Algebra

Vorlesung von
Prof. Dr. Niko Naumann
im Wintersemester 2011/2012
Überarbeitung und Textsatz in LyX von
Andreas Völklein

Stand: 10. Februar 2012

ACHTUNG

Diese Mitschrift ersetzt *nicht* die Vorlesung.
Es wird daher *dringend* empfohlen, die Vorlesung zu besuchen.

Copyright Notice

Disclaimer of Warranty

Limitation of Liability

Links

Der Text der „GNU Free Documentation License" kann auch auf der Seite

`https://www.gnu.org/licenses/fdl-1.3.de.html`

nachgelesen werden.
Eine transparente Kopie der aktuellen Version dieses Dokuments kann von

`https://github.com/andiv/algebra`

heruntergeladen werden.

Literatur

- Siegfried Bosch: *Algebra*, Springer, 2009
  ISBN 3-540-40388-4, http://dx.doi.org/10.1007/978-3-540-92812-6
- Gerd Fischer: *Lehrbuch der Algebra*, Vieweg + Teubner, 2011
  ISBN 978-3-8348-1249-0, http://dx.doi.org/10.1007/978-3-8348-9455-7
- Jens C. Jantzen, Joachim Schwermer: *Algebra*, Springer, 2006
  ISBN 3-540-21380-5, http://dx.doi.org/10.1007/3-540-29287-X
- Falko Lorenz, Franz Lemmermeyer: *Einführung in die Algebra*, Spektrum, 2007/8
  ISBN 978-3-8274-1609-4/978-0-387-72487-4
- Serge Lang: *Algebra*, Springer, 2005
  ISBN 0-387-95385-X
- Michael F. Atiya, Ian G. MacDonald: *Introduction to commutative algebra*, Westview Press, 1994
  ISBN 0-201-40751-5, Lokalisierungen: Seite 36-39

Inhaltsverzeichnis

1 Gruppentheorie I

Aus der Linearen Algebra wird die Kenntnis der Definition folgender Begriffe vorausgesetzt:

- Quantoren, insbesondere der Existenzquantor $\exists$ und der Allquantor $\forall$,
- (disjunkte) Mengen,
- (endliche, abelsche) Gruppen,
- (echte) Untergruppen (Abkürzung: UG),
- Abbildungen, insbesondere die Identitätsabbildung id_X einer Menge X, und deren Komposition,
- Injektivität, Surjektivität, Bijektivität,
- die natürlichen Zahlen $\mathbb{N}$, die ganzen Zahlen $\mathbb{Z}$ und die rationalen Zahlen $\mathbb{Q}$,
- die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$,
- die Permutationsgruppe $\Sigma(X)$ für eine Menge X, insbesondere $S_n := \Sigma(\{1,\ldots,n\})$,
- Äquivalenzrelationen,
- Körper k und die Gruppe der invertierbaren $n \times n$-Matrizen $\mathrm{Gl}_n(k)$ für $n \in \mathbb{N}_{\geq 1}$ und
- Primzahlen $p \in \mathbb{Z}$.

1.1 **Definition** (Gruppenhomomorphismus)

Seien G,G' Gruppen.
Ein *Gruppenhomomorphismus* (*von G nach G'*) ist eine Abbildung $\varphi : G \to G'$ mit:

$$\underset{a,b\in G}{\forall} \varphi(ab) = \varphi(a) \cdot \varphi(b) \tag{1.1}$$

Ferner heißt φ

$$\begin{aligned} Mono(morphismus) &\Leftrightarrow \varphi \text{ injektiv,} \\ Epi(morphismus) &\Leftrightarrow \varphi \text{ surjektiv,} \\ Iso(morphismus) &\Leftrightarrow \varphi \text{ ein bijektiver Gruppenhomomorphismus,} \\ Endo(morphismus) &\Leftrightarrow G = G' \text{ und} \\ Auto(morphismus) &\Leftrightarrow \varphi \text{ ein Isomorphismus von } G \text{ nach } G \text{ ist.} \end{aligned}$$

1.2 Beispiel

Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann gelten:

i) $\varphi(e) = e'$ mit den neutralen Elementen $e \in G$ und $e' \in G'$.

ii) $\underset{a \in G}{\forall} \varphi\left(a^{-1}\right) = \varphi(a)^{-1}$

Beweis

i) $$e' \cdot \varphi(e) = \varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \quad / \cdot \varphi(e)^{-1}$$
$$\overset{\text{Kürzen}}{\Rightarrow} \quad e' = \varphi(e)$$

$\square_{\text{i)}}$

ii) $$\varphi(a) \cdot \varphi(a)^{-1} = e' \overset{\text{i)}}{=} \varphi(e) = \varphi\left(a \cdot a^{-1}\right) = \varphi(a) \cdot \varphi\left(a^{-1}\right) \quad / \varphi(a)^{-1} \cdot$$
$$\overset{\text{Kürzen}}{\Rightarrow} \quad \varphi(a)^{-1} = \varphi\left(a^{-1}\right)$$

$\square_{1.2}$

1.3 Proposition und Definition (Kern und Bild)

Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus.

i) $\ker(\varphi) := \{a \in G | \varphi(a) = e'\} \subseteq G$ ist eine Untergruppe, der *Kern von* φ, und es gilt:
$$\varphi \text{ ist ein Monomorphismus} \Leftrightarrow \ker(\varphi) = \{e\}$$

ii) $\operatorname{im}(\varphi) \subseteq G'$ ist eine Untergruppe.

Beweis

i) Wegen $\varphi(e) = e'$ folgt $e \in \ker(\varphi)$.
Seien a,$b \in \ker(\varphi)$, also $\varphi(a) = e' = \varphi(b)$, dann folgt:
$$\varphi\left(a \cdot b^{-1}\right) = \varphi(a) \cdot \varphi(b)^{-1} = e' \cdot \left(e'\right)^{-1} = e'$$
Also ist auch $a \cdot b \in \ker(\varphi)$ und daher $\ker(\varphi) \subseteq G$ eine Untergruppe.
Ist φ ein Monomorphismus, also injektiv, so gilt für $a \in \ker(\varphi)$:
$$\varphi(a) = e' = \varphi(e)$$
Da φ injektiv ist, folgt schon $a = e$ und damit $\ker(\varphi) = \{e\}$.
Gelte umgekehrt $\ker(\varphi) = \{e\}$.
Dann folgt für a,$b \in G$:
$$\varphi(a) = \varphi(b)$$
$$e' = \varphi(a)^{-1} \cdot \varphi(b) = \varphi\left(a^{-1} b\right)$$

Also gilt $a^{-1}b \in \ker(\varphi) = \{e\}$ und damit:

$$\begin{aligned} a^{-1}b &= e \\ b &= a \end{aligned}$$

Also ist φ injektiv.

ii) Wegen $\varphi(e) = e'$ folgt $e' \in \operatorname{im}(\varphi)$.
Seien $g,h \in \operatorname{im}(\varphi)$, also gibt es $a,b \in G$ mit $\varphi(a) = g$ und $\varphi(b) = h$.
Damit folgt:

$$g \cdot h^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi\left(ab^{-1}\right)$$

Also ist $ab^{-1} \in \operatorname{im}(\varphi)$ und daher $\operatorname{im}(\varphi) \subseteq G'$ eine Untergruppe.

$\square_{1.3}$

1.4 Proposition

Sei G eine Gruppe. Dann ist die Abbildung

$$\{\varphi | \varphi : \mathbb{Z} \to G \text{ Gruppenhomomorphismus}\} \xrightarrow{\sim} G, \varphi \mapsto \varphi(1) \tag{1.2}$$

bijektiv.

Beweis

TODO: Beweis aus Linearer Algebra I einfügen

$\square_{1.4}$

1.5 Beispiel und Definition (Automorphismengruppe, Konjugation)

Sei G eine Gruppe. Dann ist $\operatorname{Aut}(G) := \{\varphi | \varphi : G \to G \text{ Automorphismus}\}$ eine Gruppe bezüglich der Komposition $\circ$ mit dem neutralem Element id_G (Nebenbemerkung: im Allgemeinen ist $\operatorname{Aut}(G) \lneq \Sigma(G)$ eine echte Untergruppe) und heißt die *Automorphismengruppe von G*.
Die Abbildung $\phi : G \to \operatorname{Aut}(G)$, definiert durch $\phi(g)(h) = ghg^{-1}$ $\forall_{g,h \in G}$ ist wohldefiniert und ein Gruppenhomomorphismus.
$\forall_{g \in G}$ heißt die Abbildung $\phi(g)$ die *Konjugation mit g*.

Beweis

ϕ ist wohldefiniert, das heißt $\forall_{g \in G}$ ist $\phi(g) \in \operatorname{Aut}(G)$, denn:

- $\underset{h,h' \in G}{\forall} : \phi(g)\left(hh'\right) = g\left(heh'\right)g^{-1} = \left(ghg^{-1}\right)\left(gh'g^{-1}\right) = \phi(g)(h) \cdot \phi(g)\left(h'\right)$
  Also ist $\phi(g)$ ein Gruppenhomomorphismus.

- $\underset{g,h\in G}{\forall}: \left(\phi(g)\circ\phi\left(g^{-1}\right)\right)(h) = g\cdot\phi\left(g^{-1}\right)(h)\cdot g^{-1} = \underbrace{gg^{-1}}_{=e} h \underbrace{\underbrace{\left(g^{-1}\right)^{-1}}_{=g} g^{-1}}_{=e} = h$

  $\Rightarrow\ \phi(g)\circ\phi\left(g^{-1}\right) = \mathrm{id}_G$; Also ist $\phi(g)\in\mathrm{Aut}(G)$.

- Für $g,g',h\in G$ gilt:

  $$\left(\phi(g)\circ\phi\left(g'\right)\right)(h) = \phi(g)\left(g'hg'^{-1}\right) = gg'hg'^{-1}g^{-1} = \left(gg'\right)h\left(gg'\right)^{-1} = \phi\left(gg'\right)(h)$$

  Also ist ϕ ein Gruppenhomomorphismus.

$\square_{1.5}$

Beispiel

$G = {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} = \{\overline{0},\overline{1},\overline{2}\}$; $\mathrm{Aut}(G)\subseteq\Sigma(G) = \Sigma\{\overline{0},\overline{1},\overline{2}\} = S_3$
$\mathrm{Aut}(G)\cong\left({}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\right)^* = \{\overline{1},\overline{2}\}$
Insbesondere: $|\mathrm{Aut}(G)| = 2$, $|\Sigma(G)| = 3! = 6$

1.6 Proposition und Definition (Linksnebenklasse, Index)

Seien G eine Gruppe und $H\subseteq G$ eine Untergruppe. Dann ist die Relation $\sim$ auf G definiert durch

$$\underset{g,g'\in G}{\forall} g\sim g' \Leftrightarrow g^{-1}g'\in H \tag{1.3}$$

eine Äquivalenzrelation.
Für $g\in G$ heißt die Äquivalenzklasse

$$[g] = \left\{g'\in G | g\sim g'\right\} \overset{(1.3)}{=} \{gh | h\in H\} =: gH\subseteq G \tag{1.4}$$

die *Linksnebenklasse von g bezüglich H*. Wir schreiben

$${}^{G}\!/_{H} := \{gH | g\in G\}$$

und

$$(G:H) := \left|{}^{G}\!/_{H}\right|$$

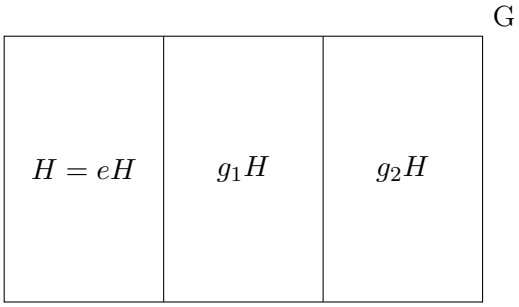
heißt der *Index von H in G*. Es gelten:

i) $\underset{g,g'\in G}{\forall}: gH = g'H \Leftrightarrow gH\cap g'H\neq\emptyset \Leftrightarrow g\in g'H \Leftrightarrow g^{-1}g'\in H$

ii) Für alle $g,g'\in G$ ist die Abbildung $gH\xrightarrow{\sim} g'H, gh\mapsto g'h$ bijektiv.
Für $|H|<\infty$ ist $|gH| = |g'H|$.

iii) $G = \dot{\bigcup\limits_{gH\in {}^{G}\!/_{H}}}(gH)$ (disjunkte Vereinigung)

Skizze



Beweis

Zeige zunächst, dass $\sim$ eine Äquivalenzrelation ist:

- $\sim$ ist *reflexiv*: $\underset{g\in G}{\forall} g \cdot g^{-1} \overset{H \text{ ist UG}}{=} e \in H \overset{(1.3)}{\Rightarrow} g \sim g$
- $\sim$ ist *symmetrisch*:

$$\underset{g,g'\in G}{\forall} g \sim g' \overset{(1.3)}{\Rightarrow} g^{-1} \cdot g' \in H \overset{H \text{ ist UG}}{\Rightarrow} H \ni \left(g^{-1} \cdot g'\right)^{-1} = g'^{-1} \cdot g \overset{(1.3)}{\Rightarrow} g' \sim g$$

- $\sim$ ist *transitiv*: Seien $g,g',g'' \in G$: $g \sim g' \wedge g' \sim g'' \Rightarrow g^{-1}g', g'^{-1} \cdot g'' \in H$
$\overset{H \text{ ist UG}}{\Rightarrow} H \ni \left(g^{-1}g'\right)\left(g'^{-1}g''\right) = g^{-1}g'' \overset{(1.3)}{\Rightarrow} g \sim g''$

Also ist $\sim$ eine Äquivalenzrelation.
Daraus folgen direkt i) und iii).
ii) ist klar. $\square_{1.6}$

1.7 **Korollar** (Satz von Lagrange)

Seien G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt

$$|G| = (G : H) \cdot |H| \tag{1.5}$$

und insbesondere ist $|H|$ ein Teiler der Anzahl der Elemente von $|G|$.

Beweis

$$|G| \overset{1.6\,\text{iii)}}{=} \left| \dot{\bigcup_{gH \in G/H}} (gH) \right| = \sum_{gH \in G/H} |gH| = \left|G/H\right| \cdot |H| \overset{\text{Def.}}{=} (G : H) \cdot |H|$$

$\square_{1.7}$

1.8 **Beispiel** (Symmetrische und alternierende Gruppe vom Grad 3)

Sei $S_3 = \Sigma(\{1,2,3\})$. Dann sind

$$A_3 := \{\sigma \in S_3 | \operatorname{sgn}(\sigma) = 1\} = \left\{ 1, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{=:\omega}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}_{=:\omega^2} \right\} \subseteq S_3 \tag{1.6}$$

und

$$H := \left\{ 1, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}_{=:\tau} \right\} \subseteq S_3 \tag{1.7}$$

Untergruppen mit $|A_3| = 3, |H| = 2$, also:

$$(S_3 : A_3) = 2 \qquad\qquad (S_3 : H) = 3$$

Explizit gilt:

$$S_3 = A_3 \dot\cup \tau A_3 = H \dot\cup \omega H \dot\cup \omega^2 H$$

1.9 **Definition** (Normalteiler)

Seien G eine Gruppe und H eine Untergruppe.
Dann heißt H *Normalteiler* (*von* G, in Zeichen: $H \trianglelefteq G$, Abkürzung: NT), wenn gilt:

$$\underset{g\in G, h\in H}{\forall} ghg^{-1} \in H$$

Man sagt auch, H ist *stabil unter Konjugation*.

1.10 **Beispiel**

- In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler, denn es gilt:

$$ghg^{-1} = h \underbrace{gg^{-1}}_{=e} = h \in H$$

- In 1.8 gilt $A_3 \trianglelefteq S_3$, aber $H \subseteq S_3$ ist kein Normalteiler.

1.11 **Proposition** (Kern ist Normalteiler)

Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, so ist $\ker(\varphi) \trianglelefteq G$ ein Normalteiler.

Beweis

Nach 1.3 i) ist $\ker(\varphi) \subseteq G$ eine Untergruppe. Prüfe nun die Definition 1.9:

$$g \in G, h \in \ker(\varphi) \Rightarrow \varphi\left(ghg^{-1}\right) = \varphi(g) \underbrace{\varphi(h)}_{=e'} \varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e' \Rightarrow ghg^{-1} \in \ker(\varphi)$$

$\square_{1.11}$

1.12 **Beispiel und Definition** (Zentrum)

Ist G eine Gruppe, so ist $Z(G) := \left\{ g \in G \,\middle|\, \underset{h \in G}{\forall} gh = hg \right\} \trianglelefteq G$ ein Normalteiler, das *Zentrum von* G.

Beispiel

- Ist k ein Körper und $n \in \mathbb{N}_{\geq 1}$, dann ist $Z(\mathrm{Gl}_n(k)) = k^* \cdot \mathrm{id}_{k^n}$
- $Z(S_3) \overset{(!)}{=} \{e\}$
- $G = Z(G) \Leftrightarrow G$ ist abelsch.

Beweis zu 1.12

Für die Abbildung $\phi : G \to \mathrm{Aut}(G)$ aus 1.5 sieht man leicht, dass $\ker(\phi) = Z(G)$ ist.
Also folgt die Behauptung aus 1.11. $\square_{1.12}$

1.13 **Proposition** (kanonische Projektionsabbildung)

Seien G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler.
Dann existiert genau eine Gruppenstruktur auf der Menge G/N, sodass die kanonische Abbildung

$$\pi : G \to G/N, \pi(g) \mapsto gN \tag{1.8}$$

ein Gruppenhomomorphismus ist.
Es gilt $\ker(\pi) = N$.

Beweis

- Eindeutigkeit: Falls eine solche Struktur existiert, so ist sie eindeutig festgelegt durch:

$$\underset{g,g' \in G}{\forall} (gN) \cdot (g'N) = \pi(g) \cdot \pi(g') = \pi(gg') = (gg') \cdot N \tag{1.9}$$

- Existenz: Zeige nur, dass (1.9) wohldefiniert ist, das heißt:

$$\underset{g,g',g_1,g_1' \in G}{\forall} (gN = g_1N) \wedge (g'N = g_1'N) \quad \Rightarrow \quad (gg')N = (g_1g_1')N \tag{1.10}$$

Dies ergibt sich aus folgender Überlegung:
Wegen (1.3) in 1.6 betrachte:

$$(gg')^{-1} \cdot (g_1 g_1') = (g')^{-1} \cdot g^{-1} \cdot g_1 \cdot g_1' = (g')^{-1} \cdot \underbrace{g_1' \cdot (g_1')^{-1}}_{=e} \cdot \underbrace{g^{-1} \cdot g_1}_{=:n \in N, \text{ da } gN = g_1 N} \cdot g_1' =$$

$$= \underbrace{(g')^{-1} \cdot g_1'}_{\in N, \text{ da } g'N = g_1'N} \underbrace{(g_1')^{-1} \cdot n \cdot g_1'}_{\in N, \text{ da } N \trianglelefteq G} \in N$$

Also gilt $(gg')\,N = (g_1 g_1')\,N$.
Ferner gilt:

$$\ker(\pi) = \left\{ g \in G | gN = \pi(g) = e' = eN = N \in {}^{G}\!/_{N} \right\} \overset{1.6\,\text{i)}}{=} N$$

$\square_{1.13}$

1.14 **Beispiel** (H ist kein Normalteiler)

Sei $H = \{1, (12)\} \subseteq S_3$ wie in 1.8.
Die „Abbildung“ ${}^{G}\!/_{H} \times {}^{G}\!/_{H} \dashrightarrow {}^{G}\!/_{H}$, $(gH, g'H) \mapsto (gg')\,H$ ist nicht wohldefiniert, denn es gelten

$$eH = (12)\,H$$

(da $(12) \in H$) und

$$(123)\,H = (123)\,H,$$

aber $(e \cdot (123))\,H \neq ((12)\,(123))\,H$, denn:

$$(e\,(123))^{-1}\,(12)\,(123) = (132)\,(23) = (13) \notin H$$

Dieses Beispiel zeigt, dass für (1.10) im Beweis von 1.13 auf die Voraussetzung „Normalteiler“ nicht verzichten kann, und dass $H \subseteq S_3$ kein Normalteiler ist.

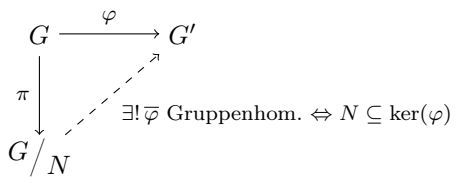
1.15 **Satz** (universelle Eigenschaft der Projektionsabbildung π)

Seien G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $\varphi : G \to G'$ ein Gruppenhomomorphismus.
Dann sind äquivalent:

i) $N \subseteq \ker(\varphi)$

ii) $\underset{\text{Grphom. } \overline{\varphi}: {}^{G}\!/_{N} \to G'}{\exists!} \varphi = \overline{\varphi} \circ \pi$

Kommutatives Diagramm



Beweis

TODO: Beweis als Übung einfügen

$\square_{1.15}$

1.16 Korollar (Isomorphiesatz)

Ist $\varphi : G \to G'$ ein Epimorphismus, so ist $\overline{\varphi} : {}^{G}\!/_{\ker(\varphi)} \to G'$ wohldefiniert und ein Isomorphismus.

Beweis

Nach 1.15 ist $\overline{\varphi}$ wohldefiniert und ein Gruppenhomomorphismus.
(Wähle in 1.15 $N = \ker(\varphi)$)
Weil φ ein Epimorphismus ist, ist auch $\overline{\varphi}$ ein Epimorphismus.
Aus

$$\ker(\overline{\varphi}) = {}^{\ker(\varphi)}\!/_{N} = {}^{\ker(\varphi)}\!/_{\ker(\varphi)} = \{e\}$$

und 1.3 folgt, dass $\overline{\varphi}$ injektiv, also ein Isomorphismus ist. $\square_{1.16}$

1.17 Satz (Primzahlordnung)

Seien G eine Gruppe und $p := |G|$ eine Primzahl (Abkürzung: PZ). Dann gilt:

$$G \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \tag{1.11}$$

1.18 Beispiel

i) ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \ncong {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$ (vergleiche Strukturensatz für endlich erzeugte abelsche Gruppen).

ii) $S_3 \ncong {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$ (denn S_3 ist nicht abelsch).

Beide Beispiele zeigen, dass man in 1.17 auf die Voraussetzung „Primzahl“ nicht verzichten kann.

Beweis von 1.17

Wegen $1 \neq p = |G|$ existiert ein $e \neq g \in G$.
Nach 1.4 existiert genau ein Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$ mit $\varphi(1) = g$. Es folgt nach 1.7:

$$1 \neq |\mathrm{im}(\varphi)| \,\big|\, |G| = p$$

Weil p eine Primzahl ist, folgt $|\mathrm{im}(\varphi)| = |G|$, das heißt φ ist ein Epimorphismus.
Nach 1.16 existiert ein Isomorphismus ${}^{\mathbb{Z}}\!/_{\ker(\varphi)} \xrightarrow{\sim} G$.
Damit ist $\ker(\varphi) \subseteq \mathbb{Z}$ eine Untergruppe vom Index $|G| = p$.
Es folgt $\ker(\varphi) = p\mathbb{Z}$, also $G \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.
TODO: Beweis für letzten Schritt aus Linearer Algebra I einfügen

$\square_{1.17}$

1.19 **Proposition und Definition** (erzeugte Untergruppe)

Seien G eine Gruppe, $x \in G$ und $\varphi : \mathbb{Z} \to G$ der eindeutige Gruppenhomomorphismus mit $\varphi(1) = g$. Dann ist

$$\langle x \rangle := \operatorname{im}(\varphi) = \{x^n | n \in \mathbb{Z}\} \subseteq G$$

die kleinste Untergruppe von G, die x enthält.
Sie heißt *die von x (in G) erzeugte Untergruppe.*

Beweis

Wegen 1.3 ii) ist $\langle x \rangle \subseteq G$ eine Untergruppe und es gilt:

$$x = \varphi(1) \in \operatorname{im}(\varphi) = \langle x \rangle$$

Ist $H \subseteq G$ eine Untergruppe mit $x \in H$, so folgt $x^n \in H$ für alle $n \in \mathbb{Z}$, das heißt $\langle x \rangle \subseteq H$. $\square_{1.19}$

1.20 **Proposition und Definition** (zyklische Gruppe, Erzeuger)

Für eine Gruppe G sind äquivalent:

i) $\exists_{x \in G} \langle x \rangle = G$

ii) Es gibt einen Epimorphismus $\varphi : \mathbb{Z} \to G$.

In diesem Fall heißt G *zyklisch*, und jedes $x \in G$ mit $\langle x \rangle = G$ heißt *Erzeuger von G*.

Beweis

i) $\Rightarrow$ ii): Wähle $\varphi : \mathbb{Z} \to G$ mit $\varphi(1) = x$.
ii) $\Rightarrow$ i): Wähle $x := \varphi(1)$. $\square_{1.20}$

1.21 **Satz** (Klassifizierung zyklischer Gruppen)

Bis auf Isomorphie existieren genau die zyklischen Gruppen $\mathbb{Z}/m\mathbb{Z}$ für $m \in \mathbb{N}_{\geq 1}$ und $\mathbb{Z}$ (erzeugt zum Beispiel durch $\overline{1}$ und 1).

Beweis

Es ist klar, dass die angegebenen Gruppen zyklisch und paarweise nicht isomorph sind.
Sei nun G eine beliebige zyklische Gruppe, dann existiert nach 1.20 ii) ein Epimorphismus $\varphi : \mathbb{Z} \to G$, weswegen nach 1.16 ein Isomorphismus $\tilde{\varphi} : \mathbb{Z}/\ker(\varphi) \xrightarrow{\sim} G$.
Nun ist $\ker(\varphi) \subseteq \mathbb{Z}$ eine Untergruppe, womit aus der linearen Algebra für ein $m \geq 0$ schon folgt:

$$\ker(\varphi) = (m) = m\mathbb{Z}$$

Daher folgt:

$$G \cong \begin{cases} \mathbb{Z} & \text{für } m = 0 \\ \mathbb{Z}/m\mathbb{Z} & \text{für } m > 0 \end{cases}$$

$\square_{1.21}$

1.22 **Satz** (Untergruppe, Kern und Bild zyklischer Gruppen)

Sei G eine zyklische Gruppe. Dann gilt:

i) Jede Untergruppe $H \subseteq G$ ist zyklisch.

ii) Für jeden Gruppenhomomorphismus $\varphi : G \to G'$ sind $\ker(\varphi)$ und $\operatorname{im}(\varphi)$ zyklisch.

Beweis

i) Ohne Einschränkung ist $H \neq \{e\}$. Wähle einen Epimorphismus $\varphi : \mathbb{Z} \to G$.
Dann ist auch $\psi := \varphi|_{\varphi^{-1}(H)} : \varphi^{-1}(H) \to H$ ein Epimorphismus.

Kommutatives Diagramm

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & G \\ \uparrow & & \uparrow \\ \varphi^{-1}(H) & \xrightarrow{\psi} & H \end{array}$$

Wegen $H \neq \{e\}$ ist $\{0\} \neq \varphi^{-1}(H) \subseteq \mathbb{Z}$ eine nicht triviale Untergruppe.
Daher ist $\varphi^{-1}(H) = m\mathbb{Z}$ für ein $m \geq 1$, also:

$$\begin{aligned} \mathbb{Z} &\cong \varphi^{-1}(H) \\ x &\mapsto mx \end{aligned}$$

Also ist $\psi : \mathbb{Z} \to H$ ein Epimorphismus, das heißt H ist zyklisch. $\square_{\text{i)}}$

ii) Ist $\psi : \mathbb{Z} \to G$ ein Epimorphismus, so auch die Komposition:

$$\mathbb{Z} \overset{\psi}{\twoheadrightarrow} G \overset{\varphi}{\twoheadrightarrow} \operatorname{im}(\varphi)$$

Daher ist $\operatorname{im}(\varphi)$ zyklisch.
Weil $\ker(\varphi) \subseteq G$ eine Untergruppe ist, ist $\ker(\varphi)$ zyklisch nach i).

$\square_{1.22}$

1.23 **Definition** (Ordnung)

Seien G eine Gruppe und $x \in G$, dann heißt

$$\operatorname{ord}(x) := |\langle x \rangle| \overset{(!)}{=} \min\{n \geq 1 | x^n = e\} \in \mathbb{N} \cup \{\infty\}$$

die Ordnung von x (in G).

1.24 Beispiel

Betrachte $G := \left(\mathbb{Z}/5\mathbb{Z}\right)^* = \mathbb{F}_5^*$

$x \in \mathbb{F}_5^*$	x^2	x^3	x^4	$\operatorname{ord}(x)$
$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	1
$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	4
$\overline{3}$	$\overline{4}$	$\overline{2}$	$\overline{1}$	4
$\overline{4}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	2

Man erkennt:

- $\overline{2}$ und $\overline{3}$ sind Erzeuger von G, denn $\operatorname{ord}(x) = 4$.
- Die Ordnung $\operatorname{ord}(x)$ ist immer ein Teiler von $4 = |G|$.

Die Rechnung zeigt: $G = \mathbb{F}_5^* \cong \mathbb{Z}/4\mathbb{Z}$.

1.25 (kleiner Fermatscher) Satz

Seien G eine endliche Gruppe und $x \in G$.
Dann gilt $\operatorname{ord}(x) \mid |G|$ und $x^{|G|} = e$ in G.

Beweis

Nach Definition ist $\operatorname{ord}(x) = |H|$ für die Untergruppe $H := \langle x \rangle \subseteq G$.
Nun folgt $\operatorname{ord}(x) \mid |G|$ aus 1.7.
Klar ist $x^{\operatorname{ord}(x)} = e$, womit folgt:

$$x^{|G|} \overset{1.7}{=} x^{\operatorname{ord}(x)\cdot(G:\langle x\rangle)} = e^{(G:x)} = e$$

$\square_{1.25}$

1.26 Korollar

i) Seien $n \geq 1$ und $a \in \mathbb{Z}$ teilerfremd zu n, dann folgt $a^{\varphi(n)} \equiv 1 \bmod n$.
(Hier ist $\varphi(n)$ die Eulersche φ-Funktion.)

ii) Ist p eine Primzahl und $a \in \mathbb{Z}$ mit $p \neq a$, so gilt:

$$a^{p-1} \equiv 1 \bmod p$$

(vergleiche 1.24)

Beweis

i) Wegen $\operatorname{ggT}(a,n) = 1$ ist $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ und mit $\varphi(n) := \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right|$ folgt die Behauptung aus 1.25.

ii) Falls $n = p$ eine Primzahl ist, gilt in i) nach linearer Algebra I:

$$\varphi(p) = p - 1$$

$\square_{1.26}$

1.27 **Proposition** (Kriterium für zyklische Gruppen)

Seien G eine endliche Gruppe und für alle $d \mid |G|$ gelte:

$$\left|\left\{x \in G | x^d = e\right\}\right| \leq d \tag{1.12}$$

Dann ist G zyklisch.

Beweis

Für $d \mid |G| =: n$ setze $\psi(d) := |\{x \in G | \text{ord}(x) = d\}|$.
Aus 1.25 folgt dann:

$$\sum_{1 \leq d | n} \psi(d) = |G| = n \tag{1.13}$$

Seien $d|n$ und es gelte $\psi(d) \neq 0$, das heißt es gibt ein $z \in G$ mit $\text{ord}(z) = d$.
Aus 1.25 folgt für alle $g \in \langle z \rangle$ schon $g^d = e$.
Aus $|\langle z \rangle| = d$ und (1.12) folgt damit $\left\{x \in G | x^d = e\right\} \subseteq \langle z \rangle$ und insbesondere:

$$\{x \in G | \text{ord}(x) = d\} \subseteq \langle z \rangle \cong \mathbb{Z}/d\mathbb{Z}$$

Es gilt aber:

$$\left|\left\{\omega \in \left(\mathbb{Z}/d\mathbb{Z}\right) | \text{ord}(\omega) = d\right\}\right| = \left|\left(\mathbb{Z}/d\mathbb{Z}\right)^*\right| = \varphi(d)$$

Insgesamt folgt für alle $d \in \mathbb{Z}$ mit $d \mid |G|$:

$$\psi(d) \leq \varphi(d) \tag{1.14}$$

Denn für $\psi(d) = 0$ ist das trivial.
Die Summation liefert:

$$|G| \overset{(1.13)}{=} \sum_{1 \leq d | n} \psi(d) \overset{(1.14)}{\leq} \sum_{1 \leq d | n} \varphi(d) = n$$

Dann muss (1.14) für alle $d|n$ eine Gleichheit sein, insbesondere für $d = n$ folgt wegen $1 \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$:

$$\psi(n) = \varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right| \neq 0$$

Das heißt es gibt ein $x \in G$ mit $\text{ord}(x) = n$, also ist $G = \langle x \rangle$ und G ist zyklisch. $\square_{1.27}$

1.28 Korollar

Seien k ein Körper und $G \subseteq k^*$ eine endliche Untergruppe.
Dann ist G zyklisch.

Bemerkung

Die Gruppe $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$ ist nicht zyklisch.

Beweis von 1.28

Wegen 1.27 zeige nur, dass für alle $d \geq 1$ gilt:

$$\left|\left\{x \in k^* | x^d = 1\right\}\right| \leq d$$

Das ist klar, denn das Polynom $T^d - 1 \in k[T]$ hat höchstens d Nullstellen in k nach linearer Algebra II. $\square_{1.28}$

1.29 Bemerkung

$\mathbb{Q}^*$ ist nicht zyklisch (!), also kann man in 1.28 nicht auf „endlich“ verzichten.

1.30 Korollar

i) Ist k ein endlicher Körper, so ist k^* zyklisch.

ii) Ist p eine Primzahl, so ist $\mathbb{F}_p^*$ zyklisch. (vergleiche 1.24)

Beweis

i) 1.28 für $G := k^*$.

ii) Folgt aus i) für $k = \mathbb{F}_p$.

$\square_{1.30}$

2 Lokalisierungen

Stichworte

(kommutativer) Ring, Ringhomomorphismus, Integritätsring (Abkürzung: IR), Modul, Tensorprodukt, Primideal, Einheiten, exakte Folge

Referenz

Siehe Literaturliste am Anfang.

2.1 Proposition und Definition (multiplikativ abgeschlossen)

Seien A,B kommutative Ringe, $\varphi : A \to B$ ein Ringhomomorphismus und $S : \varphi^{-1}(B^*) \subseteq A$.
Dann gelten:

i) $1 \in S$

ii) $\underset{s,t \in S}{\forall} st \in S$

Eine Teilmenge $S \subseteq A$ mit i), ii) heißt *multiplikativ abgeschlossen.*

Beweis

i) $\varphi(1) = 1 \in B^* \Rightarrow 1 \in \varphi^{-1}(B^*) = S$

ii) $s,t \in S \Rightarrow \varphi(s), \varphi(t) \in B^* \Rightarrow B^* \ni \varphi(s) \cdot \varphi(t) = \varphi(st) \Rightarrow st \in S$

$\square_{2.1}$

Fixiere in Kapitel 2 (Lokalisierungen)

Seien A ein kommutativer Ring und $S \subseteq A$ multiplikativ abgeschlossen.

2.2 Konstruktion und Definition (Quotientenring)

Die Relation auf der Menge $A \times S$ definiert durch

$$\underset{(a,s),(h,t) \in A \times S}{\forall} (a,s) \sim (b,t) :\Leftrightarrow \underset{u \in S}{\exists} u(at - bs) = 0 \tag{2.1}$$

ist eine Äquivalenzrelation.

Schreibe für alle $(a,s) \in A \times S$ für die Äquivalenzklasse $[(a,s)] =: \frac{a}{s}$ von (a,s) und:

$$S^{-1}A := \left\{ \frac{a}{s} \middle| (a,s) \in A \times S \right\}$$

Damit gilt:

$$\frac{a}{s} = \frac{b}{t} \in S^{-1}A \Leftrightarrow \underset{u \in S}{\exists} u\,(at - bs) = 0$$

Die Abbildungen

$$+ : S^{-1}A \times S^{-1}A \to S^{-1}A, \left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \left(\frac{at+bs}{st}\right)$$
$$\cdot : S^{-1}A \times S^{-1}A \to S^{-1}A, \left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \left(\frac{ab}{st}\right)$$

sind wohldefiniert und

$$\left(S^{-1}A, +, \cdot, \frac{0}{1}, \frac{1}{1}\right)$$

ist ein kommutativer Ring, der *Quotientenring von A bezüglich S*.

2.3 **Beispiel** (Quotientenkörper)

Ist A in 2.2 ein Integritätsring und gilt $0 \notin S$, so vereinfacht sich (2.1) zu:

$$\frac{a}{s} = \frac{b}{t} \in S^{-1}A \Leftrightarrow at = bs \in A$$

Die Teilmenge $A \setminus \{0\} \subseteq A$ ist multiplikativ abgeschlossen und der Ring

$$\text{Quot}\,(A) := (A \setminus \{0\})^{-1}\,A = \left\{ \frac{a}{s} \middle| a \in A, 0 \neq s \in A \right\}$$

heißt *der Quotientenkörper von A*, zum Beispiel $\text{Quot}\,(\mathbb{Z}) = \mathbb{Q}$.

Beweis von 2.2

Die Reflexivität und Symmetrie von $\sim$ sind klar.
Seien $a,b,c \in A$, $s,t,u \in S$ mit $(a,s) \sim (b,t)$ und $(b,t) \sim (c,u)$. gegeben.
Dann folgt aus (2.1), dass es $v,w \in S$ gibt mit:

$$\begin{array}{rcl} (at - bs) \cdot v = 0 \quad / \cdot uw & & (bu - ct) \cdot w = 0 \quad / \cdot sv \\ atvuw = bsvuw & = & buwsv = ctwsv \end{array}$$

Damit folgt in A:

$$(au - cs)\,tvw = 0$$

Wegen $tvw \in S$ folgt aus (2.1) schon $(a,s) \sim (c,u)$.
Also ist $\sim$ eine Äquivalenzrelation.
TODO: Restlichen Beweis als Übung einfügen

$\square_{2.2}$

2.4 Proposition (Universelle Eigenschaft von $S^{-1}A$)

i) Die Abbildung

$$\varphi : A \to S^{-1}A, \varphi(a) := \frac{a}{1}$$

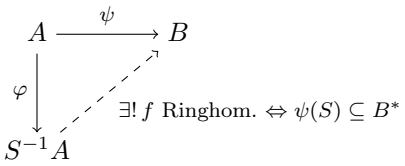
ist ein Ringhomomorphismus.

ii) Für einen Ringhomomorphismus $\psi : A \to B$ (mit B kommutativ) sind äquivalent:

a) $\psi(S) \subseteq B^*$

b) Es existiert genau ein Ringhomomorphismus $f : S^{-1}A \to B$ mit $\psi = f \circ \varphi$.

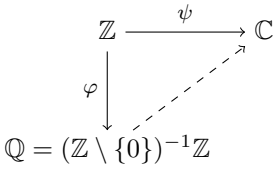
Kommutatives Diagramm



Beispiel

Es gibt genau einen Ringhomomorphismus $\mathbb{Q} \to \mathbb{C}$, denn:
Es gibt genau einen Ringhomomorphismus $\psi : \mathbb{Z} \to \mathbb{C}$ und es gilt $\psi(\mathbb{Z} \setminus \{0\}) \subseteq \mathbb{C}^*$.

Kommutatives Diagramm



Beweis von 2.4

i) $\varphi : A \to S^{-1}A, a \to \frac{a}{1}$ ist ein Ringhomomorphismus.
Rechne zum Beispiel $\varphi(a) + \varphi(b) = \varphi(a+b)$ nach:

$$\varphi(a) + \varphi(b) = \frac{a}{1} + \frac{b}{1} \overset{2.2}{=} \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a+b}{1} = \varphi(a+b)$$

Der Rest geht analog. $\square_{i)}$

ii) b) $\Rightarrow$ a): Es gilt $\varphi(S) \subseteq \left(S^{-1}A\right)^*$, denn für alle $s \in S$ folgt in $S^{-1}A$:

$$\frac{1}{s} \cdot \varphi(s) = \frac{1}{s} \cdot \frac{s}{1} = 1$$

Damit ergibt sich:

$$\psi(s) \overset{b)}{=} f(\varphi(s)) \overset{\varphi(S) \subseteq \left(S^{-1}A\right)^*}{=} f\left(\left(S^{-1}A\right)^*\right) \overset{\text{klar}}{\subseteq} B^*$$

a) $\Rightarrow$ b):

– *Eindeutigkeit:* Für alle $a \in A$,$s \in S$ gilt:

$$f\left(\frac{a}{s}\right) = f\left(\frac{a}{1} \cdot \left(\frac{s}{1}\right)^{-1}\right) = f\left(\varphi(a) \cdot \varphi(s)^{-1}\right) = \psi(a) \cdot \psi(s)^{-1}$$

Daher ist f eindeutig bestimmt.

– *Existenz:* Zeige nur, dass die Abbildung

$$f : S^{-1}A \dashrightarrow B, \frac{a}{s} \mapsto \psi(a) \cdot \psi(s)^{-1}$$

wohldefiniert ist.
Zunächst gilt nach a) für alle $s \in S$:

$$\psi(s) \in B^* \Rightarrow \underset{b \in B^*}{\exists} : \underbrace{b}_{=:\psi(s)^{-1}} \cdot \psi(s) = 1$$

Zeige noch, dass für alle a,$b \in A$ und für alle s,$t \in S$ mit

$$\frac{a}{s} = \frac{b}{t}$$

in $S^{-1}A$ schon in B gilt:

$$\psi(a)\,\psi(s)^{-1} = \psi(b)\,\psi(t)^{-1}$$

Beweis
Aus $\varphi(S) \subseteq \left(S^{-1}A\right)^*$ in 2.2 folgt in A:

$$\underset{u \in S}{\exists} : u(at - bs) = 0$$

Weil ψ eindeutig ist, folgt in B:

$$\begin{aligned} \psi(u) \cdot (\psi(a)\,\psi(t) - \psi(b)\,\psi(s)) &= 0 \\ \psi(a)\underbrace{\psi(t)}_{\in B^*} &= \psi(b)\underbrace{\psi(s)}_{\in B^*} \\ \psi(a)\,\psi(s)^{-1} &= \psi(b)\,\psi(t)^{-1} \end{aligned}$$

$\square_{2.4}$

2.5 Korollar

i) $\ker\left(\varphi : A \to S^{-1}A\right) = \{a \in A \mid \exists_{s \in S} : a \cdot s = 0 \in A\}$

ii) $S^{-1}A = \{0\} \Leftrightarrow 0 \in S$

Beweis

i) Für alle $a \in A$ gilt in $S^{-1}A$:

$$\frac{0}{1} = \varphi(a) = \frac{a}{1}$$

Dies ist nach 2.2 äquivalent dazu, dass es ein $s \in S$ gibt, für dass in A gilt:

$$0 = s \cdot (a \cdot 1 - 0 \cdot 1) = s \cdot a$$

$\square_{\text{i)}}$

ii) Es gilt:

$$S^{-1}A = \{0\} \Leftrightarrow \frac{1}{1} = \frac{0}{1}$$

Dies ist definitionsgemäß äquivalent dazu, dass es ein $s \in S$ gibt mit:

$$0 = s\underbrace{(1 \cdot 1 - 0 \cdot 1)}_{=1} = s$$

Das bedeutet $s = 0 \in S$.

