]Sei α, β Nulstellen von $X^q - X$, das heißt $\alpha^q = \alpha,\ \beta^q = \beta \Rightarrow (\alpha \cdot \beta)^q = \alpha^q \cdot \beta^q = \alpha\beta$ und $(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$. etc.

Die Galoistheorie endlicher Körper ist sehr übersichtlich:

Lemma 1.4. *Sei $E|K$ eine Erweiterung endlicher Körper, $|K| = q$, $|E| = q^n$. Dann gilt:*

*(a) $E|K$ ist **galoissch** mit zyklischer Galoisgruppe, ein Erzeuger der Gruppe ist $x \mapsto x^q$.*

*(b) Ist F Zwischenkörper von $E|K$, dann ist $|F| = q^m$ mit $m \mid n$, und zu jedem $m|n$ existiert auch **genau ein** Zwischenkörper der Mächtigkeit q^m.*

Beweis. (a) $E|K$ ist sowieso separabel, und auch normal nach Lemma 1.3 d), also galoisch. Wir wissen $[E : K] = n = |\mathrm{Gal}(E|K)|$. $\sigma : s \mapsto x^q$ [4] ist Automorphismus von E.

$$\mathrm{Fix}(\sigma) = \{x \in E \mid x^q - x = 0\} \overset{1.3d)}{=} K$$

Nach dem Hauptsatz der Galoistheorie

$$\Rightarrow \mathrm{Gal}(E|K) = < \sigma > .$$

(b) Die zyklische Gruppe $< \sigma >$ (der Ordnung $n = [E : K]$) hat zu jedem Teiler Ihrer Ordnung genau eine Untergruppe. Nach dem Hauptsatz der Galoistheorie existiert dann zu jedem $m|n$ ein Zwischenkörper F der Ordnung $q^{\frac{n}{m}}$ nämlich $\mathrm{Fix}(U)$

□

1.3 Spuren und Normen

Sei $E \mid K$ endlich, separabel, $\bar{K}$ algebraischer Abschluss von K. Sei S die Menge der K-Homomorphismen $E \to \bar{K}$[5].

Definition. Norm und **Spur**:
Wir definieren die **Norm** $N_K^E(\alpha)$ und $\alpha \in E$ durch

$$N_K^E(\alpha) = \prod_{\sigma \in S} \alpha^\sigma \tag{1.1}$$

Genauso definieren wir die **Spur** als

$$T_K^E(\alpha) = \sum_{\sigma \in S} \alpha^\sigma \tag{1.2}$$

Im folgenden zeigen wir unter Anderem, dass $N_K^E(\alpha)$ und $T_K^E(\alpha)$ immer in K liegen. Da sich zwei algebraische Abschlüsse von K nur durch einen K-Isomorphismus unterscheiden, ist die Definition von der Norm und Spur also unabhängig von der konkreten Wahl von $\bar{K}$.

Satz 1.5. *Satz $E|K$ endliche separable Erweiterung. Dann gilt:*

a) N_K^E ist ein multiplikativer (Gruppen-) Homomorphismus $E^\times \to K^\times$

[4] auch der **Frobenius-Automorphismus** genannt
[5] falls $E \mid K$ sogar galoisch, dann ist $S = \mathrm{Gal}(E|K)$

b) T_K^E *ist ein additiver (Gruppen-) Homomorphismus* $E \to K$

c) Ist $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ *das* K*-Minimalpolynom von* $\alpha \in E$ *dann gilt* $N_K^{K(\alpha)}(\alpha) = (-1)^n \cdot a_0$ *und* $T_K^{K(\alpha)}(\alpha) = -a_{n-1}$.

Beweis. Sei L eine Galoishülle von $E|K$, $\alpha \in E$. Jedes $\sigma \in S$ lässt sich fortsetzen zu einem K-Automorphismus σ von L, also einem Element aus $\mathrm{Gal}(L|K)$. Sei $\tau \in \mathrm{Gal}(L|K)$, $\sigma \in S$. Da $E^\sigma \leq L$ (sogar $L^\sigma = L$), ist $\sigma\tau$ definiert und ein Element von S. Daher ist $S \to S,\ \sigma \mapsto \sigma\tau$ eine Bijektion[6]. Also permutiert τ die Elemente von S:

$$\left(\prod_{\sigma\in S} \alpha^\sigma\right)^\tau = \prod_{\sigma\in S} \alpha^{\sigma\tau} = \prod_{\sigma\in S} \alpha^\sigma.$$

Also $N_K^E(\alpha) \in \mathrm{Fix}(\mathrm{Gal}(L|K)) = K$. Genauso:

$$T_K^E(\alpha) \in K$$

20.05.09

Homomorphismeneigenschaften sind offensichtlich, zum Beispiel:

$$N_K^E(\alpha \cdot \beta) = \prod_{\sigma\in S} (\alpha\beta)^\sigma = \prod_{\sigma\in S} \alpha^\sigma\beta^\sigma = \prod_{\sigma\in S} \alpha^\sigma \prod_{\sigma\in S} \beta^\sigma$$

damit sind (a) und (b) gezeigt. Zu (c): Zu jeder Nullstelle α_i von f existiert genau ein $\sigma \in S$ mit $\alpha \mapsto \alpha_i$

$$\Rightarrow N_K^{K(\alpha)}(\alpha) = \prod_{i=1}^n \alpha_i$$

und

$$T_K^{K(\alpha)}(\alpha) = \sum_{i=1}^n \alpha_i$$

es gilt::

$$\begin{aligned} f &= (x - \alpha_1) \cdot \ldots (x - \alpha_n) \\ \Rightarrow a_0 &= (-1)n \cdot \prod \alpha_i \end{aligned}$$

und

$$a_{n-1} = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n)$$

Dies liefert die Behauptung. □

[6] $\sigma\tau = \varrho\tau \Rightarrow \sigma\tau\tau^{-1}\varrho\tau\tau^{-1}$

1.4 Lineare Unabhängigkeit von Charakteren

Sei $(G, \cdot)$ eine **Magma**, das heißt, eine Menge mit einer (zweistelligen) Verknüpfung (zum Beispiel Halbgruppe, Monoid, Gruppe,...), und K ein Körper.

Definition. Charakter:
Ein **Charakter** von G ist eine Abbildung $\varphi : G \to K^\times$ mit $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. Man sagt, dass eine Menge $\{\varphi_i \mid i \in I\}$ von Charakteren **linear unabhängig** ist, wenn gilt:
Ist $\sum_i a_i \varphi_i \equiv 0$, mit $a_i \in K$ und $a_i = 0$ bis auf endlich viele Ausnahmen, dann sind schon alle alle $a_i = 0$

Satz 1.6. *von* E. Artin*:*
Die verschiedenen Charaktere $G \to K^\times$ eines Magmas (mit einem festen Körper K) sind linear unabhängig.

Beweis. Sei

$$a_1\varphi_1 + \ldots + a_n\varphi_n = 0 \tag{1.3}$$

eine kürzeste lineare Abhängigkeitsrelation (das heißt, $a_1, \ldots, a_n$ sind alle $\neq 0$). Es gilt natürlich $n \geq 2$. Da φ_1 und φ_2 verschieden sind , gibt es ein Element $g \in G$ mit

$$\varphi_1(g) \neq \varphi_2(g).$$

Für alle $x \in G$ gilt:

$$\begin{aligned} 0 &= a_1\varphi_1(gx) + \ldots + a_n\varphi_n(gx) && (1.4)\\ &= a_1\varphi_1(g)\varphi(x) + \ldots + a_n\varphi_n(g)\varphi_n(x) && (1.5) \end{aligned}$$

und (1.3)$\cdot\varphi_1(g)$ liefert

$$0 = a_1\varphi_1(g)\varphi_1(g) + \ldots a_n\varphi_1(g)\varphi_n(x). \tag{1.6}$$

Subtraktion von (1.6) von (1.5) liefert:

$$b_2\varphi_2(x) + \ldots + b_n\varphi_n(x) = 0$$

mit $b_i := a_i(\varphi_i(g) - \varphi_1(g))$. Wegen $\varphi_2(g) \neq \varphi_1(g)$ ist $b_2 \neq 0$, und damit habe wir eine kürzere Abhängigkeitsrelation als zu Beginn! Dies ist ein Widerspruch zur Minimalität! □

1.5 Zyklische Erweiterungen

Definition.
- Eine Galoiserweiterung $E \mid K$ heißt **zyklisch**, bzw **abelsch** bzw. **auflösbar**, wenn $\mathrm{Gal}(E \mid K)$ zyklisch bzw abelsch bzw. auflösbar ist.

- Sei $n \in \mathbb{N}$. Eine **primitive Einheitswurzel** in einem Körper K ist ein $a \in K$ mit multiplikativer Ordnung n, das heißt $a^n = 1$, $a^k \neq 1$ für alle $1 \leq k < n$.
  Die von a erzeugte multiplikative Gruppe hat also Ordnung n und offensichtlich sind alle Potenzen von a Nullstellen von $X^n - 1$ ($(a^k)^n = (a^n)^k = 1$), das heißt falls K **eine** primitive n-te Einheitswurzel enthält, dann zerfällt $X^n - 1$ über K in Linearfaktoren, und K enthält insbesondere **alle** primitiven n-ten Einheitswurzeln[7]

Der folgende Satz hat in einer fundamentalen Arbeit von HILBERT die Nummer 90, daher der Name.

Satz 1.7. ***Hilberts Satz 90***
Sei $E \mid K$ eine zyklische Körpererweiterung der Ordnung n mit der Galoisgruppe $\langle\sigma\rangle =: G$. Sei $\beta \in E$. Dann gilt

$$N_K^E(\beta) = 1 \tag{1.7}$$

genau dann, wenn es ein

$$0 \neq \alpha \in E \tag{1.8}$$

gibt mit

$$\beta = \frac{\alpha}{\alpha^\sigma}. \tag{1.9}$$

Beweis. Setze $N := N_K^E$. Sei $\alpha \neq 0$. Es gilt

$$N(\alpha) = \prod_{\tau \in G} \alpha^\tau,$$

insbesondere

$$N(\alpha^\sigma) = \prod_{\tau \in G} (\alpha^\sigma)^\tau$$

mit $G = \{\sigma\tau \mid \tau \in G\} = \{\tau \mid \tau \in G\}$ erhalten wir

$$= \prod_{\tau \in G} \alpha^\tau = N(\alpha) \neq 0,$$

und daher

$$N(\alpha/(\alpha^\sigma)) = \frac{N(\alpha)}{N(\alpha^\sigma)} = 1$$

[7] In $\mathbb{C}$ sind die n-ten Einheitswurzeln: $e^{\frac{2\pi i k}{n}}$.

Bemerkung. primitive n-te Einheitswurzeln gibt es nicht über jedem Körper, zum Beispiel git es über $\mathbb{F}_2$ keine primitive 2-te Einheitswurzel, denn $X^2 - 1 = (X-1)^2$.