$\square_{2.5}$

2.6 **Beispiel** (Lokalisierung)

Seien A ein Integritätsring und $\mathfrak{p} \subseteq A$ ein Primideal.
Dann ist $A \setminus \{\mathfrak{p}\} \subseteq A$ multiplikativ abgeschlossen und

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} A$$

heißt *Lokalisierung von A bei $\mathfrak{p}$*.
Es gilt $A \subseteq A_{\mathfrak{p}} \subseteq A_{(0)} = \mathrm{Quot}\,(A)$.
Für $A = \mathbb{Z}$ und $\mathfrak{p} = (p)$ (für eine Primzahl $p \in \mathbb{Z}$) gilt zum Beispiel:

$$A = \mathbb{Z} \subseteq A_{\mathfrak{p}} = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \middle| a,b \in \mathbb{Z}, p \not| b \right\} \subseteq A_{(0)} = \mathbb{Q}$$

Einheiten:

$$\{\pm 1\} \subseteq \mathbb{Z}_{(p)}^* \overset{(!)}{=} \mathbb{Z}_{(p)} \setminus (p) = \left\{ \frac{a}{b} \middle| a,b \in \mathbb{Z}, p \not| a,b \right\} \subseteq \mathbb{Q} \setminus \{0\}$$

Beweis

Zeige nur, dass $A \setminus \mathfrak{p} \subseteq A$ multiplikativ abgeschlossen ist, prüfe also die Definition 2.1 i) und ii) für $S = A \setminus \mathfrak{p}$:

i) $1 \in A \setminus \mathfrak{p}$, sonst gilt $1 \in \mathfrak{p}$, dass bedeutet $\mathfrak{p} = A$, weil $\mathfrak{p}$ ein Ideal ist. Dies steht im Widerspruch zur Definition eines „Primideals“.

ii) $s,t \in A \setminus \mathfrak{p} \Rightarrow st \in A \setminus \mathfrak{p}$, denn sonst wäre $st \in \mathfrak{p}$, und weil $\mathfrak{p}$ ein Primideal ist, folgt damit:

$$\begin{aligned} & (s \in \mathfrak{p}) \vee (t \in \mathfrak{p}) \\ \Rightarrow \quad & (s \notin A \setminus \mathfrak{p}) \vee (t \notin A \setminus \mathfrak{p}) \end{aligned}$$

Dies ist ein Widerspruch zu $s,t \in A \setminus \mathfrak{p}$.

$\square_{2.6}$

2.7 **Konstruktion** (Lokalisierung)

Seien M und N zwei A-Moduln und $S \subseteq A$ multiplikativ abgeschlossen.
Auf der Menge $M \times S$ ist folgende Relation in M

$$(m,s) \sim (m',t) :\Leftrightarrow \underset{u \in S}{\exists} : u\,(tm - sm') = 0$$

eine Äquivalenzrelation.
Schreibe $S^{-1}M := {}^{(M \times S)}\big/_{\sim}$ und $\dfrac{m}{s} := [(m,s)] \in S^{-1}M$ für alle $(m,s) \in M \times S$.
Dann ist $S^{-1}M$ ein $S^{-1}A$-Modul vermöge:

$$\frac{m}{s} + \frac{m'}{t} := \frac{tm + sm'}{st}$$
$$\frac{a}{s} \cdot \frac{m}{t} := \frac{a \cdot m}{st}$$

($m,m' \in M$, $a \in A$, $s,t \in S$)
Ist $\varphi : M \to N$ A-linear, so ist

$$S^{-1}\varphi : S^{-1}M \to S^{-1}N$$
$$\left(S^{-1}\varphi\right)\left(\frac{m}{s}\right) := \frac{\varphi\,(m)}{s}$$

$S^{-1}A$-linear.

Beweis

Analog zu 2.2. $\square_{2.7}$

2.8 Proposition

Sei

$$M \overset{\varphi}{\to} N \overset{\psi}{\to} P \tag{2.2}$$

eine exakte Folge von A-Moduln, das heißt $\operatorname{im}(\varphi) = \ker(\varphi)$.
Dann ist auch die Folge von $S^{-1}A$-Moduln

$$S^{-1}M \overset{S^{-1}\varphi}{\longrightarrow} S^{-1}N \overset{S^{-1}\psi}{\longrightarrow} S^{-1}P$$

exakt.

Beweis

Zeige: $\operatorname{im}\left(S^{-1}\varphi\right) = \ker\left(S^{-1}\psi\right)$
„$\subseteq$“: Folgt aus:

$$S^{-1}\psi \circ S^{-1}\varphi \overset{(!)}{=} S^{-1}\,(\psi \circ \varphi) \overset{(2.2)\text{ exakt}}{=} S^{-1}\,(0) = 0$$

„$\supseteq$“: Sei $x \in \ker\left(S^{-1}\psi\right)$, dann gibt es ein $n \in N$ und ein $s \in S$ mit $x = \dfrac{n}{s}$, weswegen gilt in $S^{-1}P$:

$$0 = \left(S^{-1}\psi\right)(x) = \left(S^{-1}\psi\right)\left(\frac{n}{s}\right) \overset{2.7}{=} \frac{\psi\,(n)}{s}$$

Nach 2.7 gibt es ein $t \in S$, für das in P gilt:

$$\psi(ts \cdot n) = ts \cdot \psi(n) = 0$$

Daher ist $ts \cdot n \in \ker(\psi) \overset{\text{Vor.}}{=} \operatorname{im}(\varphi)$.
Also gibt es ein $m \in M$, für das in N gilt:

$$\varphi(m) = ts \cdot n$$

Damit folgt:

$$\left(S^{-1}\varphi\right)\left(\frac{m}{ts^2}\right) = \frac{\varphi(m)}{ts^2} = \frac{t \cdot s \cdot n}{ts^2} = \frac{n}{s} = x \in \operatorname{im}\left(S^{-1}\varphi\right)$$

$\square_{2.8}$

2.9 Proposition

Sei M ein A-Modul.
Dann existiert genau eine A-lineare Abbildung

$$f : S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$$

mit

$$f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s}$$

für alle $a \in A$,$s \in S$ und $m \in M$ und f ist $S^{-1}A$-linear und ein Isomorphismus.

Beweis

Wegen der universellen Eigenschaft des Tensorprodukts ist die eindeutige Existenz von f äquivalent dazu, dass die Abbildung

$$\begin{aligned} S^{-1}A \times M &\to S^{-1}M \\ \left(\frac{a}{s}, m\right) &\mapsto \frac{am}{s} \end{aligned}$$

A-bilinear ist. Dies sieht man leicht.
f ist sogar $S^{-1}A$-linear, da gilt:

$$f\left(\frac{a}{s} \cdot \left(\frac{b}{t} \otimes m\right)\right) = f\left(\frac{ab}{st} \otimes m\right) = \frac{abm}{st} = \frac{a}{s} \cdot f\left(\frac{b}{t} \otimes m\right)$$

Nach 2.7 ist klar, dass f surjektiv ist, denn $\frac{m}{s} = f\left(\frac{1}{s} \otimes m\right)$.

Behauptung
Für alle $x \in S^{-1}A \otimes_A M$ existieren $t \in S$ und $m \in M$ mit:

$$x = \frac{1}{t} \otimes m$$

Beweis
Zunächst ist x eine endliche Summe

$$x = \sum_i \underbrace{\frac{a_i}{s_i} \otimes m_i}_{\text{„elementarer Tensor“}} \tag{2.3}$$

mit geeigneten $a_i \in A$,$s_i \in S$ und $m_i \in M$.
Definiere:

$$t := \prod_j s_j \qquad\qquad t_i := \frac{t}{s_i} = \prod_{j \neq i} s_j \in S \tag{2.4}$$

Damit folgt:

$$tx \overset{(2.3)}{=} \sum_i \left(\frac{a_i}{s_i} \cdot t \right) \otimes m_i \overset{(2.4)}{=} \sum_i \underbrace{(a_i t_i)}_{\in A} \otimes m_i = \sum_i (1 \otimes (a_i t_i m_i)) = 1 \otimes \underbrace{\left(\sum_i a_i t_i m_i \right)}_{=:m \in M}$$

Daraus folgt in $S^{-1}A \otimes_A M$:

$$x = \frac{1}{t} \otimes m$$

$\square_{\text{Behauptung}}$

f ist injektiv: Sei $x \in \ker(f)$, dann folgt aus obiger Behauptung:

$$x = \frac{1}{t} \otimes m \tag{2.5}$$

Für geeignete $t \in S$ und $m \in M$.
Damit folgt in $S^{-1}M$:

$$0 = f(x) \overset{(2.5)}{=} \frac{m}{t}$$

Und deswegen gibt es ein $s \in S$, für das in M gilt:

$$0 = s \cdot t \cdot m \tag{2.6}$$

Damit ergibt sich:

$$x \overset{(2.5)}{=} \frac{1}{t} \otimes m = \frac{1}{t^2 s} \otimes \underbrace{(stm)}_{=0} = 0$$

Es folgt $\ker(f) = 0$, also ist f injektiv. $\square_{2.9}$

2.10 Beispiel

Sei $M \overset{\varphi}{\to} N \overset{\psi}{\to} P$ eine exakte Folge abelscher Gruppen(, das heißt $\mathbb{Z}$-Moduln).
Dann ist die Folge von $\mathbb{Q}$-Vektorräumen(, das heißt $S^{-1}\mathbb{Z}$-Moduln für $S = \mathbb{Z} \setminus \{0\}$,)

$$M \otimes_{\mathbb{Z}} \mathbb{Q} \overset{\varphi \otimes \mathrm{id}_{\mathbb{Q}}}{\to} N \otimes_{\mathbb{Z}} \mathbb{Q} \overset{\psi \otimes \mathrm{id}_{\mathbb{Q}}}{\to} P \otimes_{\mathbb{Z}} \mathbb{Q}$$

exakt.

Beweis

Betrachte das Diagramm:

$$\begin{array}{ccccc} M \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{\varphi \otimes \mathrm{id}} & N \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{\psi \otimes \mathrm{id}} & P \otimes_{\mathbb{Z}} \mathbb{Q} \\ \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\ (\mathbb{Z} \setminus \{0\})^{-1} M & \xrightarrow{(\mathbb{Z} \setminus \{0\})^{-1} \varphi} & (\mathbb{Z} \setminus \{0\})^{-1} N & \xrightarrow{(\mathbb{Z} \setminus \{0\})^{-1} \psi} & (\mathbb{Z} \setminus \{0\})^{-1} P \end{array}$$

Nach 2.8 mit $A = \mathbb{Z}$, $S = \mathbb{Z} \setminus \{0\}$ ist die zweite Zeile exakt.
Die senkrechten Isomorphismen sind wie in 2.9, beachte $S^{-1}A \cong \mathbb{Q}$.
Man prüft, dass das Diagramm kommutiert, das heißt man prüft, dass eines der Quadrate kommutiert.
(vergleiche Übungsaufgaben aus linearer Algebra II)
TODO: Restlichen Beweis einfügen
Es folgt die Exaktheit der ersten Zeile. $\square_{2.10}$

3 Der Satz von Gauß

Fixiere in Kapitel 3 (Der Satz von Gauß)

Seien R ein faktorieller Ring, $Q := \operatorname{Quot}(R) = (R \setminus \{0\})^{-1} R$ und $\mathcal{P} \subseteq R$ ein Vertretersystem der Primelemente bis auf Assoziiertheit.

Beispiel

- $R = \mathbb{Z}$, $\mathcal{P} = \{2,3,5,7,\ldots\}$ (positive Primzahlen)
- $R = k[X]$ (für einen Körper k), $\mathcal{P} = \{f \in R | f \text{ ist normiert und irreduzibel}\}$
- $R = \mathbb{Z}[\mathbf{i}]$, $\mathcal{P} =$?

3.1 **Erinnerung** (Primfaktorzerlegung)

Für alle $p \in \mathcal{P}$ ist

$$\begin{aligned} \nu_p : Q^* &\to \mathbb{Z} \\ \frac{a}{b} &\mapsto \nu_p(a) - \nu_p(b) \end{aligned}$$

die *p-adische Bewertung von* $\frac{a}{b}$ ein Homomorphismus und für alle $a \in R \setminus \{0\}$ ist mit einem geeigneten $\varepsilon \in R^*$ die *Primfaktorzerlegung*:

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$$

Die Abbildung

$$\begin{aligned} R^* \oplus \left(\bigoplus_{p \in \mathcal{P}} \mathbb{Z} \right) &\xrightarrow{\sim} \mathbb{Q}^* \\ (\varepsilon, (\nu_p)) &\mapsto \varepsilon \cdot \prod_{p \in \mathcal{P}} p^{\nu_p} \end{aligned}$$

ist ein Isomorphismus von Gruppen mit der inversen Abbildung:

$$q \mapsto \left(\frac{q}{\prod_{p \in \mathcal{P}} p^{\nu_p}}, (\nu_p(q))_{p \in \mathcal{P}} \right)$$

Für alle $q \in Q^*$ gilt:

$$q \in R \Leftrightarrow \underset{p \in \mathcal{P}}{\forall} : \nu_p(q) \geq 0 \tag{3.1}$$

Setze $\nu_p(0) := \infty$ für alle $p \in \mathcal{P}$.

3.2 Bemerkung

Für jeden Ringhomomorphismus $\varphi : R \to R'$ existiert genau ein Ringhomomorphismus

$$\varphi[X] : R[X] \to R'[X]$$

mit $\varphi[X]\left(\sum_i a_i X^i\right) = \sum_i \varphi(a_i) X^i$.
Es gilt:

$$\ker(\varphi[X]) = \left\{ \sum_i a_i X^i \middle| a_i \in \ker(\varphi) \subseteq R \right\}$$

Ist zum Beispiel $p \in R$, so ist

$$\pi : R[X] \to \left(R/(p)\right)[X]$$
$$\sum_i a_i X^i \mapsto \sum_i (a_i \bmod p) X^i$$

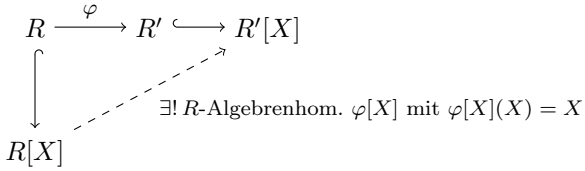
ein surjektiver Ringhomomorphismus mit:

$$\ker(\pi) = \left\{ \sum_i a_i X^i \middle| \forall_i : p | a_i \right\} \tag{3.2}$$

(Wähle $\varphi : R \to R'$ als den kanonischen Homomorphismus $R \to R/(p)$.)

Beweis

Betrachte:



Es existiert genau ein R-Algebrenhomomorphismus $\varphi[X]$ mit $\varphi[X](X) = X$.
Daher gilt:

$$\varphi[X]\left(\sum_i \underbrace{a_i}_{\in Q} X^i\right) = \sum_i \underbrace{\varphi[X](a_i)}_{=\varphi(a_i)} \cdot \underbrace{\varphi[X](X)^i}_{=X^i} = \sum_i \varphi(a_i) \cdot X^i$$

$\square_{3.2}$

3.3 Proposition und Definition (Lemma von Gauß)

Sei $p \in \mathcal{P}$. Für $f = \sum_i a_i X^i \in Q[X]$ heißt $\nu_p(f) = \min_i \{\nu_p(a_i)\} \in \mathbb{Z} \cup \{\infty\}$ *die p-adische Bewertung von* f. ($Q \subseteq Q[X]$).
Zum Beispiel ist:

$$\nu_3\left(7X^2 + \frac{1}{8}X + 27\right) = \min\left\{\nu_3(7) = 0, \nu_3\left(\frac{1}{8}\right) = 0, \nu_3(27) = 3\right\} = 0$$

Es gelten:

i) $f = 0 \Leftrightarrow \forall_{p \in \mathcal{P}} : \nu_p(f) = \infty$

ii) $f \in R[X] \Leftrightarrow \forall_{p \in \mathcal{P}} : \nu_p(f) \geq 0$

iii) Lemma von Gauß: $\forall_{f,g \in Q[X]} : \nu_p(fg) = \nu_p(f) + \nu_p(g)$

Beweis

i) $\forall_p : \nu_p(f) = \infty \Leftrightarrow \forall_{p,i} : \nu_p(a_i) = \infty \overset{3.1}{\Leftrightarrow} \forall_i : a_i = 0 \Leftrightarrow f = 0$

ii) $f \in R[X] \Leftrightarrow \forall_i : a_i \in R \overset{3.1}{\Leftrightarrow} \forall_{p \in \mathcal{P}, i} : \nu_p(a_i) \geq 0 \Leftrightarrow \forall_{p \in \mathcal{P}} \nu_p(f) \geq 0$

iii) 1. Fall: $f \in Q \subseteq Q[X]$ und $g \in Q[X]$ beliebig.
Schreibe $g = \sum_i b_i X^i$. Dann folgt:

$$\nu_p(f \cdot g) = \nu_p\left(\sum_i (fb_i) X^i\right) \overset{\text{Def.}}{=} \min\{\nu_p(fb_i)\} \overset{3.1,\ \text{da } f \in Q}{=} \min\{\nu_p(f) + \nu_p(b_i)\} =$$
$$= \nu_p(f) + \min\{\nu_p(b_i)\} = \nu_p(f) + \nu_p(g)$$

2. (allgemeiner) Fall: Seien ohne Einschränkung $f,g \neq 0$, sonst ist nur $\infty = \infty$ zu zeigen.
Wegen dem 1. Fall dürfen f und g durch αf und βg mit beliebigen $\alpha,\beta \in Q^*$ ersetzt werden.
Für geeignete $\alpha,\beta \in Q^*$ gilt:

$$\tilde{f} := \alpha f, \tilde{g} := \beta g \in R[X]$$

$$\nu_p\left(\tilde{f}\right) = 0 \qquad\qquad \nu_p(\tilde{g}) = 0$$

Dann ist $\nu_p\left(\tilde{f}\tilde{g}\right) = 0$ zu zeigen:

Sei $\pi : R[X] \to \left(R/_{(p)}\right)[X]$ wie in 3.2. Für $\tilde{f} = \sum_i a_i X^i$ gilt:

$$0 = \nu_p\left(\tilde{f}\right) = \min_i\{\underbrace{\nu_p(a_i)}_{\geq 0 \left(\text{da } \tilde{f} \in R[X]\right)}\}$$

Also gibt es ein i mit $\nu_p(a_i) = 0$, das heißt $p \nmid a_i$. Nach 3.2 folgt damit $\pi\left(\tilde{f}\right) \neq 0$.

Analog gilt: $\pi(\tilde{g}) \neq 0$ und es folgt in $\left(R/_{(p)}\right)[X]$, weil dies ein Integritätsring ist:

$$0 \neq \underbrace{\pi\left(\tilde{f}\right)}_{\neq 0} \cdot \underbrace{\pi(\tilde{g})}_{\neq 0} = \pi\left(\tilde{f}\tilde{g}\right)$$

Wie oben folgt $\nu_p\left(\tilde{f}\tilde{g}\right) = 0$.

$\square_{3.3}$

3.4 Korollar

Sei $h \in R[X]$ normiert und es gelte in $Q[X]$ mit normierten $f,g \in Q[X]$:

$$h = f \cdot g \tag{3.3}$$

Dann gilt $f,g \in R[X]$.

Beweis

Für alle $p \in \mathcal{P}$ gelten $\nu_p(h) = 0$, da h in $R[X]$ normiert ist und $\nu_p(1) = 0$, sowie $\nu_p(f), \nu_p(g) \leq 0$, da f,g in $Q[X]$ normiert sind.
Weil für alle $p \in \mathcal{P}$

$$0 = \nu_p(h) \overset{(3.3)}{\underset{3.3 \text{ iii)}}{=}} \underbrace{\nu_p(f)}_{\leq 0} + \underbrace{\nu_p(g)}_{\leq 0}$$

gilt, folgt:

$$\nu_p(f) = \nu_p(g) = 0$$

Daher sind $f,g \in R[X]$. $\square_{3.4}$

3.5 Beispiel

Seien $h = \sum_i a_i X^i \in R[X]$ normiert und $\alpha \in Q$ mit $h(\alpha) = 0$.
Dann folgt $\alpha \in R$ und $\alpha | a_o$ in R.

Beweis

Aus $h(\alpha) = 0$ folgt $h = (X - \alpha) \cdot g$ in $Q[X]$ für ein geeignetes $g \in Q[X]$.
Weil h und $(X - \alpha)$ normiert sind, ist auch g normiert.
Aus 3.4 folgt $(X - \alpha), g \in R[X]$, also insbesondere $\alpha \in R$.
Ferner gilt in R:

$$0 = h(\alpha) = \sum_{i \geq 0} a_i \alpha^i = \alpha \left(\sum_{i \geq 1} a_i \alpha^{i-1} \right) + a_0$$

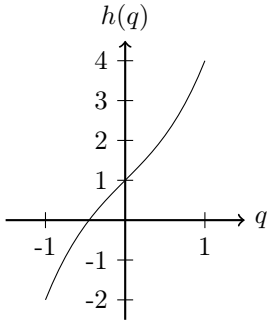
$$a_0 = \alpha \cdot \underbrace{\left(- \sum_{i \geq 1} a_i \alpha^{i-1} \right)}_{\in R, \text{ da } a_i, \alpha \in R}$$

Also gilt $\alpha | a_0$ in R. $\square_{3.5}$

3.6 Beispiel

Es existiert keine rationale Zahl $q \in \mathbb{Q}$ mit $q^3 + 2q + 1 = 0$, obwohl diese Gleichung, wie jede Gleichung dritten Grades, eine Lösung in $\mathbb{R}$ hat.

Skizze



Beweis

$h := X^3 + 2X + 1 \in \mathbb{Z}[X]$ ist normiert und $R := \mathbb{Z}$ ist ein Hauptidealring, also insbesondere faktoriell. Gäbe es ein $q \in \mathbb{Q} = \text{Quot}(R)$ mit $h(\alpha) = 0$, so folgte aus 3.5 schon $q \in \mathbb{Z}$ und $q | a_0 = 1$, das heißt $q \in \{\pm 1\}$, aber es gilt:

$$h(\pm 1) = 1 \pm 3 \neq 0$$

$\square_{3.6}$

3.7 Proposition und Definition (primitiv)

Für $f = \sum_i a_i X^i \in R[X]$ gilt:

i) $\underset{p \in \mathcal{P}}{\forall} : \nu_p(f) = 0 \Leftrightarrow \text{ggT}(a_0, a_1, \ldots) = 1$; In diesem Fall heißt f *primitiv*.
Also ist jedes normierte Polynom primitiv, aber auch $3X + 2 \in \mathbb{Z}[X]$.

ii) Für alle $f \in Q[X] \setminus \{0\}$ existieren ein $\alpha \in Q^*$ und ein primitives $\tilde{f} \in R[X]$ mit $f = \alpha \cdot \tilde{f}$.

Beweis

i) Für alle $p \in \mathcal{P}$ gilt:

$$\nu_p(\text{ggT}(a_0, a_1, \ldots)) = \min\{\nu_p(a_i)\} = \nu_p(f)$$

Wendet man

$$\underset{q \in Q^*}{\forall} : \left(\underset{p \in \mathcal{P}}{\forall} : \nu_p(q) = 0 \overset{3.1}{\Leftrightarrow} q \in R^* \right)$$

auf $q = \text{ggT}(a_i)$, so folgt:

$$\left(\underset{p \in \mathcal{P}}{\forall} : \nu_p(f) = 0 \right) \Leftrightarrow \text{ggT}(a_i) \in Q^* \Leftrightarrow \text{ggT}(a_i) = 1$$

$\square_{\text{i)}}$

ii) Wegen $f \neq 0$ gilt nach 3.3 i) für alle $p \in \mathcal{P}$ schon $\nu_p(f) \neq \infty$.
Es ist klar, dass für fast alle $p \in \mathcal{P}$ schon $\nu_p(f) = 0$ gilt, nämlich für alle Primzahlen $p \in \mathcal{P}$, die weder Zähler noch Nenner eines Koeffizienten von f teilen.

Deswegen ist $\alpha := \prod_{p \in \mathcal{P}} p^{\nu_p(f)} \in Q^*$ wohldefiniert und für $\tilde{f} := \alpha^{-1} f$ gilt für alle $p \in \mathcal{P}$:

$$\nu_p\left(\tilde{f}\right) = \nu_p\left(\alpha^{-1} f\right) \overset{3.3\text{ iii)}}{=} -\underbrace{\nu_p(\alpha)}_{=\nu_p(f)} + \nu_p(f) = 0$$

Also ist $\tilde{f} \in R[X]$ nach Teil i) primitiv.

$\square_{3.7}$

Beispiel

$$f := \frac{2}{3}x^{\mathbf{2}} + \frac{1}{6} \in \mathbb{Q}[X] \setminus \{0\}$$

Dann gilt:

$$18 \cdot f = 12x^{\mathbf{2}} + 3 \in \mathbb{Z}[X]$$

ist nicht primitiv, aber

$$6 \cdot f = 4x^{\mathbf{2}} + 1 \in \mathbb{Z}[X]$$

ist primitiv.

3.8 Satz (von Gauß)

Der Ring $R[X]$ ist faktoriell.
Für alle $q \in R[X]$ sind äquivalent:

i) $q \in R[X]$ ist ein Primelement (Abkürzung: PE).

ii) Es gilt

$$q \in R \subseteq R[X]$$

und q ist ein Primelement in R oder

$$q \in R[X]$$

ist primitiv und $q \in Q[X]$ ist ein Primelement.

Insbesondere sind für ein primitives Polynom $f \in R[X]$ äquivalent:

a) $f \in R[X]$ ist ein Primelement.

b) $f \in Q[X]$ ist ein Primelement.

3.9 Beispiel

$\mathbb{Z}[X]$ ist faktoriell, aber kein Hauptidealring, denn zum Beispiel ist $(2,X) \subseteq \mathbb{Z}[X]$ kein Hauptideal.
Das Polynom $2X \in \mathbb{Z}[X]$ ist nicht primitiv, $2X \in \mathbb{Q}[X]$ ist ein Primelement, da $2 \in (\mathbb{Q}[X])^* = \mathbb{Q}^*$ und $X \in \mathbb{Q}[X]$ ein Primelement ist, aber $2X \in \mathbb{Z}[X]$ hat die Primfaktorzerlegung $2X = 2 \cdot X$ in $\mathbb{Z}[X]$ und 2 und X sind nicht assoziierte Primelemente in $\mathbb{Z}[X]$.

$$\mathbb{Z}[X]/(2) \cong \mathbb{F}_2[X]$$
$$\mathbb{Z}[X]^* = \mathbb{Z}^* = \{\pm 1\}$$

Beweis von 3.8

ii) $\Rightarrow$ i):

- 1. Fall: Es ist $q \in R$ ein Primelement, also ist $\pi : R[X] \twoheadrightarrow \left(R/(q)\right)[X]$ wie in 3.2 surjektiv mit:

  $$\ker(\pi) = (q) \subseteq R[X]$$

  Also folgt aus dem Isomorphiesatz:

  $$\left(R/(q)\right)[X] \cong R[X]/(q) \tag{3.4}$$

  Weil $q \in R$ ein Primelement ist, ist die linke Seite von (3.4) ein Integritätsring, also ist auch $R[X]/(q)$ ein Integritätsring, was äquivalent dazu ist, dass $q \in R[X]$ ist ein Primelement ist.

- 2. Fall: $q \in R[X]$ ist primitiv und $q \in Q[X]$ ist ein Primelement.
  Zeige nach Definition, dass $q \in R[X]$ ein Primelement ist:
  Seien f,$g \in R[X]$ mit $q|fg$ in $R[X]$ gegeben, dann folgt $q|fg$ in $Q[X]$ und ohne Einschränkung folgt, weil $q \in Q[X]$ ein Primelement ist, schon $q|f$ in $Q[X]$.
  Damit ergibt sich in $Q[X]$ mit einem geeigneten $h \in Q[X]$:

  $$f = qh \tag{3.5}$$

  Es folgt für alle $p \in \mathcal{P}$:

  $$0 \underset{q \text{ prim}}{\overset{3.7\text{i})}{=}} v_p(q) \underset{3.3\text{iii})}{\overset{(3.5)}{=}} -v_p(h) + \underbrace{v_p(f)}_{\geq 0 (\text{da } f \in R[X])}$$

  Daher ist $\nu_p(h) \geq 0$ und aus 3.3 ii) folgt dann $h \in R[X]$, also gilt $f = qh$ auch in $R[X]$ und daher $q|f$ in $R[X]$.
  Also ist $q \in R[X]$ ein Primelement. $\square_{\text{ii)} \Rightarrow \text{i)}}$

Zeige noch:
Jedes

$$0 \neq f \in R[X] \setminus R[X]^*$$

(Nebenbemerkung: $R[X]^* = R^*$) ist ein Produkt von Primelementen obiger Gestalt.
Dann folgt sowohl, dass $R[X]$ faktoriell ist, als auch die Implikation i)$\Rightarrow$ii).
Schreibe $f = a \cdot \tilde{f}$ mit $a \in R$,$\tilde{f} \in R[X]$ primitiv (vergleiche 3.7 ii)). Weil R faktoriell ist, ist a ein Produkt von Primelementen obiger Gestalt, also sei ohne Einschränkung $f = \tilde{f} \in R[X]$ primitiv.
Schreibe in $Q[X]$ mit Primelementen $f_i \in Q[X]$ ($Q[X]$ ist ein Hauptidealring, also faktoriell.)

$$f = \prod_{i=1}^{n} f_i \overset{3.7,\text{i})}{=} a \cdot \prod_{i=1}^{n} \tilde{f}_i \tag{3.6}$$

mit $a \in Q^*$ und primitiven Primelementen $\tilde{f}_i \in R[X]$ in $Q[X]$.
Dann folgt für alle $p \in \mathcal{P}$:

$$v_p(a) \overset{3.3\text{iii})}{=} \underbrace{v_p(f)}_{=0} - \sum_{i=1}^{n} \underbrace{v_p\left(\tilde{f}_i\right)}_{=0} = 0$$

Daraus folgt mit 3.1 schon $a \in R^* = Q^*$ und:

$$f = \underbrace{\left(a\tilde{f}_1\right)}_{\text{primitiv, da } a \in R^*} \cdot \prod_{i=2}^{n} \tilde{f}_i$$

Damit ist f ein Produkt von primitiven Faktoren, die Primelemente in $Q[X]$ sind. $\square_{3.8}$

3.10 **Beispiel und Definition** (rationale Funktionen)

Sei k ein Körper. Dann heißt

$$k(X) := \operatorname{Quot}(k[X]) = \left\{ \frac{f}{g} \middle| f,g \in k[X], g \neq 0 \right\}$$

der Körper der rationalen Funktionen (in einer Variablen X über k).
Die k-Algebra $k[X,Y] := (k[X])[Y]$ heißt *der Polynomring in den Variablen X,Y (über k).*
Wegen 3.8 ist $k[X,Y]$ faktoriell.

Behauptung

$f := X^3 + Y^2 \in k[X,Y]$ ist irreduzibel.

Beweis

Wegen 3.8 „Primelement $\Leftrightarrow$ irreduzibel“ folgt mit $R := k[X]$ und weil $f \in R[Y]$ normiert vom Grad 2 ($f = Y^2 + X^3 \cdot Y^0$), also primitiv ist, dass $f \in R[X,Y]$ ein Primelement ist.
Dies ist äquivalent dazu, dass $f \in \operatorname{Quot}(R)[Y] = k(X)[Y]$ irreduzibel ist.
Wegen $\deg(f) = 2$ ist dies äquivalent dazu, dass f keine Nullstelle in $k(X)$ hat, denn angenommen f hat doch eine Nullstelle, so würde in $k(X)$ folgen:

$$\underset{\alpha \in k(X)}{\exists} 0 = f(\alpha) = \alpha^2 + X^3$$

Aus 3.5 mit $h := f$ und $R := k(X)$ folgt $\alpha \in k[X]$, also $-\alpha^2 = X^3$ in $k[X]$ und damit

$$2 \cdot \deg(\alpha) = \deg\left(X^3\right) = 3$$

in $\mathbb{Z}$, was ein Widerspruch ist. $\square_{3.10}$

4 Irreduzibilitätskriterien

Fixiere in Kapitel 4 (Irreduzibilitätskriterien)

Es sei R ein faktorieller Ring und $Q := \text{Quot}(R)$ sein Quotientenkörper.

4.1 **Proposition** (Äquivalenz von Primelement in R und Q)

Sei $0 \neq f \in Q[X]$.

i) Es gibt ein $\alpha \in Q^*$, sodass $\tilde{f} := \alpha f \in R[X]$ primitiv ist.

ii) Folgende Aussagen sind äquivalent:

   a) $\tilde{f} \in R[X]$ ist ein Primelement.

   b) $f \in Q[X]$ ist ein Primelement.

4.2 Bemerkung

Proposition 4.1 führt die Untersuchung von Irreduzibilität von $Q[X]$ auf $R[X]$ zurück.

Beweis von 4.1

i) Die Aussage wurde bereits in 3.7 ii) bewiesen.

ii) b) $\overset{\alpha \in (Q[X])^*}{\Leftrightarrow}$ $\tilde{f} \in Q[X]$ ist ein Primelement $\overset{3.8,\text{a})\Leftrightarrow\text{b})}{\Leftrightarrow}$ a)

$\square_{4.1}$

4.3 **Satz** (Reduktionskriterium)

Seien

$$f = \sum_{i=0}^{d} a_i X^i \in R[X]$$

und $p \in R$ ein Primelement. Es gelte: $p \nmid a_d$ und $d > 0$.
Sei $\pi : R[X] \to \left(R/(p)\right)[X]$ wie in 3.2.
Ist dann $\pi(f) \in \left(R/(p)\right)[X]$ irreduzibel, so auch $f \in Q[X]$.
Ist f zusätzlich primitiv, so ist $f \in R[X]$ irreduzibel.
(„keine Reduktionshomomorphismen auf $Q[X]$“!)

4.4 Beispiel

Wähle in 4.3 zum Beispiel:

i) $R = \mathbb{Z}, p = 3, f = 2X \in \mathbb{Z}[X]$
Dann ist $\pi(f) = -X \in \mathbb{F}_3[X]$ irreduzibel, also ist $2X \in \text{Quot}(R)[X] = \mathbb{Q}[X]$ irreduzibel, aber $2X \in \mathbb{Z}[X]$ ist nicht irreduzibel, vergleiche 3.9. (Hier ist f nicht primitiv.)

ii) $R = \mathbb{Z}, p = 2, f = 2X^2 + X \in \mathbb{Z}[X]$
Dann ist $\pi(f) = X \in \mathbb{F}_2[X]$ irreduzibel, aber $f = X(2X+1) \in \mathbb{Z}[X]$ ist nicht irreduzibel. (Hier gilt $p | a_d$.)

iii) $R = \mathbb{Z}[Y], p = Y, f = 2 \in R[X]$
Dann ist $\pi(f) = 2 \in \left(R/(Y)\right)[X]$ irreduzibel, aber $f = 2 \in Q[X] = \text{Quot}(\mathbb{Z}[Y])$ ist eine Einheit, denn aus $\mathbb{Z} \subseteq \mathbb{Z}[Y]$ folgt $\mathbb{Q} \subseteq \text{Quot}(\mathbb{Z}[Y])$, also ist f nicht irreduzibel. (Hier gilt $d = 0$.)

Beweis von 4.3

1. Fall: Sei f primitiv und $\pi(f)$ irreduzibel.
Angenommen f wäre reduzibel, das heißt $f = gh$ in $R[X]$ mit $g, h \in R[X] \setminus (R[X])^* = R[X] \setminus R^*$.
Weil f primitiv ist, gilt:

$$\deg(g), \deg(h) > 0$$

Wegen $p \nmid a_d$ können die höchsten Koeffizienten von g und h nicht durch p teilbar sein, also gilt:

$$\deg(\pi(g)) = \deg(g) > 0 \qquad \deg(\pi(h)) = \deg(h) > 0 \tag{4.1}$$

Es folgt in $\left(R/(p)\right)[X]$:

$$\pi(f) = \pi(fg) = \pi(g) \cdot \pi(h)$$

und wegen (4.1) gilt:

$$\pi(g) | \pi(h) \notin \left(\left(R/(p)\right)[X]\right)^*$$

Also ist $\pi(f) \in \left(R/(p)\right)[X]$ reduzibel, im Widerspruch zur Voraussetzung. $\square_{\text{1. Fall}}$

2. (allgemeiner) Fall: Sei nun $f \in R[X]$ mit $p \nmid a_d$ und $d > 0$ beliebig.
Dann gibt es ein $c \in R \setminus \{0\}$ und ein primitives Polynom $\tilde{f} \in R[X]$ mit:

$$f = c\tilde{f}$$

Wegen $p \nmid a_d$ gilt $p \nmid c$ in R und $p \nmid \tilde{a}_d$, wobei $\tilde{a}_d$ der höchste Koeffizient von $\tilde{f}$ ist.
Dann gilt in $\left(R/(p)\right)[X]$:

$$\pi(f) = \pi(c) \cdot \pi\left(\tilde{f}\right)$$

Weil $\pi(f)$ irreduzibel ist, muss auch $\pi\left(\tilde{f}\right)$ irreduzibel sein.

Nach dem 1. Fall ist dann $\tilde{f} \in R[X]$ irreduzibel und mit 3.8 folgt, dass $\tilde{f} \in Q[X]$ irreduzibel ist.
Weil $c \in Q^* = (Q[X])^*$ ist, ist $f = c\tilde{f} \in Q[X]$ irreduzibel.

$\square_{4.3}$

4.5 Korollar (Eisensteinkriterium)

Sei $p \in R$ ein Primelement und

$$f = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0 \in R[X]$$

ein primitives Polynom mit:

$$p \nmid a_d \qquad p | a_i \qquad p^2 \nmid a_0$$

$(0 \leq i \leq d-1)$
Dann ist $f \in R[X]$ (und damit nach 3.8 auch $f \in Q[X]$) irreduzibel.

Beweis

Angenommen $f \in R[X]$ wäre reduzibel, dann folgt, weil f primitiv ist, schon $f = gh$ in $R[X]$ mit:

$$g = \alpha_a X^a + \ldots + \alpha_0$$
$$h = \beta_b X^b + \ldots + \beta_0$$

$$\deg(g) > 0 \qquad \deg(h) > 0$$

Also gilt in $\left(R/(p)\right)[X] \subseteq \text{Quot}\left(R/(p)\right)[X] =: \tilde{Q}[X]$:

$$\begin{aligned} \pi(f) &= \pi(g)\,\pi(h) = \\ &= \underbrace{\tilde{a}_d}_{\neq 0} X^d + \underbrace{\tilde{a}_{d-1}}_{\equiv 0} X^{d-1} + \ldots + \underbrace{\tilde{a}_0}_{\equiv 0} \equiv \tilde{a}_d X^d \end{aligned} \tag{4.2}$$

Weil $\tilde{a}_d = \pi(a_d) \in \left(Q/(p)\right)^*$ und $X \in \tilde{Q}[X]$ Primelemente sind, folgt aus der Primfaktorzerlegung in $\tilde{Q}[X]$ und wegen (4.2) folgt mit $\alpha,\beta \in \tilde{Q}^*$, $a,b \geq 0$ und $a+b=d$:

$$\pi(g) = \alpha X^a \qquad \pi(h) = \beta X^b$$

Wegen $p \nmid a_d$ sind die höchsten Koeffizienten von g und h nicht durch p teilbar, also gilt:

$$a = \deg(\pi(g)) > 0 \qquad b = \deg(\pi(h)) > 0$$

Damit sind die konstanten Terme von g und h durch p teilbar, da die konstanten Terme von $\pi(g)$ und $\pi(h)$ schon Null sind.
Es folgt in R:

$$p^2 | \alpha_0 \cdot \beta_0 = a_0$$

Dies ist ein Widerspruch zur Voraussetzung $p^2 \nmid a_0$. $\square_{4.5}$

4.6 Beispiel

i) Für alle $n \in \mathbb{N}_{\geq 1}$ ist $\text{Mipo}_{\mathbb{Q}}\left(\alpha := \sqrt[n]{2}\right) = X^n - 2 =: f(X) \in \mathbb{Q}[X]$

Beweis

$f(\alpha) = 0$ und f ist normiert.
Zeige noch: f ist in $\mathbb{Q}[X]$ irreduzibel.
Dies folgt sofort aus dem Eisensteinkriterium (Korollar 4.5) mit $R = \mathbb{Z}$ und $p = 2$.
Man sagt: „f ist Eisenstein bezüglich 2.“ $\square_{\text{i)}}$

ii) Seien k ein Körper und $n \in \mathbb{N}_{\geq 1}$.
Dann ist $f(X) := X^n - t \in k(t)[X]$ irreduzibel.

Beweis

$R := k[t]$ ist faktoriell mit $\mathrm{Quot}(R) = k(t)$ und $p := t \in R$ ist ein Primelement.
Die Bedingungen in 4.5 sind erfüllt und f ist primitiv, da es normiert ist. $\square_{\text{ii)}}$

iii) Seien p eine Primzahl und $\zeta_p := \exp\left(\frac{2\pi\mathbf{i}}{p}\right) \in \mathbb{C}$.