(das erste Gleichheitszeichen gilt nach der Multiplikativität der Norm!). Damit ist die Rückrichtung gezeigt. Sei nun $N(\beta) = 1$. Für $0 \leq i \leq n-1$ sind die Abbildungen $x \mapsto x^{\sigma^i}$ verschiedene Charaktere der multiplikativen Gruppe von E (auf sich selbst). Daher ist nach dem Satz 1.6 die Abbildung

$$x \mapsto \varphi(x) := x + \beta \cdot x^{\sigma} + \beta \cdot \beta^{\sigma} x^{\sigma^2} + \ldots + \beta \cdot \ldots \cdot \beta^{\sigma^{n-2}} x^{\sigma^{n-1}}$$

nicht die Nullabbildung von E nach E . Sei also $\gamma \in E$ mit

$$\varphi(\gamma) =: \alpha \neq 0$$

dann gilt

$$\alpha - \beta\alpha^{\sigma} = \cancel{\gamma} + \cancel{\beta\gamma^{\sigma}} + \cancel{\beta\beta^{\sigma}\gamma^{\sigma^2}} + \ldots + \cancel{\beta \cdot \ldots \cdot \beta^{\sigma^{n-2}} \cdot \gamma^{\sigma^{n-1}}}$$
$$\cancel{-\beta\gamma^{\sigma}} - \cancel{\beta\beta^{\sigma}\gamma^{\sigma^2}} - \ldots \cancel{-\beta \cdot \ldots \cdot \beta^{\sigma^{n-2}} \gamma^{\sigma^{n-1}}} - \underbrace{\cancel{\beta \cdot \beta^{\sigma} \cdot \ldots \cdot \beta^{\sigma^{n-1}}}}_{=N(\beta)=1} \underbrace{\gamma^{\sigma^n}}_{=\gamma,\ \text{da}\ \sigma^n=\mathrm{id}}$$
$$= 0 \Rightarrow \beta = \frac{\alpha}{\alpha^{\sigma}}$$

□

Wir wissen schon, dass eine quadratische Körpererweiterung $E \mid K$ für $\mathrm{Char}(K) \neq 2$, immer von der Form $K(\alpha)$ mit $\alpha^2 \in K$ ist.
Man beachte, dass $\mathrm{Char}(K) \neq 2 \Leftrightarrow K$ enthält eine primitive 2. Einheitswurzel.

Satz 1.8. *Sei $E \mid K$ zyklische Galoiserweiterung vom Grad n. K enthalte eine primitive n-te Einheitswurzel. Dann existiert $\alpha \in E$ mit $E = K(\alpha)$ und $\alpha^n \in K$ („$E = K(\sqrt[n]{\ldots})$“).*

Beweis. Sei ζ eine primitive n-te Einheitswurzel in K, σ eine Erzeuger von $\mathrm{Gal}(E \mid K)$. Es gilt

$$N_K^E(\zeta) = \zeta^n = 1.$$

Nach Satz 1.7 existiert $0 \neq \alpha \in E$ mit $\alpha^{\sigma} = \zeta \cdot \alpha$: Iterierte Anwendung von σ liefert

$$\begin{aligned} \alpha^{\sigma^i} &= (\alpha^{\sigma})^{\sigma^{i-1}} = (\zeta \cdot \alpha)^{\sigma^{i-1}} \\ &= \ldots = \zeta^i \cdot \alpha \end{aligned}$$

Da ζ die multiplikative Ordnung n hat, sind die α^{σ^i}, $0 \leq i \leq n-1$, alle verschieden, das heißt das Minimalpolynom von α hat mindestens die n verschiedenen Nullstellen $\alpha^{\sigma^i} = \zeta^i\alpha$.

$$\Rightarrow [K(\alpha) : K] \geq n,$$

mit $[E : K] = n$, was auf

$$E = K(\alpha)$$

führt und wir erhalten:

$$\begin{aligned} (\alpha^n)^{\sigma} = (\alpha^{\sigma})^n = (\zeta\alpha)^n = \zeta^n\alpha^n = \alpha^n \\ \Rightarrow \alpha^n \in \mathrm{Fix}(\langle\sigma\rangle) = K. \end{aligned}$$

□

1.6 Einheitswurzeln und Kreisteilungspolynome

Definition. Im Folgenden sei $n \in \mathbb{N}$, K ein Körper mit entweder $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K)$ teilerfremd zu n. Dann ist $X^n - 1$ separabel. Sei $\bar{K}$ algebraischer Abschluss von K. Die Nullstellen von $X^n - 1$ in $\bar{K}$ bilden eine multiplikative Gruppe der Ordnung n; diese ist dann auch zyklisch, da endliche Untergruppe von $\bar{K}^\times$. Die Erzeuger dieser zyklischen Gruppe sind die primitiven n-ten Einheitswurzeln (davon gibt es genau $\varphi(n)$ Stück). Das **n-te Kreisteilungspolynom** $\Phi_n(X)$ ist das Minimalpolynom einer primitiven n-ten Einheitswurzel über $\mathbb{Q}$. Wir müssen zuerst zeigen, dass $\Phi_n(X)$ **unabhängig** von der gewählten primitiven Einheitswurzel ist.

Satz 1.9. *Die Nullstellen von $\Phi_n(X)$ sind **genau** die primitiven n-ten Einheitswurzeln in $\mathbb{C}$. Außerdem ist $\Phi_n(X) \in \mathbb{Z}[X]$*

Bemerkung. Man kann daraus

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

folgern.

27.05.09

Beweis. $\Phi_n(x) \mid \underbrace{X^n - 1}_{\in \mathbb{Z}[X], \text{normiert}}$, also folgt der zweite Teil schon mit dem Gauß-Lemma. Sei nun $X^n - 1 = \Phi_n(X) \cdot g(X)$, mit $g(X) \in \mathbb{Z}[X]$. Da jede primitive n-te Einheitswurzel die Potenz (mit zu n teilerfremdem Exponenten) einer **festen** primitiven Einheitswurzel ist, genügt es folgendes zu zeigen:
Sei p prim und $p \nmid n$, und $\zeta \in \mathbb{C}$ mit $\Phi(\zeta) = 0$, dann auch $\Phi_n(\zeta^p) = 0$. Nehmen wir an:

$$\Phi_z(\zeta^p) \neq 0, \Rightarrow g(\zeta^p) = 0$$

das heißt, ζ ist Nullstelle von $g(X^p)$, also ist $\Phi_n(X) \mid g(X^p)$, das heißt $g(X^p) = \Phi_n(X) \cdot h(X), h \in \mathbb{Z}[X]$. Mit $\bar{f}$ bezeichnen wir das natürliche Bild des Polynoms f in $\mathbb{F}_p[X]$

$$\Rightarrow \bar{g}(X^P) = \bar{\Phi}_n(X) \cdot \bar{h}(X)$$

Nebenrechnung: Sei

$$\begin{aligned} \bar{g} &= X^k + a_{k-1}X^{k-1} + \ldots + a_0 \\ \Rightarrow \bar{g}(X^p) &= X^{k \cdot p} + \underbrace{a_{k-1}}_{=(a_{k-1})^p} X^{(k-1)\cdot p} + \ldots + \underbrace{a_0}_{=a_0^p} \end{aligned}$$

in $\mathbb{F}_p$ ist $a^p + b^p = (a+b)^p$

$$= (X^k + a_{k-1}X^{k-1} + \ldots + a_0)^p = [\bar{g}(X)]^p$$

Ende Nebenrrechnung. Dies führt auf:

$$\Rightarrow \underbrace{\bar{g}(X^P)}_{=[\bar{g}(X)]^p} = \bar{\Phi}_n(X) \cdot \bar{h}(X)$$

Insbesondere sind $\bar{\Phi}_n$ und $\bar{g}$ nicht teilerfremd! Aber

$$X^n - 1 = \bar{\Phi}_n \cdot \bar{g},$$

das heißt, $X^n - 1$ hat eine doppelte Nullstelle über $\mathbb{F}_p$, ist also nicht separabel. Dies führt auf einen **Widerspruch**, denn für $p \not| n$ ist $X^n - 1$ **immer separabel** über $\mathbb{F}_p$. Noch zu zeigen ist, dass Φ_n keine weitere Nullstelle hat. Sei also $\Phi_n(\beta) = 0$, β **keine** primitive n-te Einheitswurzel. Dann ist β eine primitive k-te Einheitswurzel für ein $k < n$ ($\beta^n - 1 = 0$, da $\Phi_n \mid X^n - 1$). Wir haben bereits gezeigt, dass

$$\Phi_n(\beta) = 0. \Rightarrow \Phi_n = \Phi_k,$$

da diese irreduziblen Poylnome die gemeinsame Nullstelle β haben, was auf $\Phi_n \mid X^k - 1$ führt. Aber dann sind die primitiven n-ten Einheitswurzeln Nullstellen von $X^k - 1$, $k < n$. Wiederum ein Widerspruch! □

Korollar 1.10. *Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ galoissch mit Gruppe isomorph zu $(\mathbb{Z}/n\mathbb{Z})^\times$*

Bemerkung. Zur Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$: Mit dem Chin-. Restsatz:
Ist $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ dann ist $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}(p_r^{e_r}\mathbb{Z})$, also auch $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$. Man kann diese Einheitengruppe genau angeben, wir begnügen uns vorerst mit $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$

Beweis. $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ ist galoissch, da Zerfällungskörper von $X^n - 1$. Jede primitive n-te Einheitswurzel ist von der Form ζ^k, mit $k \in \mathbb{Z}$, k teilerfremd zu n. Weiter ist $\zeta^k = \zeta^l$ genau dann wenn $k - l \in n\mathbb{Z}$, also ist für $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ die primitive Einheitswurzel ζ^a wohldefiniert.
Die Galoisbilder von ζ sind wieder primitive n-te Einheitswurzeln, jedes $\sigma \in G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ ist durch ζ^σ eindeutig festgelegt.
Daraus erhalten wir: Die Abbildung

$$G \to (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \sigma \mapsto a_\sigma$$

(wobei $\zeta^\sigma =: \zeta^{a_\sigma}$) ist also ein Gruppenhomomorphismus[8]. Weiter wird ζ nur von $\mathrm{id} \in G$ fixiert, das heißt $\sigma \mapsto 1$ nur für $\sigma = \mathrm{id}$, das heißt der Homomorphismus ist injektiv und da $|G| = [\mathbb{Q}(\zeta) \mid \mathbb{Q}] = \operatorname{grad} \Phi_n = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, ist der Homomorphismus auch surjektiv. □

[8] $\zeta^{a_{\sigma\tau}} = \zeta^{\sigma\tau} = (\zeta^\sigma)^\tau = (\zeta^{a_\sigma})^{a_\tau}$

1.7 Auflösbarkeit durch Radikale

Eine klassische Frage ist die nach der Auflösbarkeit von Polynomen, das heißt die Beschreibung der Nullstellen durch die vier Grundrechenarten und Wurzelziehen, Das kann man körpertheoretisch präzisieren:

Bemerkung. Sei in diesem Kapitel die Charakteristik =0!