Dann gilt:

$$\mathrm{Mipo}_{\mathbb{Q}}(\zeta_p) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1 =: f_p(X) \in \mathbb{Q}[X]$$

Beweis

f_p ist normiert und erfüllt:

$$f_p(\zeta_p) = \frac{\zeta_p^p - 1}{\zeta_p - 1} = \frac{\left(\exp\left(\frac{2\pi\mathbf{i}}{p}\right)\right)^p - 1}{\exp\left(\frac{2\pi\mathbf{i}}{p}\right) - 1} = \frac{\overbrace{\exp\left(\frac{p}{p}2\pi\mathbf{i}\right) - 1}^{=0}}{\underbrace{\exp\left(\frac{2\pi\mathbf{i}}{p}\right) - 1}_{\neq 0}} = 0$$

Zeige noch, dass $f \in \mathbb{Q}[X]$ irreduzibel ist:
Es existiert genau ein $\mathbb{Q}$-Algebrenhomomorphismus $\sigma : \mathbb{Q}[X] \xrightarrow{\sim} \mathbb{Q}[X]$ mit $\sigma(X) = X + 1$ (und $\sigma^{-1}(X) = X - 1$) und σ ist ein Automorphismus.
Es genügt also zu zeigen, dass

$$g_p := \sigma(f_p)(X) = f_p(\sigma(X)) = f_p(X + 1)$$

irreduzibel ist.
Rechne:

$$g_p(X) = f_p(X + 1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{1}{X}\left(\left(X^p + pX^{p-1} + \ldots + pX + 1\right) - 1\right) =$$
$$= X^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} X^{i-1} + p \in \mathbb{Z}[X]$$

g_p ist daher normiert.
Um zu sehen, dass g_p Eisenstein bezüglich p ist, ist noch zu zeigen:

$$\underset{1 \leq i \leq p-1}{\forall} \quad p \left| \binom{p}{i} \right.$$

Es gilt:

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{1 \cdot 2 \cdot \ldots \cdot i}$$

Und wegen $p \nmid (p-1), (p-2), \ldots, (p-i+1), 1, 2, \ldots, i$ für $i < p$ folgt sogar:

$$\nu_p\left(\binom{p}{i}\right) = 1$$

Insbesondere ist g_p also Eisenstein bezüglich p. $\square_{\text{iii)}}$

iv) $f(X) := X^3 + 3X^2 - 4X - 1 \in \mathbb{Q}[X]$ ist irreduzibel.

Beweis

$f \in \mathbb{Z}[X]$ ist primitiv und modulo 3 gilt:

$$\pi(f) =: \overline{f}(X) = X^3 - X - 1 \in \mathbb{F}_3[X]$$

Rechne:

$$f(-1,0,1) = -1 \neq 0$$

Wegen $\deg\left(\overline{f}\right) = 3$ ist also $\overline{f} \in \mathbb{F}_3[X]$ irreduzibel und aus 4.3 folgt die Behauptung. $\square_{\text{iv)}}$

v) $f(X,Y) = X^2Y + XY^2 - X - Y + 1 \in \mathbb{Q}[X,Y]$ ist irreduzibel.

Beweis

Schreibe:

$$f = \underbrace{Y}_{=a_2} X^2 + \underbrace{\left(Y^2 - 1\right)}_{=a_1} X + \underbrace{(1 - Y)}_{=a_0} \in \underbrace{(\mathbb{Q}[Y])}_{:=R}[X]$$

Dann ist f primitiv, da bereits a_2 und a_0 in R teilerfremd sind.
$p := Y - 1 \in R$ ist ein Primelement und es gelten:

$$\begin{aligned} Y - 1 = p &\nmid a_2 = Y^2 \\ Y - 1 = p &\mid a_1 = Y^2 - 1 = (Y-1)(Y+1) \\ Y - 1 = p &\mid a_0 = 1 - Y = -(Y-1) \\ (Y-1)^2 = p^2 &\nmid a_0 = 1 - Y = -(Y-1) \end{aligned}$$

Die Behauptung folgt aus Korollar 4.5. $\square_{\text{v)}}$

vi) $f(X) = X^4 + 3X^3 + X^2 - 2X + 1 \in \mathbb{Q}[X]$ ist irreduzibel.

Beweis

$f \in \mathbb{Z}[X]$ ist normiert. Wegen 3.5 und $f(\pm 1) = 3 \pm 1 \neq 0$ folgt, dass f keinen Linearfaktor in $\mathbb{Q}[X]$ besitzt.
Reduktion modulo 2 liefert:

$$\overline{f} := \pi(f) = X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$$

Offenbar gilt $\overline{f}(1) = 0$, und Division liefert:

$$\overline{f} = (X+1)\left(X^3 + X + 1\right) \in \mathbb{F}_2[X] \tag{4.3}$$

Beide Faktoren sind irreduzibel, da sie keine Nullstellen und Grad ≤ 3 haben.
Also ist (4.3) die Primfaktorzerlegung von $\overline{f} \in \mathbb{F}_2[X]$.
Wäre nun $f \in \mathbb{Q}[X]$ reduzibel, so wäre wegen 3.8 auch $f \in \mathbb{Z}[X]$ reduzibel, also:

$$f = gh \in \mathbb{Z}[X]$$

Da f keinen Linearfaktor in $\mathbb{Q}[X]$ besitzt, müsste $\deg(g) = \deg(h) = 2$ gelten.
Dann würde $\overline{f} = \overline{g} \cdot \overline{h}$ in $\mathbb{F}_2[X]$ mit $\deg(\overline{g})$,$\deg\left(\overline{h}\right) \leq 2$ folgen und weil $\deg\left(\overline{f}\right) = 4$ ist, also schon $\deg(\overline{g}) = \deg\left(\overline{h}\right) = 2$.
Wegen (4.3) besitzt aber $\overline{f} \in \mathbb{F}_2[X]$ bis auf Assoziiertheit genau die Teiler $1, X+1, X^3+X+1$ und $\overline{f}$, und keines dieser Polynome besitzt Grad 2. Dies ist ein Widerspruch zu der angenommenen Reduzibilität. $\square_{\text{vi)}}$

vii) Seien p eine Primzahl und $F_p(X) := \dfrac{X^p-1}{X-1} = X^p + \ldots + 1 \in \mathbb{Z}[X]$ wie in iii).

Für $r \geq 1$ setze $n := p^r$, $\zeta_{p^r} := \exp\left(\dfrac{2\pi\mathbf{i}}{n}\right)$ und ferner:

$$F_{p^r}(X) := F_p\left(X^{p^{r-1}}\right) \in \mathbb{Z}[X] \tag{4.4}$$

Es folgt $\deg(F_{p^r}) = (p-1)\,p^{r-1} = \varphi(p^r)$.
Dann gilt: $F_{p^r}(X) = \mathrm{Mipo}_{\mathbb{Q}}(\zeta_{p^r})$

Beweis

Wegen $X^p - 1 = (X-1)\,F_p(X)$ folgt durch Ersetzten von X durch $X^{p^{r-1}}$:

$$X^{p^r} - 1 = \left(X^{p^{r-1}} - 1\right) F_{p^r}(X)$$

Wegen $\zeta_{p^r}^{p^r} = 1$ aber $\zeta_{p^r}^{p^{r-1}} \neq 1$ folgt $F_{p^r}(\zeta_{p^r}) = 0$ und offenbar ist F_{p^r} normiert.
Zeige noch analog zu iii), dass $G_{p^r}(X) := F_{p^r}(X+1) \in \mathbb{Z}[X]$ Eisenstein bezüglich p ist.
Mit $F_{p^r}(X)$ ist auch $G_{p^r}(X)$ normiert, und für den konstanten Term gilt:

$$G_{p^r}(0) = F_{p^r}(1) \overset{(4.4)}{=} F_p(1) \overset{\text{iii)}}{=} p$$

Zeige noch durch Rechnen in ${}^{\mathbb{Z}[X]}\!/_{(p)} \overset{\sim}{=} \mathbb{F}_p[X]$, dass alle weiteren Koeffizienten von G_{p^r} durch p teilbar sind:

$$\begin{aligned} G_{p^r}(X) &\overset{\text{Def.}}{=} F_{p^r}(X+1) = \\ &\overset{(4.4)}{=} F_p\left((X+1)^{p^{r-1}}\right) \overset{(!)}{\equiv} F_p\left(X^{p^{r-1}}+1\right) \overset{F_p(X+1)\equiv X^{p^{r-1}}(\text{iii}))}{\equiv} X^{\left(p^{r-1}\right)(p-1)} \mod p \end{aligned}$$

$\square_{\text{vii)}}$

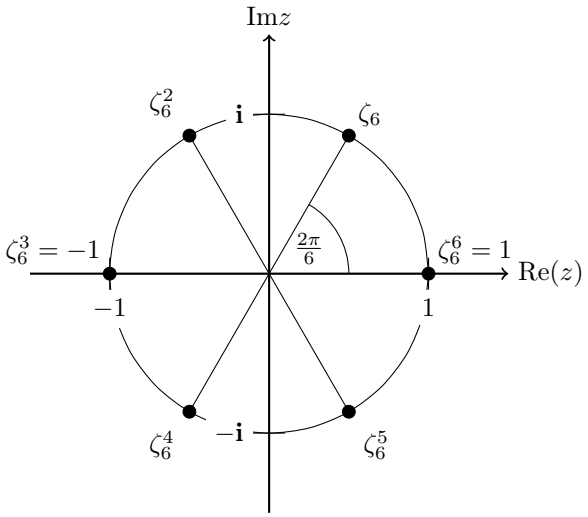
4.7 Bemerkung

Für alle n,$m \in \mathbb{N}_{\geq 1}$ gilt:

$$\left(\exp\left(\frac{2\pi\mathbf{i}}{n}\right)\right)^m = 1 \Leftrightarrow n|m$$

Das heißt $\zeta_n := \exp\left(\dfrac{2\pi\mathbf{i}}{n}\right) \in \mathbb{C}^*$ hat die Ordnung n.

Skizze



Beweis

$$\zeta_n^m = \exp\left(2\pi\mathbf{i} \cdot \frac{m}{n}\right)$$

Aus der Analysis folgt, dass der surjektive Homomorphismus

$$\begin{aligned} \exp : \mathbb{C} &\twoheadrightarrow \mathbb{C}^* \\ z &\mapsto e^z \end{aligned}$$

folgenden Kern hat:

$$\ker(\exp) = 2\pi\mathbf{i} \cdot \mathbb{Z} \subseteq \mathbb{C}$$

Also gilt:

$$\zeta_n^m = 1 \Leftrightarrow \frac{m}{n} \in \mathbb{Z} \Leftrightarrow n|m$$

$\square_{4.7}$

5 (Algebraische) Körpererweiterungen

5.1 **Proposition und Definition** (Charakteristik, Primkörper)

i) Sei R ein Integritätsring, dann existiert genau ein $p \in \mathbb{N}_{\geq 0}$ und ein eindeutiger Ringhomomorphismus $\varphi : \mathbb{Z} \to R$ mit:

$$\ker(\varphi) = (p)$$

Es gilt $p = 0$ oder $p > 0$ ist eine Primzahl. In jedem Fall heißt p *die Charakteristik von* R, in Zeichen:

$$\operatorname{char}(R) := p$$

ii) Sei $k = R$ wie in i) ein Körper. Dann existiert genau ein kleinster Teilkörper $Q \subseteq k$, und es gilt:

$$Q \cong \begin{cases} \mathbb{Q} & \text{falls } \operatorname{char}(k) = 0 \\ \mathbb{F}_p & \text{falls } \operatorname{char}(k) > 0 \end{cases}$$

$Q \subseteq k$ heißt der *Primkörper von* k.

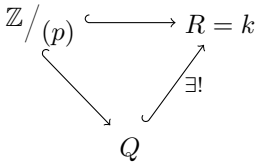
Beweis

i) $\mathbb{Z}/(p) \hookrightarrow R$ ist ein Unterring, also ist $\mathbb{Z}/(p)$ ein Integritätsring, womit aus der linearen Algebra II schon $p = 0$ oder $p > 0$ ist eine Primzahl folgt. $\square_{\text{i)}}$

ii) Ist in i) $R = k$ ein Körper, so erhalte mit

$$Q := \operatorname{Quot}\left(\mathbb{Z}/(p)\right)$$

den Ringhomomorphismus:



Es ist klar, dass $Q \subseteq k$ der kleinste Teilkörper ist, und man erhält für

$$p = 0 : Q \cong \operatorname{Quot}\Big(\underbrace{\mathbb{Z}/(p)}_{\cong \mathbb{Z}}\Big) \cong \mathbb{Q}$$

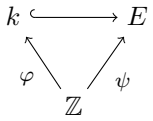
$$p > 0 : Q \cong \operatorname{Quot}\Big(\underbrace{\mathbb{Z}/(p)}_{\cong \mathbb{F}_p}\Big) \cong \mathbb{F}_p$$

$\square_{5.1}$

5.2 Bemerkung und Definition (Körpererweiterung)

Eine *Körpererweiterung* ist ein injektiver Ringhomomorphismus $k \hookrightarrow E$, bei dem k und E Körper sind.

Kommutatives Diagramm



Daraus folgt $\ker(\varphi) = \ker(\psi)$ und daher gilt $\operatorname{char}(k) = \operatorname{char}(E)$, denn $k \hookrightarrow E$ ist injektiv.
Für den Ringhomomorphismus von Integritätsringen $\mathbb{Z} \to \mathbb{F}_p$ gilt:

$$\operatorname{char}(\mathbb{Z}) = 0 \neq p = \operatorname{char}(\mathbb{F}_p)$$

5.3 Proposition und Definition (Frobenius)

Sei k ein Körper mit $\operatorname{char}(k) = p > 0$.

i) $\underset{x,y \in k}{\forall} \underset{n \in \mathbb{N}_{\geq 1}}{\forall} : (x+y)^{p^n} = x^{p^n} + y^{p^n} \in k.$

ii) Die Abbildung

$$\operatorname{Frob}_k : k \hookrightarrow k, x \mapsto x^p$$

ist ein injektiver Ringhomomorphismus, *der Frobenius von k.*

iii) Ist k endlich, so ist $\operatorname{Frob}_k : k \xrightarrow{\sim} k$ ein Isomorphismus.

iv) $\operatorname{Frob}_k = \mathrm{id}_k \Leftrightarrow k = \mathbb{F}_p$

Beweis

i) TODO: Beweis einfügen

$\square_{\text{i)}}$

ii) Klar sind

$$\operatorname{Frob}_k(0) = 0 \qquad \operatorname{Frob}_k(1) = 1 \qquad \operatorname{Frob}_k(x \cdot y) = \operatorname{Frob}_k(x) \cdot \operatorname{Frob}_k(y)$$

und

$$\operatorname{Frob}_k(x+y) = \operatorname{Frob}_k(x) + \operatorname{Frob}_k(y)$$

folgt aus i) für $n = 1$.

Damit ist $\operatorname{Frob}_k : k \to k$ ein Ringhomomorphismus, und $\operatorname{Frob}_k(x) = x^p = 0 \overset{k \text{ Körper}}{\Leftrightarrow} x = 0$, also ist Frob_k injektiv. $\square_{\text{ii)}}$

iii) Jede injektive Selbstabbildung, wie zum Beispiel Frob_k, einer endlichen Menge, wie zum Beispiel k, ist surjektiv. $\square_{\text{iii)}}$

iv) „⇐“: Für alle $x \in \mathbb{F}_p$ gilt:

$$\mathrm{Frob}_{\mathbb{F}_p}(x) - x = x^p - x = x\left(x^{p-1} - 1\right) = 0$$

Dies ist klar für $x = 0$ und für $x \in \mathbb{F}_p^*$ gilt $x^{p-1} = 1$ nach 1.26 ii).
„⇒“: Nach Voraussetzung ist $\mathrm{char}(k) = p$ und nach 5.1 folgt, dass $\mathbb{F}_p \subseteq k$ der Primkörper ist.
Für alle $x \in k$ folgt:

$$0 = \mathrm{Frob}_k(x) - x = x^p - x$$

und das Polynom $T^p - T \in k[T]$ hat höchstens p Nullstellen in k.
Jedes $x \in \mathbb{F}_p \subseteq k$ ist aber eine Nullstelle nach Beweis von „⇐“, also gilt $k = \mathbb{F}_p$.

$\square_{5.3}$

5.4 **Proposition und Definition** (algebraisch, transzendent, Zwischenkörper)

Sei $E \supseteq k$ eine Körpererweiterung.
Dann ist E insbesondere eine k-Algebra und insbesondere ein k-Vektorraum.
Ein $\alpha \in E$ heißt genau dann *algebraisch über k*, wenn ein $f \in k[X] \setminus \{0\}$ existiert mit $f(\alpha) = 0$ in E, ansonsten heißt α *transzendent über k*.
Falls α algebraisch ist, ist $\mathrm{Mipo}_k(\alpha) \in k[X]$ das eindeutige, normierte, irreduzible Polynom in $k[X]$, das α annulliert.
Ein Körper K mit $k \subseteq K \subseteq E$ heißt *Zwischenkörper (der Körpererweiterung $k \subseteq E$).*

Beweis

TODO: Beweis einfügen

$\square_{5.4}$

5.5 **Definition** (Grad)

Sei $E \supseteq k$ eine Körpererweiterung.
Dann heißt

$$[E : k] := \dim_k(E) \in (\mathbb{N} \setminus \{0\}) \cup \{\infty\}$$

der Grad von E über k (schreibe E/k für „die Körpererweiterung E über k“)

5.6 (Grad-)**Satz**

Seien $E \supseteq K \supseteq k$ eine Körpererweiterung, dann gilt:

$$[E : k] = [E : K] \cdot [K : k]$$

Beweis

1. Fall: Es gelte:

$$[E : k], [K : k] < \infty$$

Dann folgt als k-Vektorraum:

$$E \cong k^{[E:k]} \qquad\qquad K \cong k^{[K:k]}$$

Damit ergibt sich:

$$k^{[E:k]} \cong E \cong K^{[E:K]} \cong \left(k^{[K:k]}\right)^{[E:K]} \cong k^{[E:K]\cdot[K:k]}$$

Also gilt für die Dimension von E:

$$\dim_k (E) = [E : k] = [E : K] \cdot [K : k]$$

2. Fall: Ist $[E : k] = \infty$ (oder $[K : k] = \infty$), so existiert eine unendliche k-linear unabhängig Menge $X \subseteq E$ (oder $X \subseteq K \subseteq E$).
In beiden Fällen ist $X \subseteq E$ schon k-linear unabhängig und es folgt $[E : k] = \infty$.

$\square_{5.6}$

5.7 Korollar

Sind $E \supseteq K \supseteq k$ Körpererweiterungen und $[E : k]$ eine Primzahl, so folgt $E = K$ oder $E = k$.

Beweis

TODO: Beweis einfügen

$\square_{5.7}$

5.8 **Beispiel** (Verfahren von Kronecker)

i) Seien k ein Körper und $f \in k[X]$ mit $n := \deg(f)$.
Dann liefert die Komposition

$$k \hookrightarrow k[X] \xrightarrow{\pi} k[X]/(f)$$

mit der kanonischen Projektion π einen Homomorphismus, der als Körperhomomorphismus schon injektiv ist, also ist $k[X]/(f) =: E \supseteq k$ eine Körpererweiterung und es gilt $[E : k] = n$.
Das Element $\alpha := \pi(X) = X + (f) \in E$ erfüllt in E:

$$f(\alpha) = f(\pi(X)) = \pi(f(X)) = (f) \equiv 0$$

Man sagt „$E = k(\alpha)$ entsteht durch Adjunktion der Nullstelle α von f.“ und nennt dieses Vorgehen das *Verfahren von Kronecker*.

ii) $\mathbb{C} \supseteq \mathbb{R}$ und $\mathbb{Q}(\sqrt{2}) := \mathbb{Q}[X]/(X^2 - 2) \supseteq \mathbb{Q}$ sind Körpererweiterungen vom Grad 2.

Beachte

Es gibt zwei $\mathbb{Q}$-Algebrenhomomorphismen

$$\mathbb{Q}[X]/(X^2-2) \hookrightarrow \mathbb{R}$$

nämlich:

$$X \mapsto \sqrt{2} \qquad\qquad X \mapsto -\sqrt{2}$$

iii) Sei k ein Körper, dann ist $[k(T):k] = \infty$, da $k \subseteq k[T] \subseteq k(T)$ ja k-Vektorräume sind und $\dim_k(k[T]) = \infty$ ist.

iv) $[\mathbb{R}:\mathbb{Q}] = \infty$

Beweis

Jede endliche Erweiterung von $\mathbb{Q}$ ist eine abzählbare Menge! $\mathbb{R}$ ist jedoch überabzählbar.
Alternativ: Seien $n \in \mathbb{N}_{\geq 1}$ und $\alpha \in \mathbb{R}$ mit $\alpha^n = 2$.
Schreibe:

$$\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{R}$$

für die von α erzeugte $\mathbb{Q}$-Unteralgebra von $\mathbb{R}$. Wegen

$$\mathrm{Mipo}_{\mathbb{Q}}(\alpha) = X^n - 2$$

(vergleiche 4.6 i)) ist

$$\mathbb{Q}[X]/X^n - 2 \cong \mathbb{Q}(\alpha)$$

ein Körper mit $[\mathbb{Q}(\alpha):\mathbb{Q}] = n$ (vergleiche 5.8 i)).
Aus $\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{R}$ und 5.6 folgt $n \mid [\mathbb{R}:\mathbb{Q}]$.
Weil dabei $n \in \mathbb{N}_{\geq 1}$ beliebig groß gewählt werden kann, folgt $[\mathbb{R}:\mathbb{Q}] = \infty$. $\square_{\text{iv)}}$

5.9 **Definition** (algebraische Körpererweiterung)

Eine Körpererweiterung $E \supseteq k$ heißt genau dann *algebraisch*, wenn alle $\alpha \in E$ algebraisch über k sind.

5.10 Beispiel

Die Körpererweiterung $k(t) : k$ ist nicht algebraisch, aber $\alpha := 0 \in k(t)$ ist algebraisch über k.

5.11 **Bemerkung und Definition** (Grad von $\alpha \in E$)

Seien $E \supseteq k$ eine Körpererweiterung und $\alpha \in E$.
Dann erhält man eine k-Algebra $k \subseteq k[\alpha] \subseteq E$ und es gilt:

$$\alpha \text{ ist algebraisch über } k. \Leftrightarrow k[\alpha] \text{ ist ein Körper.}$$

Damit folgt

$$k[\alpha] \cong k[X]/\mathrm{Mipo}_k(\alpha) = k(\alpha)$$

und $[\alpha : k] := [k(\alpha) : k]$ heißt *der Grad von α über k.*
Ist α transzendent über k, so ist der Einsetzungshomomorphismus

$$\begin{aligned} k[X] &\xrightarrow{\sim} k[\alpha] \\ X &\mapsto \alpha \end{aligned}$$

ein k-Algebrenisomorphismus.

Beweis

TODO: Beweis als Übung einfügen

□5.11

5.12 Satz

Jede endliche Körpererweiterung ist algebraisch.

Beweis

Dies wurde in der Linearen Algebra II gezeigt. (Satz von Cayley-Hamilton)
TODO: Beweis einfügen

□5.12

5.13 **Proposition und Definition** (Polynomring; endlich erzeugte, einfache Körpererweiterung)

Sei k ein Körper.

i) Für $n \in \mathbb{N}_{\geq 2}$ definiere

$$k[X_1, \ldots, X_n] := (k[X_1, \ldots, X_{n-1}])[X_n]$$

den Polynomring in den Variablen $X_1, \ldots, X_n$ über k.
Dann ist für jede kommutative k-Algebra A die Abbildung von Mengen

$$\begin{aligned} \mathrm{Hom}_{k\text{-Alg.}}(k[X_1, \ldots, X_n], A) &\xrightarrow{\sim} A^n \\ \varphi &\mapsto (\varphi(X_i))_{1 \leq i \leq n} \end{aligned}$$

injektiv. Dies ist die universellen Eigenschaft der k-Algebra $k[X_1, \ldots, X_n]$.

ii) Sei $E \supseteq k$ eine Körpererweiterung und $X \subseteq E$ eine Teilmenge.
Dann ist

$$k(X) := \bigcap_{\substack{k \subseteq K \subseteq E \\ \text{ZK mit } X \subseteq K}} K$$

der kleinste Zwischenkörper von $k \subseteq E$, der X enthält.

iii) Gilt in ii) schon $X = \{\alpha_1, \ldots, \alpha_n\}$, das heißt ist X endlich, so folgt

$$k(\alpha_1, \ldots, \alpha_n) := k(\{\alpha_1, \ldots, \alpha_n\}) = \mathrm{Quot}(k[\alpha_1, \ldots, \alpha_n])$$

wobei

$$k[\alpha_1, \ldots, \alpha_n] := \mathrm{im}\left(k[X_1, \ldots, X_n] \xrightarrow{\varphi} E\right)$$

und φ der nach i) eindeutige k-Algebrenhomomorphismus mit $\varphi(X_i) = \alpha_i$ für $1 \leq i \leq n$ ist.

iv) Eine Körpererweiterung $E \supseteq k$ heißt genau dann *endlich erzeugt*, wenn endlich viele $\alpha_1, \ldots, \alpha_n \in E$ existieren mit $E = k(\alpha_1, \ldots, \alpha_n)$.

v) Eine Körpererweiterung $E \supseteq k$ heißt genau dann *einfach*, wenn ein $\alpha \in E$ existiert mit $E = k(\alpha)$.

Beweis

i) Die universelle Eigenschaft folgt durch Induktion aus dem bekannten Fall $n = 1$.

ii) TODO: Beweis als Übung einfügen

iii) TODO: Beweis als Übung einfügen

$\square_{5.13}$

5.14 Satz

Sei $E = k(\alpha_1, \ldots, \alpha_n)$ eine endlich erzeugte Körpererweiterung und die α_i $(1 \leq i \leq n)$ über k algebraisch. Dann gelten:

i) $E = k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n]$

ii) $[E : k] < \infty$

Beweis

Induktion über $n \geq 1$:
$n = 1$: Siehe 5.11.
$n > 1$: Nach Induktionsvoraussetzung ist $E' := k[\alpha_1, \ldots, \alpha_{n-1}] \supseteq k$ eine endliche Körpererweiterung.
Da α_n algebraisch über k ist, ist es insbesondere algebraisch über E' und nach 5.11 ist $E'[\alpha_n] \supseteq E'$ eine endliche Körpererweiterung.
Mit 5.6 für $k \subseteq E' \subseteq E'[\alpha_n]$ folgt, dass $E'[\alpha_n] = k[\alpha_1, \ldots, \alpha_n] \supseteq k$ eine endliche Körpererweiterung ist.
Insbesondere ist $k[\alpha_1, \ldots, \alpha_n]$ ein Körper und somit $E = k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n]$.
Es folgten i) und ii). $\square_{5.14}$

5.15 Beispiel

Für jedes $n \in \mathbb{N}_{\geq 1}$ ist $\cos\left(\frac{\pi}{n}\right) \in \mathbb{R}$ algebraisch über $\mathbb{Q}$.

Beweis

Nach Euler gilt:

$$\cos\left(\frac{\pi}{n}\right) = \frac{1}{2}\left(e^{\frac{\pi \mathbf{i}}{n}} + e^{-\frac{\pi \mathbf{i}}{n}}\right)$$

Außerdem ist

$$\alpha := e^{\frac{\pi \mathbf{i}}{n}} \; (= \zeta_{2n})$$

algebraisch über $\mathbb{Q}$, denn $\alpha^{2n} = 1$ (vergleiche Bemerkung 4.7).

Dann folgt nach 5.14 ii) schon $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ und mit 5.12 folgt, dass $\mathbb{Q}(\alpha)/\mathbb{Q}$ algebraisch ist.

Nach 5.9 ist *jedes* Element von $\mathbb{Q}(\alpha)$ algebraisch über $\mathbb{Q}$ ist, insbesondere also $\cos\left(\frac{\pi}{n}\right) = \frac{1}{2}\left(\alpha + \alpha^{-1}\right)$.
$\square_{5.15}$

Problem

Bestimme explizit $0 \neq f \in \mathbb{Q}[X]$ mit $f\left(\cos\left(\frac{\pi}{n}\right)\right) = 0$.

5.16 **Proposition** (endlich $\Leftrightarrow$ endlich erzeugt und algebraisch)

Sei $E \supseteq k$ eine Körpererweiterung.

i) Es sind äquivalent:

   a) ${}^{E}\!/_{k}$ ist endlich.

   b) ${}^{E}\!/_{k}$ ist endlich erzeugt und algebraisch.

ii) Es sind äquivalent:

   a) ${}^{E}\!/_{k}$ ist algebraisch.

   b) Es gibt eine Menge $X \subseteq E$ mit $E = k(X)$ und für alle $x \in X$ ist x algebraisch über k.

Beweis

i) a) $\Rightarrow$ b): Ist ${}^{E}\!/_{k}$ endlich, so offenbar auch endlich erzeugt und nach 5.12 algebraisch.
   b) $\Rightarrow$ a): Dies wurde in 5.14 ii) gezeigt.

ii) a) $\Rightarrow$ b): Wähle $X = E$.
   b) $\Rightarrow$ a): $I := \{X' | X' \subseteq X \text{ ist endlich}\}$
   Damit folgt:

$$E = k(X) = \bigcup_{X' \in I} k(X')$$

   Seien nun $\alpha \in E$, dann gibt es ein $X' \in I$ mit $\alpha \in k(X')$.
   Wegen 5.14 ist $k(X') \supseteq k$ endlich und nach 5.12 ist $\alpha \in k(X')$ algebraisch über k.
   Weil dabei $\alpha \in E$ beliebig ist, folgt, dass ${}^{E}\!/_{k}$ algebraisch ist.

$\square_{5.16}$

5.17 **Satz** (Transitivität der Algebraizität)

Seien $E \supseteq K \supseteq k$ Körpererweiterungen.

i) Ist $\alpha \in E$ algebraisch über K und ${}^{K}\!/_{k}$ algebraisch, dann ist α algebraisch über k.

ii) Sind ${}^{E}\!/_{K}$ und ${}^{K}\!/_{k}$ algebraisch, so ist auch ${}^{E}\!/_{k}$ algebraisch.

Beweis

i) Sei $\text{Mipo}_K(\alpha) = X^n + c_{n-1}X^{n-1} + \ldots + c_0$, dann ist α algebraisch über $K' := k[c_0, \ldots, c_{n-1}] \subseteq K$. Es folgt:

$$[K'(\alpha) : K'] < \infty$$

Mit 5.14 ii) folgt:

$$[K' : k] < \infty$$

Mit 5.6 folgt insgesamt:

$$[K'(\alpha) : k] < \infty$$

Nach 5.12 ist dann α algebraisch über k. $\square_{\text{i)}}$

ii) Dies folgt aus i), angewendet auf alle $\alpha \in E$.

$\square_{5.17}$

5.18 Beispiel

Es sind

$$\mathbb{C} \supseteq \overline{\mathbb{Q}}^{\mathbb{C}} := \{\alpha \in \mathbb{C} | \alpha \text{ ist algebraisch über } \mathbb{Q}\} \supseteq \mathbb{Q}$$

Körpererweiterung.

Wegen 5.16 ii) b) $\Rightarrow$ a) ist $\overline{\mathbb{Q}}^{\mathbb{C}} \big/ \mathbb{Q}$ algebraisch.

Nach dem Beweis von 5.8 iv) gilt $\left[\overline{\mathbb{Q}}^{\mathbb{C}} : \mathbb{Q}\right] = \infty$. (Nebenbemerkung: $\mathbb{Q}\left[2^{\frac{1}{n}}\right] \subseteq \overline{\mathbb{Q}}^{\mathbb{C}}$)

Also ist die Körpererweiterung $\overline{\mathbb{Q}}^{\mathbb{C}} \big/ \mathbb{Q}$ wegen 5.16 i) b) $\Rightarrow$ a) nicht endlich erzeugt.

6 Der algebraische Abschluss eines Körpers

6.1 Proposition und Definition (algebraisch abgeschlossen)

Für einen Körper k sind folgende Aussagen äquivalent:

i) Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in k.

ii) Jedes irreduzible $f \in k[X]$ ist linear.

iii) Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ ist ein Produkt linearer Polynome.

iv) Für alle algebraischen Körpererweiterungen E/k gilt $E = k$.

Gelten i) bis iv), so heißt k *algebraisch abgeschlossen.*

Beweis

i)⇒ii)⇒iii) sind klar, iii)⇒iv): Seien $\alpha \in E$ und $f := \mathrm{Mipo}_k(\alpha)$.
Weil f irreduzibel ist, folgt aus iii) $\deg(f) = 1$, also $\alpha \in k$.
iv)⇒i): Sei $f \in k[X]$ mit $\deg(f) \geq 1$. Es existiert ein irreduzibles $g \in k[X]$ mit:

$$g|f \tag{6.1}$$

Nach 5.6 ist $E := k[X]/(g) \supseteq k$ eine endliche (und damit algebraische) Körpererweiterung, und nach 5.8 i) ist $\alpha := (X + (g)) \in E$ eine Nullstelle von g.
Nach iv) gilt $k = E$, also besitzt g und wegen (6.1) auch f, eine Nullstelle in k. $\square_{6.1}$

6.2 Proposition und Definition (Polynomring)

Seien $\mathfrak{X}$ eine Menge und für jede endliche Teilmenge $\mathfrak{X}' = \{X_1, \ldots, X_n\} \subseteq \mathfrak{X}$ sei definiert:

$$k[\mathfrak{X}'] := k[X_1, \ldots, X_n]$$

Dann heißt

$$k[\mathfrak{X}] := \bigcup_{\mathfrak{X}' \subseteq \mathfrak{X} \text{ endlich}} k[\mathfrak{X}'] \tag{6.2}$$

der Polynomring in den Variablen $\mathfrak{X}$ über k.
Er besitzt folgende universelle Eigenschaft:
Für jede kommutative k-Algebra A ist die Abbildung von Mengen

$$\mathrm{Hom}_{k\text{-Alg.}}(k[\mathfrak{X}], A) \xrightarrow{\sim} A^{\mathfrak{X}}, \varphi \mapsto (\mathfrak{X} \ni x \mapsto \varphi(x))$$

bijektiv.

Beweis

Wegen (6.2) ist die Abbildung

$$\mathrm{Hom}_{k\text{-Alg.}}\left(k\left[\mathfrak{X}\right],A\right) \xrightarrow{\sim} \left\{ \left(\varphi_{\mathfrak{X}'}\right)_{\mathfrak{X}'\subseteq\mathfrak{X}\text{ endl.}} \,\middle|\, \underset{\mathfrak{X}'\subseteq\mathfrak{X}''\subseteq\mathfrak{X}\text{ endl.}}{\forall} \varphi_{\mathfrak{X}''}\big|_{k[\mathfrak{X}']} = \varphi_{\mathfrak{X}'} \right\}$$

bijektiv, wobei $\varphi_{\mathfrak{X}'} \in \mathrm{Hom}_{k\text{-Alg.}}\left(k\left[\mathfrak{X}\right],A\right)$.
Wegen 5.13 ist folgende Abbildung bijektiv:

$$\mathrm{Hom}_{k\text{-Alg.}}\left(k\left[\mathfrak{X}\right],A\right) \xrightarrow{\sim} \left\{ \left(f_{\mathfrak{X}'}\right)_{\mathfrak{X}'\subseteq\mathfrak{X}\text{ endl.}} \,\middle|\, f_{\mathfrak{X}'}:\mathfrak{X}'\to A; \underset{\mathfrak{X}'\subseteq\mathfrak{X}''\subseteq\mathfrak{X}\text{ endl.}}{\forall} f_{\mathfrak{X}''}\big|_{\mathfrak{X}'} = f_{\mathfrak{X}'} \right\} =: \Sigma$$

Es ist klar, dass die Abbildung

$$\mathrm{Abb}\left(\mathfrak{X},A\right) \xrightarrow{\sim} \Sigma, f \mapsto \left(f_{\mathfrak{X}'} := f\big|_{\mathfrak{X}'}\right)_{\mathfrak{X}'\subseteq\mathfrak{X}\text{ endl.}}$$

bijektiv ist, und man prüft, dass die resultierende Bijektion

$$\mathrm{Hom}_{k\text{-Alg.}}\left(\mathfrak{X},A\right) \xrightarrow{\sim} \mathrm{Abb}\left(\mathfrak{X},A\right)$$

wie angegeben ist. $\square_{6.2}$

6.3 Das Lemma von Zorn

6.3.1 Definition (geordnete Menge, obere Schranke)

Eine *teilweise geordnete Menge* ist ein Tupel $(M, \leq)$ wobei M eine Menge und $\leq$ eine Relation auf M sind, so dass für alle $x,y,z \in M$ gelten:

i) $x \leq x$

ii) $(x \leq y \wedge y \leq z) \Rightarrow (x \leq z)$

iii) $(x \leq y \wedge y \leq x) \Rightarrow (x = y)$

$(M, \leq)$ heißt genau dann *total geordnet*, wenn für alle $x,y \in M$ schon $x \leq y$ oder $y \leq x$ gilt.
$x \in M$ heißt genau dann *maximales Element*, wenn für alle $y \in M$ aus $x \leq y$ schon $x = y$.
Für eine Teilmenge $N \subseteq M$ heißt $x \in M$ genau dann *obere Schranke für* N, wenn für alle $y \in N$ schon $y \leq x$.

6.3.2 Beispiel

Seien R ein kommutativer Ring, $M := \{I | I \subsetneq R \text{ ist ein Ideal}\}$ und $I \leq J :\Leftrightarrow I \subseteq J$.
Dann ist $(M, \leq)$ teilweise geordnet, aber im Allgemeinen nicht total geordnet, zum Beispiel ist für $R = \mathbb{Z}$ schon $(2), (3) \in M$ und weder $(2) \leq (3)$ noch $(3) \leq (2)$.

6.3.3 Satz (Lemma von Zorn)

Sei $(M, \leq)$ eine teilweise geordnete Menge, $M \neq \emptyset$ und jede total geordnete Teilmenge $N \subseteq M$ besitze eine obere Schranke.
Dann besitzt M ein maximales Element.

(ohne Beweis)

Diese Aussage ist äquivalent zum Auswahlaxiom:
Sei $I \neq \emptyset$ eine Menge. Für alle $i \in I$ gilt:

$$\emptyset \neq X_i \Rightarrow \prod_{i \in I} X_i \neq \emptyset$$

6.3.4 Beispiel

Sei $(M, \leq)$ wie in 6.3.2 für $R \neq \{0\}$.
Dann ist $\{0\} \in M$, also $M \neq \emptyset$.
Sei $N \subseteq M$ total geordnet.

Behauptung

$J := \bigcup_{I \in N} I \subsetneq R$ ist ein Ideal (also ist $J \in M$ eine obere Schranke für N).

Beweis

1. Ist $x \in J$, so gibt es $I \in N$ mit $x \in I \subseteq J$ und da I ein Ideal ist, folgt für alle $a \in R$ schon $ax \in I \subseteq J$.
2. Sind $x,y \in J$, so existieren $I_1,I_2 \in N$ mit $x \in I_1,y \in I_2$.
   Weil N total geordnet ist, gilt $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$. Durch eventuelles Vertauschen von x und y sei ohne Einschränkung $I_1 \subseteq I_2$. Dann gilt $x,y \in I_2$ und es folgt $x + y \in I_2 \subseteq J$.

Also ist $J \subseteq R$ ein Ideal.
Wäre $J = R$, so würde $1 \in J = \bigcup_{I \in N} I$ folgen. Dann müsste ein $I \in N$ existieren mit $1 \in I$, also $I = R$ im Widerspruch zu $I \in M$, das heißt $I \subsetneq R$. $\square_{\text{Behauptung}}$
Damit erfüllt $(M, \leq)$ alle Voraussetzungen von 6.3.3 und es folgt:

6.3.5 **Satz** (Existenz eines maximalen Ideals)

Ist $R \neq \{0\}$ ein kommutativer Ring, so existiert ein maximales Ideal $\mathfrak{m} \subseteq R$.

Beweis

Siehe 6.3.4. $\square_{6.3.5}$

6.4 **Satz und Definition** (algebraischer Abschluss)

Sei k ein Körper.
Dann existieren eine algebraische Körpererweiterung $\overline{k} \subseteq k$, die algebraisch abgeschlossen ist.
Jedes solches $\overline{k}$ heißt *ein algebraischer Abschluss von k.*

Bemerkung

Die Notation $\overline{k}$ wird später durch 6.7 gerechtfertigt.

Beweis von 6.4 (Emil Artin)

Setze $I := \{f \in k[X] \,|\deg(f) \geq 1\}$, $\mathfrak{X} := \{X_f | f \in I\}$, und betrachte das Ideal:

$$I := (f(X_f) \,|f \in I) \subseteq k[\mathfrak{X}]$$

Behauptung

$I \neq k[\mathfrak{X}]$

Beweis

Sonst würde $1 \in I$ gelten, woraus folgt:

$$1 = \sum_{i=1}^{n} g_i \cdot f_i(X_{f_i}) \tag{6.3}$$

Dabei ist $n \in \mathbb{N}_{\geq 1}$, $g_i \in k[\mathfrak{X}]$ und $f_i \in I$ geeignet.
Aus 5.8 i) induktiv angewendet auf alle irreduziblen Teiler von $f_1, \ldots, f_n$ folgt, dass es eine endliche Körpererweiterung $K \supseteq k$ und $\alpha_1, \ldots, \alpha_n \in K$, sodass für alle $1 \leq i \leq n$ gilt:

$$f_i(\alpha_i) = 0 \tag{6.4}$$

Wegen 6.2 existiert ein k-Algebrenhomomorphismus $\phi : k[X] \to k$, sodass für alle $1 \leq i \leq n$ schon

$$\phi(X_{f_i}) = \alpha_i \tag{6.5}$$

gilt, und es folgt in K:

$$1 = \phi(1) \overset{(6.3)}{=} \sum_{i=1}^{n} \phi(g_i) \cdot \underbrace{\phi(f_i(X_{f_i}))}_{=f_i\left(\underbrace{\phi(X_{f_i})}_{=\alpha_i}\right)} \overset{(6.4)}{=} 0 \qquad \lightning$$

$\square_{6.4}$

Wegen der Behauptung ist ${}^{k[\mathfrak{X}]}\!/_{I} \neq \{0\}$ und wegen 6.3.5 existiert ein maximales Ideal $\mathfrak{m} \subseteq {}^{k[\mathfrak{X}]}\!/_{I}$.
Erhalte eine Körpererweiterung $\alpha(k) \supseteq k$ als Komposition $k \hookrightarrow k[\mathfrak{X}] \twoheadrightarrow {}^{k[\mathfrak{X}]}\!/_{I} \twoheadrightarrow \underbrace{{}^{k[\mathfrak{X}]}\!/_{I}\!/_{\mathfrak{m}}}_{=:\alpha(k)}$.

Zeige noch:

i) ${}^{\alpha(k)}\!/_{k}$ ist algebraisch.

ii) $\overline{k} := \bigcup_{n \geq 1} \alpha^n(k)$ ist algebraisch über k.

iii) ${}^{\overline{k}}\!/_{k}$ ist algebraisch abgeschlossen.