Definition. auflösbar durch Radikale:
Sei K ein Körper mit $\mathrm{Char}(K) = 0$. $F|K$ eine Körpererweiterung. Dann heißt F **auflösbar durch Radikale**, wenn es eine Körperkette

$$K =: E_0 \subseteq E_1 \subseteq \ldots \subseteq E_r \supseteq F,$$

sodass jeweils

$$E_i = E_{i-1}(\alpha_i)$$

mit $\alpha_i^{m_i} \in E_{i-1}$ für ein $m_i \in \mathbb{N}$ ($\hat{=}$ Adjunktion einer Wurzel). Das heißt eine Nullstelle α von $f \in K[X]$ lässt sich genau dann über K durch Grundrechenarten und Wurzelziehen ausdrücken, wenn $K(\alpha) \mid K$ auflösbar durch Radikale ist.

Das Hauptergebnis hierbei ist:

Satz 1.11. *Sei $F|K$ endliche Erweiterung in Charakteristik 0, und L eine Galoishülle von $F|K$. Dann ist $F|K$ auflösbar durch Radikale, genau dann, wenn* $\mathrm{Gal}(L|K)$ *auflösbar ist.*

Beweis.

„⇐“ Sei $G = \mathrm{Gal}(L|K)$ auflösbar.

Nach Satz (2.71) (Wintersemester) existiert dann eine Reihe $1 \lhd N_r \lhd \ldots \lhd N_0 = G$ mit N_{i-1}/N_i zyklisch von Primzahlordnung. Sei

$$E_i = \mathrm{Fix}(N_i).$$

Dann ist $E_{i+1}|E_i$ galoisch mit Gruppe N_i/N_{i+1}, also zyklisch. Sei $n := [L : K]$ und ζ eine primitive n-te Einheitswurzel. Die Galoisgruppe $E_{i+1}(\zeta) \mid E_i(\zeta)$ ist (via Einschränkung von Automorphismen) isomorph zu einer Untergruppe von N_i/N_{i+1} (siehe Übung 3). Mit

$$m_i := [E_{i+1}(\zeta) \mid E_i(\zeta)] \;\mid\; [E_{i+1} \mid E_i] \;\mid n$$

enthält $E_i(\zeta)$ insbesondere die m_i-ten Einheitswurzeln. Nach 1.8 ist $E_{i+1}(\zeta)|E_i(\zeta)$ eine Radikalerweiterung, also $F|K$ auflösbar durch Radikale.

„⇒“ Sei $F|K$ auflösbar durch Radikale, E_i wie in der Definition. Sei n das Produkt der m_i (wie in Definition) und ζ eine primitive n-te Einheitswurzel. Setze $F_0 := K$ und $F_i = E_{i-1}(\zeta),\ i \geq 1$. Betrachte die Körperkette $K = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{r+1}$. Sei E eine Galoishülle von $F_{r+1}|K$. Setze $A := \mathrm{Gal}(E|K)$ und $U_i = \mathrm{Gal}(E|F_i)$. Wir wissen: $F_1|F_0 = K(\zeta)|K$ ist galoissch mit abelscher Galoisgruppe A/U_1.
Wir betrachten $F_{i+1}|F_i$ mit $i \geq 1$. Dann ist $F_{i+1} = F_i(\alpha)$, mit $\alpha^{m_i} \in F_i$. Wegen $m_i \mid n$ enthält F_i alle m_i-ten Einheitswurzeln, das heißt F_{i+1} ist Zerfällungskörper von $\underbrace{X^{m_i} - \alpha^{m_i}}_{\text{Nst. sind „}\alpha \cdot m_i\text{-te Einheitswurzel“}}$ über F_i Damit erhalten wir, dass $F_{i+1}|F_i$ galoissch ist.
DIe Elemente von $\mathrm{Gal}(F_{i+1}|F_i)$ bilden α immer auf „$\alpha \cdot m_i$-te Einheitswurzel“ ab, damit sieht man, dass diese Gruppe **abelsch** ist.
Wir wissen aus dem Wintersemester: Ist G/H abelsch , $(H \lhd G)$ dann gilt: $G' \leq H$. Nachdem aber $A/U_1,\ U_1/U_2, \ldots, U_r/U_{r+1}$ jeweils abelsch sind, muss $A^{(r+1)} \leq U_{r+1}$ sein. und $A^{(r+1)} \lhd A$.

In U_{r+1} liegt aber außer $\{1\}$ **kein** Normalteiler N von A denn sonst wäre $\mathrm{Fix}(N)|K$ normal, $F_{r+1} \subset \mathrm{Fix}(N) \neq E$, im Widerspruch dazu, dass E Galoishülle von $F_{r+1}|K$ ist.

$$\Rightarrow A^{(r+1)} = \{1\},$$

also ist A auflösbar,

□

Bemerkung. Für Polynome vom Grad ≤ 4 waren schon seit dem Spätmittelalter Lösungsformeln bekannt. Erst Abel (≈ 1825) konnte zeigen, dass es für Grad 5 i. Allg **keine** Lösungsformel mehr gibt.

Hierzu zwei Hilfslemmata:

Lemma 1.12. *Sei $p \in \mathbb{P}$, $G \leq S_p$ transitiv, G enthält eine Transposition. Dann ist $G = S_p$.*

Beweis. G transitiv $\Rightarrow p \mid |G|$, G enthält also einen p-Zykel und wie angegeben eine Transposition.

$$\Rightarrow G = S_p$$

(siehe Übung 2 Wintersemester) □

Lemma 1.13. *Das irreduzible Polynom $f \in \mathbb{Q}[X]$ habe Grad $p \in \mathbb{P}$ und genau $p-2$ reelle Nullstellen. Dann ist* $\mathrm{Gal}(f|\mathbb{Q}) = S_p$

Beweis. Da f irreduzibel, ist $\mathrm{Gal}(f|\mathbb{Q}) \leq S_p$ transitiv. Komplexe Konjugation ist ein Automorphismus des Zerfällungskörpers der alle reellen Nullstellen fixiert und die beiden anderen vertauscht, also eine Transposition in S_p.

$$\overset{1.12}{\Rightarrow} \mathrm{Gal}(f|\mathbb{Q}) = S_p.$$

□

03.06.09

Bemerkung. $n \geq 5 : S_n' = A_n,\ S_n'' = A_n' = A_n \Rightarrow S_n, A_n$ nicht auflösbar

Beispiel. $f = X^5 - 80X - 2 \in \mathbb{Q}[X]$ ist (nach Eisenstein) irreduzibel. Einfache Kurvendiskussion zeigt, dass f genau drei reelle Nullstellen hat $\Rightarrow \mathrm{Gal}(f|\mathbb{Q}) \cong S_5$

1.8 Zirkel- und Linealkonstruktion regulärer *n*-Ecke

Mit Hilfe der Galoistheorie können wir zeigen, welche regulären n-Ecke mit Zirkel und Lineal konstruierbar sind.

Lemma 1.14. *Sei $2 \leq n \in \mathbb{N}$ und $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist das reguläre n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine 2er Potenz ist.*

Beweis. Aus dem Wintersemester folgt sofort $\Rightarrow$ (also wenn es **keine** Zweierpotenz ist, geht es nicht). Sei also $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Zweierpotenz. Sei $a := \zeta + \frac{1}{\zeta} = 2 \operatorname{Re} \zeta$. $\operatorname{Gal}(\mathbb{Q}(\zeta) \mid \mathbb{Q})$, und damit auch $G := \operatorname{Gal}(\mathbb{Q}(a) \mid \mathbb{Q})$, ist eine abelsche 2 Gruppe. Das heißt, es gibt eine Kette von Gruppen $1 = G_0 < G_1 < \ldots G_r = G$ mit $[G_{i+1}|G_i] = 2$. Die Kette der Fixkörper der G_i besteht dann aus einer Folge quadratischer Körpererweiterungen. Diese entstehen bekanntlich jeweils durch Quadratwurzeladjunktion. Damit ist a konstruierbar, also auch ζ. □

Bemerkung. Wir wissen $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Sei $n = \prod p_i^{e_i}$. Dann ist

$$\varphi(n) = \prod \underbrace{(p_i - 1)p_i^{e_i - 1}}_{=\varphi(p_i^{e_i})}$$

Damit sieht man sofort:

Lemma 1.15. *Das reguläre n-Eck ist genau dann konstruierbar, wenn $n = 2^k \cdot u$, u ein Produkt paarweise verschiedener Primzahlen der Form $2^l + 1$ (genannt: **Fermat-Primzahlen**; damit das prim wird, muss $l = 2^m$ sein).*

1.9 Die Galoisgruppe von $X^n - a$

Sei K ein Körper, dessen Charakteristik $=0$ ist oder n nicht teilt, und $0 \neq a \in K$. Dann ist $f = \underbrace{X^n - a}_{f' = n \cdot X^{n-1} = 0 \Leftrightarrow X = 0}$ separabel. Sei α eine Nullstelle von $X^n - a$, ζ eine primitive n-te Einheitswurzel. Dann sind die Nullstellen von $X^n - a$ gerade die $\alpha \cdot \zeta^i$, $i = 0, \ldots, n-1$. Das heißt $L = K(\zeta, a)$ ist Zerfällungskörper von $X^n - a$, also $\operatorname{Gal}(L|K)$ die Galoisgruppe dieses Polynoms. Wie sieht diese Galoisgruppe aus?

$$\begin{array}{ccc} K(\zeta, \alpha) & & 1 \\ | & & | \\ K(\zeta) & & N \quad = \operatorname{Gal}(L|K(\zeta)) \\ | & & | \\ K & & G \quad = \operatorname{Gal}(L|K) \end{array}$$

$K(\zeta)|K$ ist normal also $N \lhd G$, und $G/N = \operatorname{Gal}(K(\zeta|K))$ (wobie $\operatorname{Gal}(K(\zeta)|K)$ immer eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$)

Lemma 1.16. *Sei α eine Nullstelle von $X^n - a \in E[X]$ mit $\operatorname{Char}(E) \nmid n$. E enthalten die n-ten Einheitswurzeln. Dann ist $E(\alpha)|E$ galoissch mit $\operatorname{Gal}(E(\alpha)|E) \leq C_n$ (insbesondere zyklisch).*

Beweis.

$$\sigma \in G = \mathrm{Gal}(E(\alpha)|E)$$

bildet α auf $\alpha \cdot \zeta_n^{k_\sigma}$ ab (und ist damit eindeutig festgelegt). Sei σ so, dass $k_\sigma \in \mathbb{N}$ minimal ist. Sei $\tau \in G$,

$$\tau : \alpha \mapsto \alpha \cdot \zeta_n^{k_\tau} \overset{DivisionmitRest}{=} \alpha \cdot \zeta_n^{m \cdot k_\sigma + r}, \qquad 0 \leq r < k_\sigma$$

Damit gilt:

$$\begin{aligned} \tau\sigma^{-m}(\alpha) &= \tau\left(\alpha \cdot \zeta_n^{-m \cdot k_\sigma}\right) = \alpha\zeta_n^{m \cdot k_\sigma + r} \cdot \zeta_n^{-m \cdot k_\sigma} \\ &= \alpha \cdot \zeta_n^r \end{aligned}$$

Damit erhalten wir $r = 0$, da k_r minimal war, das heißt: $\tau = \sigma^m$

$$\Rightarrow \mathrm{Gal}(E(\alpha)|E) = < \sigma >$$

und

$$\begin{aligned} \sigma^n(\alpha) &= \alpha \cdot \zeta^{n \cdot k_\sigma} = \alpha \\ \Rightarrow \sigma^n &= \mathrm{id} \end{aligned}$$

damit folgt: $\mathrm{ord}(\sigma)$ teilt n! □

Lemma 1.17. *$char(K)$ teile nicht n, und sei $f = X^n - a \in K[X]$, $a \neq 0$. Daraus folgt, $\mathrm{Gal}(f|K)$ ist **isomorph** zu einer Untergruppe der affinen linearen Gruppe*

$$AGL_1(\mathbb{Z}/n\mathbb{Z}) := \left\{ g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto cx + b \mid c \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\} \tag{1.10}$$

(Anm: $|AGL_1(\mathbb{Z}/n\mathbb{Z})| = n\varphi(n)$)

Beweis. Sei $\sigma \in \mathrm{Gal}(f|K)$, α eine Nullstelle von f, ζ eine primitive n-te Einheitswurzel.

$$\begin{aligned} \sigma : \alpha &\mapsto \zeta^b \alpha, \\ \zeta &\mapsto \zeta^c \end{aligned}$$

für ein $b \in \mathbb{Z}/n\mathbb{Z}$, $c \in (\mathbb{Z}/n\mathbb{Z})^\times$. Betrachte die Abbildung:

$$G \mapsto AGL_1(\mathbb{Z}/n\mathbb{Z}) \qquad \sigma \mapsto (x \mapsto cx + b)$$

Das ist ein Homomorphismus, denn: Sei $\tau \in G$:

$$\begin{aligned} \alpha \mapsto \zeta^{b'}\alpha, \qquad \zeta \mapsto \zeta^{c'} \\ \Rightarrow \sigma\tau(\alpha) = \sigma(\zeta^{b'}\alpha) = \sigma(\zeta^{b'}) \cdot \sigma(\alpha) \\ = \zeta^{b' \cdot c} \cdot \zeta^b \cdot \alpha = \zeta^{b + b'c} \cdot \alpha. \end{aligned}$$

und:

$$\sigma\tau(\zeta) = \zeta^{cc'}.$$

Das heißt

$$\sigma\tau \mapsto (x \mapsto cc'x + b + b'c) = (x \mapsto c\overbrace{(c'x + b')}^{\varphi(\tau)(x)} + b) = (x \mapsto \varphi(\sigma)\varphi(\tau)(x))$$

φ ist auch injektiv, denn $\varphi(\sigma) = \mathrm{id} \Rightarrow c = 1,\ b = 0$. Damit also schließlich $\sigma = \mathrm{id}$. □

Im Allgemeinen ist $X^n - a$ **nicht** irreduzibel. In bestimmten Fällen kann man aber einfach entscheiden, ob irreduzibel, zum Beispiel für $n = p \in \mathbb{P}$:

Lemma 1.18. *K wie in 1.17, $p \in \mathbb{P}$, $a \in K\backslash\{0\}$. Dann ist $f = X^p - a$ entweder irreduzibel über K, oder hat eine Nullstelle in K.*

Beweis. Sei f reduzibel, α eine Nullstelle mit $[K(\alpha) : K] = d < p$, Wegen der Separabilität von f gibt es genau d K-Homomorphismen $K(\alpha) \to \bar{K}$

$$\Rightarrow N_K^{K(\alpha)}(\alpha) = \alpha^d \cdot \zeta_p^k$$

ζ_p ist eine primitive p-te Einheitswurzel , $k \in \mathbb{N}$

$$\Rightarrow N(\alpha)^p = \alpha^{dp} = a^d$$

Wegen $\mathrm{ggT}(d, p) = 1$ existiert $u, v \in \mathbb{Z}$: $du + pv = 1$

$$\Rightarrow a = a^{du+pv} = N(\alpha)^{up} \cdot a^{vp} = (\underbrace{N(\alpha)^u \cdot a^v}_{\in K})^p$$

Es gibt also in K eine p-te Wurzel aus a, das heißt eine Nullstelle von $X^p - a$. □

Bemerkung. In Anwendungen stößt man oft auf die Frage, wie sich Kreisteilungspolynome modulo einer Primzahl p zerlegen. Da Φ_n ganzzahliges Polynom ist, können wir es mod p betrachten (das heißt über einem Körper der Charakteristik p).

Satz 1.19. *Sei K endlicher Körper, $\mathrm{Char}(K) \not| n$. Dann ist jede Nullstelle von $\Phi_n(X)$ in einem Erweiterungskörper von K eine **primitive** n-te Einheitswurzel. Sei $r \in \mathbb{N}$ minimal, sodass n ein Teiler von $|K|^r - 1$. Dann zerfällt Φ_n über K in irreduzible Faktoren vom Grad r.*

Beweis. Wegen $X^n - 1 = \prod_{d|n} \Phi_d(X)$ kann eine Nullstelle ζ von Φ_n über K nicht gleichzeitig Nullstelle eines Φ_d, $d < n$ sein, also insbesondere keine Nullstelle von $X^d - 1$. Also ist ζ eine **primitive** n-te Einheitswurzel.

10.06.09

Sei f irreduzibler Faktor von Φ_n über K, grad $f =: r$, $q = |K|$, sei α eine Nullstelle von f. Dann ist $K(\alpha)$ ein Körper der Mächtigkeit q^r, und somit $n|q^r - 1$. Umgekehrt sei nun s minimal, so dass n ein Teiler von $q^s - 1$ ist, und $E|K$ eine Erweiterung vom Grad s. Da die multiplikative Gruppe $E^\times$ zyklisch von Ordnung $q^s - 1$ ist, enthält sie eine (und damit auch **alle**) primitiven n-ten Einheitswurzeln. Insbesondere zerfällt f über E in Linearfaktoren, das heißt $K(\alpha) \subset E$, also $r \leq s$. Mit $r \geq s$ (s.o.) folgt die Behauptung. □

1.10 Symmetrische Polynome und die allgemeine Gleichung *n*-ten Grades

Definition. allg. Gleichung n-ten Grades:
Seien $u_1, \ldots, u_n$ Unbestimmte über dem Körper K , dann heißt

$$f(z) := z^n - u_1 z^{n-1} + u_2 z^{n-2} - + \ldots + (-1)^n u_n, \qquad f \in K(u_1, \ldots, u_n)[z] \tag{1.11}$$
$$f(z) = 0 \tag{1.12}$$

Dann ist (1.12) die **allgemeine Gleichung n-ten Grades**

Seien $v_1, \ldots, v_n$ Nullstellen von f, dann ist

$$\begin{aligned} u_1 &= v_1 + \ldots + v_n \\ u_2 &= v_1 v_2 + v_1 v_3 + \ldots v_{n-1} v_n \\ \vdots &= \cdots \\ u_n &= v_1 \cdot \ldots \cdot v_n \end{aligned}$$

Betrachte weiter die Gleichung (mit Unbestimmten x_i):

$$0 = (z - x_1) \cdot \ldots \cdot (z - x_n) =: z^n - \sigma_1 z^{n-1} + - \ldots + (-1)^n \sigma_n$$

Definition. elementarsymmetrische Funktionen und **symmetrische Polynome**:
Die **elementarsymmetrische Funktion**en in $x_1, \ldots, x_n$ sind genau die σ_i wie oben

$$\begin{aligned} \sigma_1 &= x_1 + \ldots + x_n \\ \vdots &= \cdots \\ \sigma_n &= x_1 \cdot \ldots \cdot x_n \end{aligned}$$

Ein **symmetrisches Polynom** in $x_1, \ldots, x_n$ ist eines, das unter **allen Permutationen** der x_i **invariant** bleibt.

(1.13) ist separabel, da

$$\mathrm{Gal}(K(x_1, \ldots, x_n) \mid K(\sigma_1, \ldots, \sigma_n)) = S_n,$$

denn jede Permutation der x_i bewirkt einen Automorphismus von $K(x_1, \ldots, x_n)$ und lässt $K(\sigma_1, \ldots, \sigma_n)$ elementenweise fest. Per Definition liegt jedes symmetrische Polynom in

$$\mathrm{Fix}(\mathrm{Gal}(K(x_1, \ldots, x_n) \mid K(\sigma_1, \ldots, \sigma_n))) = K(\sigma_1, \ldots, \sigma_n),$$

ist also als rationale Funktion in den σ_i's darstellbar.

Mann kann leicht zeigen, dass jedes $\underbrace{\text{symmetrische Polynom}}_{=:f(x_1,\ldots,x_n)}$ sogar als $\underbrace{\textbf{Polynom} \text{ in den } \sigma_i\text{'s}}_{\to h(\sigma_1,\ldots,\sigma_n)}$ (und nicht nur als rationale Funktion) darstellbar ist. Diese Darstellung ist sogar **eindeutig**, denn

Sei $f(\sigma_1, \ldots, \sigma_n) = g(\sigma_1, \ldots, \sigma_n)$, das heißt: $\underbrace{(f-g)}_{=:h}(\sigma_1, \ldots, \sigma_n) = 0$ dann insbesondere (durch Einsetzen $x_i \mapsto v_i$)

$$0 = h(v_1 + \ldots + v_n, \ldots, v_1 \cdot \ldots \cdot v_n) = h(u_1, \ldots, u_n)$$
$$\Rightarrow h = 0.$$

Aus der Eindeutigkeit folgt, dass

$$\tau : K[u_1, \ldots, u_n] \to K[\sigma_1, \ldots, \sigma_n]$$
$$f(u_1, \ldots, u_n) \mapsto f(\sigma_1, \ldots, \sigma_n)$$

nicht nur ein **Epi**morphismus, sondern sogar ein **Iso**morphismus ist. Also ist τ erweiterbar zu einen Isomorphismus der **Quotientenkörper** $K(u_1, \ldots, u_n)$, $K(\sigma_1, \ldots, \sigma_n)$, also fortsetzbar zu einem Isomorphismus der Zerfällungskörper $K(v_1, \ldots, v_n)$ (von f) und $K(x_1, \ldots, x_n)$ (von f^τ).
Hierbei ist $v_i \mapsto x_k$, und ohne Einschränkung $v_i \mapsto x_i$ da Permutation der x_i ein $K(\sigma_1, \ldots, \sigma_n)$-Automorphismus von $K(x_1, \ldots, x_n)$ ist.