Beweis

i) Die k-Algebra $\alpha(k)$ wird durch die Bilder $\alpha_f \in \alpha(k)$ der X_f $(f \in I)$ erzeugt.
Für jedes $f \in I$ gilt wegen $f(X_f) \in I$: $f(\alpha_f) = 0$ in $\alpha(k)$.
Teil i) folgt aus 5.16 ii) b) $\Rightarrow$ a).
Nach Definition von I folgt auch: Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in $\alpha(k)$.
$\square_{\text{i)}}$

ii) Betrachte nun den Körperturm:

$$k \subseteq \alpha(k) \subseteq \alpha(\alpha(k)) =: \alpha^2(k) \subseteq \ldots \subseteq \bigcup_{n \geq 1} \alpha^n(k) =: \overline{k}$$

Für alle $n \in \mathbb{N}_{\geq 1}$ folgt nach i), dass $\alpha^n(k) \big/ \alpha^{n-1}(k)$ algebraisch ist. $(\alpha^0(k) := k)$

Induktiv folgt aus 5.17 für alle $n \in \mathbb{N}_{\geq 0}$, dass $\alpha^n(k) \big/ k$ algebraisch ist.

ii) folgt, da jedes Element von $\overline{k}$ in einem $\alpha^n(k)$ liegt. $\square_{\text{ii)}}$

iii) Sei $f \in \overline{k}[X]$ nicht konstant.
Da f nur endlich viele Koeffizienten hat, folgt, dass ein $n \in \mathbb{N}_{\geq 0}$ existiert mit $f \in \alpha^n(k)[X]$.
Also hat f eine Nullstelle in $\alpha^{n+1}(k) \subseteq \overline{k}$. Damit folgt aus 6.1 i) die Behauptung.

$\square_{6.4}$

6.5 Notation und Bemerkung

Sei $z : K \to L$ ein Körperhomomorphismus.
Schreibe für alle $f = \sum_i a_i X^i \in k[X]$:

$$f^\sigma := \sum_i \sigma(a_i) X^i \in L[X]$$

Dann gilt für alle $\alpha \in k$:

$$\sigma(f(\alpha)) = \sigma\left(\sum_i a_i \alpha^i\right) = \sum_i \sigma(a_i) \cdot \sigma(\alpha)^i = f^\sigma(\sigma(\alpha))$$

Insbesondere gilt für alle $\alpha \in k$:

$$f(\alpha) = 0 \Rightarrow f^\sigma(\sigma(\alpha)) = 0$$

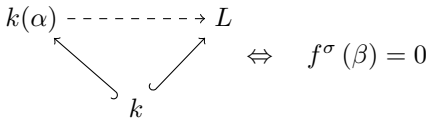
6.6 Lemma

Seien k ein Körper, $k(\alpha) \supseteq k$ eine einfache, algebraische Körpererweiterung, $f := \text{Mipo}_k(\alpha) \in k[X]$ und $\sigma : k \hookrightarrow L$ eine Körpererweiterung.
Dann ist die Abbildung

$$\begin{aligned} \text{Hom}_{k\text{-Alg.}}(k(\alpha), L) &\xrightarrow{\sim} \{\beta \in L | f^\sigma(\beta) = 0\} \\ \tau &\mapsto \tau(\alpha) \end{aligned}$$

wohldefiniert und bijektiv.
Insbesondere gilt:

$$|\text{Hom}_{k\text{-Alg.}}(k(\alpha), L)| \leq [k(\alpha) : k]$$



$\Leftrightarrow \quad f^{\sigma}(\beta) = 0$

Beweis

Die erste Aussage folgt aus der universellen Eigenschaf von $k \hookrightarrow k[X]$ und $k[X] \twoheadrightarrow {}^{k[X]}\!/_{(f)} \cong k(\alpha)$.
Die zweite Aussage folgt aus $\deg(f^{\sigma}) = \deg(f) = [k(\alpha) : k]$. $\square_{6.6}$

6.7 Satz und Definition (Fortsetzung)

Seien $k' \supseteq k$ eine algebraische Körpererweiterung und $\sigma : k \hookrightarrow L = \overline{L}$ eine Körpererweiterung und L algebraisch abgeschlossen.
Dann existiert ein k-Algebrenhomomorphismus $\sigma' : k' \to L$. Man nennt diesen eine *Fortsetzung von σ auf k'*.
Sind zusätzlich k' algebraisch abgeschlossen und L algebraisch über $\sigma(k) \subseteq L$, so ist jedes solche σ' ein Isomorphismus.

Beweis

Betrachte die Menge:

$$M := \{(K,\tau) \,|\, k \subseteq K \subseteq k' \text{ ist ein Zwischenkörper und } \tau : K \to L\}$$

Wegen $(k,\sigma) \in M$ ist $M \neq \emptyset$.
Setze für alle $(K,\tau), (K',\tau') \in M$:

$$(K,\tau) \leq (K',\tau') :\Leftrightarrow K \subseteq K' \wedge \tau'|_K = \tau$$

Dann ist $(M, \leq)$ eine teilweise geordnete Menge und jede total geordnete Teilmenge besitzt eine obere Schranke in M, nämlich die Vereinigung aller Elemente Elemente der total geordneten Teilmenge.
Nach 6.3.3 existiert ein maximales Element in $(K,\sigma') \in M$.
Zeige nur $K = k'$:
Angenommen $K \subsetneq k'$.
Wähle $\alpha \in k' \setminus K$, dann besitzt das Minimalpolynom $\mathrm{Mipo}_K(\alpha) \in K[X] \subseteq L[X]$ wegen $L = \overline{L}$ eine Nullstelle in L.
Nach 6.6 besitzt $\sigma' : K \hookrightarrow L$ eine Fortsetzung $\sigma'' : K(\alpha) \hookrightarrow L$.
Wegen $\sigma''|_k = \sigma'|_k$ ist $(K(\alpha), \sigma'') \in M$, was wegen $K \subsetneq K(\alpha)$ der Maximalität von $(K,\sigma) \in M$ widerspricht.
Damit ist $\sigma' : k \hookrightarrow L$ eine Fortsetzung von σ.
Seien nun zusätzlich k' algebraisch abgeschlossen und ${}^{L}\!/_{\sigma(k)}$ algebraisch.
Dann ist auch ${}^{L}\!/_{\sigma'(k)}$ algebraisch, da $\sigma'(k') \supseteq \sigma(k)$ ist.
Weil $\sigma'(k') \cong k'$ algebraisch abgeschlossen ist, folgt nach 5.9 iv) schon $L = \sigma'(k')$, das heißt $\sigma' : k' \twoheadrightarrow L$ ist surjektiv, also ein Isomorphismus. $\square_{6.7}$

6.8 Korollar

Seien k ein Körper und $\overline{k}_i \supseteq k$ (für $i \in \{1,2\}$) algebraische Abschlüsse von k.
Dann existiert ein k-Algebrenhomomorphismus $\overline{k}_1 \xrightarrow{\sim} \overline{k}_2$ und jeder solche ist ein Isomorphismus.

Beweis

Aus 6.7 folgt mir $k' := \overline{k}_1$, $L := \overline{k}_2$ und $\sigma : k \to \overline{k}_2$ wie gegeben schon die Behauptung. $\square_{6.8}$

7 Zerfällungskörper

Fixiere in Kapitel 7 (Zerfällungskörper)

Sei k ein Körper und $\emptyset \neq \mathcal{F} \subseteq \{f \in k[X] \,|\deg(f) \geq 1\}$.

Definition (k-Homomorphismus)

Definiere *k-Homomorphismus* (Abkürzung: k-Hom.) als k-Algebrenhomomorphismus (nicht zu verwechseln mit einer k-linearen Abbildung).

7.1 Definition (Zerfällungskörper)

Ein *Zerfällungskörper von $\mathcal{F}$* ist eine Körpererweiterung $E \supseteq k$:

i) Für alle $f \in \mathcal{F}$ gilt in $E[X]$:

$$f = \alpha \cdot \prod_{i=1}^{n} (X - \alpha_i)$$

mit geeigneten $n \in \mathbb{N}_{\geq 1}$ und $\alpha, \alpha_i \in E$, das heißt f zerfällt über E in Linearfaktoren.

ii) $E = k\left(\alpha \middle| \alpha \in E \wedge \exists_{f \in \mathcal{F}} f(\alpha) = 0\right)$, das heißt E/k wird von den Nullstellen der $f \in \mathcal{F}$ erzeugt.

7.2 Beispiel

Wähle $k = \mathbb{Q}$, $\mathcal{F} = \{f\}$ mit $f := X^3 - 2 \in \mathbb{Q}[X]$ und $k = \mathbb{Q} \subseteq E := \mathbb{Q}(\alpha)$ mit $\alpha^3 = 2$ (vergleiche 5.8 i)). Dann hat f eine Nullstelle in E (nämlich α), und in $E[X]$ gilt:

$$f = (X - \alpha) \cdot \underbrace{\left(X^2 + \alpha X + \alpha^2\right)}_{=:g(X)} \tag{7.1}$$

Hätte f eine weitere Nullstelle $\beta \neq \alpha$ in E, so folgte $\left(\frac{\beta}{\alpha}\right)^3 = \frac{2}{2} = 1$, also $1 \neq \zeta := \frac{\beta}{\alpha} \in E : \zeta^3 = 1$.

Mit 4.6 iii) folgt:

$$\begin{aligned} & \operatorname{Mipo}_{\mathbb{Q}}(\zeta) = X^2 + X + 1 \\ \Rightarrow \quad & [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 \end{aligned}$$

Wegen $\zeta \in E$ erhalte den Körperturm $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq E$ und es folgt der Widerspruch:

$$\underbrace{[E : \mathbb{Q}]}_{=3} = \underbrace{[E : \mathbb{Q}(\zeta)]}_{\in \mathbb{Z}} \cdot \underbrace{[\mathbb{Q}(\zeta) : \mathbb{Q}]}_{=2}$$

Also ist (7.1) die Primfaktorzerlegung von f in $E[X]$, denn:
$g \in E[X]$ ist irreduzibel, sonst gäbe es ein $\beta \in E$ mit $g(\beta) = 0$, woraus $\beta = \alpha = 0$ und der Widerspruch

$$0 = g(\alpha) = 3\alpha^2 \left(= f'(\alpha)\right) \neq 0$$

folgt (siehe oben).
Insbesondere zerfällt f über E nicht in Linearfaktoren, das heißt E ist kein Zerfällungskörper von

7.3 **Satz** (Existenz und Eindeutigkeit von Zerfällungskörpern)

i) Es existiert ein Zerfällungskörper $E \supseteq k$ von $\mathcal{F}$.

ii) Seien $E_1 \supseteq k$, $E_2 \supseteq k$ Zerfällungskörper von $\mathcal{F}$ und $\overline{\sigma} : E_1 \hookrightarrow \overline{E}_2$ ein k-Homomorphismus.
Dann gilt $\overline{\sigma}(E_1) = E_2$, also $\overline{\sigma} : \left(E_1 \xrightarrow{\sim} E_2 \hookrightarrow \overline{E}_2\right)$.

iii) Sind $E_i \supseteq k$ Zerfällungskörper von $\mathcal{F}$ $(i \in \{1,2\})$, dann gibt es einen k-Isomorphismus:

$$\phi : E_1 \xrightarrow{\sim} E_2$$

Beweis

i) Wähle einen algebraischen Abschluss $\overline{k} \supseteq k$ (vergleiche 6.4) und setze:

$$E := k\left(\alpha \middle| \alpha \in \overline{k} \wedge \exists_{f \in \mathcal{F}} f(\alpha) = 0\right)$$

Wegen 6.1 i) ist dann $E_i/_k$ ein Zerfällungskörper von $\mathcal{F}$. $\square_{\text{i)}}$

ii) Weil $E_i/_k$ ein Zerfällungskörper von $\mathcal{F}$ ist, gilt mit

$$\mathcal{N}_i := \left\{\alpha \in E_i \middle| \exists_{f \in \mathcal{F}} f(\alpha) = 0\right\}$$

für $i \in \{1,2\}$:

$$E_i = k(\mathcal{N}_i) \tag{7.2}$$

Damit folgt:

$$\overline{\sigma}(E_1) = k(\overline{\sigma}(\mathcal{N}_1)) \tag{7.3}$$

Behauptung

$$\overline{\sigma}(\mathcal{N}_1) \subseteq \mathcal{N}_2 \tag{7.4}$$

Beweis
Weil $\alpha \in \mathcal{N}_1$ ist, gibt es ein $f \in \mathcal{F}$ mit $f(\alpha) = 0$, womit folgt:

$$0 = \overline{\sigma}(0) = \overline{\sigma}(f(\alpha)) = \underbrace{f^{\overline{\sigma}}}_{=f}(\overline{\sigma}(\alpha))$$

Daher ist $\overline{\sigma}(\alpha) \in \mathcal{N}_2$. $\square_{\text{Behauptung}}$

Dabei ist $f^{\overline{\sigma}} = f$, da $f \in k[X]$ und $\overline{\sigma}|_k = \mathrm{id}_k$.
Es folgt:

$$k \subseteq \overline{\sigma}(E_1) \overset{(7.3)}{=} k(\overline{\sigma}(\mathcal{N}_1)) \overset{(7.4)}{\subseteq} k(\mathcal{N}_2) \overset{(7.2)}{=} E_2$$

Und da sowohl ${\overline{\sigma}(E_1)}/{k}$, als auch ${E_2}/{k}$ Zerfällungskörper von $\mathcal{F}$ sind, gilt sogar $\overline{\sigma}(E_1) = E_2$. $\square_{\text{ii)}}$

iii) Nach 6.7 mit $k' := E_1$ und $L := \overline{E}_2$ existiert ein $\overline{\sigma}$ ($= \sigma$ in 6.7) wie in ii).
Nebenbemerkung: Ist ${E}/{k}$ Zerfällungskörper, so ist ${E}/{k}$ algebraisch.

$\square_{7.3}$

7.4 Satz und Definition (normale Körpererweiterung)

Für eine algebraische Körpererweiterung $E \supseteq k$ ist äquivalent:

i) Jeder k-Homomorphismus $\overline{\sigma} : E \to \overline{E}$ erfüllt $\overline{\sigma}(E) = E$.

ii) Es existiert eine nicht-leere Teilmenge $\mathcal{F} \subseteq \{f \in k[X] \,|\deg(f) \geq 1\}$ so, dass ${E}/{k}$ ein Zerfällungskörper von F ist.

iii) Für alle irreduziblen Polynome $f \in k[X]$ gilt:

$$\left(\exists_{\alpha \in E} f(\alpha) = 0\right) \Rightarrow (f \text{ zerfällt über } E \text{ in Linearfaktoren})$$

In diesem Fall heißt ${E}/{k}$ *normal*.

Beweis

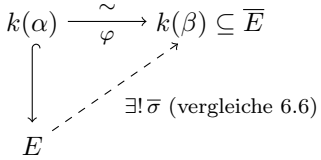
- i) $\Rightarrow$ iii): Da f über $\overline{E}$ in Linearfaktoren zerfällt, zeige nur:

$$\left(\beta \in \overline{E} \wedge f(\beta) = 0\right) \Rightarrow \beta \in E$$

Weil f irreduzibel und ohne Einschränkung normiert ist, gilt:

$$f = \mathrm{Mipo}_k(\alpha) = \mathrm{Mipo}_k(\beta)$$

Nach 5.8 i) folgt, dass es einen k-Isomorphismus $\varphi : k(\alpha) \xrightarrow{\sim} k(\beta)$ mit $\varphi(\alpha) = \beta$ gibt.
Betrachte $k(\alpha) \xrightarrow{\sim} k(\beta) \subseteq E$:



Es folgt:

$$\beta = \varphi(\alpha) \overset{(*)}{=} \overline{\sigma}(\alpha) \in \overline{\sigma}(E) \overset{\text{i)}}{=} E$$

$\square_{\text{i)} \Rightarrow \text{iii)}}$

- iii) $\Rightarrow$ ii): Setze $\mathcal{F} := \{f \in k[X] \,|f \text{ irreduzibel und } \exists_{\alpha \in E} f(\alpha) = 0\}$.
Zeige: ${E}/{k}$ ist ein Zerfällungskörper von $\mathcal{F}$, das heißt es gelten 7.1 i) und ii):

1. $f \in \mathcal{F} \overset{\text{Def.}}{\Rightarrow} \exists_{\alpha \in E}\, f(\alpha) = 0 \overset{\text{iii)}}{\Rightarrow} f$ zerfällt in Linearfaktoren über E. $\square_{\text{iii)} \Rightarrow \text{ii)}}$

- ii) $\Rightarrow$ i): Es sind $E \subseteq \overline{E}$ und $\overline{\sigma}(E) \subseteq \overline{E}$ Zerfällungskörper von $\mathcal{F}$, also $E = \overline{\sigma}(E)$. (vergleiche Beweis von 7.3 ii))

  1. Weil $E/_k$ algebraisch ist, ist für alle $\alpha \in E$ schon $f := \text{Mipo}_k(\alpha) \in \mathcal{F}$ und $f(\alpha) = 0$.
     Also wird $E/_k$ von den Nullstellen aller $f \in \mathcal{F}$ erzeugt.

$\square_{7.4}$

7.5 Beispiel

Wegen 7.2 und 7.4 iii) ist die algebraische Körpererweiterung $E := \mathbb{Q}\left(\sqrt[3]{2}\right)/_k := \mathbb{Q}$ nicht normal, denn das irreduzible Polynom $X^3 - 2 \in k[X]$ besitzt in E eine Nullstelle, zerfällt aber nicht über E in Linearfaktoren.

7.6 **Proposition** (algebraischer Abschluss ist normal)

Sei $E = \overline{E} \supseteq k$ eine algebraische Körpererweiterung, die algebraisch abgeschlossen ist(, das heißt E ist ein algebraischer Abschluss von k). Dann ist $E/_k$ normal.

Beweis

Folgt aus 7.4 iii) und 6.1 iii). $\square_{7.6}$

7.7 Beispiel

i) Sei $E \supseteq k$ eine Körpererweiterung mit $[E : k] = 2$. Dann ist $E/_k$ normal.

ii) Seien $E \supseteq K \supseteq k$ algebraische Körpererweiterungen mit $E/_k$ normal. Dann ist $E/_K$ normal (aber im Allgemeinen nicht $K/_k$). ($k \subseteq E \subseteq \overline{k}$ (!))

Beweis

i) Prüfe 7.4 iii): Sei $f \in k[X]$ irreduzibel und es gibt ein $\alpha \in E$ mit $f(\alpha) = 0$.
Aus $[E : k] = 2$ folgt dann:

$$\deg(f) = [k(\alpha) : k] \overset{k \subseteq k(\alpha) \subseteq E}{\in} \{1,2\}$$

Der Fall $\deg(f) = 1$ ist trivial, denn dann ist $k(\alpha) = k$.
Sei $\deg(f) = 2$ und ohne Einschränkung f normiert:

$$f(X) = X^2 + aX + b; \quad a,b \in k$$

Dann gilt in $E[X]$:

$$f(X) = (X - \alpha)\left(X - \underbrace{(a - \alpha)}_{\in E}\right)$$

$\square_{\text{i)}}$

ii) Klar nach 7.4 ii).

$\square_{7.7}$

7.8 **Beispiel** (Normalität ist nicht-transitiv)

Betrachte den Körperturm:

$$k := \mathbb{Q} \overset{2}{\subseteq} K := \mathbb{Q}\left[\sqrt{2}\right] \overset{2}{\subseteq} E := \mathbb{Q}\left(\sqrt[4]{2}\right)$$

Es gilt $K \subseteq E$, da $\left(\left(\sqrt[4]{2}\right)^2\right)^2 = 2$ ist, also $\left(\sqrt[4]{2}\right)^2 = \sqrt{2}$ gilt.

Beide Erweiterungen sind vom Grad 2 (man nennt sie *quadratisch*) und insbesondere normal, aber ${}^{E}\!/_{k}$ ist nicht normal. (vergleiche mit 5.17)

Beweis

$X^2 - 2, X^4 - 2 \in \mathbb{Q}[X]$ sind irreduzibel, da Eisenstein bezüglich 2, und aus dem Gradsatz folgt die erste Aussage.
Nun existieren $\alpha \in \mathbb{R}$ und $\beta \in \mathbb{C} \setminus \mathbb{R}$ mit $\alpha^4 = \beta^4 = 2$. Erhalte $\mathbb{Q}$-Homomorphismen:

$$i : \mathbb{Q}\left[\sqrt[4]{2}\right] \hookrightarrow \mathbb{R}, \sqrt[4]{2} \to \alpha$$
$$j : \mathbb{Q}\left[\sqrt[4]{2}\right] \hookrightarrow \mathbb{C}, \sqrt[4]{2} \to \beta$$

Wegen $\beta \notin \mathbb{R}$ und $i(E) \subseteq \mathbb{R}$ (also $i(E) \neq j(E)$) kann ${}^{E}\!/_{k}$ nach 7.4 i) (oder auch 7.4 iii)) nicht normal sein. $\square_{7.8}$

7.9 **Definition** (normale Hülle)

Sei $E \supseteq k$ eine algebraische Körpererweiterung. Eine *normale Hülle von E über k* ist eine (algebraische) Körpererweiterung $E \subseteq E'$ mit:

i) ${}^{E'}\!/_{k}$ ist normal.

ii) Ist $E \subseteq K \subseteq E'$ ein Zerfällungskörper mit ${}^{K}\!/_{k}$ normal, so folgt $K = E'$.

7.10 **Satz und Definition** (Konjugierte)

Sei $E \supseteq k$ eine algebraische Körpererweiterung.

i) Es existiert eine bis auf Isomorphie eindeutige normale Hülle ${}^{E'}\!/_{k}$ von ${}^{E}\!/_{k}$.

ii) $[E : k] < \infty \Rightarrow [E' : k] < \infty$

iii) Ist $k \subseteq E \subseteq L$ ein Körperturm und ${}^{L}\!/_{k}$ normal (zum Beispiel $L = \overline{k}$, 7.6), so ist

$$E' = k(\sigma(E) \,|\, \sigma : E \to L \text{ ist } k\text{-Homomorphismus})$$

eine normale Hülle von ${}^{E}\!/_{k}$, die *normale Hülle von E in ${}^{L}\!/_{k}$*.
Die Zerfällungskörper von $k \subseteq \sigma(E) \subseteq L$ heißen die *Konjugierten von E in L*.

Beweis

i) Ein Zerfällungskörper E' von $\mathcal{F} := \{f \in k[X] \mid \deg(f) \geq 1 \text{ und } \exists_{\alpha \in E} f(\alpha) = 0\}$ über k leistet das Gewünschte. (vergleiche 7.3)

ii) Dann kann in i) $|\mathcal{F}| < \infty$ gewählt werden und aus 5.16 i) b) $\Rightarrow$ a) folgt $[E' : k] < \infty$.

iii) Folgt mit 6.6.
TODO: Beweis als Übung einfügen

$\square_{7.10}$

7.11 Beispiel

Wähle $k := \mathbb{Q} \subseteq E := \mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq L := \mathbb{C}$ in 7.10 iii). Dann gibt es den Isomorphismus:

$$\mathrm{Hom}_{\mathbb{Q}\text{-Alg.}}(E,L) \xrightarrow{\sim} \left\{\alpha \in \mathbb{C} | \alpha^3 = 2\right\}; \varphi \mapsto \varphi\left(\sqrt[3]{2}\right)$$

Es existiert genau ein $\alpha \in \mathbb{R}$ mit $\alpha^3 = 2$ (Analysis) und setzte:

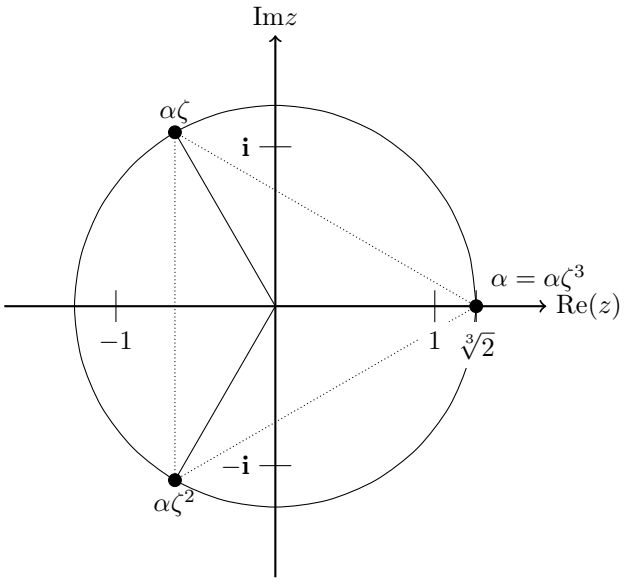
$$\zeta := \zeta_3 = \exp\left(\frac{2\pi \mathbf{i}}{3}\right)$$

Dann gilt $\mathcal{N} = \left\{\alpha, \alpha\zeta, \alpha\zeta^2\right\}$, denn für alle $i \in \mathbb{Z}$ gilt:

$$\left(\alpha\zeta^i\right)^3 = \alpha^3 \cdot \left(\zeta^3\right)^i = 2 \cdot 1 = 2$$

Wegen $\mathrm{ord}(\zeta \in \mathbb{C}^*) = 3$ (vergleiche Bemerkung 4.7) sind $\alpha, \alpha\zeta, \alpha\zeta^2 \in \mathbb{C}$ paarweise verschieden, also *alle* Nullstellen von $X^3 - 2$ in $\mathbb{C}$.

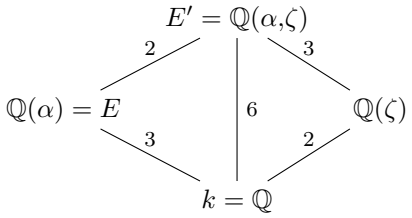
Skizze



Für die normale Hülle E' von E in $\mathbb{C}$ folgt mit 7.10 iii):

$$E' = \mathbb{Q}\left(\alpha, \alpha\zeta, \alpha\zeta^2\right) = \mathbb{Q}(\alpha, \zeta)$$

(Denn: „$\subseteq$“ ist klar, „$\supseteq$“ $\zeta = \frac{\alpha\zeta}{\alpha}$.)
Es gilt $[E' : \mathbb{Q}] = 6$:


$E' = \mathbb{Q}(\alpha,\zeta)$
2
3
$\mathbb{Q}(\alpha) = E$
6
$\mathbb{Q}(\zeta)$
3
2
$k = \mathbb{Q}$

8 Separabilität

Sei k ein Körper.

8.1 Definition ((formale) Ableitung)

Die Abbildung

$$\begin{aligned} k[X] &\to k[X] \\ f = \sum_{i=0} a_i X^i &\mapsto f' := \sum_{i=1} i \cdot a_i X^{i-1} \end{aligned}$$

heißt *(formale) Ableitung.*
Für $f,g \in k[X]$,$a \in k$ gelten:

i) $(af)' = a \cdot f'$
ii) $(f+g)' = f' + g'$
iii) $(fg)' = f'g + fg'$

Beweis

i) und ii) sind klar.
iii): Direktes Nachrechnen. (Wegen i), ii) kann $f = X^m$,$g = X^n$ für $n,m \geq 0$ angenommen werden.)
TODO: Rechnung einfügen

$\square_{8.1}$

8.2 Beispiel

$$\{f \in k[X] \mid f' = 0\} = \begin{cases} k & \text{falls } \operatorname{char}(k) = 0 \\ \{g(X^p) \mid g \in k[X]\} & \text{falls } \operatorname{char}(k) = p > 0 \end{cases}$$

Beweis

TODO: Beweis als Übung einfügen

$\square_{8.2}$

8.3 Satz und Definition (mehrfache Nullstelle)

Seien $f \in k[X] \setminus \{0\}$ und $\alpha \in k$ eine Nullstelle von f.
Dann ist α genau dann eine mehrfache Nullstelle von f, wenn $f'(\alpha) = 0$ gilt.

Beweis

In dem Polynomring $k[X]$ gilt:

$$f(X) = (X-\alpha)^r \cdot g(X) \qquad (1) \tag{8.1}$$

mit $g(\alpha) \neq 0$ und $r \geq 1$, da $f(\alpha) = 0$.
Hierbei heißt r die *Vielfachheit der Nullstelle* α und α heißt genau dann *mehrfache Nullstelle*, wenn $r \geq 2$ ist, sonst *einfache Nullstelle*.
Zeige also:

$$r \geq 2 \Leftrightarrow f'(\alpha) = 0$$

Rechne:

$$f'(X) \overset{8.1}{=} r(X-\alpha)^{r-1} \cdot g(X) + (X-\alpha)^r \cdot g'(X)$$

Wegen $r \geq 1$ folgt:

$$f'(\alpha) = r \cdot (\alpha-\alpha)^{r-1} \cdot g(\alpha) = 0 \overset{g(\alpha)\neq 0, r\neq 0}{\Leftrightarrow} r-1 \geq 1$$

$\square_{8.3}$

8.4 Lemma

Sei $f \in k[X]$ nicht konstant.

i) Für $\alpha \in \overline{k}$ sind äquivalent:

   a) α ist mehrfache Nullstelle von f.
   b) $f(\alpha) = f'(\alpha) = 0$
   c) $(\mathrm{ggT}(f,f'))(\alpha) = 0$

ii) Ist f irreduzibel, so sind äquivalent:

   a) In $\overline{k}$ existiert eine mehrfache Nullstelle von f.
   b) $f' = 0$ in $k[X]$

Beweis

i) Wegen $f \in k[X] \setminus \{0\} \subseteq \overline{k}[X] \setminus \{0\}$ folgt a) $\Leftrightarrow$ b) aus 8.3. Dann gilt:
   b) $\Leftrightarrow (X-\alpha) \mid f,f'$ in $\overline{k}[X] \Leftrightarrow (X-\alpha) \mid \mathrm{ggT}(f,f')$ in $\overline{k}[X] \Leftrightarrow \mathrm{ggT}(f,f')(\alpha) = 0 \Leftrightarrow$ c) $\square_{\text{i)}}$

ii) a) $\Rightarrow$ b):
   Sei $\alpha \in \overline{k}$ eine mehrfache Nullstelle von f. Weil f irreduzibel und ohne Einschränkung normiert (denn $(af)' = a \cdot f'$) ist, gilt:

$$f = \mathrm{Mipo}_k(\alpha) \tag{8.2}$$

   Nach i), a) $\Rightarrow$ b) gilt $f'(\alpha) = 0$. Wegen $\deg(f') < \deg(f)$ folgt aus (8.2) schon $f' = 0$.
   b) $\Rightarrow$ a):
   Weil $\overline{k}$ algebraisch abgeschlossen und f nicht konstant ist, existiert ein $\alpha \in \overline{k}$ mit $f(\alpha) = 0$.
   Wegen $f'(\alpha) = 0\,(\alpha) = 0$ und i) b) $\Rightarrow$ a) ist α eine mehrfache Nullstelle von f.

$\square_{8.4}$

8.5 Definition (separables Polynom)

Ein Polynom $f \in k[X] \setminus k$ heißt *separabel*, wenn alle Nullstellen von f in $\overline{k}$ einfache Nullstellen sind.

8.6 Proposition

Ist $\operatorname{char}(k) = 0$ und $f \in k[X]$ irreduzibel, so ist f separabel.

Beweis

Wegen $\operatorname{char}(k) = 0$ und 8.2 ist $f' \neq 0$. Aus 8.4 ii) folgt die Behauptung. $\square_{8.6}$

8.7 Beispiel

Sei $k := \mathbb{F}_p(t)$ und $f(X) = X^p - t \in k[X]$.
Dann ist f irreduzibel nach 4.6 iii).
In $k[X]$ gilt:

$$f'(X) = pX^{p-1} = 0 \in k[X]$$

Also ist f nach 8.4 ii) nicht separabel, genauer gilt:
Setze $k \subseteq E := k(\alpha)$ mit $0 = f(\alpha) = \alpha^p - t$.
Dann gilt in $E[X]$:

$$f(X) = X^p - t = X^p - \alpha^p = (X - \alpha)^p$$

Damit ist E/k ein Zerfällungskörper von f und es folgt:

$$\operatorname{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right) \underset{6.6}{\simeq} \left\{\beta \in \overline{k} | \beta^p = t\right\} \overset{5.4}{=} \{\alpha\}$$

Denn aus $\beta \in \overline{k}$ und $\beta^p = t$ folgt mit 6.6 schon $\beta^p = t = \alpha^p$ und damit

$$0 = \alpha^p - \beta^p = (\alpha - \beta)^p$$

in $\overline{k}$, das heißt $\alpha = \beta$.
Insbesondere folgt:

$$1 = \left|\operatorname{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)\right| < [k(\alpha) = E : k] = p$$

(vergleiche „$\leq$“ in 6.6)

8.8 Definition (separable(s) Element/Körpererweiterung)

Sei $k \subseteq E$ eine algebraische Körpererweiterung.

i) $\alpha \in E$ heißt *separabel über k*, wenn $\operatorname{Mipo}_k(\alpha)$ in $k[X]$ separabel ist.

ii) E/k heißt *separabel über k*, wenn jedes $\alpha \in E$ separabel ist.

8.9 **Definition** (vollkommener Körper)

k heißt *vollkommen*, wenn jede algebraische Körpererweiterung von k separabel ist.

8.10 Beispiel

i) Jeder Körper der Charakteristik 0 ist vollkommen. (folgt aus 8.6)

ii) $\mathbb{F}_p(t)$ ist nicht vollkommen, denn nach 8.7 ist $\alpha \in \overline{\mathbb{F}}_p(t)$ mit $\alpha^p = t$ nicht separabel über $\mathbb{F}_p(t)$.

iii) Jeder endliche Körper ist vollkommen.

8.11 **Definition** (Separabilitätsgrad)

Sei $E \supseteq k$ eine algebraische Körpererweiterung, so heißt

$$[E:h]_S := \left|\mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)\right| \in \mathbb{N} \cup \{\infty\}$$

der Separabilitätsgrad von E/k.

8.12 **Satz** (vollkommene Körper)

i) Im Fall $\mathrm{char}(k) = p > 0$ gilt:

$$h \text{ vollkommen} \Leftrightarrow \mathrm{Frob}_k : k \xrightarrow{\sim} k \text{ ist ein Isomorphismus}$$

ii) Jeder endliche Körper ist vollkommen.

Beweis

i) „⇒“: Zeige, dass $\mathrm{Frob}_k : k \twoheadrightarrow k$ surjektiv ist.

Sei $\alpha \in k$ und E/k der Zerfällungskörper von $f(X) = X^p - \alpha \in k[X]$.

In $E[X]$ gilt $f(X) = (X-\beta)^p$ für ein geeignetes $\beta \in E$.

Vergleiche 8.7 für $g = \mathrm{Mipo}_k(\beta)$ mit $g|f$.

Weil nun h vollkommen ist, ist g separabel, womit folgt $g = X - \beta \in h[X]$, also $\beta \in k$ und $\alpha = \beta^p = \mathrm{Frob}_k(\beta)$.

Daher ist Frob_k schon ein Isomorphismus, da er als Körperhomomorphismus schon injektiv ist.

„⇐“: Sonst existiert ein irreduzibles und nicht separables $f \in k[X]$, woraus mit 8.4 ii) schon $f' = 0$ in $k[X]$ folgt und sich aus 8.2 schon $f(X) = g(X^p)$ mit einem geeigneten $g = \sum a_i X^i \in k[X]$ ergibt.

Weil Frob_k surjektiv ist, folgt $a_i = b_i^p$ für geeignete $b_i \in k$. Es folgt in $k[X]$:

$$f(X) = g(X^p) = \sum a_i (X^p)^i = \sum b_i^p (X^p)^i = \sum \left(b_i X^i\right)^p = \left(\sum b_i X^i\right)^p$$

$\square_{\text{i)}}$

Dies ist wegen $p \geq 2$ ein Widerspruch dazu, dass f irreduzibel ist.

ii) Dies folgt aus i) und 5.3 iii).

$\square_{8.12}$

8.13 Lemma

Sei $E =: k(\alpha) \supseteq k$ eine einfache algebraische Körpererweiterung.

i) $[k(\alpha) : k]_S = \left|\left\{\beta \in \overline{k} | \text{Mipo}_k(\alpha)(\beta) = 0\right\}\right|$ (Anzahl der Nullstellen des Minimalpolynoms)

ii) α ist genau dann separabel über k, wenn $[k(\alpha) : k] = [k(\alpha) : k]_S$.

Beweis

i) $[k(\alpha) : k]_S \overset{8.11}{=} |\text{Hom}_{k\text{-Alg.}}(k(\alpha), k)| \overset{6.6}{=} \left|\left\{\beta \in \overline{k} | \text{Mipo}_k(\alpha)(\beta) = 0\right\}\right|$

ii) $f := \text{Mipo}_k(\alpha) \in k[X]$ zerfällt über k in Linearfaktoren, also gilt:

$$[k(\alpha) : k] = \deg(f) \geq \left|\left\{\beta \in \overline{k} | f(\beta) = 0\right\}\right| = [k(\alpha) : k]_S$$

Zudem gilt Gleichheit genau dann, wenn alle Nullstellen in $\overline{k}$ einfach sind, also f separabel ist.

$\square_{8.13}$

8.14 Satz (Separabilitäts-Gradsatz)

Seien $E \supseteq K \supseteq k$ algebraische Körpererweiterungen, dann gilt:

$$[E : k]_S = [E : K]_S \cdot [K : k]_S$$

Beweis

Sei $\overline{k} \supseteq E$ ein algebraischer Abschluss.
Weil E/K und K/k algebraisch sind, sind $\overline{k}/K$ und $\overline{k}/k$ algebraische Abschlüsse und nach Definition gilt:

$$\begin{aligned}[E : k]_S &= \left|\text{Hom}_{k\text{-Alg.}}\left(E, \overline{k}\right)\right| \\ [E : K]_S &= \left|\text{Hom}_{K\text{-Alg.}}\left(E, \overline{k}\right)\right| \\ [K : k]_S &= \left|\text{Hom}_{k\text{-Alg.}}\left(K, \overline{k}\right)\right|\end{aligned}$$

Für jedes $\sigma \in \text{Hom}_{k\text{-Alg.}}\left(K, \overline{k}\right)$ existiert nach 6.7 ein k-Isomorphismus $\overline{\sigma} : \overline{k} \to \overline{k}$ mit:

$$\overline{\sigma}|_K = \sigma \tag{8.3}$$

Es ist nun klar, dass 8.14 aus folgender Behauptung folgt:

Behauptung: Die Abbildung

$$\text{Hom}_{K\text{-Alg.}}\left(E, \overline{k}\right) \times \text{Hom}_{k\text{-Alg.}}\left(K, \overline{k}\right) \to \text{Hom}_{k\text{-Alg.}}\left(E, \overline{k}\right), (\tau, \sigma) \mapsto \overline{\sigma} \circ \tau$$

ist wohldefiniert und bijektiv.

Beweis: Die Abbildung ist wohldefiniert, da τ ein k-Homomorphismus ist.
Injektivität: Gelte:

$$\overline{\sigma}_1 \circ \tau_1 = \overline{\sigma}_2 \circ \tau_2 \tag{8.4}$$

Dabei sind $\sigma_i \in \mathrm{Hom}_{k\text{-Alg.}}\left(k,\overline{k}\right)$, $\tau_i \in \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)$ und $i \in \{1,2\}$.
Damit folgt:

$$\begin{array}{ccc} \left(\overline{\sigma}_1 \circ \tau_1\right)|_k & = & \left(\overline{\sigma}_2 \circ \tau_2\right)|_k \\ \| & & \| \\ \overline{\sigma}_1|_k & & \overline{\sigma}_2|_k \\ \| & & \| \\ \sigma_1 & = & \sigma_2 \end{array}$$

Damit folgt $\sigma_1 = \sigma_2$, also $\overline{\sigma}_1 = \overline{\sigma}_2$ und mit (8.4) ergibt sich $\tau_1 = \tau_2$. $\square_{\text{injektiv}}$
Surjektivität: Sei $\alpha \in \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)$, $\sigma := \alpha|_K \in \mathrm{Hom}_{k\text{-Alg.}}\left(K,\overline{k}\right)$ und $\left(\overline{\sigma}^{\,-1} \circ \alpha\right)|_K = \mathrm{id}$.
Also gilt $\tau = \overline{\sigma}^{\,-1} \circ \alpha \in \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)$. Es folgt:

$$\overline{\sigma} \circ \tau = \overline{\sigma} \circ \left(\overline{\sigma}^{\,-1} \circ \alpha\right) = \alpha$$

$\square_{8.14}$

8.15 Satz

Für eine endliche Körpererweiterung $E \supseteq k$ sind äquivalent:

i) ${}^{E}\!/_{k}$ ist separabel.

ii) Es gibt $\alpha_1, \ldots, \alpha_n \in E$, die separabel über k sind mit:

$$E = k\left(\alpha_1, \ldots, \alpha_n\right)$$

iii) $[E : k]_S = [E : k]$

Beweis

i) $\Rightarrow$ ii) ist trivial.
ii) $\Rightarrow$ iii): Wegen den Gradsätzen 8.14 und 5.6 kann man durch Induktion $n = 1$ annehmen und dann folgt die Behauptung aus 8.13 ii) „$\Rightarrow$“.
iii) $\Rightarrow$ i): Sei $\alpha \in E$ beliebig. Da E endlich ist, ist es insbesondere endlich erzeugt, also $E = k\left(\alpha_1 := \alpha, \ldots, \alpha_n\right)$.
Sei $K_m := k\left(\alpha_1, \ldots, \alpha_m\right)$, also $K_n = E$ und $K_0 = k$.
Dann gilt wegen den Gradsätzen 8.14 und 5.6:

$$\begin{array}{ccc} [E : k] & = & \displaystyle\prod_{m=1}^{n} [K_m : K_{m-1}] \\ \| & & \vee| \\ [E : k]_S & = & \displaystyle\prod_{m=1}^{n} [K_m : K_{m-1}]_S \end{array}$$

Daher folgt schon:

$$[K_m : K_{m-1}] = [K_m : K_{m-1}]_S$$

Dabei folgen die Ungleichungen aus dem Beweis von 8.13 ii).
Es folgt insbesondere:

$$[K_1 = k(\alpha) : K_0 = k]_S = [K_1 = k(\alpha) : K_0 = k]$$

Also ist α separabel über k (nach 8.13 iii) „$\Leftarrow$“). $\square_{8.15}$

8.16 **Korollar** (Transitivität der Separabilität)

Für eine algebraische Körpererweiterung $E \supseteq K \supseteq k$ sind äquivalent:

i) ${}^{E}\!/_{k}$ ist separabel.

ii) ${}^{E}\!/_{K}$ und ${}^{K}\!/_{k}$ sind separabel.

Beweis

i) $\Rightarrow$ ii): ${}^{K}\!/_{k}$ separabel ist trivial.
Sei $\alpha \in E$, dann folgt $\mathrm{Mipo}_K(\alpha) \,|\mathrm{Mipo}_k(\alpha)$, also ist mit $\mathrm{Mipo}_k(\alpha)$ auch $\mathrm{Mipo}_K(\alpha)$ separabel, das heißt α ist separabel über K.

ii) $\Rightarrow$ i): Sei $\alpha \in E$, $f := \mathrm{Mipo}_K(\alpha) = \sum_{i=0}^{n} a_i X^i \in K[X]$ und $K' := k(a_i | 0 \leq i \leq n) \subseteq K$.

Dann folgt:

1. ${}^{K'}\!/_{k}$ ist endlich und separabel (8.15 ii) $\Rightarrow$ i)).
2. $f \in K'[X]$ ist separabel $\left(\text{da } {}^{E}\!/_{k} \text{ separabel ist}\right)$.