Dies beweist schon das nachfolgende Korollar:

Korollar 1.20. $\approx$ABEL*:*
Die allgemeine Gleichung n-ten Grades ist separabel mit Galoisgruppe

$$\mathrm{Gal}(K(v_1, \ldots, v_n) \mid K(u_1, \ldots, u_n)) = S_n \tag{1.13}$$

Korollar. $\hat{=}$ABEL*:*
Insbesondere ist die allgemeine Gleichung n-ten Grades für $n \geq 5$ ***nicht auflösbar*** *durch Radikale.*

1.11 Diskriminanten

Für Unbestimmte $z, x_1, \ldots, x_n$ über einem Körper K betrachte

$$f := (z - x_1) \cdot \ldots \cdot (z - x_n) \in K(x_1, \ldots x_n)[z]$$

Das Element

$$D := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

ist **symmetrisches Polynom** in den x_i das heißt als Polynom in den elementarsymmetrischen Funktionen $\sigma_1, \ldots, \sigma_n$ darstellbar.
Setzt man für x_i die Nullstellen α_i eines Grad n-Polynoms $g \in K[z]$ Polynoms ein, dann erhält man Satz 1.21

Satz 1.21. *Sei $n \in \mathbb{N}$ und K ein Körper. Dann existiert ein Polynom $D(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, so dass für*

$$f = X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n \in K[X]$$

gilt:

$$D(f) := D(a_1, \ldots, a_n) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

wobei die α_i die Nullstellen von f sind.

Beweis. $\prod_{i<j}(\alpha_i - \alpha_j)^2$ ist nach obigen darstellbar als polynomialer Ausdruck der elem.-symm. Ausdrücke in den α_i's. Letztere sind bis auf Vorzeichen die Koeffizienten von f. □

Definition. Das Polynom $D(x_1, \ldots, x_n)$ heißt auch **Diskriminantenpolynom**, und $D(f)$ heißt **Diskriminante von** f.

Beispiel. für Diskriminanten:

$$\begin{aligned} f(x) &= x^2 + bx + c \\ \Rightarrow a_{1/2} &= \frac{-b \pm \sqrt{b^2 - 4c}}{2} \\ \Rightarrow D(f) &= b^2 - 4c \end{aligned}$$

Beispiel.

$$f(X) = X^3 + pX + q.$$

Dann ist

$$D(f) \overset{\text{Übg } 4}{=} -4p^3 - 27q^2$$

Bemerkung. Offensichtlich erhalten wir $D(f) \neq 0 \Leftrightarrow f$ separabel!

Eine weitere Anwendung ist:

Satz 1.22. *Sei $f \in K[X]$ separabel vom Grad n und* $\operatorname{Char} K \neq 2$. *Dann gilt:*

$$\operatorname{Gal}(f|K) \le A_n \Leftrightarrow D(f) \text{ Quadrat in } K. \tag{1.14}$$

Beweis. Betrachte

$$\begin{aligned} \Delta &:= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \\ \Rightarrow \Delta^2 &= D(f) \end{aligned}$$

Es genügt zu zeigen, dass eine Transposition $\tau \in S_n$ das Vorzeichen von Δ ändert. Das heißt genau dann wird Δ von $\operatorname{Gal}(f|K)$ fixiert ($\Leftrightarrow \Delta \in K$), wenn hier nur gerade Permutationen vorliegen □

1.12 Bestimmung beliebiger Galoisgruppen und Reduktion modulo *p*

Wir wollen eine Methode finden, mit der man Galoisgruppen beliebiger Polynome explizit ausrechnen kann[9].
Sei $f \in K[X]$ seperabel und mit Nullstellen in $\alpha_1, \ldots, \alpha_n$. $L := K(\alpha_1, \ldots, \alpha_n)$. $u_1, \ldots, u_n$ seien Unbestimmte über K. Schreibe $u := (u_1, \ldots, u_n)$. Setze

$$\vartheta := \alpha_1 u_1 + \ldots + \alpha_n u_n,$$

und

$$F(z, u) := \prod_{\sigma \in S_n} (z - \vartheta^\sigma),$$

wobei

$$\vartheta^\sigma := \alpha_{\sigma(1)} u_1 + \ldots + \alpha_{\sigma(n)} u_n;$$

σ permutiert also in diesem Ausdruck die α_i's. $L(u)[z] \ni F$ ist symmetrisch in den α_i's, woraus $f \in K(u)[z]$ folgt. Zerlege F über $K(u)$ irreduzibel:

$$F(z, u) = F_1(z, u) \cdot \ldots \cdot F_r(z, u).$$

ohne Einschränkung sei $(z - \vartheta)$ Faktor von F_1. Setze

$$G := \mathrm{Stab}(F_1) \leq S_n.$$

(S_n operiert ja auf den Linearfaktoren von F).

Behauptung:

$$G = \mathrm{Gal}(f|K)$$

17.06.09

Beweis. Wir zeigen zuerst $\mathrm{Gal}(f|K) \overset{(*)}{=} \mathrm{Gal}(F_1|K(u))$ ($(*)$ Hier ist Gleichheit als Untergruppen der S_n gemeint). Jeder K-Homomorphismus von L lässt sich erweitern zu einem $K(u)$ Homomorphismus von $L(u)$, und dann wieder einschränken auf zu einem $K(u)$ Homomorphismus des Zerfällungskörpers von F_1. Umgekerht lässt sich jeder $K(u)$-Homomorphismus des Zerfällungskörpers von F_1 über $K(u)$ erweitern auf $L(u)$ und dann auf L einschränken. Diese Entsprechungen sind **bijektiv**, denn

[9] Dies ist eher eine theoretische Methode und ist bei der konkreten Berechnung im Staatsexamen nicht sonderlich hilfreich!

genauso, wie $\sigma \in \mathrm{Gal}(f|K)$ auf α_i's operiert, so permutiert der entsprechende Homomorphismus vom Zerfällungskörper $(F_1|K(u))$ die Indizes der α_i im Ausdruck ϑ. Also haben wir gezeigt, dass

$$\mathrm{Gal}(f|K) \overset{(*)}{=} \mathrm{Gal}(F_1|K(u))$$

(gleich als Untergruppen der S_n). Zu jedem Linearfaktor $z - \vartheta^\sigma$ von F_1 gibt es ein Element von $\mathrm{Gal}(F_1|K(u))$, das $z-\vartheta$ auf diesen abbildet, und zwar **genau** eines, da die Elemente von $\mathrm{Gal}(F_1|K(u))$ (als Elemente der S_n gesehen) durch ihre Wirkung auf ϑ schon festgelegt sind!

$$\Rightarrow \mathrm{Gal}(F_1|K(u)) = \{\sigma \in S_n \mid z - \vartheta^\sigma \text{ ist wieder Linearfaktor von } F_1\} \supseteq \mathrm{Stab}(F_1)$$

Da andererseits alle diese $K(u)$-Automorphismen F_1 fixieren, folgt die umgekehrte Inklusion. Damit folgt die Behauptung. □

Bemerkung. Tatsächlich ist sogar $Gal(f|K) = \mathrm{Stab}(F_i)$ für jeden beliebigen Faktor F_i von F, denn besondere Eigenschaften des Linearfaktors $(z-\vartheta)$ von F_1 haben wir gar nicht benutzt!

Bemerkung. Theoretisch kann man damit beliebige endliche Galoisgruppen bestimmen, indem man F faktorisiert. Praktisch nicht, denn $\mathrm{grad}(F) = n!$, und das ist unangenehm tatsächlich zu berechnen.

Bemerkung. Trotzdem können wir aus obigen Argument ein Argument ableiten, mit dem man oft sehen kann, dass eine Galoisgruppe **mindestens** eine gewisse Größe hat.

Satz 1.23. ***Satz von Dedekind:***
Sei R ein faktorieller Ring, $K = \mathrm{Quot}(R)$, P ein Primideal von R, $\bar{K} := \mathrm{Quot}(\underbrace{R/P}_{=:\bar{R}})$.
Falls $f \in K[X]$ normiert, sodass $\bar{f} \in \bar{R}[X]$ separabel, dann ist f separabel, und

$$\mathrm{Gal}(\bar{f}|\bar{K}) \leq \mathrm{Gal}(f|K) \tag{1.15}$$

Beweis. $\bar{f}$ separabel, das heißt $\underbrace{D(\bar{f})}_{=\overline{D(f)}} \neq 0$, das heißt $D(f) \notin P$, also insbesondere $D(f) \neq 0$, das heißt, f ist also separabel.
Wir betrachten das zu f gehörige Polynom F (wie vorher). Da F Polynom in den Koeffizienten[10] von f über $R(u)$ ist, und das zu $\bar{f}$ gehörige Polynom das selbe Polynom in den Koeffizienten von $\bar{f}$ ist, gilt:
Das zu $\bar{f}$ gehörige Polynom ist gleich $\bar{F}$. Sei

$$F = F_1 \cdot \ldots \cdot F_r,$$

mit F_i wie oben definiert. Da R faktoriell ist, kann diese Zerlegung über R angenommen werden (siehe auch Gauss-Lemma im Wintersemester)

$$\Rightarrow \bar{F} = \bar{F}_1 \cdot \ldots \cdot \bar{F}_r,$$

[10] $\hat{=}$ elementarsymmetrischen Funktionen der α_i

$\bar{\sigma} \in \mathrm{Gal}(\bar{f}|\bar{K})$führt nach obigem Argument einen - und nach der ersten Bemerkung oben sogar *alle* - irreduziblen Faktoren von $\bar{F}_1$ in sich über, also insbesondere $\bar{\sigma}(\bar{F}_1) = \bar{F}_1$. $\bar{\sigma}$ operiert auch auf den F_i (man permutiere einfach statt den Nullstellen von $\bar{f}$ die Nullstellen von f in gleicher Weise).

Wäre nun $\bar{\sigma}(F_1) \neq F_1$, dann hätten zwei verschiedene F_i die gleiche Reduktion mod P. Insbesondere wäre damit $\bar{F}$ inseparabel.

D.h. insbesondere hat $\bar{F}$ zwei gleiche Nullstellen

$$v_{1^\sigma} u_1 + ... + v_{n^\sigma} u_n \overset{!}{=} v_{1^\tau} u_1 + ... + v_{n^\tau} u_n, \ \sigma \neq \tau \in S_n$$

(seien hierbei $v_1, ..., v_n$ die Nullstellen von $\bar{f}$).
Da die u_i Transzendente sind, ist das nur möglich wenn mindestens zwei Nullstellen v_i, v_j von $\bar{f}$ gleich sind, was im Widerspruch zur Separabilität von $\bar{f}$ steht.
Es folgt also insgesamt:

$$\Rightarrow \bar{\sigma} \in \mathrm{Stab}(F_1) = \mathrm{Gal}(f|K)$$

□

Korollar 1.24. *Sei $f \in \mathbb{Z}[X]$ normiert und $\bar{f} \in \underbrace{\mathbb{F}_p}_{=\mathbb{Z}/p\mathbb{Z}}[X]$ sei separabel für ein $p \in \mathbb{P}$. Sei $\bar{f}$ über $\mathbb{F}_p$ in irreduzible Faktoren der Grade $(j_1, \ldots, j_r)$ zerlegt.*
Dann enthält $\mathrm{Gal}(f|\mathbb{Q})$ ein Element vom Zykeltyp $(j_1, \ldots, j_r)$

Beweis. $\mathrm{Gal}(\bar{f}|\mathbb{F}_p)$ ist zyklisch und ein Erzeuger operiert auf den Nullstellen von $\bar{f}$ als $(j_1, \ldots, j_r)$-Zykel. Nach 1.23 ist dieses Element dann auch ein Element von $\mathrm{Gal}(f|\mathbb{Q})$. □

Bemerkung. Indem man ein Polynom modulo verschiedener geeigneter Primzahlen reduziert, kann man dann zum Beispiel manchmal genügend Zykel in $\mathrm{Gal}(f|\mathbb{Q})$ finden, um S_n zu erzeugen. Allgemein kann man aber nur herausfinden, dass $\mathrm{Gal}(f|\mathbb{Q})$ **oberhalb** einer bestimmten Gruppe liegt. Es gibt auch Kriterien, mit denen man allgemein feststellen kann, dass sie **höchstens** eine bestimmte Größe hat.

In unseren „elementaren“ Fällen kann man zum Beispiel oft den Körpergrad des Zerfällungskörpers einfach sehen. Weiter konnten wir mit dem Diskriminanen-Argument immer überprüfen, ob $\mathrm{Gal}(f|\mathbb{Q}) \leq A_n$ ist. Bessere Abschätzungen erhält man beispielsweise durch sog. **Resolventenpolynome**.

Spezialfall: kubische Resolvente für Grad 4, siehe Übung. Für f vom Grad 4, und r die **kubische Resolvente** von f gilt:

$$\begin{array}{ll} \mathrm{Zerf}(f) & \\ \quad | & \leq C_2 \times C_2 \\ \mathrm{Zerf}(r) & \\ \quad | & \quad ?? \\ \quad \mathbb{Q} & \end{array}$$

Die Nullstellen von r sind per Definition $\vartheta_1 := (\alpha_1 + \alpha_2) \cdot (\alpha_3 + \alpha_4)$, $\vartheta_2 := (\alpha_1 + \alpha_3) \cdot (\alpha_2 + \alpha_4)$ und $\vartheta_3 := (\alpha_1 + \alpha_4) \cdot (\alpha_3 + \alpha_2)$, wobei α_i die Nullstellen von f sind. Damit sieht man, dass nur Permutationen aus $V_4 := \{id, (12)(34), (13)(24), (14)(23)\} (\cong C_2 \times C_2)$ alle Nullstellen von r fest lassen.

Es folgt:[11]
Ist $f \in \mathbb{Q}[X]$ irreduzibel vom Grad 4, r die kubische Resolvente von f, dann ist $Gal(f|\mathbb{Q}) =$

- S_4, falls $Gal(r|\mathbb{Q}) = S_3$.
- A_4, falls $Gal(r|\mathbb{Q}) = C_3$.
- D_4 oder C_4, falls $Gal(r|\mathbb{Q}) = C_2$ (d.h. r zerfällt in Grad 1 und Grad 2 über $\mathbb{Q}$).
- V_4, falls $Gal(r|\mathbb{Q}) = \{1\}$.

=

[11] Details als Übung.

2 Auflösbare und nichtauflösbare Gruppentheorie

24.06.09

2.1 Gruppen kleiner Ordnung

Bei der Betrachtung von Gruppen kleiner Ordnung kann man sich zum Beispiel folgende Fragen stellen:

- Welche Isomorphietypen gibt es zu einer gegeben Ordnung?
- Sind alle Gruppen einer Gegebenen Ordnung auflösbar?

Wiederholung. Wiederholung Auflösbarkeit:
G heißt auflösbar:$\Leftrightarrow$ für ein $n \in \mathbb{N}$ $G^{(n)} = \{1\}$, wobei

$$\begin{aligned} G' &= \langle \{[a,b] \mid a,b \in G\} \rangle, \\ [a,b] &:= a^{-1}b^{-1}ab \\ G^{(k)} &:= (G^{(k-1)})' \end{aligned}$$

- Äquivalent dazu ist: G ist auflösbar :$\Leftrightarrow$ Es gibt eine Reihe $1 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$ und G_{i+1}/G_i sind jeweils zyklisch.
- G ist auflösbar, falls ein Normalteiler N existiert, sodass N und G/N auflösbar sind

Um Isomorphietypen zu bestimmen, braucht man oft den Begriff des semidirekten Produktes:

Wiederholung. Für Gruppen N, U mit einem Homomorphismus $\varphi : U \to \mathrm{Aut}(N)$ ist das (äußere) semidirekte Produkt $U \ltimes_\varphi N$ definiert als Menge $U \times N$ zusammen mit der Gruppenoperation

$$(u_1, n_1) \cdot (u_2, n_2) := (u_1 u_2, n_1^{\varphi(u_2)} \cdot n_2)$$

Falls in einer gegebenen Gruppe G ein Normalteiler N und eine Untergruppe U mit $U \cap N = \{1\}$ liegen, dann bilden diese auch ihr semidirektes Produkt (der jeweilige Automorphismus $\varphi(u_2)$ ist dabei Konjugation mit u_2).
Achtung:

- Ohne Angaben des Homomorphismus φ ist noch kein Isomorphietyp festgelegt.

- unter Umständen können verschiedene Homomorphismen φ_1, φ_2 zum selben Isomorphietyp führen.

Anmerkung: $\varphi : U \to \{1\}$ bildet das direkte Produkt $U \times N$.

Für zwei einfache Fälle geben wir die Automorphismengruppe $\mathrm{Aut}(N)$ an.

Satz 2.1.

$$\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times \tag{2.1}$$

Beweis. Sei x ein Erzeuger von C_n. Dann sind die übrigen Erzeuger gerade die x^k, wobei k teilerfremd zu n ist. Die Automorphismen von C_n sind eindeutig durch ihre Wirkung auf x bestimmt, und es gibt genau die Möglichkeitente $\sigma : x \mapsto x^k$, k teilerfremd zu n.
Die Abbildung $\mathrm{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma \mapsto k + n\mathbb{Z}$ ist dann ein Isomorphismus. □

Bemerkung. Es ist klar, dass $|\mathbb{Z}/n\mathbb{Z}| = \varphi(n)$. Die Gruppenstruktur von $\mathbb{Z}/n\mathbb{Z}$ ist damit noch nicht klar, aber zum Beispiel wissen wir $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$.

Schon aus der Linearen Algebra weiß man außerdem:

Satz 2.2. *Für* $G = \underbrace{C_p \times \ldots \times C_p}_{n \text{ mal}}$, $p \in \mathbb{P}$ *ist* $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$

Beweis. G ist als additive Gruppe isomorph zu einem n-dimensionalen $\mathbb{F}_p$-Vektorraum. □

Nun wollen wir Gruppenordnungen mit einer kleinen Anzahl von Primfaktoren betrachten:

Ist $p \in \mathbb{P}$, dann ist jede Gruppe der Ordnung p isomorph zu C_p. Wir wissen auch schon, dass es zur Ordnung p^2 nur die beiden abelschen Gruppen C_{p^2}, $C_p \times C_p$ gibt. Bei etwas komplizierteren Gruppenordnungen kann man oft noch zeigen, dass zum Beispiel eine p-Sylowgruppe normal sein muss (manchmal direkt mit Sylowsätzen, $n_p \equiv 1 \mod p$ und $n_p \left| \frac{|G|}{p^k} \right.$, manchmal mit Abzählargumenten, das heißt, lauter nicht-normale Sylowgruppen führen unter Umständen zu mehr Elementen, als die Gruppe hat).
Außerdem kann man manchmal nicht-triviale Normalteiler finden, in dem man kleine Permutationsoperationen von G betrachtet (zum Beispiel auf den Nebenklassen einer großen Untergruppe); aus Ordnungs- oder Teilbarkeitsgründen kann der zugehörige Homomorphismus $G \to \mathrm{Sym}(n)$ oft nicht injektiv sein, also existiert ein nicht-trivialer Kern.
Normale p-Sylowgruppen sind auch nützlich, da man dann immer automatisch ein semidirektes Produkt $G = P \rtimes U$ erhält. Das folgt aus dem (nicht einfach zu beweisenden) **Satz von Schur-Zassenhaus**[1]. In den von uns betrachteten Fällen folgt die semidirekte Produkteigenschaft aber auch immer einfacher.

Warnung. Sylow-Argumente helfen natürlich nicht weiter bei der Betrachtung von p-Gruppen.

[1] Sei $N \lhd G$, $\mathrm{ggT}(|N|, |G/N|) = 1$. Dann ist G ein semidirektes Produkt $N \rtimes U$.

2.1.1 $|G| = pq,\ p < q$ Primzahlen

Seien $P; Q$ eine p-bzw. eine q-Sylowgruppe von G_j n_p, n_q die Anzahl der p-bzw. q-Sylowgruppen. Dann ist $n_q \equiv 1 \mod q$ und $n_q | p < q \Rightarrow n_q = 1$, also ist Q normal in G und

$$\begin{aligned} P \cap Q &= \{1\}, \\ |PQ| &= \frac{|P| \cdot |Q|}{|P \cap Q|} = pq = |G| \end{aligned}$$

Also ist

$$G = P \ltimes Q.$$

Falls dieses Produkt **nicht** direkt ist, dann gilt:

$$P \hookrightarrow \mathrm{Aut}(Q) \cong C_{q-1},$$

das heißt insbesondere $p | q-1$. In letzterem Fall gibt es dann (genau) einen nicht-abelschen Isomorphietyp, ansonsten gibt es nur die zyklische Gruppe C_{pq}. (Insbesondere sind die Gruppen der Ordnung pq auflösbar).

2.1.2 $|G| \leq 15$

- Ordnung 1, Primzahlordnungen und Primzahlquadratordnungen sind klar.
  - $|G| = 2 \cdot 3 \overset{\text{Kapitel 2.1.1}}{\Longrightarrow}$ Es gibt genau die Isomorphietypen $C_6 = C_2 \times C_3$ und $S_3 (= C_3 \rtimes C_2)$
  - $|G| = 2 \cdot 5 \overset{\text{Kapitel 2.1.1}}{\Longrightarrow}$ Es gibt genau die Isomorphietypen $C_{10} = C_2 \times C_5$ und D_5 (wobei D die **Diedergruppe** ist).
  - Analog für $|G| = 2 \cdot 7$.

    allgemein sieht man $|G| = 2p$, p ungerade $\Rightarrow G = C_{2p}$ oder $G = D_p$.
  - $|G| = 3 \cdot 5 \overset{\text{Kapitel 2.1.1}}{\Longrightarrow} G \cong C_{15}$
  - $|G| = 8$ Wir kennen die (paarweise nicht-isomorphen) Gruppen $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4$ und die Quaternionengruppe. Wir wollen zeigen, dass das schon alle sind.