Es folgt:

$$\infty \overset{1.}{>} [K'(\alpha) : k] \overset{5.6}{=} [K'(\alpha) : K'] \cdot [K' : k] \underset{8.15\ \text{i)} \Leftrightarrow \text{ii)}}{\overset{1.,\ 2.}{=}} [K'(\alpha) : K']_S \cdot [K' : k]_S =$$

$$\overset{8.14}{=} [K'(\alpha) : k]_S$$

Daher ist ${}^{K'(\alpha)}\!/_{k}$ separabel, also α separabel über k. $\square_{8.16}$

8.17 **Satz** (vom primitiven Element) **und Definition**

Sei $k \subseteq E = k(\alpha_1, \ldots, \alpha_n)$ eine endliche Körpererweiterung und seien $\alpha_2, \ldots, \alpha_n$ separabel über k.
Dann existiert ein $\alpha \in E$ mit $E = k(\alpha)$.
Jedes solche α heißt *primitives Element von* ${}^{E}\!/_{k}$.

Bemerkung

Sei p eine Primzahl, $E := \mathbb{F}_p(X,Y)$ und $k := \mathrm{Frob}_E(E) \subseteq E$, dann ist $[E : k] = p^2$ und ${}^{E}\!/_{k}$ ist nicht einfach (ohne Beweis).
TODO: Beweis einfügen

Beweis von 8.17

1. Fall: k ist endlich, also ist E endlich und nach 1.30 i) existiert ein $\alpha \in E^*$ mit $E^* = \langle \alpha \rangle$, womit sich sofort $E = k(\alpha)$ ergibt.
2. Fall: k ist unendlich. Induktiv kann man $n = 2$ annehmen.
   Schreibe $\mathrm{Hom}_{k\text{-Alg.}}\left(E, \overline{k}\right) = \{\sigma_1, \ldots, \sigma_n\}$, das heißt $n := [E : k]_S$.
   Setze:

$$P(X) := \prod_{\substack{1 \leq i,j \leq n \\ i \neq j}} \left((\sigma_i(\alpha_1) - \sigma_j(\alpha_1)) + X(\sigma_i(\alpha_2) - \sigma_j(\alpha_2)) \right) \in \overline{k}[X]$$

Behauptung
In $\overline{k}[X]$ gilt:

$$P(X) \neq 0$$

Beweis:
Sonst existieren $1 \leq i,j \leq n$, $i \neq j$ mit $\sigma_i(\alpha_k) = \sigma_j(\alpha_k)$, $k \in \{1,2\}$. Damit folgt $\sigma_i = \sigma_j$ im Widerspruch zu $i \neq j$. $\square_{\text{Behauptung}}$

Weil $P(X) \neq 0$ und k unendlich ist, gibt es ein $\beta \in k$ mit $P(\beta) \neq 0$.
Darum folgt, dass für $\alpha := \alpha_1 + \beta\alpha_2 \in E$ die Elemente $\sigma(\alpha_1), \ldots, \sigma(\alpha_1) \in \overline{k}$ paarweise verschieden sind, denn:

$$0 \neq P(\beta) = \prod_{\substack{1 \leq i,j \leq n \\ i \neq j}} \left(\underbrace{(\sigma_i(\alpha_1) - \sigma_j(\alpha_1)) + \beta \cdot (\sigma_i(\alpha_2) - \sigma_j(\alpha_2))}_{\overset{\beta \in k}{=} (\sigma_i(\alpha) - \sigma_j(\alpha))} \right)$$

Für $k \subseteq E' := k(\alpha) \subseteq E$ folgt:

$$[E' : k]_S \geq n = [E : k]_S$$

Da die $\sigma_i|_{E'} \in \operatorname{Hom}_{k\text{-Alg.}}\left(E', \overline{k}\right)$ paarweise verschieden sind.
Wegen $E' \subseteq E$ folgt:

$$[E : k]_S = [E' : k]_S \tag{8.5}$$

$\square_{\text{Behauptung}}$

Behauptung
$E = E' = k(\alpha)$, also folgt die Behauptung von 8.17.

Beweis
Weil α_2 separabel über k ist, folgt mit 8.15:

$$\alpha_2 \text{ ist separater über } E' \tag{8.6}$$

Und damit folgt:

$$[E'(\alpha_2) : E']_S = [E'(\alpha_2) : E']$$

Ferner gilt:

$$[E : k]_S \overset{8.14}{\geq} [E'(\alpha_2) : E']_S \cdot [E' : k]_S \overset{(8.5),\,(8.6)}{=} [E'(\alpha_2) : E'] \cdot [E : k]_S$$

Daraus folgt $[E'(\alpha_2) : E'] = 1$, also $\alpha_2 \in E'$.
Wegen $\alpha_1 = \alpha - \beta\alpha_2$ folgt damit auch $\alpha_1 \in E'$ und insgesamt:

$$E' \supseteq k(\alpha_1, \alpha_2) = E$$

Also ist $E = E'$.

$\square_{8.17}$

9 Endliche Körper

9.1 Lemma

Sei k ein endlicher Körper. Dann gelten:

i) $p := \operatorname{char}(k) > 0$ und $\mathbb{F}_p \subseteq k$ ist der Primkörper.

ii) $n := \dim_{\mathbb{F}_p}(k) < \infty$ und $|k| = p^n$.

iii) k ist der Zerfällungskörper von

$$X^{(p^n)} - X \in \mathbb{F}_p[X]$$

über $\mathbb{F}_p$.

Beweis

i) Andernfalls müsste $\operatorname{char}(k) = 0$ gelten, also $\mathbb{Q} \subseteq k$ im Widerspruch zu $|k| < \infty$. (vergleiche 5.1) $\square_{\text{i)}}$

ii) $|k| < \infty$, also folgt $n < \infty$ und aus $k \cong \mathbb{F}_p^n$ als $\mathbb{F}_p$-Vektorraum folgt $|k| = p^n$. $\square_{\text{ii)}}$

iii) **Behauptung**

$$X^{(p^n)} - X = \prod_{\alpha \in k} (X - \alpha) \tag{9.1}$$

in $k[X]$, woraus iii) nach Definition 7.1 folgt.

Beweis

Beide Seiten von (9.1) sind nach iii) normierte Polynome vom Grad p^n und es genügt zu zeigen:

$$\forall_{\alpha \in k} \alpha^{p^n} = \alpha$$

Das ist klar für $\alpha = 0$ und für $0 \neq \alpha \in k^*$ folgt aus 1.25 (für $G = k^*$):

$$\alpha^{p^n - 1} = 1 \qquad \Rightarrow \quad \alpha^{p^n} = \alpha$$

$\square_{9.1}$

9.2 Satz und Definition $(\mathbb{F}_{p^n})$

Seien p eine Primzahl und $n \geq 1$.

Dann ist der Zerfällungskörper von $X^{p^n} - X \in \mathbb{F}_p[X]$ der bis auf Isomorphie eindeutige Körper mit p^n Elementen, geschrieben $\mathbb{F}_{p^n}$.

Bemerkung

Für alle Primzahlen p gilt:

$$\mathbb{Z}/p\mathbb{Z} \overset{\sim}{=} \mathbb{F}_{p^n} \Leftrightarrow n = 1$$

Beweis von 9.2

Die Eindeutigkeit folgt aus 9.1 iii) und 7.3.
Sei $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ ein algebraischer Abschluss.

Behauptung
$\tilde{\mathbb{F}}_{p^n} := \left\{\alpha \in \overline{\mathbb{F}}_p \,\middle|\, \alpha^{p^n} = \alpha\right\} \subseteq \overline{\mathbb{F}}_p$ ist ein Teilkörper.

Beweis
$\mathrm{Frob}_{\overline{\mathbb{F}}_p}^n = \underbrace{\mathrm{Frob}_{\overline{\mathbb{F}}_p} \circ \ldots \circ \mathrm{Frob}_{\overline{\mathbb{F}}_p}}_{n\text{-mal}} : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ ist ein Körperisomorphismus mit:

$$\tilde{\mathbb{F}}_{p^n} = \left\{\alpha \in \overline{\mathbb{F}}_p \,\middle|\, \mathrm{Frob}_{\overline{\mathbb{F}}_p}^n(\alpha) = \alpha\right\}$$

Daraus folgt die Behauptung. $\square_{\text{Behauptung}}$

Es ist klar, dass $\tilde{\mathbb{F}}_{p^n}$ ein Zerfällungskörper von $X^{p^n} - X \in \mathbb{F}_p[X]$ ist.
Wegen $\left(X^{p^n} - X\right)' = -1$ und 8.3 ist $X^{p^n} - X \in \mathbb{F}_p[X]$ separabel, und es folgt $\left|\tilde{\mathbb{F}}_{p^n}\right| = p^n$. $\square_{9.2}$

9.3 Bemerkung

Da $\mathbb{F}_{p^n}/\mathbb{F}_p$ normal ist, gilt für jeden $\mathbb{F}_p$-Homomorphismus $i : \mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$ schon $i(\mathbb{F}_{p^n}) = \tilde{\mathbb{F}}_{p^n}$.
Schreibe daher auch $\mathbb{F}_{p^n} = \tilde{\mathbb{F}}_{p^n}$ und fasse im Folgenden alle $\mathbb{F}_{p^n}$ als Teilkörper eines festen algebraischen Abschlusses $\overline{\mathbb{F}}_p$ auf:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_{p^n}$$

9.4 Korollar

Für alle n,$m \geq 1$ gilt: $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n|m$.

Beweis

„⇐“: Schreibe $m = xn$ mit $x \in \mathbb{N}$ geeignet und sei $\alpha \in \mathbb{F}_{p^n}$, dann folgt:

$$\alpha^{p^m} = \mathrm{Frob}_{\overline{\mathbb{F}}_p}^{nx}(\alpha) = \underbrace{\mathrm{Frob}_{\overline{\mathbb{F}}_p}^n(\alpha) \circ \ldots \circ \mathrm{Frob}_{\overline{\mathbb{F}}_p}^n(\alpha)}_{x\text{-mal}} \overset{\alpha^{p^n} = \alpha}{=} \alpha$$

Also ist $\alpha \in \mathbb{F}_{p^m}$.
„⇒“: Aus

$$m = [\mathbb{F}_{p^m} : \mathbb{F}_p] \overset{\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}}{=} \underbrace{[\overline{\mathbb{F}}_{p^m} : \mathbb{F}_{p^n}]}_{\in \mathbb{N}} \cdot \underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{=n}$$

folgt $n|m$. $\square_{9.4}$

9.5 Satz und Definition (relativer Frobenius)

Seien p eine Primzahl und $1 \leq n|m$, $q := p^n$ und $q' := p^m$, also $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q'} \subseteq \overline{\mathbb{F}}_p$.

i) $F_q := \mathrm{Frob}^n_{\overline{\mathbb{F}}_p} \in \mathrm{Aut}_{\mathbb{F}_q}\left(\overline{\mathbb{F}}_p, \overline{\mathbb{F}}_p\right)$ heißt *der relative Frobenius über* $\mathbb{F}_q$.

ii) Die Gruppe $\mathrm{Aut}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \mathbb{F}_{q'}\right)$ ist zyklisch von Ordnung $\dfrac{m}{n} = [\mathbb{F}_{q'} : \mathbb{F}_q]$ und $\sigma := (F_q)\,|_{\mathbb{F}_{q'}}$ ist ein Erzeuger.

Beweis

i) Zeige $F_q|_{\mathbb{F}_q} = \mathrm{id}$.

Ist $\alpha \in \mathbb{F}_q$ so folgt $F_q(\alpha) = \alpha^q \overset{9.2}{=} \alpha$. $\square_{\text{i)}}$

ii) Es gilt:

$$\left|\mathrm{Aut}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \mathbb{F}_{q'}\right)\right| \overset{(\text{Übung})}{=} \left|\mathrm{Hom}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \mathbb{F}_{q'}\right)\right| \overset{\mathbb{F}_{q'}/\mathbb{F}_q \text{ normal}}{=} \left|\mathrm{Hom}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \overline{\mathbb{F}}_p\right)\right| =$$
$$\overset{\text{Def.}}{=} [\mathbb{F}_{q'} : \mathbb{F}_q]_S \overset{8.12\ \text{ii)}}{=} [\mathbb{F}_{q'} : \mathbb{F}_q] = \frac{m}{n} =: k$$

TODO: Übung beweisen

Weil $\mathbb{F}_{q'}/\mathbb{F}_q$ normal ist, folgt $\sigma(\mathbb{F}_{q'}) = \mathbb{F}'_q \subseteq \overline{\mathbb{F}}_p$, also $\sigma \in \mathrm{Aut}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \mathbb{F}_{q'}\right)$.

Zeige noch: $\mathrm{ord}(\sigma) = k$.

Zunächst ist $\sigma^k = F_q^k = F_{q'} = \mathrm{id}_{\mathbb{F}_{q'}}$ klar.

Wäre nun $a := \mathrm{ord}(\sigma) < k$, so wäre $\sigma^a = F_q^a = \mathrm{id}_{F'_q}$, dass heißt für alle $\alpha \in \mathbb{F}_{q'}$ würde gelten:

$$\alpha = \sigma^a(\alpha) = \alpha^{q^a} = \alpha p^{n \cdot a}$$

Es gilt aber:

$$\left|\left\{\alpha \in \overline{\mathbb{F}}_p | \alpha = \alpha p^{n \cdot a}\right\}\right| \leq p^{na} \overset{a<k}{<} p^{nk} = p^m = q'$$

Dies wird zu $|\mathbb{F}_{q'}| = q'$.

$\square_{9.5}$

10 Galoistheorie

10.1 **Proposition und Definition** (galoissch, Galoisgruppe)

Eine algebraische Körpererweiterung $E \supseteq k$ heißt genau dann *galoissch*, wenn E/k normal und separabel ist. (siehe 7.4 und 8.8 ii))
In diesem Fall heißt

$$\mathrm{Gal}\left(E/k\right) := \mathrm{Aut}_{k\text{-Alg.}}(E) \overset{\text{Blatt 8 Aufgabe 2}}{=} \mathrm{Hom}_{k\text{-Alg.}}(E,E)$$

die Galoisgruppe von E/k.

Beweis

TODO: Beweis von Blatt 8 Aufgabe 2 einfügen

$\square_{10.1}$

10.2 **Beispiel und Definition** (Galoisgruppe von f)

i) Für eine endliche Körpererweiterung $E \supseteq k$ sind äquivalent:

   a) E/k ist galoissch.

   b) E/k ist ein Zerfällungskörper eines separablen Polynoms $f \in k[X]$.

   In diesem Fall kann f in b) irreduzibel gewählt werden und $\mathrm{Gal}\left(E/k\right) =: \mathrm{Gal}(f)$ heißt *die Galoisgruppe von* f.

ii) Jede Erweiterung $E \supseteq k$ endlicher Körper ist galoissch und mit $q := |k|$, das heißt $k = \mathbb{F}_q$, gilt: $\mathrm{Gal}\left(E/k\right)$ ist zyklisch mit Ordnung $[E : k]$ und wird von $F_q|_E$ erzeugt, also $\mathrm{Gal}\left(E/k\right) = \langle F_q|_E \rangle$.

Beweis

i) a) $\Rightarrow$ b): 8.17 impliziert:

$$\exists_{\alpha \in E} : E = k(\alpha)$$

Weil E/k normal ist, folgt aus 7.4 iii), dass E/k ein Zerfällungskörper von

$$f := \mathrm{Mipo}(\alpha) \in k[X]$$

und f separabel und irreduzibel ist.

b) $\Rightarrow$ a): 7.4 ii) impliziert, dass ${}^{E}\!/_{k}$ normal ist.
Weil $f \in k[X]$ separabel ist, folgt mit 7.10 iii) und 8.15 i) $\Rightarrow$ ii), dass ${}^{E}\!/_{k}$ separabel ist.
Zusammen bedeutet das, dass ${}^{E}\!/_{k}$ galoissch ist. $\square_{\text{i)}}$

ii) Folgt aus 9.1 iii), 8.12 ii) und 9.5 ii).

$\square_{10.2}$

10.3 Proposition

Seien $E \supseteq K \supseteq k$ Körpererweiterungen und ${}^{E}\!/_{k}$ galoissch.
Dann gelten:

i) ${}^{E}\!/_{K}$ ist galoissch und

$$\operatorname{Gal}\left({}^{E}\!/_{K}\right) = \left\{\delta \in \operatorname{Gal}\left({}^{E}\!/_{k}\right) \mid \delta|_K = \mathrm{id}_K\right\} \subseteq \operatorname{Gal}\left({}^{E}\!/_{k}\right)$$

ist eine Untergruppe.

ii) Ist zusätzlich ${}^{K}\!/_{k}$ galoissch, dann ist die Abbildung

$$\begin{aligned} \pi : \operatorname{Gal}\left({}^{E}\!/_{k}\right) &\twoheadrightarrow \operatorname{Gal}\left({}^{K}\!/_{k}\right) \\ \sigma &\mapsto \sigma|_K \end{aligned}$$

wohldefiniert und ein surjektiver Gruppenhomomorphismus mit:

$$\ker(\pi) = \operatorname{Gal}\left({}^{E}\!/_{K}\right) \trianglelefteq \operatorname{Gal}\left({}^{E}\!/_{k}\right)$$

Beweis

i) Wegen 7.7 ii) und 8.16 i) $\Rightarrow$ ii) ist ${}^{E}\!/_{K}$ galoissch.
Der Rest ist klar. $\square_{\text{i)}}$

ii) π ist, weil ${}^{K}\!/_{k}$ normal ist, und wegen 7.4 i) wohldefiniert, das heiß für alle $\sigma \in \operatorname{Gal}\left({}^{E}\!/_{k}\right)$ ist

$$\sigma(K) \subseteq K$$

und daher ist $\sigma|_K \in \operatorname{Gal}\left({}^{K}\!/_{k}\right)$.
Dass π ein Gruppenhomomorphismus ist, ist klar.
Weil ${}^{E}\!/_{k}$ normal ist und wegen 6.7 ist π surjektiv.
Die Aussage über den Kern von π folgt aus i).

$\square_{10.3}$

10.4 Proposition

Sei $E \supseteq k$ eine endliche normale Körpererweiterung.
Dann gelten:

i) $|\operatorname{Aut}_k(E)| = [E:k]_s \leq [E:k]$

ii) $|\operatorname{Aut}_k(E)| = [E:k] \Leftrightarrow {}^{E}\!/_{k}$ ist galoissch.

Beweis

Folgt aus 8.11 und 8.15 iii) $\Rightarrow$ i). $\square_{10.4}$

10.5 Satz und Definition (Fixkörper)

Seien E ein Körper und

$$G \subseteq \operatorname{Aut}(E) := \left\{ \varphi : E \xrightarrow{\sim} E | \varphi \text{ ist ein Körperisomorphismus} \right\}$$

eine Untergruppe. Dann gelten:

i) $k := E^G := \{\alpha \in E | \forall_{\sigma \in G} : \sigma(\alpha) = \alpha\}$ ist ein Teilkörper und heißt *der Fixkörper von E unter G.*

ii) Aus $|G| < \infty$ folgt, dass E/k galoissch ist und dass gelten:

- Mit $\operatorname{Aut}_k(E)$ definiert als die Gruppe der Automorphismen von E, die auf k die Identität sind, gilt:

$$\operatorname{Aut}_k(E) = \operatorname{Gal}\left(E/k\right) = G \subseteq \operatorname{Aut}(E)$$

- $[E : k] = |G|$

iii) Ist E/k algebraisch (aber nicht notwendigerweise $|G| < \infty$, beziehungsweise G endlich), so ist E/k galoissch und $G \subseteq \operatorname{Gal}\left(E/k\right)$ ist eine Untergruppe.

Beweis

i) ist klar.

ii) und iii): Zeige zunächst, dass E/k separabel ist:
Sei $\alpha \in E$ und $G\alpha := \{\sigma(\alpha) | \sigma \in G\} \subseteq E$.
Dann gilt für alle $\sigma \in G$:

$$\operatorname{Mipo}_k(\alpha)(\sigma(\alpha)) = \underbrace{(\operatorname{Mipo}_k(\alpha))^\sigma}_{\in k[X] = E^G[X]}(\alpha) = \operatorname{Mipo}_k(\alpha)(\alpha) = 0$$

Damit folgt $|G\alpha| \leq \deg(\operatorname{Mipo}_k(\alpha)) < \infty$ und

$$f(X) := \prod_{\beta \in G\alpha} (X - \beta) \in E[X]$$

ist ein separables Polynom mit $f(\alpha) = 0$, da $\alpha \in G\alpha$ ist.
Zeige noch, dass $f \in k[X]$ ist, denn dann ist α separabel über k:
Weil die Abbildung

$$\begin{aligned} \sigma : G\alpha &\to G\alpha \\ \beta &\mapsto \sigma(\beta) \end{aligned}$$

bijektiv mit der Umkehrabbildung σ^{-1} ist, gilt für alle $\sigma \in G$:

$$f^\sigma(X) = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\beta \in G\alpha} (X - \beta) = f(X)$$

Daher hat $f \in E[X]$ Koeffizienten in $E^G = k$. $\square_{\text{separabel}}$

Zeige nun, dass E/k normal ist:

E/k ist ein Zerfällungskörper aller obigen Polynome $f \in k[X]$ (für $\alpha \in E$ variabel). $\square_{\text{normal}}$

Insgesamt ist also E/k galoissch.

Es ist klar, dass

$$G \subseteq \operatorname{Gal}\left(E/k\right)$$

eine Untergruppe ist.

Sei nun $n := |G| < \infty$.

Dann folgt aus

$$\deg(f) = |G\alpha| \leq |G| = n$$

für alle $\alpha \in E$:

$$[k(\alpha) : k] \leq n$$

Wegen 8.17 angewendet auf die endlichen Zwischenkörper von E/k folgt damit:

$$[E : k] \leq n$$

Dies ist klar, wenn $E \supseteq k$ endlich ist, da dann E insbesondere ein endlicher Zwischenkörper $k(\alpha)$ ist.

Wäre E nicht endlich, so gäbe es für jedes $m \in \mathbb{N}$ einen Zwischenkörper $k \subseteq K = k(\alpha) \subseteq E$ mit $[E : K] > m$, denn E ist das Kompositum aller endlichen Zwischenkörper. Dies ist ein Widerspruch zu $[K = k(\alpha) : k] \leq n$. Also ist E endlich.

TODO: Beweis für diese Aussage einfügen

Insgesamt ergibt sich:

$$n = |G| \leq \left|\operatorname{Gal}\left(E/k\right)\right| \overset{10.4}{\leq} [E : k] \leq n$$

Es folgt:

$$|G| = \left|\operatorname{Gal}\left(E/k\right)\right|$$

Wegen $G \subseteq \operatorname{Gal}\left(E/k\right)$ folgt schon:

$$G = \operatorname{Gal}\left(E/k\right)$$

$\square_{10.5}$

10.6 Beispiel

Seien p eine Primzahl, $E = \overline{\mathbb{F}}_p$, $\sigma := \operatorname{Frob}_{\overline{\mathbb{F}}_p}$ und $G := \left\langle \operatorname{Frob}_{\overline{\mathbb{F}}_p} \right\rangle \subseteq \operatorname{Aut}(E)$.

Dann gilt:

i) $G \cong \mathbb{Z}$

ii) $k := E^G = \mathbb{F}_p$

iii) $G \subsetneq \operatorname{Gal}\left(E/k\right)$ ist eine echte Untergruppe (vergleiche 10.5 ii)).

Beweis

TODO: Beweis einfügen von Zusatzaufgabe Blatt 9

$\square_{10.6}$

10.7 Korollar

Seien $E \supseteq k$ eine normale Körpererweiterung und $G := \mathrm{Aut}_k(E)$.
Dann gelten:

i) ${}^{E}\!/_{E^G}$ ist galoissch mit $\mathrm{Gal}\left({}^{E}\!/_{E^G}\right) = G$.

ii) Ist ${}^{E}\!/_{k}$ galoissch, so gilt $E^G = k$.

Beweis

i) Nach 10.5 ist ${}^{E}\!/_{E^G}$ galoissch und es gilt:

$$\mathrm{Gal}\left({}^{E}\!/_{E^G}\right) = \mathrm{Aut}_{E^G}(E) \overset{*}{=} \mathrm{Aut}\left({}^{E}\!/_{k}\right) = G$$

Zeige $*$:
„$\subseteq$“ ist klar wegen $k \subseteq E^G$.
„$\supseteq$“: Für $\sigma \in \mathrm{Aut}_k(E) = G$ gilt:

$$\sigma|_{E^G} = \mathrm{id}_{E^G}$$

Damit folgt $\sigma \in \mathrm{Aut}_{E^G}(E)$. $\square_{\text{i)}}$

ii) Klar sind $k \subseteq E^G \subseteq E$.

Behauptung

$$\left[E^G : k\right]_S = 1$$

Beweis

Seien $\sigma \in E^G \hookrightarrow \overline{k}$ eine k-Homomorphismus und $\overline{\sigma} : \overline{k} \to \overline{k}$ eine Fortsetzung von σ (vergleiche 6.7).
Nach 7.4 i) gilt, weil ${}^{E}\!/_{k}$ normal ist:

$$\tau := (\overline{\sigma}|_E : E \to E) \in \mathrm{Aut}_k(E) = G$$

Damit folgt:

$$\sigma = \tau|_{E^G} \overset{\tau \in G}{=} \mathrm{id}_{E^G}$$

Es folgt:

$$1 = \left|\mathrm{Hom}_{k\text{-Alg.}}\left(E^G, \overline{k}\right)\right| = \left[E^G : k\right]_S$$

$\square_{\text{Behauptung}}$

Weil nach Voraussetzung ${}^{E}\!/_{k}$ galoissch, also insbesondere separabel ist, ist auch ${}^{E^G}\!/_{k}$ separabel nach 8.16 i) $\Rightarrow$ ii), also gilt:

$$1 = \left[E^G : k\right]_S \overset{8.15\ \text{i)} \Rightarrow \text{ii)}}{=} \left[E^G : k\right]$$

Also gilt $E^G = k$.

$\square_{10.7}$

10.8 **Bemerkung und Beispiel** (absolute Galoisgruppe)

i) Aus 10.7 folgt insbesondere:

$$E/_k \text{ ist galoissch} \Rightarrow E^{\mathrm{Gal}(E/k)} = k$$

Das heißt für alle $\alpha \in E \setminus k$ gibt es ein $\sigma \in \mathrm{Gal}\left(E/_k\right)$ mit $\sigma(\alpha) \neq \alpha = \mathrm{id}(\alpha)$, also separieren die Automorphismen von $E/_k$ die Elemente $\alpha \in E/_k$.

ii) Ist k ein vollkommener Körper, so ist $\overline{k} \supseteq k$ galoissch (vergleiche 6.1 und 8.9) und

$$G_k := \mathrm{Gal}\left(\overline{k}/_k\right)$$

heißt *die absolute Galoisgruppe von k*.

iii) Seien $p \in \mathcal{P}$ eine Primzahl und $k := \mathbb{F}_p(t) \subseteq k(\alpha)$ mit $\alpha p = t$.
Dann ist $E/_k$ nach 8.7 normal und:

$$G := \mathrm{Aut}_k(E) = \{\mathrm{id}\}$$

Insbesondere ist also $E^G = E \supsetneq k$ und:

$$[E : k] = p \neq 1$$

(vergleiche 10.7 ii))

10.9 **Satz** (Hauptsatz der Galoistheorie)

Seien $E \supseteq k$ eine endliche, galoissche Körpererweiterung und $G := \mathrm{Gal}\left(E/_k\right)$. Dann gelten:

i) Die Abbildung

$$\phi : \{H | H \subseteq G \text{ Untergruppe}\} \rightleftarrows \{K | k \subseteq K \subseteq E \text{ Zwischenkörper}\} : \psi$$

$$\phi(H) := E^H \qquad\qquad \psi(K) := \mathrm{Gal}\left(E/_K\right) \subseteq G$$

sind wohldefiniert und zueinander invers.

ii) Für eine Untergruppe $H \subseteq G$ sind äquivalent:

a) $H \trianglelefteq G$ ist ein Normalteiler.

b) $E^H/_k$ ist galoissch.

In diesem Fall ist die Abbildung

$$\begin{aligned} \mathrm{Gal}\left(E/_k\right) = G &\twoheadrightarrow \mathrm{Gal}\left(E^H/_k\right) \\ \sigma &\mapsto \sigma|_{E^H} \end{aligned}$$

ein surjektiver Gruppenhomomorphismus, der einen Isomorphismus

$$\mathrm{Gal}\left(E/_k\right)/\mathrm{Gal}\left(E/_{E^H}\right) \xrightarrow{\sim} \mathrm{Gal}\left(E^H/_k\right)$$

induziert.

Beweis

i) Die Wohldefiniertheit von ϕ ist klar und die von ψ folgt aus 10.3 i).

- $\phi \circ \psi = \mathrm{id}$
  Für den Zwischenkörper $k \subseteq K \subseteq E$ folgt aus 10.7 ii):
  $$K = \phi(\psi(K)) = E^{\mathrm{Gal}(E/K)}$$
- $\psi \circ \phi = \mathrm{id}$
  Für die Untergruppe $H \subseteq G$ gilt nach 10.5 ii) in G:
  $$\mathrm{Gal}\left(E/E^H\right) = H$$

$\square_{\text{i)}}$

ii) b) $\Rightarrow$ a) und zweite Aussage folgen aus 10.3 ii).
a) $\Rightarrow$ b): Wegen 8.16 i) $\Rightarrow$ ii) ist mit E/k auch E^H/k separabel.
Zeige also noch, dass E^H/k normal ist und dazu nach 7.4 i):

Behauptung
Für jeden k-Homomorphismus $\sigma : E^H \hookrightarrow \overline{E}$ gilt $\sigma\left(E^H\right) \subseteq E^H$.

Beweis
Für eine Fortsetzung $\overline{\sigma} : E \hookrightarrow \overline{E}$ von σ gilt, weil E/k normal ist, $\overline{\sigma}(E) = E$, also ist $\overline{\sigma} \in \mathrm{Aut}_k(E) = G$.
Seien nun $\alpha \in E^H$ und $\omega \in H$ beliebig, dann folgt:
$$\omega(\sigma(\alpha)) = (\omega \circ \overline{\sigma})(\alpha)$$
Rechne:
$$\omega \circ \overline{\sigma} = \overline{\sigma} \circ \underbrace{\overline{\sigma}^{-1} \circ \omega \circ \overline{\sigma}}_{=:\omega' \in H, \text{ da } H \trianglelefteq G}$$
Also ist:
$$\omega(\sigma(\alpha)) = \overline{\sigma}(\underbrace{\omega'(\alpha)}_{=\alpha, \text{ da } \omega' \in H, \alpha \in E^H}) = \overline{\sigma}(\alpha) = \sigma(\alpha)$$
Weil α und ω beliebig sind, folgt $\sigma\left(E^H\right) \subseteq E^H$.

$\square_{10.9}$

10.10 Korollar

Ist E/k eine endliche separable Körpererweiterung, so besitzt E/k nur endlich viele Zwischenkörper.

1. Beweis

Die normale Hülle E'/k ist endlich (nach 7.10 ii)), normal und separabel, also galoissch, und
$$G := \mathrm{Gal}\left(E'/k\right)$$
ist endlich, genauer $|G| = [E' : k] < \infty$.
G besitzt nur endlich viele Untergruppen, also besitzt E'/k nach 10.9 i) nur endlich viele Zwischenkörper.
Jeder Zwischenkörper von E/k ist aber insbesondere einer von E'/k. $\square_{\text{1. Beweis}}$

2. Beweis

Nach 8.17 existiert ein $\alpha \in E$ mit $E = k(\alpha)$.
Dann folgt die Aussage aus Blatt 6, Aufgabe 4.
TODO: Beweis einfügen

$\square_{10.10}$

10.11 Definition und Bemerkung (Kompositum)

Seien $E \supseteq k$ eine Körpererweiterung und $k \subseteq K_1, K_2 \subseteq E$ Zwischenkörper.
Dann ist $K_1 \cdot K_2 := K_1(K_2) = K_2(K_1) \subseteq E$ der kleinste Zwischenkörper von E/k, der K_1 und K_2 enthält und heißt *das Kompositum von K_1 und K_2 (in E).*

10.12 Satz und Definition (Galoiserweiterung)

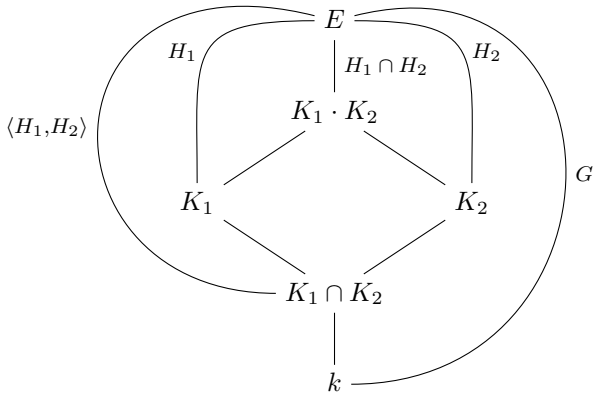
Sei $E \supseteq k$ eine endliche *Galoiserweiterung,* das heißt eine Körpererweiterung, die galoissch ist.
Seien $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ Zwischenkörper und

$$H_i := \mathrm{Gal}\left(E/K_i\right) \subseteq G := \mathrm{Gal}\left(E/k\right)$$

die zugehörigen Untergruppen.
Dann gelten:

i) $K_1 \subseteq K_2 \Leftrightarrow H_2 \subseteq H_1$ (!)
ii) $K_1 \cdot K_2 = E^{H_1 \cap H_2}$
iii) $K_1 \cap K_2 = E^{\langle H_1, H_2 \rangle}$, wobei $\langle H_1, H_2 \rangle \subseteq G$ die von H_1 und H_2 erzeugte Untergruppe ist.

Skizze



Bemerkung

Ist E/k endlich und separabel und E'/k normale Hülle von E/k, dann ist E'/k endlich, separabel und normal.

Beweis

Aus 8.17 gibt es ein $\alpha \in E$ mit:

$$E = k(\alpha)$$

Wähle einen algebraischen Abschluss $\overline{k}$:

$$E \hookrightarrow \overline{E} = \overline{k}$$

Nach 7.10 folgt:

$$E' = k\left(\sigma(\alpha) \,|\, \sigma \in \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{E}\right)\right)$$

Aus

$$\left|\mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{E}\right)\right| = [E:k]_S = [E:k] < \infty$$

folgt nach 7.10 ii):

$$[E':k] < \infty$$

Für alle $\sigma \in \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{E}\right)$ ist

$$\mathrm{Mipo}_k(\sigma(\alpha)) \overset{(!)}{=} \mathrm{Mipo}_k(\alpha) \in k[X]$$

separabel, also ist E'/k nach 8.15 separabel.

Beweis von 10.12

i) „$\Rightarrow$“: $H_2 = \mathrm{Aut}_{K_2}(E) \overset{K_1 \subseteq K_2}{\subseteq} \mathrm{Aut}_{K_1}(E) = H_1$
„$\Leftarrow$“: $K_1 \overset{10.9\,\mathrm{i})}{=} E^{H_1} \overset{H_2 \subseteq H_1}{\subseteq} E^{H_2} \overset{10.9\,\mathrm{i})}{=} K_2$ $\square_{\mathrm{i})}$

ii) $K_1 \cdot K_2 = E^{H_1} \cdot E^{H_2} \overset{\mathrm{i})}{\subseteq} \left(E^{H_1 \cap H_2}\right) \cdot \left(E^{H_1 \cap H_2}\right) = E^{H_1 \cap H_2}$
Ferner gilt:

$$\mathrm{Gal}\left(E/K_1 \cdot K_2\right) \overset{K_i \subseteq K_1 \cdot K_2}{\subseteq} \mathrm{Aut}_{K_1}(E) \cap \mathrm{Aut}_{K_2}(E) = H_1 \cap H_2$$

Daraus folgt mit i):

$$E^{H_1 \cap H_2} \subseteq K_1 \cdot K_2$$

$\square_{\mathrm{ii})}$

iii) $E^{\langle H_1, H_2 \rangle} = E^{H_1} \cap E^{H_2} = K_1 \cap K_2$
(Da jedes Element von $\langle H_1, H_2 \rangle$ ein Produkt von Elementen aus H_1 oder H_2 ist.)

$\square_{10.12}$

10.13 **Beispiel und Definition** (Untergruppen-Diagramm)

Nach Blatt 7, Aufgabe 2 ist die Galoisgruppe von $f := X^3 - 2 \in \mathbb{Q}[X]$ isomorph zu S_3.
TODO: Beweis einfügen

Genauer: Seien $\alpha \in \mathbb{C}$ mit $\alpha^3 = 2$ und $\zeta := \exp\left(\frac{2\pi\mathbf{i}}{3}\right) \in \mathbb{C}$.

Dann ist $E := \mathbb{Q}(\alpha,\zeta)/\mathbb{Q}$ ist ein Zerfällungskörper von f und die Abbildung

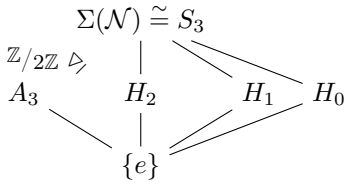
$$\begin{aligned} \mathrm{Gal}\left(E/\mathbb{Q}\right) &\xrightarrow{\sim} \sum \underbrace{\{\alpha,\alpha\zeta,\alpha\zeta^2\}}_{=:\mathcal{N}} \\ \sigma &\mapsto \sigma|_{\mathcal{N}} \end{aligned}$$

ist wohldefiniert und ein Gruppenisomorphismus.
Aus der linearen Algebra I ist folgendes *Untergruppen-Diagramm* der S_3 mit

$$H_0 := \langle \tau_0 := \begin{pmatrix} \alpha\zeta & \alpha\zeta^2 \end{pmatrix} \rangle \qquad H_1 := \langle \tau_1 := \begin{pmatrix} \alpha & \alpha\zeta^2 \end{pmatrix} \rangle \qquad H_2 := \langle \tau_2 := \begin{pmatrix} \alpha & \alpha\zeta \end{pmatrix} \rangle$$

$$A_3 := \langle \begin{pmatrix} \alpha & \alpha\zeta & \alpha\ \zeta^2 \end{pmatrix} \rangle$$

bekannt:



$A_3 \trianglelefteq S_3$ ist der einzige nicht-triviale Normalteiler und es gilt:

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$

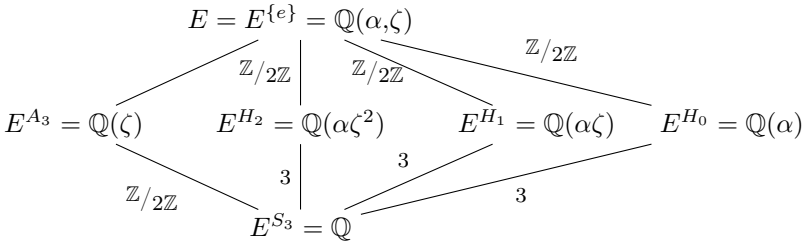
Die H_i sind alle von Ordnung 2 und nicht normal. (vergleiche Übungsaufgabe ?)
TODO: Beweis einfügen
Außerdem können der Durchschnitt und die Erzeugerrelation abgelesen werden, zum Beispiel

$$\begin{aligned} \langle A_3, H_i \rangle &= S_3 \\ H_i \cap A_3 &= \{e\} \end{aligned}$$

für alle $0 \leq i \leq 2$.
Außerdem gilt:

$$E = E^{\{e\}} = \mathbb{Q}(\alpha,\zeta)$$

Aus 10.9 und 10.12 folgt daraus folgendes Diagramm von Zwischenkörpern:



Weil $H_i \subseteq S_3$ nicht normal ist, ist $\mathbb{Q}\left(\alpha\zeta^i\right)/\mathbb{Q}$ nicht normal (vergleiche 7.2).
Weil $A_3 \trianglelefteq S_3$ ist, ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoissch mit:

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) \cong S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$

Zur Bestimmung der Fixkörper:

1. $\sigma := \begin{pmatrix} \alpha & \alpha\zeta & \alpha\zeta^2 \end{pmatrix} \in A_3$ ist ein Erzeuger und es gilt:

   $$\sigma(\zeta) = \sigma\left(\frac{\alpha\zeta}{\alpha}\right) = \frac{\alpha\zeta^2}{\alpha\zeta} = \zeta$$

   Daher ist $\zeta \in E^{A_3}$.
   Wegen $\left[E^{A_3} : \mathbb{Q}\right] = 2$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, da das Minimalpolynom

   $$\mathrm{Mipo}_{\mathbb{Q}}(\zeta) = X^2 + X + 1$$

   Grad 2 hat, folgt also $E^{A_3} = \mathbb{Q}(\zeta)$.
2. Für $\mathrm{id} \neq \tau_i \in H_i$ mit $0 \leq i \leq 2$ gilt:

   $$\tau_i\left(\alpha\zeta^i\right) = \alpha\zeta^i$$

   Also gilt:

   $$\alpha\zeta^i \in E^{H_i}$$

   Wegen $\left[\alpha\zeta^i : \mathbb{Q}\right] = 3$, da

   $$\mathrm{Mipo}_{\mathbb{Q}}\left(\alpha\zeta^i\right) = X^3 - 2$$

   Grad 3 hat, und

   $$\left[E^{H_i} : \mathbb{Q}\right] = \left[E^{H_i} : E^{S_3}\right] = [S_3 : H_i] = 3$$

   folgt $E^{H_i} = \mathbb{Q}\left(\alpha\zeta^i\right)$ für $0 \leq i \leq 2$.

Bemerkung

Seien $E \supseteq k$ eine endliche und galoissche Körpererweiterung, $G := \mathrm{Gal}\left(E/k\right)$ und $H \subseteq G$ eine Untergruppe.
Dann gilt:

a) $\left[E : E^H\right] = [G : H]$
b) $\left[E^H : k\right] = [G : H]$

Beweis

$$\mathrm{Gal}\left(E/E^H\right) = H$$

Aus 10.3 folgt damit a).
Dann gilt:

$$\left[E : E^H\right] \cdot \left[E^H : k\right] = [E : k] = [G : H] \cdot |H| \overset{\text{a)}}{=} [G : H] \cdot \left[E : E^H\right]$$

Und damit folgt:

$$\left[E^H : k\right] = [G : H]$$

$\square_{\text{Bemerkung}}$

10.14 **Definition** (abelsche und zyklische Galoiserweiterung)

Eine Galoiserweiterung ${}^{E}\!/_{k}$ heißt genau dann *abelsch* (beziehungsweise *zyklisch*), wenn $\mathrm{Gal}\left({}^{E}\!/_{k}\right)$ abelsch (beziehungsweise zyklisch) ist.

10.15 Korollar

Seien ${}^{E}\!/_{k}$ eine endliche, abelsche (beziehungsweise zyklische) Körpererweiterung und $k \subseteq K \subseteq E$ ein Zwischenkörper.
Dann ist ${}^{K}\!/_{k}$ abelsch (beziehungsweise zyklisch).

Beweis

$G := \mathrm{Gal}\left({}^{E}\!/_{k}\right)$ ist abelsch und damit folgt, dass $H := \mathrm{Gal}\left({}^{E}\!/_{K}\right) \trianglelefteq G$ gilt.

Aus 10.9 ii) folgt damit, dass ${}^{K}\!/_{k}$ galoissch ist und $\mathrm{Gal}\left({}^{K}\!/_{k}\right) \cong {}^{G}\!/_{H}$ endlich und abelsch (beziehungsweise zyklisch nach 1.22 ii)) ist. $\square_{10.15}$

10.16 Satz

Seien $E \supseteq k$ eine Körpererweiterung, $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ Zwischenkörper und ${}^{K_i}\!/_{k}$ endlich und galoissch für $i \in \{1,2\}$.
Dann gilt:

i) Das Kompositum $K_1 \cdot K_2$ ist endlich und galoissch und die Abbildung

$$\begin{aligned} \varphi : \mathrm{Gal}\left({}^{K_1 \cdot K_2}\!/_{K_1}\right) &\xrightarrow{\sim} \mathrm{Gal}\left({}^{K_2}\!/_{K_1 \cap K_2}\right) \\ \sigma &\mapsto \sigma|_{K_2} \end{aligned}$$

ist wohldefiniert und ein Gruppenisomorphismus.

ii) Die Abbildung

$$\begin{aligned} \psi : \mathrm{Gal}\left({}^{K_1 \cdot K_2}\!/_{k}\right) &\hookrightarrow \mathrm{Gal}\left({}^{K_1}\!/_{k}\right) \times \mathrm{Gal}\left({}^{K_2}\!/_{k}\right) \\ \sigma &\mapsto (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

ist wohldefiniert und ein injektiver Gruppenhomomorphismus.
Im Fall $K_1 \cap K_2 = k$ ist ψ ein Isomorphismus.

Beweis

i) Es existieren separable $f_i \in k[X]$ so, dass

$${}^{K_i}\!/_{k}$$

Zerfällungskörper von f_i für $i \in \{1,2\}$ sind (siehe 10.2 a) $\Rightarrow$ b)).
Nach 8.17 gibt es $\alpha_i \in K_i$ mit $K_i = k(\alpha_i)$ für $i \in \{1,2\}$.
Es gilt $\mathrm{Mipo}_{K_1}(\alpha_2) \,|\, \mathrm{Mipo}_k(\alpha_2)$, da $\mathrm{Mipo}_{K_1}(\alpha_2) \in K_1[X]$ schon α_2 annulliert.

Mit $\mathrm{Mipo}_k(\alpha_2)$ ist damit auch $\mathrm{Mipo}_{K_1}(\alpha_2)$ separabel.
Also gilt

$$k \overset{\text{endlich, separabel}}{\subseteq} K_1 \overset{\text{endlich, separabel}}{\subseteq} K_1(\alpha_2) = K_1(k(\alpha_2)) = K_1(K_2) = K_1 \cdot K_2$$

nach der Gradformel und Transitivität der Separabilität (vergleiche 5.6, 8.14 und 8.16).
Dann ist

$$K_1 \cdot K_2 \big/ k$$

also endlich und galoissch.
φ ist wohldefiniert, da aus

$$\sigma|_{K_1} = \mathrm{id}$$

schon

$$(\sigma|_{K_2})\big|_{K_1 \cap K_2} = \mathrm{id}$$

folgt. Außerdem ist φ offenbar ein Gruppenhomomorphismus.
Für $\sigma \in \ker(\varphi)$ gilt:

$$\begin{aligned} & \mathrm{id} = \sigma|_{K_2} = \sigma|_{K_1} \\ \Rightarrow \quad & \sigma|_{K_1 \cdot K_2} = \sigma = \mathrm{id} \end{aligned}$$

Also ist φ injektiv.
Ferner gilt:

$$K_2^{\mathrm{im}(\varphi)} \overset{\text{Def. von } \varphi}{=} (K_1 \cdot K_2)^{\mathrm{Gal}\left(K_1 \cdot K_2 \big/ K_1\right)} \cap K_2 \overset{10.9\,\mathrm{i})}{=} K_1 \cap K_2 = K_2^{\mathrm{Gal}\left(K_2 \big/ K_1 \cap K_2\right)}$$

Mit 10.9 i) folgt:

$$\mathrm{im}(\varphi) = \mathrm{Gal}\left(K_2 \big/ K_1 \cap K_2\right)$$

Also ist φ surjektiv.

ii) Wohldefiniertheit und, dass ψ ein Gruppenhomomorphismus ist, sind klar.
Aus $\sigma \in \ker(\psi)$ folgt für $i \in \{1,2\}$ schon

$$\sigma|_{K_i} = \mathrm{id}$$

und damit ergibt sich:

$$\sigma = \sigma|_{K_1 \cdot K_2} = \mathrm{id}$$

Deswegen ist ψ injektiv.
Gelte nun $K_1 \cap K_2 = k$ und sei

$$(\sigma, \sigma') \in \mathrm{Gal}\left(K_1 \big/ k\right) \times \mathrm{Gal}\left(K_2 \big/ k\right)$$

beliebig.
Aus i) folgt damit, dass es ein

$$\tilde{\sigma} \in \mathrm{Gal}\left(K_1 \cdot K_2 \big/ K_2\right)$$

mit $\tilde{\sigma}|_{K_1} = \sigma$ gibt, und ebenso ein

$$\tilde{\sigma}' \in \mathrm{Gal}\left(K_1 \cdot K_2 \big/ K_1\right)$$

mit $\tilde{\sigma}'|_{K_2} = \mathrm{id}$.
Dann gilt:

$$\psi\left(\tilde{\sigma}' \cdot \tilde{\sigma}\right) = \left(\tilde{\sigma}' \cdot \tilde{\sigma}|_{K_1}, \tilde{\sigma}' \cdot \tilde{\sigma}|_{K_2}\right) = \left(\mathrm{id} \cdot \sigma, \sigma' \cdot \mathrm{id}\right) = \left(\sigma, \sigma'\right)$$

Daher ist ψ surjektiv.

$\square_{10.16}$

Bemerkung

1. $f_1, f_2 \in k[X]$ separabel $\not\Rightarrow$ $f_1 \cdot f_2 \in k[X]$ separabel, zum Beispiel $f_1 = f_2 = X$.
2. Sind $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ Zwischenkörper und $K_i \big/ k$ endlich und separabel für $i \in \{1,2\}$. Dann ist $K_1 \cdot K_2 \big/ k$ endlich und separabel.

10.17 Proposition

Seien k ein Körper, $f \in k[X]$ separabel, $E \big/ k$ ein Zerfällungskörper von f, $G := \mathrm{Gal}\left(E \big/ k\right)$ (vergleiche 10.2 ii)) und $\mathcal{N} := \{\beta \in E | f(\beta) = 0\}$.
Beachte: $|\mathcal{N}| = \deg(f)$
Dann gilt für alle $\sigma \in G$ schon $\sigma(\mathcal{N}) \subseteq \mathcal{N}$ und es sind äquivalent:

i) $f \in k[X]$ ist irreduzibel.

ii) Für alle $\alpha, \beta \in \mathcal{N}$ gibt es ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$.

Beweis

Aus $\alpha \in \mathcal{N}$ und $\sigma \in G$ folgt:

$$0 = \sigma(\underbrace{f(\alpha)}_{=0}) = f^\sigma(\sigma(\alpha)) \overset{f = f^\sigma, \text{ da } f \in k[X]}{=} f(\sigma(\alpha))$$

Damit folgt $\sigma(\alpha) \in \mathcal{N}$, das heißt für alle $\sigma \in G$ ist $\sigma(\mathcal{N}) \subseteq \mathcal{N}$.
i) $\Rightarrow$ ii):
Ist $\overline{k} \supseteq E$ ein algebraischer Abschluss, so existiert ein $\tilde{\sigma} : \overline{k} \to \overline{k}$ mit $\tilde{\sigma}(\alpha) = \beta$. (Blatt 8, A3,d) $\Rightarrow$ a))
TODO: Beweis einfügen
Weil $E \big/ k$ normal ist, ist $\sigma := \tilde{\sigma}|_E \in G$ und es gilt $\sigma(\alpha) = \tilde{\sigma}(\alpha) = \beta$.
ii) $\Rightarrow$ i):
Für $g := \mathrm{Mipo}_k(\alpha)$ gelten $g | f$ in $k[X]$ und für alle $\beta \in \mathcal{N}$ gibt es ein $\sigma \in G$ mit:

$$\sigma(\alpha) = \beta \qquad \Rightarrow \qquad 0 = \sigma(\underbrace{g(\alpha)}_{=0}) = g^\sigma(\sigma(\alpha)) = g(\beta)$$

Also gilt:

$$g|_{\mathcal{N}} = 0 \tag{10.1}$$

Weil f separabel ist, gilt:

$$|\mathcal{N}| = \deg(f)$$

Aus (10.1) folgt:

$$\deg(g) \geq \deg(f)$$

Wegen $g|f$ sind damit f und g in $k[X]$ assoziiert, also ist mit g auch f irreduzibel. $\square_{10.17}$

10.18 **Beispiel** (biquadratische Erweiterung)

Seien $\alpha,\beta \in \overline{\mathbb{Q}}$ mit $\alpha_1^2 = 2$ und $\alpha_2^2 = 3$ und $E := \mathbb{Q}(\alpha_1,\alpha_2)$.
Dann gelten:

$$\mathrm{Gal}\left(E/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\begin{aligned} \beta &:= \alpha_1 + \alpha_2 \\ E &= \mathbb{Q}(\beta) \\ \mathrm{Mipo}_{\mathbb{Q}}(\beta) &= X^4 - 10X^2 + 1 \in \mathbb{Q}[X] \end{aligned}$$

Beweis

Seien $k := \mathbb{Q}, K_1 := \mathbb{Q}(\alpha_1), K_2 := \mathbb{Q}(\alpha_2)$ und $E = K_1 \cdot K_2$.
Mit $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ ist klar, dass K_i/k für $i \in \{1,2\}$ galoissch vom Grad 2 ist, also folgt:

$$\mathrm{Gal}\left(K_i/k\right) \cong \mathbb{Z}/2\mathbb{Z}$$

Man kann zeigen, dass $K_1 \cap K_2 = k$ gilt (Übung).
TODO: Beweis einfügen
Nach 10.16 ii) ist

$$\begin{aligned} \varphi : \mathrm{Gal}\left(E/k\right) &\xrightarrow{\sim} \mathrm{Gal}\left(K_1/k\right) \times \mathrm{Gal}\left(K_2/k\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \varphi(\sigma) &:= (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

ein Isomorphismus.
Für $i \in \{1,2\}$ gilt:

$$\mathrm{Gal}\left(K_i/k\right) = \{1,\tau_i\}$$

Dabei $\tau_i : K_i \xrightarrow{\sim} K_i$ durch $\tau_i(\alpha_i) = -\alpha_i$ eindeutig bestimmt ist.
Nach Definition von φ folgt:

$$\mathrm{Gal}\left(E/k\right) = \{1,\sigma_1,\sigma_2,\sigma_1\sigma_2\}$$

Dabei sind diese Elemente eindeutig bestimmt durch folgende Tabelle:

$x \in G$	$x(\alpha_1)$	$x(\alpha_2)$
1	α_1	α_2
σ_1	$-\alpha_1$	α_2
σ_2	α_1	$-\alpha_2$
$\sigma_1\sigma_2$	$-\alpha_1$	$-\alpha_2$

Rechne nun für $\beta := \alpha_1 + \alpha_2 \in E$ nach:

$$\begin{aligned} f(X) := & \prod_{\sigma \in \mathrm{Gal}\left(E/k\right)} (X - \sigma(\beta)) = \\ & \overset{\text{Tabelle}}{=} (X - (\alpha_1 + \alpha_2))(X + (\alpha_1 + \alpha_2))(X - (\alpha_1 - \alpha_2))(X + (\alpha_1 - \alpha_2)) = \\ & = \left(X^2 - (\alpha_1 + \alpha_2)^2\right)\left(X^2 - (\alpha_1 - \alpha_2)^2\right) = \left(X^2 - (5 + 2\alpha_1\alpha_2)\right)\left(X^2 - (5 - 2\alpha_1\alpha_2)\right) = \\ & = X^4 - 10X^2 + (5 + 2\alpha_1\alpha_2)(5 - 2\alpha_1\alpha_2) = X^4 - 10X^2 + 25 - 24 = \\ & = X^4 - 10X^2 + 1 \in \mathbb{Q}[X] \end{aligned}$$

Offenbar sind die Nullstellen von f genau $\{\beta, \sigma_1(\beta), \sigma_2(\beta), \sigma_1\sigma_2(\beta)\}$, woraus folgt, dass E/k ein Zerfällungskörper von f ist.
Aus 10.17 i) $\Rightarrow$ ii) folgt nun, dass $f \in k[X]$ irreduzibel ist, und weil f normiert ist, gilt $f = \mathrm{Mipo}_k(\beta)$. $\square_{10.18}$

11 Bestimmung einiger Galoisgruppen

Fixiere in Kapitel 11 (Bestimmung einiger Galoisgruppen)

Sei k ein Körper.

11.1 Satz und Definition (Die Permutationsdarstellung)

Seien $f \in k[X]$ separabel, $n := \deg(f) > 0$, $E \supseteq k$ ein Zerfällungskörper von f und

$$\mathcal{N} := \{\alpha \in E | f(\alpha) = 0\}$$

mit $|\mathcal{N}| = n$.
Dann ist die Abbildung

$$p : \mathrm{Gal}\left(E/k\right) \hookrightarrow \sum(\mathcal{N}) \left(\underset{\text{einer Nummerierung}}{\overset{\text{nach Wahl}}{\cong}} \mathcal{N} = \{\alpha_1, \ldots, \alpha_n\} \right)$$

mit

$$p(\sigma)(\alpha) = \sigma(\alpha)$$

für alle $\alpha \in \mathcal{N}$ und $\sigma \in \mathrm{Gal}\left(E/k\right)$ wohldefiniert und ein injektiver Gruppenhomomorphismus.

p heißt *die Permutationsdarstellung von* $Gal\left(E/k\right)$.
Es gelten:

$$f \in k[X] \text{ irreduzibel} \overset{\text{a)}}{\Leftrightarrow} \left(\underset{\alpha,\beta \in \mathcal{N}}{\forall} \underset{\sigma \in \mathrm{Gal}\left(E/k\right)}{\exists} : p(\sigma)(\alpha) = \beta \right) \overset{\text{b)}}{\Leftarrow} p \text{ ist ein Isomorphismus}$$

Beweis

E/k ist endlich und galoissch nach 10.2 b) $\Rightarrow$ a).
Die Aussagen über p folgen wie in Aufgabe 2, ii) auf Blatt 7.
TODO: Beweis einfügen
a) ist 10.17 i) $\Leftrightarrow$ ii).
b) ist klar. $\square_{11.1}$

11.2 Quadratische Gleichungen

$f = X^2 + aX + b \in k[X]$ besitze keine Nullstelle in k.

Dann ist $E := {}^{k(\alpha)}/_{k}$ für $f(\alpha) = 0$ ein Zerfällungskörper von f, und in $E[X]$ gilt nach 7.1 i):

$$f(X) = (X - \alpha) \cdot (X - (-\alpha - a))$$

Weiter ist die Separabilität von $f \in k[X]$, weil f irreduzibel ist, äquivalent zu folgender Äquivalenz in $k[X]$:

$$0 = f'(X) = 2X + a \Leftrightarrow (\operatorname{char}(k) = 2 \wedge a = 0)$$

Gelte nun $\operatorname{char}(k) \neq 2$ oder $a \neq 0$.
Dann ist ${}^{E}/_{k}$ galoissch mit $\operatorname{Gal}\left({}^{E}/_{k}\right) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ und das eindeutige $\sigma \in \operatorname{Gal}\left({}^{E}/_{k}\right) \setminus \{1\}$ ist durch $\sigma(\alpha) = -\alpha - a$ eindeutig bestimmt.

11.3 Kubische Gleichungen

Es gelte $\operatorname{char}(k) \neq 2{,}3$ und $F(X) = X^3 + AX^2 + BX + C \in k[X]$ besitze keine Nullstellen in k.
Dann ist $F \in k[X]$ irreduzibel.

11.3.1 **Lemma** (Normalform)

Jede kubische Gleichung der Form $F(X)$ lässt sich reduzieren auf:

$$f(X) =: X^3 + aX + b$$

Beweis

Betrachte ähnlich der quadratischen Ergänzung:

$$f(X) := F\left(X - \frac{A}{3}\right) = X^3 + X^2\left(-3 \cdot \frac{A}{3} + A\right) + \left(B - \frac{A^2}{3}\right)X + \frac{2A^3}{27} - \frac{AB}{3} + C =$$
$$=: X^3 + aX + b$$

(Hier geht $\operatorname{char}(k) \neq 3$ ein.)
Da $k[X] \xrightarrow{\sim} k[X], X \mapsto X - \frac{A}{3}$ ein Isomorphismus ist, folgt die Behauptung. $\square_{11.3.1}$

11.3.2 Bestimmung der Galoisgruppe

Betrachte im Folgenden $f(X)$.
Es gilt $f'(X) = 3X^2 + a \neq 0$, da $3 \neq 0$ wegen $\operatorname{char}(k) \neq 3$, also ist $f \in k[X]$ separabel nach 8.4 ii), und der Zerfällungskörper ${}^{E}/_{k}$ von f ist galoissch.
Nummeriere:

$$\mathcal{N} := \{\alpha \in E | f(\alpha) = 0\} = \{\alpha_1, \alpha_2, \alpha_2\}$$

Nach 11.1 existiert genau ein Gruppenhomomorphismus $\varrho : \operatorname{Gal}\left({}^{E}/_{k}\right) \hookrightarrow S_3$ mit:

$$\underset{\sigma \in \operatorname{Gal}({}^{E}/_{k}), 1 \leq i \leq 3}{\forall} : \sigma(\alpha_i) = \alpha_{\varrho(\sigma)(i)} \tag{11.1}$$

Weil f irreduzibel ist, folgt $[E : k] \geq 3$ und aus der bekannten Untergruppenstruktur von S_3 (vergleiche 10.13) folgt:

$$\operatorname{Gal}\left({}^{E}/_{k}\right) \cong \operatorname{im}(\varrho) = \begin{cases} A_3 \\ S_3 \end{cases}$$

Betrachte:

$$\delta := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in E^*$$

(Dies gilt, da f separabel ist.)

Behauptung

Für alle $\sigma \in \mathrm{Gal}\left(E/k\right)$ gilt in E^*:

$$\sigma(\delta) = \mathrm{sgn}(\varrho(\sigma)) \cdot \delta$$

Beweis

Die Behauptung ist klar wegen (11.1), der Definition von σ und δ und der Definition von $\mathrm{sgn}(\varrho(\sigma))$ als Anzahl der Fehlstände. $\square_{\text{Behauptung}}$

Es folgt in $\mathbb{Z}$:

$$\mathrm{im}(\varrho) = A_3 \overset{\text{Definition von } A_3}{\Leftrightarrow} \underset{\sigma \in \mathrm{Gal}(E/k)}{\forall} : \mathrm{sgn}(\varrho(\sigma)) = 1 \overset{\substack{\text{Behauptung} \\ \mathrm{char}(k) \neq 2}}{\Leftrightarrow} \underset{\sigma \in \mathrm{Gal}(E/k)}{\forall} : \sigma(\delta) = \delta$$

Dies ist äquivalent zu $\delta \in E^{\mathrm{Gal}(E/k)} = k$.

Ferner gilt mit $\Delta := \delta^2$ für alle $\sigma \in \mathrm{Gal}\left(E/k\right)$:

$$\sigma(\Delta) = (\pm\delta)^2 = \Delta$$

Damit folgt $\Delta \in k$.

Später wird noch gezeigt:

$$\Delta = -4a^3 - 27b^2$$

Damit gilt für die Galoisgruppe der irreduziblen Gleichung $X^3 + aX + b$:

$$\mathrm{Gal}\left(E/k\right) \cong \begin{cases} A_3 & \Delta = -3a^3 - 27b^2 \in (k^*)^2 \\ S_3 & \text{sonst} \end{cases}$$

$\square_{11.3.2}$

11.3.3 Beispiel

Seien $k = \mathbb{Q}$ und $f(X) := X^3 - X + 1 \in \mathbb{Q}[X]$.

Wegen $f(\pm 1) \neq 0$ besitzt f keine Nullstelle in $\mathbb{Q}$ (benutzt, dass ein ganzzahliges Polynom ohne Nullstellen in $\mathbb{Z}$ keine Nullstellen in $\mathbb{Q}$ hat und eine ganzzahlige Nullstelle eines normierten Polynoms den letzten Koeffizienten teilt).

Außerdem gilt hier:

$$\Delta = -4 \cdot (-1)^3 - 27 \cdot 1^2 = -23 \notin (\mathbb{Q}^*)^2$$

Also hat die Gleichung $X^3 - X + 1 = 0$ über $\mathbb{Q}$ die Galoisgruppe S_3.

Ferner gilt mit dem Zerfällungskörper E von f für den eindeutigen Zwischenkörper $\mathbb{Q} \subseteq K \subseteq E$ mit $[K : \mathbb{Q}] = 2$ (vergleiche 10.13):

$$K = \mathbb{Q}(\delta) = \mathbb{Q}\left(\sqrt{-23}\right)$$

11.4 Die allgemeine Gleichung

Sei $n \geq 1$ fixiert und $E := k(t_1, \ldots, t_n)$.
Dann existiert genau eine Abbildung

$$\varrho : S_n \to \mathrm{Aut}(E)$$

für die für alle $\sigma \in S_n$ mit $1 \leq i \leq n$ gilt:

$$\varrho(\sigma)(t_i) = t_{\sigma(i)}$$

Benutze zum Beweis die universelle Eigenschaft des Polynomrings und des Quotientenkörpers.
Zudem ist ϱ ein injektiver Gruppenhomomorphismus, vermöge dessen wir $S_n \subseteq \mathrm{Aut}(E)$ als Untergruppe auffassen.
TODO: Beweis einfügen

11.4.1 Proposition und Definition (symmetrische rationale Funktionen)

Die Körpererweiterung $K := E^{S_n} \subseteq E$ ist galoissch mit $\mathrm{Gal}\left(E/K\right) = S_n$.
K heißt *der Körper der symmetrischen rationalen Funktionen (in den Variablen $t_1, \ldots, t_n$ über k).*

Beweis

Folgt aus 10.7 i). $\square_{11.4.1}$

11.4.2 Beispiel

Sei $n = 2$, betrachte also $S_2 = \left\{1, \begin{pmatrix} 1 & 2 \end{pmatrix} =: \sigma\right\}$.
Wegen

$$\sigma(t_1 + t_2) = t_2 + t_1 = t_1 + t_2$$

ist $t_1 + t_2 \in k(t_1, t_2)^{S_2}$, aber, falls $\mathrm{char}(k) \neq 2$ ist, ist wegen

$$\sigma(t_1 - t_2) = t_2 - t_1 = -(t_1 - t_2) \neq t_1 - t_2$$

das Polynom $t_1 - t_2 \notin k(t_1, t_2)^{S_2}$, da $1 \neq -1$.

11.4.3 Definition (elementarsymmetrische Polynome)

Die in der Entwicklung

$$k[t_1, \ldots, t_n][X] \ni f(X) := \prod_{i=1}^{n} (X - t_i) =: \sum_{j=0}^{n} (-1)^j \cdot s_j(t_1, \ldots, t_n) \cdot X^{n-j}$$

auftretenden $s_j \in k[t_1, \ldots, t_n]$ $(0 \leq j \leq n)$ heißen *die j-ten elementarsymmetrischen Polynome (in $t_1, \ldots, t_n$ über k).*
Es gilt für alle $0 \leq k \leq n$:

$$s_k(t_1, \ldots, t_n) = \sum_{1 \leq j_1 < \ldots < j_k \leq n} (t_{j_1} \cdot t_{j_2} \cdot \ldots \cdot t_{j_k})$$

Zum Beispiel: $s_0 = 1$, $s_1 = t_1 + \ldots + t_n$, $s_n = t_1 \cdot \ldots \cdot t_n$.

11.4.4 **Definition** (algebraische Unabhängigkeit)

Seien A eine k-Algebra und I eine Menge und für alle $i \in I$ sei $a_i \in A$.

Dann heißt $(a_i)_{i \in I}$ genau dann *algebraisch unabhängig über* k, wenn der eindeutige k-Algebrenhomomorphismus $k[I] \to A$ mit $\varphi(i) = a_i$ für alle $i \in I$ ist injektiv.

11.4.5 **Beispiel**

i) Für $I = \{1\}$ ist $a_1 \in A$ genau dann algebraisch unabhängig über k, wenn a_1 transzendent über k ist.

ii) Die Elemente

$$a_1 := X^2 \qquad\qquad a_2 := X^3$$

in $A := k[X]$ sind transzendent über k (vergleiche Blatt 6 Aufgabe 1 iii)), aber (a_1,a_2) ist nicht algebraisch unabhängig über k, da für $0 \neq f(X,Y) := X^3 - Y^2 \in k[X,Y]$ gilt $f(a_1,a_2) = 0$.

TODO: Beweis einfügen

(Beachte: (a_1,a_2) sind in A aber k-linear unabhängig.)

11.4.6 **Satz** (Hauptsatz über symmetrische Funktionen)

Es gelten:

i) $K = E^{S_n} \subseteq E$ ist ein Zerfällungskörper von $f(X) = \prod_{i=1}^{n} (X - t_i) \in K[X]$.

ii) Hauptsatz über symmetrische Funktionen:

$$K = k(s_1, \ldots, s_n)$$

iii) $(s_1, \ldots, s_n) \subseteq K$ ist algebraisch unabhängig über k (und damit ist $K = E^{S_n}$ ein rationaler Funktionenkörper über k in den Variablen $s_1, \ldots, s_n$).

Insbesondere gilt für alle $f,g \in k(T_1, \ldots, T_n)$:

$$f(s_1, \ldots, s_n) = g(s_1, \ldots, s_n) \Rightarrow f = g$$

11.4.7 **Bemerkung**

i) Sei $\operatorname{char}(k) \neq 2$. Es ist $E^{A_n} \supseteq K = E^{S_n}$ galoissch vom Grad 2 und für

$$\delta := \prod_{1 \leq i < j \leq n} (t_i - t_j)$$

gilt:

$$E^{A_n} = K(\delta) \overset{11.4.6\ \text{ii)}}{=} k(s_1, \ldots, s_n, \delta)$$

Es ist ein offenes Problem, ob $f_1, \ldots, f_n \in E^{A_n}$ existieren, die $E^{A_n} = k(f_1, \ldots, f_n)$ erfüllen.

ii) **Vermutung**

Für jede endliche Gruppe G existiert eine Galoiserweiterung $E/\mathbb{Q}$ mit $\operatorname{Gal}\left(E/\mathbb{Q}\right) \cong G$.

Beweis von 11.4.6

i) Zunächst gilt für alle $\sigma \in S_n$:

$$f^\sigma(X) = \prod_{i=1}^{n} \left(X - t_{\sigma(i)}\right) = f(X)$$

Also ist $f \in K[X]$.

Wegen $E = k(t_1, \ldots, t_n) = K(t_1, \ldots, t_n)$ ist klar, dass E/k ein Zerfällungskörper von f ist. $\square_{\text{i)}}$

ii) Wir haben $k(s_1, \ldots, s_n) \overset{\text{i)}}{\subseteq} K = E^{S_n} \subseteq E$ und nach 11.4.3 gilt sogar $f(X) \in k(s_1, \ldots, s_n)[X]$, und damit folgt wegen $\deg(f) = n$ und i):

$$[E : k(s_1, \ldots, s_n)] \leq n!$$

Aus $\left[E : E^{S_n}\right] = |S_n| = n!$ (siehe 11.4.1) folgt $K = k(s_1, \ldots, s_n)$. $\square_{\text{ii)}}$

iii) Seien $k(S_1, \ldots, S_n) \subseteq \tilde{L}$ ein Zerfällungskörper von

$$\tilde{f}(X) := \sum_{i=0}^{n} (-1)^i \cdot \mathcal{S}_i \cdot X^{n-i} \in k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X]$$

mit $\mathcal{S}_0 := 1$ und seien $T_1, \ldots T_n \in \tilde{L}$ die Nullstellen von $\tilde{f}$ in $\tilde{L}$ (gelistet mit Vielfachheit).
Dann gilt:

$$\tilde{L} = k(\mathcal{S}_1, \ldots, \mathcal{S}_n)(T_1, \ldots, T_n) \overset{(11.2)}{=} k(T_1, \ldots, T_n)$$

Denn es gilt für alle i:

$$\mathcal{S}_i = s_i(T_1, \ldots, T_n) \in k(T_1, \ldots, T_n) \tag{11.2}$$

Für den eindeutigen k-Algebrenhomomorphismus

$$\varphi : k[t_1, \ldots, t_n] \to k[T_1, \ldots, T_n]$$

mit $\varphi(t_i) = T_i$ gilt

$$\varphi(s_i) \overset{(11.2)}{=} \mathcal{S}_i$$

für alle $1 \leq i \leq n$.
Da $\{\mathcal{S}_1, \ldots, \mathcal{S}_n\} \subseteq k[\mathcal{S}_1, \ldots, \mathcal{S}_n]$ algebraisch unabhängig über k ist, ist $\{s_1, \ldots, s_n\} \subseteq k[s_1, \ldots, s_n]$ algebraisch unabhängig über k.

$\square_{11.4.6}$

11.4.8 **Definition** (allgemeines Polynom n-ten Grades)

$$p(X) := X^n + \mathcal{S}_1 X^{n-1} + \ldots + \mathcal{S}_n = X^n + \sum_{i=1}^{n} \mathcal{S}_i \cdot X^{n-i} \in k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X]$$

heißt das *allgemeine Polynom n-ten Grades über k.*

11.4.9 Bemerkung

Seien $F \supseteq k$ eine Körpererweiterung und

$$f = X^n + \sum_{i=1}^{n} a_i X^{n-i} \in F[X]$$

mit $a_i \in F$ für $1 \leq i \leq n$ ein normiertes Polynom vom Grad n.
Dann existiert genau ein k-Algebrenhomomorphismus

$$\varphi : k(\mathcal{S}_1, \ldots, \mathcal{S}_n) \to F$$

mit

$$\begin{aligned} \varphi[X] : k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X] &\to F[X] \\ \varphi[X](p(X)) &= f(X) \end{aligned}$$

also mit $\varphi(\mathcal{S}_i) = a_i$ für $1 \leq i \leq n$.

11.4.10 Satz

$p(X) \subseteq k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X]$ ist irreduzibel und separabel und es gilt:

$$\mathrm{Gal}(p(X)) \cong S_n$$

(vergleiche 10.2 i))

Beweis

Wegen 11.4.6 ii) existiert ein k-Isomorphismus

$$\varphi : k(\mathcal{S}_1, \ldots, \mathcal{S}_n) \xrightarrow{\sim} k(s_1, \ldots, s_n)$$

mit $\varphi(\mathcal{S}_i) = (-1)^i \cdot s_i$ und für diesen gilt

$$\varphi[X](p(X)) = f(X)$$

wie in 11.4.3.
Die Aussagen folgen nun aus den analogen Aussagen für f, nämlich in 11.4.6 i) und 11.4.1. $\square_{11.4.10}$

11.4.11 Satz (Hilbertscher Irreduzibilitätssatz)

Für $n \geq 1$ existieren unendlich viele Tupel $(q_1, \ldots, q_n) \in \mathbb{Q}^n$, sodass

$$f(X) = X^n + \sum_{i=1}^{n} q_i X^{n-i} \in \mathbb{Q}[X]$$

irreduzibel und separabel ist und es gilt:

$$\mathrm{Gal}(f) = S_n$$

(ohne Beweis)

Beispiel

Obiges gilt nicht für alle q_i.
Sei zum Beispiel $q_i = 0$, dann ist $f(X) = X^n$ mit der trivialen Galoisgruppe und nicht S_n.

12 Kreisteilungskörper (die Galoistheorie der Gleichung $X^n - 1 = 0$)

Fixiere in Kapitel 12 (Kreisteilungskörper (die Galoistheorie der Gleichung $X^n - 1 = 0$)**)**

Sei k ein Körper und $n,m \in \mathbb{N}_{\geq 1}$ entweder mit $\operatorname{char}(k) = 0$ oder $\operatorname{char}(k) \nmid n,m$.

12.1 Proposition und Definition (Gruppe der n-ten Einheitswurzeln)

Die Teilmenge

$$U_n := U_n(k) := \left\{ \zeta \in \overline{k}^* \middle| \zeta^n = 1 \right\} \subseteq \overline{k}^*$$

ist eine zyklische Untergruppe der Ordnung n, *die Gruppe der n-ten Einheitswurzeln* (Abkürzung: EW) *(in k)*.

Beweis

Es ist klar, dass $U_n \subseteq \overline{k}^*$ eine Untergruppe ist.
Für $\zeta \in U_n$ gelten:

$$(X^n - 1)(\zeta) = 0$$
$$(X^n - 1)'(\zeta) = n\zeta^{n-1} \neq 0$$

Denn es gilt $\zeta \neq 0$ und $n \neq 0$, da $\operatorname{char}(k) \nmid n$.
Damit ist $X^n - 1 \in k[X]$ separabel und es folgt:

$$|U_n| = \deg(X^n - 1) = n$$

Insbesondere ist $U_n \subseteq \overline{k}^*$ endlich, also zyklisch nach 1.28. $\square_{12.1}$

Bemerkung

Sei p eine Primzahl und $n \in \mathbb{N}_{\geq 1}$, dann folgt:

$$\left\{ \zeta \in \overline{\mathbb{F}}_p \middle| \zeta^{p^n} = 1 \right\} = \{1\}$$

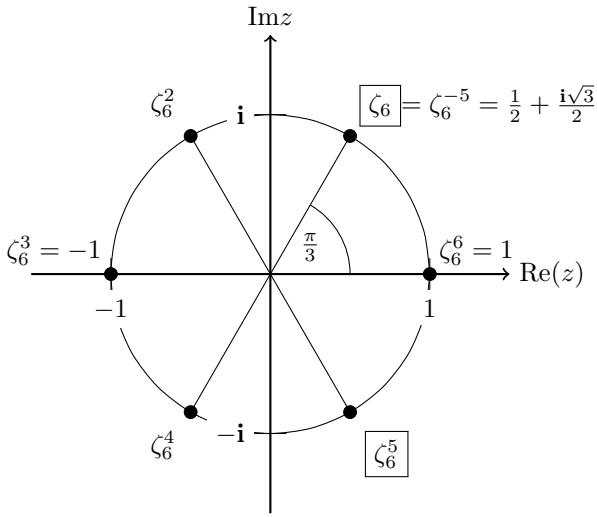
12.2 Definition (primitive Einheitswurzeln)

Eine n-te Einheitswurzel $\zeta \in U_n$ heißt genau dann *primitiv*, wenn $\langle \zeta \rangle = U_n$.

12.3 Beispiel (U_6)

Seien $k = \mathbb{C}$ und $U_6 = \left\langle \zeta_6 := \exp\left(\frac{2\pi\mathbf{i}}{6}\right) \right\rangle \subseteq \mathbb{C}^*$.

Dann sind genau ζ_6,$\zeta_6^5 = \zeta_6^{-1} \in U_6$ primitiv:



Es gilt:

$$\begin{aligned} \operatorname{ord}\left(\zeta_6^2\right) = \operatorname{ord}\left(\zeta_6^4\right) &= 3 \\ \operatorname{ord}\left(\zeta_6^3\right) &= 2 \\ \operatorname{ord}\left(\zeta_6^0\right) &= 1 \end{aligned}$$

12.4 Proposition

Sind n,m teilerfremd (und $\operatorname{char}(k) \not| (n,m)$), so ist die Abbildung

$$f : U_n \times U_m \to U_{nm}$$

wohldefiniert und ein Gruppenisomorphismus.
Sind $\zeta \in U_n$ und $\psi \in U_m$ primitiv, so auch $\zeta \cdot \psi \in U_{n \cdot m}$.

Beweis

Dass f wohldefiniert und ein Gruppenhomomorphismus ist, ist klar.
Wegen 12.1 gilt:

$$|U_n \times U_m| = |U_{nm}| = nm \tag{12.1}$$

Gelte:

$$f(\zeta \cdot \xi) = \zeta \cdot \xi = 1 \tag{12.2}$$

Da n,m teilerfremd sind, existieren a,$b \in \mathbb{Z}$ mit $1 = an + bm$. Dann folgt:

$$\zeta = \zeta^1 = \left(\underbrace{\zeta^n}_{=1}\right)^a \cdot \left(\zeta^m\right)^b \overset{(12.2)}{=} \left(\underbrace{\zeta^m}_{=1}\right)^b = 1$$

Daher ist $\xi = 1$, also ist $\ker(f) = \{(1,1)\}$.
Damit ist f injektiv und wegen (12.1) also ein Isomorphismus.
Man sieht leicht, dass für $(\zeta,\xi) \in U_n \times U_m$ gilt:

$$\operatorname{ord}((\zeta,\xi)) = \operatorname{kgV}(\operatorname{ord}(\zeta), \operatorname{ord}(\xi))$$

Sind nun $\zeta \in U_n$ und $\xi \in U_m$ primitiv, dann gilt:

$$\operatorname{ord}((\zeta,\xi)) = \operatorname{kgV}(n,m) \overset{\operatorname{ggT}(n,m)=1}{=} n \cdot m$$

Da f ein Isomorphismus ist, folgt:

$$\operatorname{ord}(f((\zeta,\xi)) = \zeta\xi) = nm$$

Also ist $\zeta\xi \in U_{nm}$ primitiv. $\square_{12.4}$

Bemerkung

Die Teilerfremdheit von n und m wird gebraucht:
$\zeta := \mathbf{i} \in U_4(\mathbb{C})$ und $\xi := \mathbf{i} \in U_4(\mathbb{C})$ sind primitiv, aber $\zeta \cdot \xi = -1 \in U_{16}(\mathbb{C})$ hat Ordnung $2 \neq 16$, ist also nicht primitiv.

12.5 Erinnerung (Eulersche φ-Funktion)

Für alle $n \geq 1$ sei die „Eulersche φ-Funktion“ definiert als:

$$\varphi(n) := \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right|$$

Es gelten:

i) $\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \left\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \middle| \operatorname{ggT}(a,n) = 1\right\}$
Insbesondere gilt:

$$\varphi(n) = |\{0 < a < n-1 | \operatorname{ggT}(a,n) = 1\}|$$

ii) φ ist multiplikativ, das heißt für alle $n,m \in \mathbb{N}_{\geq 1}$ gilt:

$$\operatorname{ggT}(n,m) = 1 \Rightarrow \varphi(n) \cdot \varphi(m) = \varphi(nm)$$

iii) Ist $p > 0$ eine Primzahl und $r \in \mathbb{N}_{\geq 1}$, dann folgt:

$$\varphi(p^r) = (p-1)\,p^{r-1}$$

12.6 Proposition

Für alle $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ gilt:

$$\overline{a} \text{ erzeugt } \left(\mathbb{Z}/n\mathbb{Z}, +\right) \Leftrightarrow \overline{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

Beweis

„⇒“: Es gibt ein $k \in \mathbb{Z}_{\geq 1}$ mit:

$$\overline{1} = \underbrace{\overline{a} + \ldots + \overline{a}}_{k \text{ mal}} = \overline{a} \cdot \overline{k} \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$$

Also ist $\overline{a} \in \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)^*$.

„⇐“: Es gibt ein $b \in \mathbb{Z}_{\geq 1}$ mit

$$\overline{a} \cdot \overline{b} = \underbrace{\overline{a} + \ldots + \overline{a}}_{b \text{ mal}} = \overline{1}$$

in ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.

Also ist $\overline{1} \in \langle \overline{a} \rangle \subseteq \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right)$.

Wegen $\langle \overline{1} \rangle = \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right)$ folgt:

$$\langle \overline{a} \rangle = \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right)$$

$\square_{12.6}$

12.7 Korollar

Für $n \in \mathbb{N}_{\geq 1}$ gelten mit $(\operatorname{char}(k) \nmid n)$:

i) $|\{\zeta \in U_n | \zeta \text{ ist primitiv}\}| = \varphi(n)$

ii) Für ein primitives $\zeta \in U_n$ und $r \in \mathbb{Z}$ gilt:

$$\zeta^r \in U_n \text{ ist primitiv} \Leftrightarrow \overline{r} \in \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)^* \left(\overset{12.5 \text{ i)}}{\Leftrightarrow} \operatorname{ggT}(r,n) = 1\right)$$

Beweis

i)
$$|\{\zeta \in U_n | \zeta \text{ ist primitiv}\}| \overset{12.1}{\underset{12.2}{=}} \left|\left\{a \in \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right) \,\middle|\, \langle a \rangle = \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right)\right\}\right| =$$
$$\overset{12.6}{=} \left|\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)^*\right| \overset{12.5}{=} \varphi(n)$$

$\square_{\text{i)}}$

ii) Aus der Primitivität von $\zeta \in U_n$ folgt:

$$\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right) \xrightarrow{\sim} U_n$$
$$\overline{a} \mapsto \zeta^a$$

Also gilt für alle $r \in \mathbb{Z}$:

$$\zeta^r \in U_n \text{ ist primitiv} \Leftrightarrow \langle \overline{r} \rangle = \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right) \overset{12.5}{=} \overline{r} \in \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)^*$$

$\square_{12.7}$

12.8 Satz

Seien $n \in \mathbb{N}_{\geq 1}$ und $\zeta_n \in \overline{k}$ eine primitive n-te Einheitswurzel. Dann gelten:

i) $k(\zeta)/k$ ist endlich und abelsch.

ii) Die Abbildung

$$\begin{aligned} \psi : \mathrm{Gal}\left(k(\zeta_n)/k\right) &\hookrightarrow \mathrm{Aut}(U_n) \\ \psi(\sigma) &:= \sigma|_{U_n} \end{aligned}$$

ist wohldefiniert und ein injektiver Gruppenhomomorphismus.

iii) Die Abbildung

$$\begin{aligned} \left(\mathbb{Z}/n\mathbb{Z}\right)^* &\xrightarrow{\sim} \mathrm{Aut}(U_n) \\ \overline{a} &\mapsto (\zeta \mapsto \zeta^a) \end{aligned}$$

ist wohldefiniert und ein Gruppenisomorphismus.

Beweis

Weil ζ_n primitiv ist, folgt:

$$U_n = \langle \zeta_n \rangle = \{\zeta_n^a | a \in \mathbb{Z}\} \subseteq k(\zeta_n) \tag{12.3}$$

Also ist $k(\zeta_n)/k$ ein Zerfällungskörper von $X^n - 1 \in k[X]$.