    Beweis. Sei $|G| = 8$, G nicht abelsch. $\Rightarrow$ Es existiert ein Element der Ordnung 4 und keines der Ordnung 8.

    1. Fall: G hat eine nicht-normale Untergruppe U der Ordnung 2.

    G operiert transitiv auf $U \backslash G$, und sogar treu, denn der Kern ist $\bigcap_{g \in G} U^g = \{1\}$, das heißt $G \hookrightarrow \mathrm{Sym}(|U \backslash G|) = S_4$, also ist G eine 2-Sylowgruppe von S_4, das heißt $G \cong D_4$.

2. Fall: Alle Untergruppen der Ordnung 2 sind normal

Dann gibt es genau eine solche Untergruppe, denn ein Normalteiler der Ordnung 2 liegt automatisch im Zentrum; wären also A, B zwei verschiedene solche Untergruppen, dann wäre $|Z(G)| \geq | < A, B > | = 4$, also G abelsch.
Sei z nun ein Erzeuger der Untergruppe der Ordnung 2. Da $< z >$ normal, ist $z^g = z$ für alle $g \in G$, das heißt $z \in Z(G)$. Sei i ein Element der Ordnung 4 $\Rightarrow i^2 = z$.
Da $< i > \neq G$, muss es ein Element $j \notin < i >$ mit der Ordnung 4 geben. $\Rightarrow j^2 = z$ und $G =< i, j > G$ ist nicht abelsch , also $i^j \neq i$. Andererseits ist $< i > \lhd G$ (Index=2!!)
$\Rightarrow i^j = i^3 = i^2 i = zi$.
Diese Beschreibung charakterisiert genau die **Quaternionengruppe** (setze $-1 := z$, und siehe Wintersemester Übung 1 und 2).

□

– $|G| = 12$: Wir wollen zeigen, dass es genau 5 Isomorphietypen gibt. nämlich:

$$C_{12}, C_6 \times C_2, D_6 (= C_3 \rtimes (C_2 \times C_2)), A_4 (= (C_2 \times C_2) \rtimes C_3)$$

und eine weitere Gruppe der Form $C_3 \rtimes C_4$.

01.07.09

Gruppen der Ordnung 12

- Ist die 3-Sylowgruppe noraml, dann ist $n_3 = 4$
  - $4 \cdot \varphi(3) = 8$ Elemente der Ordnung 3.
  - nur noch Platz für einen 2-Sylowgruppe. Die ist dann normal

  Weiter operiert G transitiv auf den vier 3-Sylowgruppen, und auch treu, denn der Kern ist der Schnitt des **Normalisator** der 3-Slyowgruppe[2], also $= \{1\}$. Das heißt

$$G \hookrightarrow S_4 \qquad \Rightarrow G \cong A_4$$

- Sei nun die 3-Sylowgruppe normal, das heißt

$$G = C_3 \rtimes_\varphi (C_2 \times C_2)$$

  oder

$$= C_3 \rtimes_\varphi C_4.$$

[2] einer gleich der 3-Sylowgruppe

– Möglichkeiten;

$$\begin{aligned} \varphi:\ C_2 \times C_2 \to \{1\} \qquad &\Rightarrow G = C_6 \times V_2 \\ \varphi:\ C_2 \times C_2 \to C_2 \qquad &\Rightarrow G = D_6 \end{aligned}$$

oder falls $C_3 \rtimes_\varphi C_4$:

$$\begin{aligned} \varphi:\ V_4 \to \{1\} \qquad & G = C_{12} \\ \varphi:\ C_4 \to C_2 \qquad & G \text{ siehe Übungsblatt 8} \end{aligned}$$

2.1.3 $|G| = pqr, p < q < r$ Primzahlen

Seien P, Q, R Sylowgruppen, n_q, n_q, n_r die Anzahlen. Wir wollen zeigen, dass eine der Sylowgruppen normal ist. Wäre keine normal dann $n_r \in \{p, q, pq\}$. Aber auch $n_r \equiv 1 \mod r \Rightarrow n_r = pq$. Weiter muss $n_p \geq q$ sein und $n_q \geq p$. Dann gibt es in G:

$$\begin{aligned} & pq \cdot (r-1) \text{ Elemente der Ordnung } r \\ \geq\ & q \cdot (p-1) \text{ Elementeder Ordnung } p \\ \geq\ & p \cdot (q-1) \text{ Elemente der Ordnung } q \end{aligned}$$

Also insgesamt

$$\geq (\underbrace{pqr}_{|G|} - pq) + pq - q + pq - p + 1$$

Elemeente in G

$$\begin{aligned} &= |G| + pq - q - p + 1 \\ &= |G| + (p-1) \cdot (q-1) > |G| \end{aligned}$$

Eine Sylsowgruppe ist also normal. Wir wollen weiter zeigen, dass R normal ist. Wäre R nicht normal, dann zum Beispiel $P \lhd G$. Dann ist $|G/P| = qr \overset{2.1.1}{\Longrightarrow}$ Die r-Sylowgruppen RP/P von G/P ist normal in G/P. Also $RP \lhd G$. Aber wieder nach 2.1.1 ist $R \lhd RP$. Damit ist R die einzige r-Sylowgruppe von RP, und da $RP \lhd G$ auch die einzigie von G. $\Rightarrow R \lhd G$.
Also ist immer $R \lhd G$.
Weiter ist $|G/R| = pq \overset{2.1.1}{\Longrightarrow} QR/R \lhd G/R \Rightarrow QR \lhd G$.
Also ist G von der Form

$$G = R \times (Q \ltimes R)$$

Mann kann noch weiter zeigen, dass

$$\begin{aligned} G &= C_p \ltimes C_{qr}, \qquad \text{bzw.} \\ G &= C_{pq} \ltimes C_r \end{aligned}$$

Insbesondere ist G immer auflösbar.

2.1.4 $p^aq^b,\ p<q$ Primzahlen, $ab, b \leq 2$

Seien P, Q Sylowgruppen. Falls $Q \lhd G$, dann ist G wieder ein Semidirektes Produkt $P \ltimes Q$. Wir wollen den Fall untersuchen, dass $Q \not\lhd G$. Dann ist $n_q = p^2$, aber auch $n_q \equiv 1 \mod q$, das heißt $q|p^2-1 = (p-1)\cdot(p+1)$. Also, da $p<q$ war, schon $q|p+1$, das heißt $q = p+1$, das heißt. $p = 2, q = 3$.

Damit bleibt nur $\underbrace{|G| = 4\cdot 3 = 12}_{\Rightarrow G \cong A_4,\ \text{(s.o)}}$ oder $|G| = 4 \cdot 9 = 36$.
Für $|G| = 36$ haben wir auch eine Operator vpn G auf den vier 3-Sylowgruppen, das heißt $G \to S_4$. Der Kern K ist hier wieder der Schritt der 3-Sylow-Normalisatoren, das heißt, hier Schnitt der 3-Sylowgruppen, hat also Ordnung 3 oder 1: letzteres geht nicht, da sonst $G \hookrightarrow S_4$ enthalten würde.
Also ist $K \cong C_3$, $G/K \cong A_4$. Insbesondere sind K und G/K auflösbar, also auch G.

Bemerkung. Für beliebige $a, b \in \mathbb{N}$ sind alle Gruppen der Ordnung p^aq^b auflösen. Das ist der **Satz von Burnsinde**, den wir hier nicht beweisen sollen und können.

2.1.5 Auflösbarkeit für $|G| < 60$

da eine kleinste nicht-auflösbare Gruppe einfach sein muss (G nicht-auflösbar und $1 \lhd N \lhd G$ $\Rightarrow G/N$ oder N nicht-auflösbar), genügt es zu zeigen, dass keine dieser Gruppen einfach, nicht abelsch ist.

Nach dem vorigen Abschnitt bleiben nur die Ordnungen $2\cdot 3^3$, $2^3\cdot 3$, $2^3\cdot 5$, $2^3\cdot 7$ und $2^4\cdot 3$. Falls eine Gruppe einer dieser Ordnungen einfach wäre und eine Untergruppe vom Index ≤ 3 hat, dann müsste $G \hookrightarrow S_3$ einbetten – ein **Widerspruch!**

Es bleibt nur noch $|G| = 2^3\cdot 5$ (Hier ist die 5-Sylowgruppe normal) und $|G| = 2^3\cdot 7$ (hier muss wieder mut Abzählargumenten **eine** der Sylowgruppen normal sein).

2.2 Der Satz von Jordan Hölder

Definition. Wir nennen eine Reihe der Bauart $G =: G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\}$ eine **Subnormalreihe** (**Achtung:** im Allgemeinen ist $G_k \not\lhd G$!) falls zusätzlich immer G_i ein **maximaler Normalteiler** in G_{i-1} ist (d.h. es gibt kein N mit $G_i \lneq N \lneq G_{i-1}$), dann heißt die obige Reihe **Kompositionsreihe** von G. Die Faktorgruppen G_{i-1}/G_i[3] heißen **Komositionsfaktoren** von G.

Bemerkung. Bei endlichen Gruppen gibt es immer Kompositionsreihen (maximaler Normalteiler in N existiert, seine Ordnung ist echt klerein als die von G_i; suche dann einen maximalen Normalteiler in $N, \ldots$ nach endlich vielen Schritten sind wir bei $\{1\}$ angekommen); man überlege sich, dass zum Beispiel $(\mathbb{Z}, +)$ keine Kompositionsreihe hat.

Das Beispiel $C_6 \rhd C_3 \rhd 1$, $C_6 \rhd C_2 \rhd 1$. zeigt, dass Kompositionsreihen nicht eindeutig sein müssen. Sogar $S_3 \rhd C_3 \rhd 1$, und die Kompositionsfaktoren hier sind C_2 und C_3 d.h.

[3] $G_{i-1} \mod G_i$

die gleichen wie für C_6. Das heißt an den Komositionsfaktoren kann man nicht den Isomoprhietyp von G ablesen.

trotzdem liefern die Kompositionsfaktoren wichtige Informationen. Die Kompositionsfaktore einer gruppe hängen nicht von der gewählten Kompositionsreihe ab. das ist der Inhalt des folgenden Satzes:

Satz 2.3. ***Jordan-Hölder***
Sei G endliche gruppe. dann haben alle Kompositionsreihen von G gleiche Länge und die Kompositionsfaktoren stimmen bis auch Reihenfolge und Isomorphie überein.

Beweis. Induktion über G:
Seien $G = C_0 > G_1 > \ldots > G_m = \{e\}$ und $G = H_0 > H_1 > \ldots > H_n = \{e\}$ zwei Kompostionsreihen. Ist $G_1 = H_1$, dann folgt die Behauptung. Sei also $G_1 \neq H_1$.

$$\begin{array}{ccccccccc} & & G_1 & - & G_2 & - & \ldots & - & G_m = \{e\} \\ & / & & \backslash & & & & & \\ G & & & & U & - & U_1 & \ldots & U_k = \{1\} \\ & \backslash & & / & & & & & \\ & & H_1 & - & H_2 & - & \ldots & - & H_n = \{e\} \end{array}$$

G_1H_1 ist dann ein Normalteiler von G der echt größer als G_1 ist, aber G_1 war maximaler Normalteiler $\Rightarrow G_1H_1 = G$.