Weil aus $\zeta^n = 1$ schon $(X^n - 1)'(\zeta) = n\zeta^{n-1} \neq 0$ folgt, ist $X^n - 1 \in k[X]$ separabel, also ist $k(\zeta_n)/k$ endlich und galoissch.

Für $\zeta \in U_n$ und $\sigma \in \mathrm{Gal}\left(k(\zeta_n)/k\right)$ gilt:

$$[\sigma(\zeta)]^n = \sigma(\zeta^n) = \sigma(1) = 1$$

Also ist $\sigma(\zeta) \in U_n$.

Ferner ist die Abbildung

$$\begin{aligned} U_n &\to U_n \\ \zeta &\mapsto \sigma(\zeta) \end{aligned}$$

Wegen $\sigma(\zeta \cdot \xi) = \sigma(\zeta) \cdot \sigma(\xi)$ ein Gruppenhomomorphismus mit Inversen $\sigma^{-1}|_{U_n}$.

Damit ist ψ in ii) wohldefiniert und ein Gruppenhomomorphismus. Wegen (12.3) ist ψ injektiv. $\square_{\text{ii)}}$

iii) folgt, da U_n nach 12.1 ein freier $\left(\mathbb{Z}/n\mathbb{Z}\right)$-Modul vom Rang 1 ist.

Zu i): Wegen ii) und iii) ist $\mathrm{Gal}\left(k(\zeta_n)/k\right)$ abelsch. $\square_{12.8}$

12.9 Bemerkung und Definition (n-ter Kreisteilungskörper)

In der Situation von 12.8 gilt:

i)
$$[k(\zeta_n) : k] = \left|\mathrm{Gal}\left(k(\zeta_n)/k\right)\right| \Big| \varphi(n)$$

ii) Für $k = \mathbb{Q}$ in 12.8 heißt $\mathbb{Q}(\zeta_n)$ *der n-te Kreisteilungskörper.*

12.10 Satz (Gauß)

Seien $n \geq 1$ und $\zeta_n \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel.
Dann ist der Gruppenhomomorphismus

$$\psi : \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \xrightarrow{\sim} \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

mit der Eigenschaft, dass für alle $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$ und $\zeta \in U_n(\mathbb{Q})$ schon

$$\sigma(\zeta) = \zeta^{\psi(\sigma)}$$

gilt, ein Isomorphismus. (vergleiche 12.8 ii), iii))
Insbesondere gilt:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

Beweis

$$f := \mathrm{Mipo}_{\mathbb{Q}}(\zeta_n) \tag{12.4}$$

Also gilt:

$$f | X^n - 1 \in \mathbb{Q}[X]$$

Weil f normiert ist und mit 3.4 mit $h = X^n - 1$ und $R = \mathbb{Z}$ folgt $f \in \mathbb{Z}[X]$ und

$$X^n - 1 = f \cdot h \in \mathbb{Z}[X] \tag{12.5}$$

für ein geeignetes $h \in \mathbb{Z}[X]$.

Behauptung 1

Ist $p > 0$ eine Primzahl mit $p \nmid n$, dann ist $f(\zeta_n^p) = 0$ und $\zeta_n^p \in U_n$ ist primitiv.

Beweis

Die zweite Aussage folgt aus 12.7 ii).
Angenommen $f(\zeta_n^p) \neq 0$, dann würde wegen $(\zeta_n^p)^n = 1$ und (12.5) gelten:

$$h(\zeta_n^p) = 0$$

Also gilt:

$$h(X^p)(\zeta_n) = 0$$

Wegen 3.4 folgt:

$$f | h(X^p) \in \mathbb{Z}[X]$$

Das heißt $h(X^p) = f \cdot g \in \mathbb{Z}[X]$ für geeignetes $g \in \mathbb{Z}[X]$.
Also gilt in $\mathbb{F}_p[X]$:

$$\overline{h}^p \underset{\text{siehe unten}}{\overset{(+)}{=}} \overline{h(X^p)} = \overline{f} \cdot \overline{g}$$

Damit folgt $\mathrm{ggT}\left(\overline{h}, \overline{f}\right) \neq 1$ in $\mathbb{F}_p[X]$.
Also besitzt $\overline{X^n - 1} = \overline{f} \cdot \overline{h} \in \mathbb{F}_p[X]$ eine mehrfache Nullstelle in $\overline{\mathbb{F}}_p$.
Dies ist ein Widerspruch zur Separabilität von $X^n - 1$ in $\mathbb{F}_p[X]$, da $p \nmid n$. (vergleiche mit dem

Beweis von 8.4 i))
Zu (+):

$$\overline{h} = \sum_i a_i X^i \qquad\qquad a_i \in \mathbb{F}_p$$

Dann gilt:

$$\overline{h\left(X^p\right)} = \sum_i a_i \left(X^p\right)^i \overset{a_i \in \mathbb{F}_p}{=} \sum_i a_i^p \left(X^i\right)^p = \left(\sum a_i X^i\right)^p = \overline{h}^p$$

$\square_{\text{Behauptung 1}}$

Behauptung 2

Ist $\zeta \in U_n$ primitiv, so ist $f(\zeta) = 0$.

Beweis

Nach 12.7 ii) gibt es ein $r \in \mathbb{Z}$ mit $\operatorname{ggT}(r,n) = 1$ und $\zeta = \zeta_n^r$.
Dann ist $r = p_1 \cdot \ldots \cdot p_m$ ein endliches Produkt von Primzahlen p_i mit $p_i \nmid n$ für alle $1 \leq i \leq n$.
Aus Behauptung 1 folgt induktiv:

$$f\left(\zeta_n^{p_1}\right) = 0$$

und $\zeta_n^{p_1} \in U_n$ ist primitiv.
Dann folgt aus der Behauptung 1 für $\zeta_n^{p_2}$, dass

$$\left(\zeta_n^{p_1}\right)^{p_2} = \zeta_n^{p_1 \cdot p_2} \in U_n$$

primitiv ist und gilt:

$$f\left(\zeta_n^{p_1 \cdot p_2}\right) = 0$$

Dann folgt:

$$0 = f\left(\zeta_n^r\right) = f(\zeta)$$

$\square_{\text{Behauptung 2}}$

Nach 12.8 ii) ist

$$\psi : \operatorname{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right) \hookrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

injektiv.
Zeige also nur:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \geq \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right| = \varphi(n)$$

Beweis

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \overset{(12.4)}{=} \deg(f) \overset{\text{Beh. 2}}{\geq} |\{\zeta \in U_n | \zeta \text{ ist primitiv}\}| \overset{\text{?? i)}}{=} \varphi(n)$$

$\square_{12.10}$

12.11 Korollar

Seien $n,m \geq 1$ teilerfremd und $\zeta_n, \zeta_m \in \overline{\mathbb{Q}}$ primitive n-te (beziehungsweise m-te) Einheitswurzeln.
Dann gelten:

i) $\mathbb{Q}(\zeta_n,\zeta_m) = \mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n \cdot \zeta_m)$

ii) $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$

iii) Die Abbildung

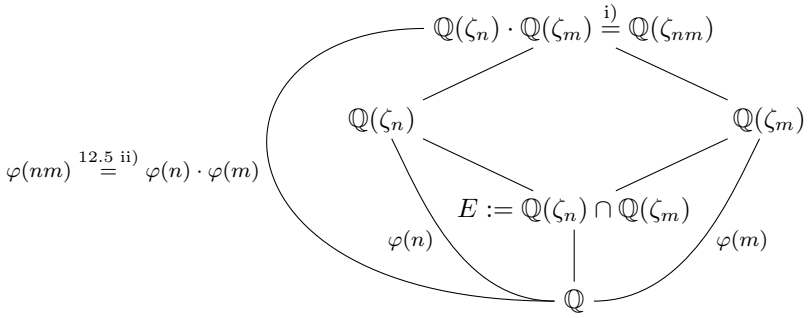
$$\begin{aligned} \mathrm{Gal}\left(\mathbb{Q}(\zeta_n,\zeta_m)/\mathbb{Q}\right) &\to \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \times \mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\right) \\ \sigma &\mapsto \left(\sigma|_{\mathbb{Q}(\zeta_n)},\sigma|_{\mathbb{Q}(\zeta_m)}\right) \end{aligned}$$

ist ein Gruppenisomorphismus.

Beweis

i) Da $\zeta_n \cdot \zeta_m$ nach 12.4 eine primitive (nm)-te Einheitswurzel ist, gelten $\zeta_n,\zeta_m \in \mathbb{Q}(\zeta_n \cdot \zeta_m)$, denn $U_n,U_m \subseteq U_{nm}$.
Der Rest ist klar. $\square_{\text{i)}}$

ii) Wir haben folgendes Körperdiagramm:



Dabei gelten die Grade nach 12.10.
Aus der Gradformel für $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{nm})$ folgt:

$$[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_m)] = \varphi(n) \leq [\mathbb{Q}(\zeta_n) : E] \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \overset{12.10}{=} \varphi(n)$$

Also folgt:

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : E] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

Also folgt wegen $\mathbb{Q} \subseteq E$ schon $E = \mathbb{Q}$. $\square_{\text{ii)}}$

iii) Dies folgt aus i), ii) und 10.16 ii).

$\square_{12.11}$

12.12 Bemerkung

In der Situation von 12.11 ist das Diagramm

$$\begin{array}{ccc} \mathrm{Gal}\left(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}\right) & \overset{\sim}{\underset{12.11}{\longrightarrow}} & \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \times \mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\right) \\ \Big\downarrow{\scriptstyle 12.10}\wr & & \Big\downarrow{\scriptstyle 12.10}\wr \\ \left(\mathbb{Z}/nm\mathbb{Z}\right)^* & \xrightarrow{\sim} & \left(\mathbb{Z}/n\mathbb{Z}\right)^* \times \left(\mathbb{Z}/m\mathbb{Z}\right)^* \\ \overline{a} & \longmapsto & (a \bmod n, a \bmod m) \end{array}$$

kommutativ.

Beweis

TODO: Beweis als Übung einfügen

$\square_{12.12}$

12.13 Definition (Kreisteilungspolynom)

Seien $n \in \mathbb{N}_{\geq 1}$ und $\{\zeta_1, \ldots, \zeta_{\varphi(n)}\} \subseteq U_n \subseteq \overline{k}^*$ die primitiven n-ten Einheitswurzeln (vergleiche 12.7 i)). Dann heißt

$$\phi_n(X) := \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \overline{k}[X]$$

das n-te Kreisteilungspolynom über k.

12.14 Satz

Für $n \geq 1$ (und $\operatorname{char}(k) \nmid n$) gelten:

i) $\phi_n(X) \in k[X]$ ist separabel und normiert mit $\deg(\phi_n) = \varphi(n)$.

ii) Aus $k = \mathbb{Q}$ folgt, dass $\phi_n(X) \in \mathbb{Z}[X]$ und irreduzibel ist.

iii) $X^n - 1 = \prod_{0<d|n} \phi_d(X) \in k[X]$

Beweis

i) Nach 12.13 ist klar, dass $\phi_n(X) \in \overline{k}[X]$ normiert, separabel und vom Grad $\varphi(n)$ ist.
Zeige also nur:

$$\phi_n(X) \in k[X]$$

Für

$$E := k(\zeta_n) = k(\zeta | \zeta \in U_n)$$

ist $\phi_n(X) \in E[X]$ und E/k ist endlich und galoissch nach 12.8 ii).
Für jedes $\sigma \in \operatorname{Gal}\left(E/k\right)$ und jedes primitive $\zeta \in U_n$ ist auch $\sigma(\zeta) \in U_n$ primitiv, womit nach 12.13 folgt:

$$\phi_n^\sigma(X) = \phi_n(X)$$

Also folgt mit dem Hauptsatz der Galoistheorie:

$$\phi_n(X) \in \left(E^{\operatorname{Gal}(E/k)}\right)[X] = k[X]$$

$\square_{\text{i)}}$

ii) $\phi_n(X) \subseteq \mathbb{Q}[X]$ ist irreduzibel, denn genauer gilt für ein primitives $\zeta \in U_n(\mathbb{Q})$:

$$[\zeta_n : \mathbb{Q}] \overset{12.10}{=} \varphi(n)$$
$$\deg(\phi_n(X)) \overset{12.13}{=} \varphi(n)$$
$$\phi_n(\zeta_n) \overset{12.13}{=} 0$$

Also gilt sogar:

$$\phi_n(X) = \mathrm{Mipo}_{\mathbb{Q}}(\zeta_n)$$

Weil $\phi_n(X)$ normiert ist, folgt $\phi_n(X) | X^n - 1$ in $\mathbb{Q}[X]$ und mit 3.4 folgt $\phi_n(X) \in \mathbb{Z}[X]$. $\square_{\text{ii)}}$

iii) Für alle $0 < d | n$ gilt:

$$P_d := \{\zeta \in U_n | \mathrm{ord}(\zeta) = d\}$$

Damit folgt:

$$U_n = \dot{\bigcup_{0<d|n}} P_d \tag{12.6}$$

Daher gilt in $\overline{k}[X]$:

$$X^n - 1 \overset{\text{klar}}{=} \prod_{\zeta \in U_n} (X - \zeta) \overset{\substack{(12.6)\\12.3}}{=} \prod_{0<d|n} \phi_d(X)$$

Beachte auch, dass für alle Teiler d von n schon $U_d \subseteq U_n$ gilt.

$\square_{12.14}$

12.15 Beispiel ($k = \mathbb{Q}$)

Sei $k = \mathbb{Q}$. Mit 12.14 iii) kann man $\phi_n(X) \in \mathbb{Z}[X]$ durch Induktion über die Anzahl der Primfaktoren von n explizit berechnen:

i) Für eine Primzahl $p > 0$ folgt mit 12.14 iii):

$$X^p - 1 = \underbrace{\phi_1(X)}_{X-1} \cdot \phi_p(X)$$

Daher gilt:

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \ldots + 1 = \mathrm{Mipo}_{\mathbb{Q}}(\zeta_p)$$

(vergleiche 4.5 iii))

ii) Seien p,$q > 0$ Primzahlen mit $p \neq q$, so folgt mit 12.14 iii):

$$X^{pq} - 1 = \phi_1(X) \cdot \phi_p(X) \cdot \phi_q(X) \cdot \phi_{pq}(X)$$

Damit folgt nach i):

$$\phi_{pq}(X) = \frac{(X^{pq} - 1)(X - 1)(X - 1)}{(X - 1)(X^p - 1)(X^q - 1)} = \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}$$

Zur Einübung:

$$\deg(\phi_{pq}) = \varphi(pq) = \varphi(p) \cdot \varphi(q) = (p - 1) \cdot (q - 1) =$$
$$= \deg\left(\frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}\right) = pq + 1 - p - q$$

Zum Beispiel gilt für $p = 2$ und $q = 3$:

$$\phi_6(X) = X^2 - X + 1 = \mathrm{Mipo}_{\mathbb{Q}}\left(\zeta_6 = e^{\frac{\pi \mathrm{i}}{3}}\right)$$

12.16 Satz und Definition (Nullstelle modulo p)

Seien $\mathbb{F}_q$ ein endlicher Körper (vergleiche 9.1), $n \in \mathbb{N}_{\geq 1}0$ eine natürliche Zahl mit $\operatorname{ggT}(n,q) = 1$ und $\zeta_n \in \overline{\mathbb{F}}_p$ eine primitive n-te Einheitswurzel. Dann gilt:

i) Der surjektive Gruppenhomomorphismus $\psi : \operatorname{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\right) \hookrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ (vergleiche 12.8 ii) und iii)) erfüllt:

$$\psi(\operatorname{Frob}_q) = \overline{q}$$

(vergleiche 9.5 i))
Insbesondere induziert ψ einen Isomorphismus:

$$\operatorname{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\right) \xrightarrow{\sim} \langle\overline{q}\rangle \subseteq \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

ii) $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \operatorname{ord}\left(\overline{q} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$

iii) $\phi_n(X) \in \mathbb{F}_q[X]$ ist genau dann irreduzibel, wenn $\langle\overline{q}\rangle = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

iv) Ist $q = p$ eine Primzahl, so gilt:

$$p \equiv 1 \bmod n \quad \Leftrightarrow \quad \zeta_n \in \mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$$

Letzteres ist äquivalent dazu, dass $\phi_n(X)$ aufgefasst als Polynom in $\mathbb{Z}[X] = \pi^{-1}(\mathbb{F}_p)[X]$ *eine Nullstelle modulo p besitzt*, das heißt:

$$\underset{x \in \pi^{-1}(\zeta_n) \subseteq \mathbb{Z}}{\exists} : \phi_n(x) \equiv 0 \bmod p$$

Dabei ist $\pi : \mathbb{Z} \to \mathbb{F}_p$ die Projektionsabbildung.

Beweis

i) $\zeta_n^{\psi(\operatorname{Frob}_q)} \overset{12.10}{=} \operatorname{Frob}_q(\zeta_n) \overset{\text{Def.}}{=} \zeta_n^q$
Also folgt wegen $\operatorname{ord}(\zeta_n) = n$ schon:

$$\psi(\operatorname{Frob}_q) \equiv \overline{q}\,(n)$$

Die zweite Aussage folgt aus:

$$\operatorname{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\right) = \langle\operatorname{Frob}_q\rangle$$

(vergleiche 9.5 ii)) $\square_{\text{i)}}$

ii) $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \left|\operatorname{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_1\right)\right| \overset{\text{i)}}{=} |\langle\overline{q}\rangle| = \operatorname{ord}\left(\overline{q} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$ $\square_{\text{ii)}}$

iii) Die Irreduzibilität von $\phi_n(X) \in \mathbb{F}_q[X]$ ist äquivalent zu folgenden Aussagen:

$$\begin{aligned}
&\Leftrightarrow && \phi_n(X) = \operatorname{Mipo}_{\mathbb{F}_q}(\zeta_n) \\
&\Leftrightarrow && [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \varphi(n) \\
&\Leftrightarrow && \psi \text{ in i) ist surjektiv.} \\
&\overset{\text{i)}}{\Leftrightarrow} && \langle\overline{q}\rangle = \left(\mathbb{Z}/n\mathbb{Z}\right)^*
\end{aligned}$$

$\square_{\text{iii)}}$

iv)
$$\begin{aligned} p \equiv 1 \bmod n \quad &\Leftrightarrow \quad \langle \overline{p} \rangle = \{1\} \subseteq \left(\mathbb{Z}/n\mathbb{Z}\right)^* \\ &\overset{\text{i)}}{\Leftrightarrow} \quad \mathrm{Gal}\left(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p\right) = \{1\} \\ &\overset{\phi_n(\zeta_n)=0}{\Leftrightarrow} \quad \phi_n \text{ besitzt eine Nullstelle in } \mathbb{F}_p. \end{aligned}$$

TODO: Restlichen Beweis einfügen

$\square_{12.16}$

12.17 Beispiel ($n = 4$)

Sei $k = \mathbb{Q}$ und $n = 4$, so folgt:

$$X^4 - 1 \overset{12.14 \text{ iii)}}{=} \phi_1(X)\,\phi_2(X)\,\phi_4(X)$$
$$\phi_4(X) = \frac{X^4-1}{\phi_1(X)\,\phi_2(X)} = \frac{X^4-1}{(X-1)\,\frac{X^2-1}{(X-1)}} = \frac{X^4-1}{X^2-1} = X^2+1$$

$p \nmid n$	3	5	7	11	13	...
Nullstelle von $X^2+1 \bmod p$	/	2	/	/	8	...
$p \bmod n$	-1	1	-1	-1	1	...

12.18 Lemma

Sei $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$ und setze:

$$P(f) := \{p | p > 0 \text{ ist eine Primzahl} \wedge f \text{ besitzt eine Nullstelle mod } p\}$$

Dann gilt:

$$|P(f)| = \infty$$

Beweis

Offenbar ist:

$$P(f) = \left\{ p \in \mathbb{Z}_{>0} \,\middle|\, p \text{ ist eine Primzahl} \wedge \exists_{z \in \mathbb{Z}} : p | f(z) \text{ in } \mathbb{Z} \right\}$$

Schreibe $f = a_n X^n + \ldots + a_0$ mit $a_i \in \mathbb{Z}$ und $a_n \neq 0$.
Ist $a_0 = 0$, so gilt $p | f(p)$ für alle Primzahlen p von $\mathbb{Z}$.
Sei also ohne Einschränkung $a_0 \neq 0$, dann folgt:

$$f(a_0 X) = a_0 \cdot \underbrace{\left(a_n a_0^{n-1} X^n + \ldots + 1\right)}_{=:g(X)}$$

Damit folgt $P(g) \subseteq P(f)$.
Zeige also nur noch $|P(g)| = \infty$.

Angenommen dies wäre nicht so, dann sei:

$$P(g) = \{p_1, \ldots, p_m\}$$

Dann existiert ein $\alpha \in \mathbb{Z}_{\geq 1}$ so, dass $0, \pm 1 \neq g(\alpha \cdot p_1 \cdot \ldots \cdot p_m) =: N$, da $\deg(g) \geq 1$ ist.

$$N \overset{\text{Def. von } g}{\equiv} 1 \bmod p_i \qquad \underset{1 \leq i \leq m}{\forall} \tag{12.7}$$

Daher gibt es eine Primzahl q mit:

$$q|N \quad \Rightarrow \quad q \in P(g)$$

Damit folgt

$$N \equiv 0 \bmod q$$

und:

$$N \equiv 1 \not\equiv 0 \bmod q$$

Dies ist ein Widerspruch zur Endlichkeit von $P(g)$. $\square_{12.18}$

12.19 Satz

Für jede Zahl $n \geq 1$ existieren unendlich viele Primzahlen p mit $p \equiv 1 \bmod n$.

Beweis

12.16 iv) und 12.18 mit $f = \phi_n(X)$. $\square_{12.19}$

12.20 Bemerkung

Allgemeiner gilt der Satz von Dirichlet:
Für $a,n \in \mathbb{N}_{\geq 1}$ mit $\text{ggT}(a,n) = 1$, gibt es unendlich viele Primzahlen p mit $p \equiv a \bmod n$.
(vergleiche Jean-Pierre Serre: *A Course in Arithmetics*)

13 Gruppentheorie II

13.1 Operationen von Gruppen auf Mengen

13.1.1 Proposition und Definition (Operation)

Seien G eine Gruppe, X eine Menge und $\varrho : G \to \Sigma(X)$ ein Gruppenhomomorphismus.
Dann gelten für die Abbildung

$$\begin{aligned} \cdot : G \times X &\to X \\ (g,x) &\mapsto g \cdot x := \varrho(g)(x) \end{aligned}$$

folgende Aussagen:

i) Für alle $x \in X$ und das neutrale Element $e \in G$ gilt:

$$e \cdot x = x$$

ii) Für alle $g,h \in G$ und alle $x \in X$ gilt:

$$g \cdot (h \cdot x) = (gh) \cdot x$$

Eine Abbildung, die i) und ii) erfüllt, heißt *Operation von G auf X*.
Ist umgekehrt $\cdot$ eine Operation von G auf X, so ist die Abbildung

$$\begin{aligned} G &\to \Sigma(X) \\ g &\mapsto (x \mapsto g \cdot x) \end{aligned} \tag{13.1}$$

wohldefiniert und ein Gruppenhomomorphismus.

Beweis

i) Da ϱ ein Gruppenhomomorphismus ist, gilt $\varrho(e) = \mathrm{id}_X$ und es folgt:

$$e \cdot x \overset{\text{Def.}}{=} \underbrace{\varrho(e)}_{=\mathrm{id}_X}(x) = x$$

$\square_{\text{i)}}$

ii) Es gilt:

$$g \cdot (h \cdot x) \overset{\text{Def.}}{=} \varrho(g)(\varrho(h)(x)) = (\varrho(g) \circ \varrho(h))(x) \overset{\varrho \text{ Gruphom.}}{=} (\varrho(gh))(x) \overset{\text{Def.}}{=} (gh) \cdot x$$

$\square_{\text{ii)}}$

Sei umgekehrt $\cdot$ eine Operation von G auf X, so gilt für alle $x \in X$, alle $g,h \in G$ und das neutrale Element $e \in G$:

$$e \cdot x = x \qquad\qquad g \cdot (h \cdot x) = (gh) \cdot x \tag{13.2}$$

Die Abbildung

$$\begin{aligned} \varrho : G &\to \Sigma(X) \\ g &\mapsto (x \mapsto g \cdot x) \end{aligned}$$

ist wohldefiniert, da die Abbildung $g\cdot$ wegen

$$g \cdot g^{-1} = g^{-1} \cdot g = \mathrm{id}_X$$

bijektiv mit der Inversen $g^{-1}\cdot$ ist, also $\varrho(g) \in \Sigma(X)$ ist.
Zudem gilt:

$$\varrho(e)(x) = e \cdot x \overset{(13.2)}{=} x \qquad\qquad \Rightarrow \quad \varrho(e) = \mathrm{id}_X$$

$$\varrho(gh)(x) = gh \cdot x \overset{(13.2)}{=} g \cdot h \cdot x = \varrho(g)(\varrho(h)(x)) = (\varrho(g) \circ \varrho(h))(x)$$

Also gilt $\varrho(gh) = \varrho(g) \circ \varrho(h)$ und daher ist ϱ ein Gruppenhomomorphismus. $\square_{13.1.1}$

13.1.2 **Beispiel und Definition** (Linkstranslation)

i) Sei

$$\begin{aligned} G \times X &\to X \\ (g,x) &\mapsto g \cdot x \end{aligned}$$

eine Operation der Gruppe G auf der Menge X.
Dann ist für jedes $\sigma \in G$ *die Linkstranslation mit* σ definiert durch

$$\begin{aligned} l_\sigma : X &\xrightarrow{\sim} X \\ x &\mapsto \sigma \cdot x \end{aligned}$$

und bijektiv.

Beweis

Man sieht leicht:

$$l_\sigma \circ l_{\sigma^{-1}} = l_{\sigma^{-1}} \circ l_\sigma = \mathrm{id}_X$$

(vergleiche Beweis von 13.1.1) $\square_{\text{i)}}$

ii) Ist E/k eine Körpererweiterung, so ist

$$\begin{aligned} \mathrm{Aut}_k(E) \times E &\to E \\ (\sigma,x) &\mapsto \sigma(x) \end{aligned}$$

eine Operation.

iii) Sei G eine Gruppe. Dann ist die Multiplikation

$$\begin{aligned} G \times G &\to G \\ (g,h) &\mapsto gh \end{aligned}$$

eine Operation der Gruppe G auf der Menge G und der zugehörige Gruppenhomomorphismus

$$\varrho : G \to \Sigma(G)$$

(vergleichen 13.1.1) ist injektiv, denn $\ker(\varrho) = \{e\}$, da das neutrale Element eindeutig ist.

iv) Sei G eine Gruppe. Dann ist

$$\begin{aligned} G \times G &\to G \\ (g,h) &\mapsto ghg^{-1} \end{aligned}$$

eine Operation, *die Operation von G auf sich selbst durch Konjugation.* Dies folgt aus 1.5 und 13.1.1.

Fixiere im Rest des Kapitels 13 (Gruppentheorie II) eine Operation $\cdot : G \times X \to X$

13.1.3 Proposition und Definition (Bahn, Standuntergruppe)

i) Für alle $x \in X$ heißt

$$Gx := \{g \cdot x | g \in G\} \subseteq X$$

die Bahn von x unter G.

ii) Für alle $x \in X$ ist

$$G_x := \{\sigma \in G | \sigma \cdot x = x\} \subseteq G$$

eine Untergruppe, *die Standuntergruppe von $x \in X$.*

Beweis

Es ist nur zu zeigen, dass die Teilmenge $G_x \subseteq G$ eine Untergruppe ist.

$$e \cdot x = x$$

Also ist $e \in G_x$ und für $\sigma,\tau \in G_x$ gilt:

$$\left(\sigma\tau^{-1}\right) \cdot \underbrace{x}_{\substack{=\tau\cdot x \\ \text{wg. } \tau \in G_x}} = \left(\sigma\left(\tau^{-1}\tau\right)\right) \cdot x = \sigma x = x$$

Also gilt $\sigma\tau^{-1} \in G_x$. $\square_{13.1.3}$

13.1.4 Proposition

Sei $y \in X$ und $x \in Gy$.
Die Untergruppe $G_x, G_y \subseteq G$ sind zueinander konjugiert.

Beweis

Wegen $x \in Gy$ gibt es nach Proposition und Definition (Bahn, Standuntergruppe) i) ein $\sigma \in G$ mit:

$$x = \sigma \cdot y \tag{13.3}$$

Dann gilt für alle $\omega \in G$:

$$\begin{aligned} \omega \in G_x &\Leftrightarrow \omega \cdot x = x \\ &\overset{(13.3)}{\Leftrightarrow} \omega \cdot (\sigma y) = \sigma y \\ &\Leftrightarrow \left(\sigma^{-1}\omega\sigma\right) \cdot y = y \\ &\Leftrightarrow \sigma^{-1}\omega\sigma \in G_y \\ &\Leftrightarrow \omega \in \sigma G_y \sigma^{-1} \end{aligned}$$

Weil $\omega \in G$ beliebig ist, folgt, dass

$$G_x = \sigma G_y \sigma^{-1}$$

gilt, also G_x konjugiert zu G_y ist. $\square_{13.1.4}$

13.1.5 **Proposition und Definition** (Menge der Bahnen)

i) Die Relation $\sim$ auf X, die für alle $x,y \in X$ durch

$$x \sim y :\Leftrightarrow \underset{\sigma \in G}{\exists} : y = \sigma \cdot x$$

definiert ist, ist eine Äquivalenzrelation, deren Äquivalenzklassen genau die Bahnen $G_x \subseteq X$ mit $x \in X$ sind.

ii) Für alle $x,y \in X$ gilt:

$$(Gx \cap Gy) = \emptyset \vee Gx = Gy$$

iii) Für *die Menge der Bahnen*

$$G\backslash X := X/_{\sim}$$

gilt:

$$X = \dot{\bigcup_{Gx \in G\backslash X}} Gx$$

Das heißt X ist die disjunkte Vereinigung aller Bahnen.

Beweis

i) Reflexivität: Sei $e \in G$, dann gilt $x = e \cdot x$, also ist $x = e \cdot x \sim x$.
Symmetrie: Sei $x \sim y$, dann existiert ein $\sigma \in G$ mit $y = \sigma \cdot x$, also gilt:

$$\sigma^{-1} \cdot y = \sigma^{-1} (\sigma \cdot x) = \left(\sigma^{-1}\sigma\right) \cdot x = e \cdot x = x$$

Daher ist $y \sim x$.
Transitivität: Sei $x \sim y \sim z$, dann gibt es $\sigma,\tau \in G$ mit:

$$\sigma \cdot x = y \qquad\qquad \tau \cdot y = z$$

Also gilt:

$$z = \tau \cdot y = \tau \cdot (\sigma \cdot x) = (\tau\sigma) \cdot x$$

Daher ist $x \sim z$.
Also ist $\sim$ eine Äquivalenzrelation auf X, und die zweite Aussage ist klar. $\square_{\text{i)}}$

ii) und iii) sind allgemeine Eigenschaften einer Äquivalenzrelation.

$\square_{13.1.5}$

13.1.6 Proposition

Für $x \in X$ ist die Abbildung

$$\begin{aligned} {}^{G}\!/_{G_x} &\xrightarrow{\sim} Gx \\ \sigma G_x &\mapsto \sigma \cdot x \end{aligned} \tag{13.4}$$

wohldefiniert und bijektiv.
Sind G und X endlich, so folgt:

$$|Gx| = \left|{}^{G}\!/_{G_x}\right| = (G : G_x)$$

Beweis

Für alle $\sigma,\tau \in G$ mit $\sigma G_x = \tau G_x$ gibt es ein $\omega \in G_x$ mit $\sigma = \tau\omega$.
Damit folgt:

$$\tau \cdot x \overset{\omega \in G_x}{=} \tau \cdot (\omega \cdot x) = (\tau\omega) \cdot x = \sigma \cdot x$$

Also ist die Abbildung (13.4) wohldefiniert und offenbar surjektiv.
Für $\sigma,\tau \in G$ mit $\sigma \cdot x = \tau \cdot x$ folgt:

$$\left(\tau^{-1}\sigma\right) \cdot x = \tau^{-1} \cdot (\sigma \cdot x) = \tau^{-1} \cdot (\tau \cdot x) = \left(\tau^{-1}\tau\right) \cdot x = e \cdot x = x$$

Damit folgt:

$$\tau^{-1}\sigma \in G_x$$

Also gilt:

$$\sigma G_x = \tau G_x$$

Daher ist die Abbildung (13.4) injektiv.
Der Rest ist klar. $\square_{13.1.6}$

13.1.7 Satz (Bahngleichung)

Sind G und X endlich und ist $\{x_1,\ldots,x_n\}$ ein Vertretersystem der Bahnen, das heißt es gilt:

$${}_{G}\!\setminus\!X = \{Gx_1,\ldots,Gx_n\}$$

Dann folgt:

$$|X| = \sum_{i=1}^{n} |Gx_i| = \sum_{i=1}^{n} (G : G_{x_i})$$

Beweis

Dies folgt aus 13.1.5 iii) und 13.1.6. $\square_{13.1.7}$

13.1.8 **Definition** (Konjugationsklasse, Zentralisator)

Sei G eine Gruppe, $\tau \in G$.
Dann heißt die Bahn von τ bezüglich der Operation von G auf G durch Konjugation die *Konjugationsklasse von τ in G*.
Die Standuntergruppe G_τ von τ bezüglich der betrachteten Operation heißt *Zentralisator von τ in G*.
Sie wird mit $Z_G(\tau)$ bezeichnet.

13.1.9 **Proposition**

Ist G eine endliche Gruppe und $\tau_1, \ldots, \tau_r$ mit $r \in \mathbb{N}_{\geq 0}$ ein vollständiges Vertretersystem derjenigen Konjugationsunterklassen von G, welche aus mehr als einem Element bestehen, so gilt:

$$|G| = |Z(G)| + \sum_{i=1}^{r} (G : Z_G(\tau_i))$$

Beweis

Die Konjugationsunterklasse eines $\tau \in G$ ist genau dann einelementig, wenn $\tau \in Z(G)$ liegt.
Damit folgt die Proposition aus der Bahngleichung 13.1.7. $\square_{13.1.9}$

13.1.10 **Definition** (p-Gruppen)

Sei p eine Primzahl.
Eine endliche Gruppe G heißt eine *p-Gruppe*, wenn die Mächtigkeit $|G|$ von G eine Potenz von p ist, also für ein $n \in \mathbb{N}_{\geq 0}$ gilt:

$$|G| = p^n$$

13.1.11 **Satz** (nicht-triviales Zentrum)

Jede nicht-triviale endliche p-Gruppe G besitzt ein nicht-triviales Zentrum.

Beweis

Es gilt $|G| = p^k$ mit $k \in \mathbb{N}_{\geq 1}$ für bestimmte $l_i \in \mathbb{N}_{\geq 1}$:

$$p \mid |G| = p^k \qquad\qquad p \mid (G : Z_G(\tau_i)) = \frac{|G|}{|Z_G(\tau_i)|} = p^{l_i}$$

Nach 13.1.9 gilt also:

$$p \mid |Z(G)|$$

Daher ist $Z(G) \neq 1$. $\square_{13.1.11}$

13.1.12 **Satz** (Kette von Normalteilern)

Sei G eine p-Gruppe der Ordnung p^m.
Dann gibt es eine Kette von Normalteilern H_i von G mit

$$H_{i-1} \supseteq H_i$$
$$(H_{i-1} : H_i) = p$$

für alle $1 \leq i \leq m$.

Beweis

Führe Induktion über m durch:
Der Fall $m = 0$ ist klar: $p^0 = 1$ und $H_0 = H_1 = \{e\} = G$.
Sei $m > 0$: Nach 13.1.11 ist $Z(G) \neq 1$ und daher gibt es ein $\alpha \in Z(G) \setminus \{1\}$.
Die zyklische Untergruppe $\langle\alpha\rangle \subseteq G$ besitzt eine Untergruppe der Ordnung p, nämlich $\left\langle \alpha^{\frac{\operatorname{ord}(\alpha)}{p}} \right\rangle$.
Wegen $H \subseteq Z(G)$ ist H ein Normalteiler in G.
Sei $\overline{G} := {}^{G}\!/_{H}$, dann ist $\left|\overline{G}\right| = p^{m-1}$.
Nach Induktionsvoraussetzung gibt es eine Kette

$$\overline{G} = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_{m-1} = \{e\}$$

von Normalteilern N_i von $\overline{G}$ mit $(N_{i-1} : N_i) = p$.
Sei φ_i die Komposition $G \to \overline{G} \to {}^{\overline{G}}\!/_{N_i}$ und $H_i := \ker(\varphi_i)$ für $0 \leq i \leq m-1$ und $H_m = \{e\}$, also $H_i \trianglelefteq G$.
Wegen

$${}^{H_{i-1}}\!/_{H_i} = \left({}^{H_{i-1}}\!/_{H}\right) / \left({}^{H_i}\!/_{H}\right) = {}^{N_{i-1}}\!/_{N_i}$$

gilt $(H_{i-1} : H_i) = p$ für $1 \leq i \leq m-1$.
Nach der Wahl von H gilt auch $(H_{m-1} : H_m) = p$, weswegen

$$G = H_0 \supseteq \ldots \supseteq H_m = \{e\}$$

eine Kette der gewünschten Art ist. □13.1.12

13.1.13 Proposition und Definition (Operation auf Potenzmenge)

G operiere auf X.
Dann operiert G auf der Potenzmenge $\mathcal{P}(X)$ von X vermöge:

$$(\sigma, M) \mapsto \sigma \cdot M := \{\sigma \cdot m | m \in M\}$$

Beweis

Sei $M \in \mathcal{P}(X)$ beliebig, so gilt:

i) $e \cdot M = \{e \cdot m | m \in M\} \overset{\substack{G \text{ operiert} \\ \text{auf } X}}{=} \{m | m \in M\} = M$

ii) Für alle $g,h \in G$ gilt:

$$g \cdot (h \cdot M) = \{g \cdot n | n \in hM\} = \{g \cdot (h \cdot m) | m \in M\} \overset{\substack{G \text{ operiert} \\ \text{auf } X}}{=} \{(gh) \cdot m | m \in M\} = (gh) \cdot M$$

Daher operiert G auf $\mathcal{P}(X)$. □13.1.13

13.1.14 Beispiel und Definition (Normalisator)

G operiere auf G durch Konjugation.
Bezeichnung:
Für $X \subseteq G$ und $\sigma \in G$ sei $X^\sigma := \sigma^{-1} X \sigma$.
Ist $X = H \subseteq G$ eine Untergruppe, so auch H^σ.
Die Standuntergruppe

$$N_G H := \left\{\sigma \in G | \sigma H \sigma^{-1} = H\right\}$$

von H heißt *der Normalisator von H in G*.
Es gilt $H \trianglelefteq N_G H$ und $H \trianglelefteq G \Leftrightarrow N_G H = G$.

13.2 Die Sylowsätze

13.2.1 Lemma

Sei G eine endliche p-Gruppe, die auf einer endlichen Menge X operiert.
Sei

$$X_0 = \left\{ x \in X \,\middle|\, \underset{\sigma \in G}{\forall} \sigma x = x \right\}$$

die Menge der Fixpunkte.
Dann ist $|X| \equiv |X_0| \mod p$.

Beweis

Sei $x_1, \ldots, x_n$ ein vollständiges Vertretersystem der Bahnen, die aus mehr als einem Element bestehen.
Die Bahngleichung 13.1.7 lautet:

$$|X| = |X_0| + \sum_{i=1}^{n} (G : G_{x_i})$$

Da G eine p-Gruppe ist, also $p \mid (G : G_{x_i})$ gilt, folgt daraus die Behauptung. $\square_{13.2.1}$

13.2.2 Definition (p-Sylowgruppe)

Seien G eine endliche Gruppe, $m \in \mathbb{N}_{\geq 1}$, $n \in \mathbb{N}_{\geq 0}$, p eine Primzahl, $\operatorname{ggT}(m,p) = 1$ und $|G| = p^n \cdot m$.
Ein $H \subseteq G$ mit $|H| = p^n$ heißt eine p-Sylowgruppe von G.

13.2.3 Beispiel

$$H := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\} \subseteq \mathrm{Gl}_n(\mathbb{F}_p) =: G$$

ist eine p-Sylowgruppe.

Beweis

Klar ist, dass H eine Untergruppe von G ist.
Ebenfalls klar ist, dass für ein $m \in \mathbb{N}_{\geq 1}$ gilt:

$$|H| = p^{\frac{n^2-n}{2}} \,\middle|\, |G| = m \cdot |H|$$

Bleibt noch $\operatorname{ggT}(p,m) = 1$ zu zeigen.
TODO: Restlichen Beweis einfügen

$\square_{13.2.3}$

13.2.4 Satz (Cauchy)

Sei p eine Primzahl.
Ist die Ordnung einer endlichen Gruppe G durch p teilbar, dann enthält G ein Element der Ordnung p.