Sei $U = G_1 \cap H_1$ und $U > U_1 > U_2 > \ldots > U_k = \{e\}$ eine Kompositionsreihe von U. Wegen $G_1/U = G_1/G_1 \cap H_1 \overset{(*)}{\cong} G_1H_1 = G/H_1$ ((*) siehe Isomorphiesätze).

Insbesondere ist U ein Maximaler Normalteiler von G_1 das heißt $G_1 > U > U_1 > \ldots > \{e\}$ ist Kompositionsreihe von G_1.
Nach induktionsannahme sind dann Faktoren und Länge dieser Kompositionsreihe gleich daer von $G_1 > G_2 > \ldots > G_m$. Ebenso für $H_1 > U > U_1 > \ldots$ und $H_1 > H_2 > \ldots$ damitfolgt insbesondere auch $m = n$.

08.07.09

Wir hatten gezeigt, dass $G/G_1 \cong H_1/U$, $G/H_1 \cong G_1/H$ und die beiden Kompositionsreihe von G_1 haben gleiche Faktoren, genauso die beiden Reihen von H_1. □

Bemerkung. Die Kompositionsfaktoren sind immer einfache Gruppe, denn

$$G_{i+1} \lhd G_i \text{ maximial } \Rightarrow G_i/G_{i+1}$$

hat keine nicht trivialen Normalteiler.

Beispiele. von Kompositionsreihen:

- Ist G abelsch der Ordnung $\prod p_i^{e_i}$, dann sind die Kompostionsfaktoren die C_{p_i} (jeweils e_i mal)
- ist $|G| = p^m$, dann sind die Kompositionsfaktoren C_p (m-mal)

Insbesondere gilt folgende Charakterisierung auflösbarer Gruppen:

Satz 2.4. *Eine endliche Gruppe ist auflösbar,* ***genau dann, wenn*** *alle Kompositionsfaktoren zyklisch von Primordnung sind.*

Beweis. Wir hatten die Charakterisierung: G auflösbar $\Leftrightarrow G \rhd G_1 \rhd G_2 \rhd \ldots \rhd \{1\}$, wobei alle Faktoren G_i/G_{i+1} zyklsich sind.
Ist $|G_i/G_{i+1}| = pq$, dann existieren Untergruppen H/G_{i+1} der Ordnung p, $H/G_{i+1} \lhd G_i/G_{i+1}$, also $H \lhd G_i$, und wir können H in die Reihe einfügen. □

„Jetzt kommt so ein bisschen 'Blabla'"

Bemerkung. Wir hatten bei der Betrachtung von Grupen kleiner Ordnung „gesehen", dass die meisten Gruppen auflösbar sind (statistisch sind sogar die meisten Gruppen p-Gruppen). Trotzdem sind nicht-auflösbare Gruppen in gewisser Hinsicht vielfältiger. Es stellt sich hierfür die Frage, welche einfachen, nicht abelschen (endlichen) Gruppen es gibt. $\rightsquigarrow$ „**Klassifikation der Endlichen einfachen Gruppen**". Dieses wurde im 19.Jhd. begonnen und ca. 1980 fertig gestellt (alle hierfür nötigen Beweise zusammen > 10.000 Seiten!!). Wir kennen die $A_n, n \geq 5$. Weitere Beispiele sind $\mathrm{SL}_n(\mathbb{F}_q)/Z(\mathrm{SL}_n) =: \mathrm{PSL}_n(q)$ ist meistens einfach, nicht abelsch.

Es gibt weitere Familien, die sich aus „natürlichen" Matrizengruppen herleiten, zum Beispiel orthogonale und unitäre Gruppen, Weiter gibt es 10 Familien „exzeptioneller einfacher Gruppen, die gewisse mit dem eben erwähnten Matrixgruppen gemeinsam haben.
Zusätzlich gibt es 26 **sporadische Gruppen** einfache Gruppen, die in keine der unendlichen Familien passen. (zum Beispiel das sog. **Monster**; Die erste sporadische Gruppe wurde ab ca. 1860 von Mathieu entdeckt, die restlichen erst ab 1960)

2.3 Eine verallgemeinerung der Sylowsätze für auflösbare Gruppen

Definition. Ist G eine endliche Gruppe, Π eine Menge von Primzahlen. Dann ist U eine **Π-Hall-Untergruppe** von G:$\Leftrightarrow |U|$ enthält genau die Primteiler aus Π, und zwar jeweils genauso oft, wie diese in $|G|$ vorkommen.

Beispiel. $G = A_5$, $\Rightarrow |G| = 3 \cdot 4 \cdot 5 \Rightarrow A_4$ ist eine $\{2,3\}$-Halluntergruppe, $\{3,5\}$-bzw $\{2,5\}$-Halluntergruppen gibt es aber **nicht**!

Für auflösbare Gruppe gilt dagegen:

Satz 2.5. ***Satz von Hall:***
Sie G auflösbar; Π eine Menge von Primzahlen von $|G|$. Dann existiert in G eine Π Hallgruppe, und alle Π-Hallgruppen in G zueinander konjugiert.

Beweis. $|G| := m \cdot n$, wobei m die Ordnung der gesuchten Π Hallgruppe sei (insbesondere $\mathrm{ggT}(m,n) = 1$). G hat einen echten Normalteiler K, sie $|K| = m_1 n_1,\ m_1|m,\ n_1|n$.

1- Fall: $n_1 < n$.

G/K (der Ordnung $\frac{mn}{m_1 n_1}$) hat induktiv eine Untergruppe S/K der Ordnung $\frac{m}{m_1}$. $|S| = \frac{m}{m_1} \cdot |K| = m \cdot n_1 < |G|$, $\Rightarrow$ induktiv hat S eine Untergruppe der Ordnung m. Seien M_1, M_2 Untergruppen von G der Ordnung m. Es gilt $M_i K/K \overset{(*)}{\cong} M_i/K \cap M_i$, $i = 1, \ldots$ (wobei in $(*)$ die Isomorphiesätze eingehen) und $|K \cap M_i|$ teilt m und auch $m_1 n_1$ teilt also m_1.

$$|M_i K/K| = \frac{|M_i|}{|K \cap M_i|} = \frac{m}{m_1} \cdot m_2,$$

m_2 ein passender Teiler von m_1, aber auch: $|M_i K/K|$ teilt $|G/K| = \frac{mn}{m_1 n_1}$. $\Rightarrow m_2$ teilt $\frac{n}{n_1}$. Also insgesamt $m_2 = 1$ da $\mathrm{ggT}(m, a) = 1$

$$\Rightarrow |M_i K/K| = \frac{m}{m_1},$$

alsi die Hallgruppen von G/K. Induktiv sind $M_1 K/K$ und $M_2 K/K$ konjugiert in G/K. das heißt

$$\begin{aligned} M_1 K/K &= (Kx)^{-1} M_2 K/K \cdot (Kx) \\ \Rightarrow M_1 K &= x^{-1}(M_2 K)x \\ \Rightarrow x^{-1} M_2 x &\leq M_1 K \end{aligned}$$

Aber M_1 und $x^{-1} M_2 x$ sind Π-Hallgruppen von $M_1 K \overset{\text{(Induktion)}}{\Longrightarrow}$ sie sind konjugiert in $M_1 K$, denn

$$\begin{aligned} |M_1 K| &= |M_1 K/K| \cdot |K| \\ &= \frac{m}{m_1} \cdot m_1 n_1 = m n_1 < mn = |G| \end{aligned}$$

Also auch $M_1,\ M_2$ in G konjugiert.

2. Fall: Für **jeden** nicht-trivialen Normalteiler K von G ist $n_1 = n$. Ein minimaler Normalteiler N einer Auflösbaren Gruppe ist immer von der Form $C_p \times \ldots C_p$.[4]. $\Rightarrow n = p^\alpha$ und jeder minimale Normalteiler K von G muss Ordnung n haben. K ist dann sogar p-Sylowgruppen von G, also K sogar einziger minimaler Normalteiler von G. G/K hat minimalen Normalteiler L/K der Ordnung q^β, $q \neq p$. L hat auch eine Untergruppe Q der Ordnung q^β (nach Sylow) $\Rightarrow \underbrace{L}_{\text{Ordnung } q^\beta p^\alpha} = K \cdot Q$ (mit

[4]

Beweis. $N \neq N' \lhd G \Rightarrow N' = \{1\}$, das heißt N ist abelsch. Sei p ein Primteiler von $|N|$, $U = \{x \in N \mid x^p = 1\}$. Da N abelsch, ist U eine Untergruppe von N, die sogar invariant unter Konjugation in G ist, also $U \lhd G \Rightarrow U = N$. □

$|L| = q^\beta p^\alpha$, $|K| = p^\alpha$ und also $|Q| = q^\beta$. $\Rightarrow G = L \cdot N_G(Q)$ (mit $L \lhd G$ und $N_G(Q)$ q-Sylowgruppe von L) (das ist das Fubini-Argument[5]).

$$G = L \cdot N_G(Q) = K \cdot Q \cdot N_G(Q) = K \cdot N_G(Q)$$

Sei $D := K \cap N_G(Q)$. Dann gilt:

1. $D \trianglelefteq K$, da K abelsch
2. $D \trianglelefteq N_G(Q)$, da $K \trianglelefteq G$

$$\Rightarrow D \trianglelefteq K \cdot N_G(Q) = G$$

Wegen Minimalität von K ist dann $D = 1$ oder $D = K$

- Wäre $D = K$, dann wäre $K \leq N_G(Q)$, dies bedeutete: $G = N_G(Q) \Rightarrow Q \lhd G$ ein Widerspruch zu $|Q| = q^\beta$, jeder minimale Normalteiler hat aber Ordnung p^α.
- Also $D = \{1\}$m das heißt $|N_G(Q)| = \frac{|G|}{|K|} = \frac{mn}{n} = m$, also haben wir eine Π-Hallgruppe gefunden.

Zur Konjugiertheit: Sei M eine weitere Π-Hallgruppe: Es gilt: $|L| = p^\alpha q^\beta$, also $G = ML$. Wegen $|G/L| = |ML/L| = |M/M \cap L|$ ist $|M \cap L| = q^\beta$. Auch Q war eine Untergruppe von L der Ordnung $q^\beta \overset{\text{Sylow}}{\Longrightarrow} Q$ und $M \cap L$ sind konjugiert in L. Sind aber zwei Untergruppen konjugiert, dann sind auch ihre Normalisatoren konjugiert. ($N(Q^g) = N(Q)^G$!). Also ist $M \subseteq N(M \cap L) = N(Q^g) = N(Q)^g$ (wobei $|M| = m$, $|N(M \cap L)| = m$ und $|N(Q)^g| = M$). Also ist M konjugiert zu der bereits gefundenen Π-Hallgruppen $N(Q)$.

□

[5] siehe WS Übung 5