Beweis

$$M := \{(a_1, \ldots, a_p) \in G^p | a_1 \cdot \ldots \cdot a_p = 1\}$$

M ist bestimmt durch $a_1, \ldots, a_{p-1}$, die frei wählbar sind, denn dann folgt:

$$a_p = (a_1 \cdot \ldots \cdot a_{p-1})^{-1} = a_{p-1}^{-1} \cdot \ldots \cdot a_1^{-1}$$

Daher gilt:

$$|M| = |G|^{p-1}$$

$\mathbb{Z}/p\mathbb{Z}$ operiere auf M durch zyklische Permutation.
Diese Operation ist wohldefiniert, denn aus

$$a_1 \cdot \ldots \cdot a_p = 1$$

folgt schon für ein $z \in \{1, \ldots, p-1\}$:

$$a_{1+z} \cdot \ldots \cdot a_p \cdot a_1 \cdot \ldots \cdot a_z = a_{1+z} \cdot \ldots \cdot a_{p-1}^{-1} \cdot \ldots \cdot a_1^{-1} \cdot a_1 \cdot \ldots \cdot a_z = 1$$

Sei M_0 die Menge der Fixpunkte unter dieser Operation, also:

$$M = \{(a, \ldots, a) \,| a^p = 1\}$$

Wegen $(e, \ldots, e) \in M_0$ ist $|M_0| > 0$.
Nach 13.2.1 folgt:

$$|M| \equiv |M_0| \mod p$$

Aus $p \,|\, G$ folgt also $p \,|\, |M| = |G|^{p-1}$, woraus also $p \,|\, |M_0|$ folgt.
Wegen $|M_0| > 0$ folgt damit $|M_0| \geq p$, weswegen es ein $(a, \ldots, a) \in M_0$ mit $a \neq e$ und $a^p = e$ gibt.
Da p eine Primzahl ist, heißt das $\operatorname{ord}(a) = p$, denn $\operatorname{ord}(a) \,|\, p$ und $\operatorname{ord}(a) \neq 1$. $\square_{13.2.4}$

13.2.5 Lemma

Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe.
Dann gilt:

$$(N_G(H) : H) \equiv (G : H) \mod p$$

Beweis

H operiere auf $M = G/H$ durch Linkstranslation und

$$M_0 = \left\{ gH \;\middle|\; \underset{h \in H}{\forall} : hgH = gH \right\}$$

sei die Menge der Fixpunkte.
Für $h \in H$ und $g \in G$ gilt:

$$hgH = gH \Leftrightarrow g^{-1}hg \in H$$

Also ist M_0 die Menge aller gH mit $g \in N_G(H)$. Damit folgt:

$$|M_0| = (N_G(H) : H)$$

Mit $|M| = (G : H)$ folgt die Behauptung aus 13.2.1. $\square_{13.2.5}$

13.2.6 Korollar

Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe.
Aus

$$p \mid (G : H)$$

folgt:

$$p \mid (N_G(H) : H)$$

Beweis

Dies folgt direkt aus 13.2.5. $\square_{13.2.6}$

13.2.7 Satz (1. Sylowsatz)

Seien G eine endliche Gruppe und p eine Primzahl.
Dann besitzt G eine p-Sylowgruppe.
Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

Beweis

Sei $H \subseteq G$ eine p-Untergruppe. ($H = \{e\}$ ist erlaubt.)
Zum Beweis des Satzes genügt es zu zeigen, dass, falls $p \mid (G : H)$ gilt, ein $H \subseteq H' \subseteq G$ mit

$$(H' : H) = p$$

existiert.
(Konstruiere dann sukzessive H' bis man bei einer p-Sylowgruppe angelangt ist.)
Es gelte also $p \mid (G : H)$.
Nach 13.2.6 gilt:

$$p \mid (N_G(H) : H)$$

Nach 13.2.4 enthält $N_G(H)/H$ eine Untergruppe der Ordnung p, deren Urbild in $N_G(H)$ ist ein H' mit den geforderten Eigenschaften. $\square_{13.2.7}$

13.2.8 Satz (2. Sylowsatz)

Seien G eine endliche Gruppe und p eine Primzahl.
Zu jeder p-Untergruppe H von G und jeder p-Sylowgruppe P von G existiert ein $g \in G$, sodass gilt:

$$gHg^{-1} \subseteq P$$

Je zwei p-Sylowgruppen von G sind konjugiert.

Beweis

H operiere auf $M := G/P$ durch Linkstranslation und M_0 sei die Menge der Fixpunkte.
Aus 13.2.1 folgt:

$$|M_0| \equiv |M| \mod p$$

Da $p \nmid |M| = (G : P)$ gilt, folgt $|M_0| \neq 0$.
Also existiert ein $g \in G$, sodass für alle $h \in H$ schon $hgP = gP$, also $g^{-1}Hg \subseteq P$ gilt.
Die erste Aussage ist damit bewiesen, die zweite folgt, da je zwei p-Sylowgruppen die gleiche Ordnung besitzen. $\square_{13.2.8}$

13.2.9 **Satz** (3. Sylowsatz)

Seien G eine endliche Gruppe, p eine Primzahl und s_p die Anzahl der p-Sylowgruppen von G.
Seien $n \in \mathbb{N}_{\geq 0}$ und $m \in \mathbb{N}_{\geq 1}$ mit $|G| = p^n \cdot m$ und $\text{ggT}\,(m,p) = 1$.
Dann gilt $s_p | m$ und $s_p \equiv 1 \bmod p$.

Beweis

G operiere auf der Menge M der p-Sylowgruppen von G durch Konjugation und P sei eine p-Sylowgruppe von G.
Nach dem zweiten Sylowsatz 13.2.8 gibt es nur eine Bahn und die Standuntergruppe G_P von P enthält P.
Damit folgt:

$$|M| = s_p = (G : G_P) \mid (G : P) = m$$

Sei P eine p-Sylowgruppe von G, P operiere auf M durch Konjugation und M_0 sei die Menge der Fixpunkte.

$$Q \in M_0 \Leftrightarrow P \subseteq N_G(Q)$$

Für $Q \in M_0$ sind P und Q bereits p-Sylowgruppen von $N_G(Q)$ und damit konjugiert nach 13.2.8, also folgt aus $P = Q$ schon $M_0 = \{P\}$.
Die Behauptung folgt nun aus 13.2.1. $\square_{13.2.9}$

13.3 Auflösbare Gruppen

13.3.1 **Definition** (auflösbar)

Eine Gruppe G heißt *auflösbar*, wenn es ein $r \in \mathbb{N}$ und eine Kette

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

von Untergruppen von G gibt, sodass für $i \in \{1, \ldots, r\}$ schon $H_i \trianglelefteq H_{i-1}$ gilt und H_i / H_{i-1} eine endliche, abelsche Gruppe ist.

Bemerkung

Aus dem Struktursatz endlicher Gruppen folgt, dass folgende Aussage äquivalent dazu ist:
Es gibt ein $r \in \mathbb{N}$ und eine Kette

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

von Untergruppen von G, sodass für $i \in \{1, \ldots, r\}$ schon $H_i \trianglelefteq H_{i-1}$ gilt und H_i / H_{i-1} endlich und zyklisch von Primzahlordnung ist.
TODO: Beweis einfügen

13.3.2 Beispiel

i) Ist G eine endliche, abelsche Gruppe, so ist G auflösbar.

Beweis

Dies folgt zum Beispiel aus dem Strukturssatz oder durch Induktion über die Gruppenordnung.
Beachte, dass jede, insbesondere jede zyklische, Untergruppe normal ist.
TODO: Beweis einfügen

$\square_{\text{i)}}$

ii) Jede endliche p-Gruppe ist auflösbar. (siehe 13.1.12)

13.3.3 Satz

Sei G eine endliche Gruppe.
Dann gelten:

i) Ist G auflösbar, so ist auch jede Untergruppe A von G auflösbar.

ii) Ist G auflösbar und $N \trianglelefteq G$ beliebig, so ist auch die Quotientengruppe G/N von G auflösbar.

iii) Sei $N \trianglelefteq G$. Sind N und G/N auflösbar, so auch G.

Beweis

TODO: Beweis als Übung einfügen

$\square_{13.3.3}$

13.4 Permutationsgruppen

Seien $n \in \mathbb{N}$, $M := \{1,\dots,n\}$ und $S := \Sigma(M) = S_n$.
Seien $\sigma \in S$ und $H := \langle\sigma\rangle \subseteq S$.
Sei $a \in M$. Die Bahn $H \cdot a$ nennen wir *die Bahn von a bezüglich σ*.
Sei H_a die Standuntergruppe und $d := (H : H_a)$.
Dann folgt:

$$Ha = \left\{\sigma, \sigma a, \sigma^2 a, \dots, \sigma^{d-1}\right\}$$

13.4.1 Definition (Zykel)

Ein $\varrho \in S$ heißt *ein Zykel der Länge d*, wenn es $d \in \mathbb{N}_{\geq 1}$ verschiedene Elemente $a_1,\dots,a_d \in M$ mit:

$$\begin{aligned} \varrho a_i &= a_{i+1} && \text{für } 1 \leq i \leq d \\ \varrho a_d &= a_1 \\ \varrho a &= a && \text{für alle } a \in M \setminus \{a_1,\dots,a_d\} \end{aligned} \tag{13.5}$$

13.4.2 Notation

Zu d verschiedenen Elementen $a_1,\dots,a_d \in M$ gibt es genau ein $\varrho \in S$ mit (13.5).
Dieser Zykel wir mit $\varrho = \begin{pmatrix} a_1 & a_2 & \dots & a_d \end{pmatrix}$ bezeichnet.

13.4.3 Bemerkung

i) Es gilt:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_d \end{pmatrix} = \begin{pmatrix} a_2 & a_3 & \dots & a_d & a_1 \end{pmatrix} = \dots = \begin{pmatrix} a_d & a_1 & \dots & a_{d-1} \end{pmatrix}$$

ii) Ein Zykel der Länge d hat die Ordnung d.

iii) Für $\tau \in S$ gilt:

$$\tau \begin{pmatrix} a_1 & a_2 & \dots & a_d \end{pmatrix} \tau^{-1} = \begin{pmatrix} \tau a_1 & \tau a_2 & \dots & \tau a_d \end{pmatrix}$$

TODO: Beweis einfügen

13.4.4 Definition (disjunkte Permutationen)

i) Für $\sigma \in S$ definiere:

$$W(\sigma) := \{a \in M | \sigma a \neq a\}$$

ii) Die Elemente σ,$\tau \in S$ heißen *disjunkt*, falls

$$W(\sigma) \cap W(\tau) = \emptyset$$

gilt. Dann gilt $\sigma\tau = \tau\sigma$.

13.4.5 Proposition

Jedes $\sigma \in S$ ist darstellbar als Produkt

$$\sigma = \varrho_1 \cdot \varrho_2 \cdot \ldots \cdot \varrho_r$$

von $r \in \mathbb{N}_{\geq 1}$ paarweise disjunkten Zykeln mit Länge $l(\varrho_i)$ für $1 \leq i \leq r$ und es gilt:

$$\sum_{i=1}^{r} l(\varrho_i) = n$$

Bis auf die Reihenfolge der Zykel ist diese Darstellung eindeutig.

Beweis

$C_1, \dots C_r$ seien die verschiedenen Bahnen bezüglich σ.
Für alle $1 \leq i \leq r$ gibt es einen Zykel ϱ_i, sodass für alle $a \in C_i$ gilt:

$$\varrho_i a = \sigma a$$

Zudem sind die ϱ_i paarweise disjunkt.
Sei $a \in M$, dann gibt es genau ein $i \in \{1, \dots, r\}$ mit $a \in C_i$.
Dann gilt $\varrho_1 \varrho_2 \dots \varrho_r a = \varrho_i a = \sigma a$.
Also ist $\sigma = \varrho_1 \varrho_2 \dots \varrho_r$. Damit ist die Existenz gezeigt.
Ist $\sigma = \gamma_1 \gamma_2 \dots \gamma_s$ mit $s \in \mathbb{N}_{>1}$, paarweise disjunkten Zykeln γ_i für $1 \leq i \leq s$ und Länge $l(\gamma_i)$ mit:

$$\sum_{i=1}^{s} l(\gamma_i) = n$$

Dann sind $W(\gamma_1), \dots, W(\gamma_2)$ die Bahnen bezüglich σ, also $r = s$ und ohne Einschränkung $W(\gamma_i) = C_i$.
Dann muss auch $\gamma_i = \varrho_i$ gelten. $\square_{13.4.5}$

13.4.6 Bemerkung

Ist $\sigma = \varrho_1 \dots \varrho_r$ mit $r \in \mathbb{N}_{\geq 1}$ und paarweise disjunkten Zykeln ϱ_i für $1 \leq i \leq r$, so ist $\operatorname{ord}(\sigma)$ das kleinste gemeinsame Vielfache der Längen der ϱ_i.

13.4.7 Definition (Typ)

Sei $\sigma \in S$ mit $\sigma = \varrho_1 \dots \varrho_r$ wie in 13.4.5.
σ besitze *den Typ* $c_1,c_2,\dots,c_n$ mit $n,c_i \in \mathbb{N}$ für $1 \leq i \leq n$, wenn in der Zerlegung von σ genau c_i Zyklen der Länge i vorkommen.

13.4.8 Proposition

Elemente $\sigma,\sigma' \in S$ sind genau dann konjugiert, wenn sie den gleichen Typ haben.

Beweis

$\sigma = \varrho_1\varrho_2 \dots \varrho_r$ wie in 13.4.5 und $\tau \in S$, dann folgt:

$$\tau\sigma\tau^{-1} = \left(\tau\varrho_1\tau^{-1}\right) \dots \left(\tau\varrho_r\tau^{-1}\right)$$

ist eine Zerlegung von $\tau\sigma\tau^{-1}$ wie in 13.4.5, also ist der Typ von σ gleich dem Typ von $\tau\sigma\tau^{-1}$.
Seien nun σ,σ' vom gleichen Typ.

$$\sigma = \varrho_1 \dots \varrho_r \qquad\qquad \sigma' = \varrho'_1 \dots \varrho'_{r'}$$

Wie in 13.4.5.
Dann folgt $r = r'$ und ohne Einschränkung ist die Länge von ϱ_i gleich der Länge von ϱ'_i für $1 \leq i \leq r$ und es gilt:

$$\varrho_i = \begin{pmatrix} a_1 & \dots & a_d \end{pmatrix} \qquad\qquad \varrho'_i = \begin{pmatrix} a'_1 & \dots & a'_d \end{pmatrix}$$

Definiere:

$$\begin{gathered} \varphi_i : \{a_1, \dots, a_d\} \to \{a'_1, \dots, a'_d\} \\ a_i \mapsto a'_i \end{gathered}$$

Da die $\varrho_1, \dots, \varrho_r$ und $\varrho'_1, \dots, \varrho'_r$ disjunkte Zykel sind, setzen sich die φ_i zu einer Bijektion $\tau : M \to M$ zusammen.
Mit \13.4.3 iii) gilt:

$$\tau\sigma\tau^{-1} = \left(\tau\varrho_1\tau^{-1}\right) \dots \left(\tau\varrho_r\tau^{-1}\right) = \varrho'_1 \dots \varrho'_r = \sigma'$$

$\square_{13.4.8}$

13.4.9 Wiederholung (Signatur)

$$\operatorname{sgn} : S \to \{\pm 1\}$$

Seien $s \in \mathbb{N}_{\geq 1}$, $\sigma = \tau_1 \dots \tau_s$ und τ_i für $1 \leq i \leq s$ Transpositionen, so gilt:

$$\operatorname{sgn}(\sigma) = (-1)^s$$

$$\begin{pmatrix} a_1 & a_2 & \dots & a_d \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \dots \begin{pmatrix} a_{d-1} & a_d \end{pmatrix}$$

Damit folgt:

$$\operatorname{sgn}\left(\begin{pmatrix} a_1 & a_2 & \dots & a_d \end{pmatrix}\right) = (-1)^{d-1}$$

Der Kern

$$\ker(\operatorname{sgn}) = A_n$$

heißt *die alternierende Gruppe.*
Für $\sigma \in S$ heißt σ *gerade*, falls $\sigma \in A_n$, sonst *ungerade.*

13.4.10 Lemma

Sei $n \in \mathbb{N}_{\geq 5}$ und G eine Untergruppe von S_4, die jeden Zykel der Länge 3 enthält.

Ist dann N ein Normalteiler von G mit abelscher Quotientengruppe G/N, so enthält auch N jeden Zykel der Länge 3.

Beweis

Sei $\begin{pmatrix} a & b & c \end{pmatrix}$ ein Dreierzykel, so gibt es $u,v \in M \setminus \{a,b,c\}$ mit $u \neq v$.

$$\sigma := \begin{pmatrix} a & c & v \end{pmatrix}$$
$$\varrho := \begin{pmatrix} a & b & u \end{pmatrix}$$

Aus 13.4.3 iii) folgt:

$$\varrho\sigma\varrho^{-1} = \begin{pmatrix} \varrho a & \varrho c & \varrho v \end{pmatrix} = \begin{pmatrix} b & c & v \end{pmatrix}$$

Also gilt:

$$\varrho\sigma\varrho^{-1}\sigma^{-1} = \begin{pmatrix} b & c & v \end{pmatrix}\begin{pmatrix} v & c & a \end{pmatrix} = \begin{pmatrix} a & b & c \end{pmatrix}$$

Also ist $\begin{pmatrix} a & b & c \end{pmatrix} \in N$. $\square_{13.4.10}$

13.4.11 Satz (Auflösbarkeit von S_n)

Die Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist.

Beweis

$n = 1$ und $n = 2$ sind klar.
Sei $n = 3$:

$$\{e\} \trianglelefteq A_3 \trianglelefteq S_3$$

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$
$$A_3/\{e\} \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$$

Sei $n = 4$:

$$V_4 := \{1, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$$

$$(12)(34)\cdot(13)(24) = (14)(23) = (13)(24)\cdot(12)(34)$$
$$(12)(34)\cdot(14)(23) = (13)(24) = (14)(23)\cdot(12)(34)$$
$$(13)(24)\cdot(14)(23) = (12)(34) = (14)(23)\cdot(13)(24)$$

Daher ist V_4 eine Untergruppe von S_4, denn jedes Element ist sein eigenes Inverses.
V_4 ist isomorph zu ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.
Wegen 13.4.3 iii) ist V_4 ein Normalteiler in S_4 und $V_4 \subseteq A_4$ mit ${}^{A_4}\!/_{V_4} \cong {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$.
Daher ist S_4 auflösbar mit $\{e\} \trianglelefteq \{e,(12)(34)\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$.
$n \geq 5$. Wäre S_n auflösbar, so gäbe es eine Kette

$$G = H_0 \trianglerighteq G_1 \trianglerighteq G_2 \ldots \trianglerighteq G_m = \{e\}$$

mit ${}^{G_{i-1}}\!/_{G_i}$ abelsch.
Nach 13.4.10 wäre induktiv jeder Dreierzykel in jedem G_i enthalten.
Dies ist ein Widerspruch zu $G_m = \{e\}$. $\square_{13.4.11}$

13.4.12 **Definition** (einfache Gruppe)

Eine Gruppe $G \neq \{e\}$ heißt *einfach*, wenn G außer $\{e\}$ und G keine weiteren Normalteiler besitzt.

13.4.13 **Bemerkung**

Es gilt folgender Satz: A_n ist einfach für $n \geq 5$.

13.5 Semidirekte Produkte

Seien N und H Gruppen und

$$\varphi : H \to \mathrm{Aut}(N)$$

ein Homomorphismus.

13.5.1 **Satz und Definition** (semidirektes Produkt)

Die auf der Menge $N \times H$ definierte Verknüpfung

$$((n_1,h_1),(n_2,h_2)) \mapsto (n_1,h_1)\cdot(n_2,h_2) := (n_1 \cdot \varphi(h_1)(n_2), h_1h_2)$$

stattet $N \times H$ mit der Struktur einer Gruppe aus.
Sie wird als *das semidirekte Produkt* $N \times_\varphi H$ *oder* $N \rtimes H$ bezeichnet.

Beweis

(e,e) ist offensichtlich ein (links- und rechts-)neutrales Element.
Assoziativität:

$$\begin{aligned}(n_1\varphi(h_1)(n_2), h_1h_2)\cdot(n_3,h_3) &= (n_1\varphi(h_1)(n_2)\,\varphi(h_1h_2)(n_3), h_1h_2h_3) = \\ &= (n_1\varphi(h_1)(n_2\varphi(h_2)(n_3)), h_1h_2h_3) = \\ &= (n_1,h_1)(n_2\varphi(h_2)(n_3), h_2h_3)\end{aligned}$$

Existenz Inverser:

$$\begin{aligned}(n,h)\left(\varphi\left(h^{-1}\right)\left(n^{-1}\right),h^{-1}\right) &= \left(n\varphi(h)\,\varphi\left(h^{-1}\right)\left(n^{-1}\right),e\right) = \left(nn^{-1},e\right) = (e,e)\\ \left(\varphi\left(h^{-1}\right)\left(n^{-1}\right),h^{-1}\right)(n,h) &= \left(\varphi\left(h^{-1}\right)\left(n^{-1}\right)\varphi\left(h^{-1}\right)(n),e\right) =\\ &= \left(\varphi\left(h^{-1}\right)\left(nn^{-1}\right),e\right) = \left(\varphi\left(h^{-1}\right)(e),e\right) = (e,e)\end{aligned}$$

$\square_{13.5.1}$

13.5.2 Definition (kurze exakte Sequenz, Split)

Betrachte die Abbildungen von Gruppen:

$$\begin{aligned}N &\xrightarrow{f} N \times_\varphi H & \qquad H &\xrightarrow{g} N \times_\varphi H\\ n &\mapsto (n,e) & \qquad h &\mapsto (e,h)\end{aligned}$$

$N \trianglelefteq N \times_\varphi H$ sei ein Normalteiler.

$$\{e\} \to N \xrightarrow{f} N \times_\varphi H \underset{\overset{\leftarrow}{g}}{\overset{p_2}{\rightarrow}} H \to \{e\}$$

ist eine *kurze* exakte Sequenz. (Kurz bedeutet, dass genau drei nicht-triviale Gruppen vorkommen.)
g ist ein *Split* von p_2, das heißt $p_2 \circ g = \mathrm{id}_H$.

13.5.3 Beispiele

i) Andersherum sei

$$\{e\} \to N \xrightarrow{f} G \underset{\overset{\leftarrow}{g}}{\overset{p}{\rightarrow}} G\big/_N =: H \to \{e\}$$

mit $p \circ g = \mathrm{id}_H$. H operiert auf N durch Konjugation und liefert den Homomorphismus:

$$\begin{aligned}\varphi : H &\to \mathrm{Aut}(N)\\ h &\mapsto \left(n \mapsto f^{-1}\left(g(h)\,f(n)\,g\left(h^{-1}\right)\right)\right)\end{aligned}$$

Damit folgt, dass die Abbildung

$$\begin{aligned}\Phi : N \times_\varphi H &\to G\\ (n,h) &\mapsto f(n) \cdot g(h)\end{aligned}$$

ein bijektiver Gruppenhomomorphismus ist.
Gruppenhomomorphismus:

$$\begin{aligned}\Phi((n_1,h_1)) \cdot \Phi((n_2,h_2)) &= f(n_1)\,g(h_1) \cdot f(n_2)\,g(h_2) =\\ &= f(n_1)\underbrace{\left(g(h_1)\,f(n_2)\,g\left(h_1^{-1}\right)\right)}_{=f(\varphi(h_1)(n_2))}g(h_1)\,g(h_2) =\\ &= f(n_1\varphi(h_1)(n_2)) \cdot g(h_1h_2) =\\ &= \Phi(n_1\varphi(h_1)(n_2),h_1h_2) = \Phi((n_1,h_1)\cdot(n_2,h_2))\end{aligned}$$

Bijektivität:

$$\begin{aligned}\Psi : G &\to N \times_\varphi H\\ x &\mapsto \left(f^{-1}\left(x \cdot g(p(x))^{-1}\right),p(x)\right)\end{aligned}$$

Es gilt:

$$\begin{aligned}(\Psi \circ \Phi)(n,h) &= \left(f^{-1}\left(f(n)\cdot g(h)\cdot g\left(p\left(f(n)\cdot g(h)\right)\right)^{-1}\right), p\left(f(n)\cdot g(h)\right)\right) = \\ &= \left(f^{-1}\left(f(n)\cdot g(h)\cdot g\left(p\left(f(n)\right)\right)^{-1}\cdot g\left(p\left(g(h)\right)\right)^{-1}\right), p\left(f(n)\right)\cdot p\left(g(h)\right)\right) = \\ &\overset{\substack{p\circ g=\mathrm{id}_H \\ \mathrm{im}(f)=\ker(p)}}{=} \left(f^{-1}\left(f(n)\cdot g(h)\cdot g(e)^{-1}\cdot g(h)^{-1}\right), e\cdot h\right) = (n,h)\end{aligned}$$

Also ist $\Psi \circ \Phi = \mathrm{id}_{N\times_\varphi H}$. Andersherum:

$$(\Phi \circ \Psi)(x) = f\left(f^{-1}\left(x\cdot g\left(p(x)\right)^{-1}\right)\right)\cdot g\left(p(x)\right) = x\cdot g\left(p(x)\right)^{-1}\cdot g\left(p(x)\right) = x$$

Daher gilt auch $\Phi \circ \Psi = \mathrm{id}_G$ und daher ist Ψ die inverse Abbildung zu Φ und somit Φ bijektiv.

ii) Die Gruppe der euklidischen Bewegungen im $\mathbb{R}^n$:

$$E(n) = \mathbb{R}^n \rtimes O(n)$$

mit der Standardoperation von $O(n)$ (den orthogonalen Matrizen) auf $\mathbb{R}^n$.

14 Konstruktion mit Zirkel und Lineal

14.1 Definition (Geraden, Kreise)

i) Für $M \subseteq \mathbb{R}^2$ sei $\mathrm{Ge}(M)$ *die Menge der Geraden*, die zwei verschiedene Punkte von M enthalten, und $\mathrm{Kr}(M)$ *die Menge der Kreise*, deren Mittelpunkt in M liegt und deren Radius gleich dem Abstand zweier Punkte aus M ist.

ii) Für $M \subseteq \mathbb{R}^2$ sei $\curlywedge M$ die kleinste Teilmenge T von $\mathbb{R}^2$, für die gilt:

   a) $M \subseteq T$
   b) Der Schnitt zweier verschiedener Geraden aus $\mathrm{Ge}(T)$ liegt in T.
   c) Der Schnitt einer Geraden aus $\mathrm{Ge}(T)$ mit einem Kreis aus $\mathrm{Kr}(T)$ liegt in T.
   d) Der Schnitt zweier verschiedener Kreise aus $\mathrm{Kr}(T)$ liegt in T.

14.2 Bemerkung (mit Zirkel und Lineal konstruierbar)

$\curlywedge M$ ist die Punktmenge aus $\mathbb{R}^2$, die aus M *mit Zirkel und Lineal konstruierbar* ist.
Im Folgenden identifizieren wir $\mathbb{R}^2$ mit $\mathbb{C}$.

14.3 Proposition

Sei $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$.
Dann gelten:

i) $\mathbf{i} \in \curlywedge M$
ii) $z \in \curlywedge M \Rightarrow \overline{z} \in \curlywedge M$
iii) $z \in \curlywedge M \Rightarrow \mathrm{Re}(z), \mathrm{Im}(z) \in \curlywedge M$
iv) $z \in \curlywedge M \Rightarrow -z \in \curlywedge M$
v) $z_1, z_2 \in \curlywedge M \Rightarrow z_1 + z_2 \in \curlywedge M$
vi) $z_1, z_2 \in \curlywedge M \Rightarrow z_1 \cdot z_2 \in \curlywedge M$
vii) $z \in \curlywedge M \setminus \{0\} \Rightarrow \frac{1}{z} \in \curlywedge M$

Beweis

i) -1 ist ein Schnittpunkt der Gerade durch 0 und 1 mit dem Kreis um 0 vom Radius 1 und liegt daher in $\bigstar M$.

Außerdem liegt $\mathbf{i} \in \bigstar M$, weil es ein Schnittpunkt der Mittelsenkrechten zu $[-1,1]$ mit dem Einheitskreis ist.

ii) $\overline{z}$ ist ein Schnittpunkt des Kreises um 0 vom Radius $|z|$ mit dem Kreis um 1 vom Radius $|z-1|$. Also ist auch $\overline{z} \in \bigstar M$.

iii) $\mathrm{Re}\,(z) \in \bigstar M$, da entweder $z \in \mathbb{R}$ ist, oder $\mathrm{Re}\,(z)$ der Schnittpunkt der Gerade durch z und $\overline{z}$ mit der Gerade durch 0 und 1 ist.

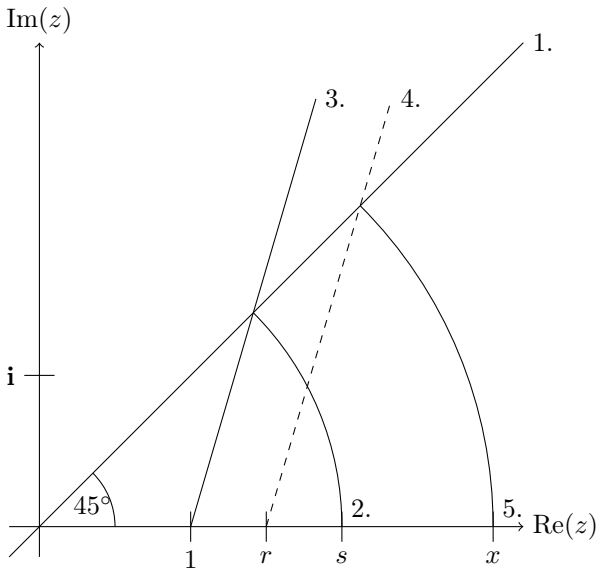
Analog folgt $\mathrm{Im}\,(z) \in \bigstar M$.

iv) Der Schnitt von Geraden durch 0 und z mit dem Kreis um 0 von Radius $|z|$ ergibt $-z$.

v) $z_1 + z_2 \in \bigstar M$, da es ein Schnittpunkt des Kreises um z_1 vom Radius $|z_2|$ mit dem Kreis um z_2 vom Radius $|z_1|$ ist.

vi) Wegen iv) und v) genügt es die Behauptung für $r,s \in \mathbb{R}_{>0} \subseteq \mathbb{C}$ zu zeigen, denn es gilt:

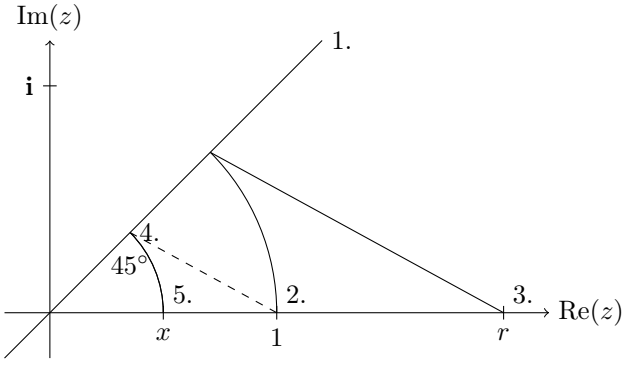
$$(a + \mathbf{i}b)\,(c + \mathbf{i}d) = ac - bd + \mathbf{i}\,(ab + bc)$$



Der Strahlensatz ergibt:

$$\frac{x}{s} = \frac{r}{1} \quad \Rightarrow \quad x = rs$$

vii) Wegen $z^{-1} = \overline{z}\,(z\overline{z})^{-1} = \overline{z} \cdot |z|^{-1}$ genügt es die Behauptung für $r := |z| \in \mathbb{R}_{>0}$ zu zeigen.



Der Strahlensatz ergibt:

$$\frac{r}{1} = \frac{1}{x} \quad \Rightarrow \quad x = \frac{1}{r}$$

$\square_{14.3}$

14.4 Korollar

Seien $M \subseteq \mathbb{C}$ und $\{0,1\} \subseteq M$.
Dann ist $\curlywedge M$ ein Teilkörper von $\mathbb{C}$.

Beweis

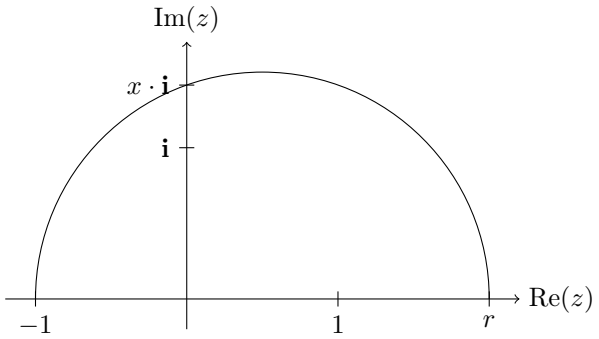
Dies folgt sofort aus 14.3. $\square_{14.4}$

14.5 Proposition

Seien $M \subseteq \mathbb{C}$, $\{0,1\} \subseteq M$ und $z \in \curlywedge M$.
Dann ist $w \in \curlywedge M$ für alle $w \in \mathbb{C}$ mit $w^2 = z$.

Beweis

Aus $w^2 = z = re^{\mathbf{i}\varphi}$ folgt $w = \pm\sqrt{r}e^{\mathbf{i}\frac{\varphi}{2}}$.
Wegen $e^{\mathbf{i}\frac{\varphi}{2}} \in \curlywedge M$, genügt es zu zeigen, dass $\sqrt{r} \in \curlywedge M$ ist.



Aus dem Höhensatz folgt:

$$x^2 = 1 \cdot r$$

Also ist $x = \sqrt{r}$. $\square_{14.5}$

14.6 Proposition und Definition (komplex konjugierte Menge)

Für $M \subseteq \mathbb{C}$ sei $\overline{M} := \{\overline{m} | m \in M\} \subseteq \mathbb{C}$ *die komplex konjugierte Menge.*
Sei $K \subseteq \mathbb{C}$ ein Teilkörper mit $K = \overline{K}$.

a) Ist z der Schnittpunkt zweier verschiedener Geraden aus $\mathrm{Ge}(K)$, so folgt $z \in K$.

b) Ist z ein Schnittpunkt einer Geraden aus $\mathrm{Ge}(K)$ mit einem Kreis aus $\mathrm{Kr}(K)$, so gilt:

$$\underset{w\in\mathbb{C}}{\exists} : w^2 \in K \wedge z \in K(w) \tag{14.1}$$

c) Ist z ein Schnittpunkt zweier verschiedener Kreise aus $\mathrm{Kr}(K)$, so gilt 14.1.

Beweis

a) Seien $z_0,z_0' \in K$ und $z_1,z_1' \in K^*$, so dass für

$$G := \{z_0 + tz_1 | t \in \mathbb{R}\}$$
$$G' := \{z_0' + tz_1' | t \in \mathbb{R}\}$$

schon $G \neq G'$ und $G \cap G' \neq \emptyset$ gilt.
Sei $z \in G \cap G'$, $z = z_0 + t_1 z_1 = z_0' + t' z_1'$.
(t,t') ist die eindeutige Lösung des linearen Gleichungssystems

$$t\mathrm{Re}(z_1) - t'\mathrm{Re}(z_1') = \mathrm{Re}(z_0') - \mathrm{Re}(z_0)$$
$$t\mathrm{Im}(z_1) - t'\mathrm{Im}(z_1') = \mathrm{Im}(z_0') - \mathrm{Im}(z_0)$$

über K, und wegen $K = \overline{K}$, also $\mathrm{Re}(z), \mathrm{Im}(z) \in K$ für alle $z \in K$, sind $t,t' \in K$.

b) Seien $a,z_0,\alpha,\beta \in K$, $r^2 := |\alpha - \beta|^2 \in \mathbb{R}_{\geq 0} \cap K$, $t \in \mathbb{R}$ und $z_1 \in K^*$.

$$k := \left\{ z \,\middle|\, (z-a)\overline{(z-a)} = r^2 \right\}$$

$$z_0 + tz_1 \in k \Leftrightarrow (z_0 + z_1 t - a)(\overline{z_0} + \overline{z_1} t - \overline{a}) = r^2$$

Also folgt

$$t^2 + pt + q = \left(t + \frac{p}{2}\right)^2 + \frac{p^2}{4} + q = 0$$

mit $p,q \in K$ wegen $K = \overline{K}$.
Für $w := t + \dfrac{p}{2}$ gilt

$$w^2 = -\frac{p^2}{4} - q \in K$$

und $z_0 + tz_1 \in K(t) = K(w)$.

c) Sei $a,b,\alpha,\alpha',\beta,\beta' \in K$ mit $a \neq b$, $r^2 := |\alpha - \beta|^2$, $s^2 := |\alpha' - \beta'|^2 \in \mathbb{R}_{\geq 0} \cap K$ und $z \in \mathbb{C}$ mit:

$$\begin{aligned} (z-a)(\overline{z} - \overline{a}) &= r^2 \\ (z-b)\left(\overline{z} - \overline{b}\right) &= s^2 \end{aligned} \tag{14.2}$$

Subtraktion der Gleichungen liefert:

$$z\left(\overline{b} - \overline{a}\right) + \overline{z}(b-a) \in K$$

Auflösen nach $\overline{z}$ und Einsetzen in 14.2 ergibt eine quadratische Gleichung. Der Rest des Beweises geht analog zur b).

$\square_{14.6}$

14.7 Satz

Sei $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$ und $K := \mathbb{Q}\left(M \cup \overline{M}\right)$, also $K = \overline{K}$.
Dann sind für ein $z \in \mathbb{C}$ äquivalent:

i) $z \in \not\bowtie M$

ii) z liegt in einem Teilkörper E von $\mathbb{C}$, der K enthält und durch sukzessive Adjunktion von Quadratwurzeln aus K entsteht.

iii) Es gibt eine endliche Kette von Teilkörpern

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$$

von $\mathbb{C}$ mit

$$[K_i : K_{i-1}] = 2$$

für alle $i \in \{1,\ldots,m\}$, sodass $z \in K_m$ ist.

iv) z ist algebraisch über K und für die normale Hülle ${}^{E}\!/_{K}$ von ${}^{K(z)}\!/_{K}$ gilt:

$$[E : K]$$

ist eine Potenz von 2.

Beweis

i) $\Rightarrow$ ii) folgt aus 14.6.
ii) $\Rightarrow$ iii): Entsteht E' aus E durch Adjunktion eine Quadratwurzel, so gilt $[E' : E] \in \{1,2\}$.
iii) $\Rightarrow$ iv): Es existiert ein $w_i \in K_i$ mit $w_i^2 \in K_{i-1}$ und $K_i = K_{i-1}(w_i)$. (quadratische Ergänzung)
Sei ${}^{E_m}\!/_{K}$ normale Hülle von ${}^{K_m}\!/_{K}$, also galoissch. Daher genügt es zu zeigen, dass $[E_m : K]$ eine Potenz von 2 ist.
Induktion nach m:
$m = 1$ ist klar.
Sei also $m > 1$ und E_{m-1} eine normale Hülle von K_{m-1} über K.
Nach Induktionsvoraussetzung ist $[E_{m-1} : K]$ eine Potenz von 2, $K_m = K_{m-1}(w_m)$.
Seien $\alpha_1 = w_m, \alpha_2, \ldots, \alpha_s$ die verschiedenen Konjugierten von w_m über K in $\mathbb{C}$.
Dann gilt $\alpha_i^2 \in E_{m-1}$, da α_i^2 über K konjugiert ist zu $w_m^2 \in K_{m-1}$.
Es gilt $E_m = E_m(\alpha_1, \ldots, \alpha_s)$.
Damit folgt mit einem geeigneten $a \in \mathbb{N}$:

$$[E_m : E_{m-1}] = 2^a$$

Also auch:

$$[E_m : K] = [E_m : E_{m-1}] \cdot [E_m : K]$$

iv) $\Rightarrow$ i): ${}^{E}\!/_{K}$ ist galoissch und $\mathrm{Gal}\left({}^{E}\!/_{K}\right)$ ist eine 2-Gruppe. Nach 13.1.12 gibt es eine Kette von Untergruppen

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

von G mit $(H_{i-1} : H_i) = 2$.

Dazu gehört eine Kette von Zwischenkörpern

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = E$$

mit $[K_i : K_{i-1}] = 2$.
Jedes K_i entsteht aus K_{i-1} durch Adjunktion einer Quadratwurzel (quadratische Ergänzung), also erhält man mit 14.5 sukzessive:

$$K = K_0 \subseteq \not\propto M \qquad K_1 \subseteq \not\propto M \qquad \ldots \qquad K_n \subseteq \not\propto M$$

Also ist $z \in \not\propto M$. $\square_{14.7}$

14.8 Beispiele

i) Delisches Problem: Volumenverdopplung eines Würfels:

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$$

Also ist ein Würfel doppelten Volumens nicht konstruierbar.

ii) Quadratur des Kreises: π ist transzendent (Lindemann 1882), das heißt nicht algebraisch.
Also kann man kein Quadrat konstruieren, dass die gleiche Fläche wie ein Kreis hat.

iii) Dreiteilung des Winkels:

Hat die normale Hülle von $\mathbb{Q}\left(e^{\frac{\mathbf{i}\varphi}{3}}\right)$ über $\mathbb{Q}\left(e^{\mathbf{i}\varphi}\right)$ einen 2er Potenzgrad?

Im Allgemeinen nicht:
Wähle φ so, dass $e^{\mathbf{i}\varphi}$ transzendent ist über $\mathbb{Q}$, dies geht, da $\mathbb{Q}$ abzählbar ist und die Anzahl der Winkel in [0,2π) überabzählbar.
Dann ist $\left[\mathbb{Q}\left(e^{\frac{\mathbf{i}\varphi}{3}}\right) : \mathbb{Q}\left(e^{\mathbf{i}\varphi}\right)\right] = 3$, denn $X^3 - t$ ist irreduzibel über $\mathbb{Q}(t)$.

iv) Konstruktion von regelmäßigen n-Ecken (n-Teilung des Kreises):

Ein n-Eck ist genau dann konstruierbar, wenn $\left[\mathbb{Q}\left(e^{\frac{2\pi\mathbf{i}}{n}}\right) : \mathbb{Q}\right] = \varphi(n)$ eine 2er-Potenz ist.

Dies ist äquivalent dazu, dass

$$n = 2^e \cdot p_1 \cdot \ldots \cdot p_r$$

mit paarweise verschiedenen Primzahlen p_i mit $p_i - 1$ ist eine Zweierpotenz.

Lemma

Für $m \in \mathbb{N}_{>0}$ ist $1 + 2^m$ höchstens dann eine Primzahl, wenn m eine Potenz von 2 ist.

Beweis

Sei $p = 1 + 2^m$ eine Primzahl.
$m = m_1 \cdot m_2$ mit $m_2 > 1$ und ungerade. Dann ist aber

$$p = 1 - (-2^{m_1})^{m_2} = (1 + 2^{m_1})\left(1 - 2^{m_1} + 2^{2m_1} - \ldots + 2^{m_1(m_2-1)}\right)$$

ein Produkt zweier Zahlen, die größer als 1 sind, was ein Widerspruch zur Primzahleigenschaft von p ist. $\square_{\text{Lemma}}$

Also $p_k = 2^{2^k} + 1$. Zum Beispiel sind 3,5,17,257,65537 solche Primzahlen.

15 Auflösbarkeit algebraischer Gleichungen

15.1 Charaktere

15.1.1 **Definition** (Charakter)

i) Ist G eine Gruppe und K ein Körper, so heißt ein Homomorphismus

$$\chi : G \to K^*$$

ein K-wertiger Charakter von G.

ii) Seien G, K wie in i). Mit Abb (G,K) wird der K-Vektorraum der mengentheoretischen Abbildungen von G nach K bezeichnet.

15.1.2 **Satz** (Charaktere sind linear unabhängig)

Paarweise verschiedene Charaktere $\chi_1, \ldots, \chi_n$ einer Gruppe G mit Werten in einem Körper K sind linear unabhängig in Abb (G,K).

Beweis

Sei

$$a_1\chi_1 + \ldots + a_n\chi_n = 0 \tag{15.1}$$

eine nicht-triviale Relation und ohne Einschränkung n minimal mit dieser Eigenschaft.
Also folgt $a_i \neq 0$ für alle $i \in \{1, \ldots, n\}$. Es gilt also für alle $g,h \in G$:

$$a_1\chi_1(gh) + \ldots + a_n\chi_n(gh) = 0$$

Wähle $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$ und lasse h variieren. Daher gilt:

$$a_1\chi_1(g) \cdot \chi_1 + \ldots + a_n\chi_n(g) \cdot \chi_n = 0$$

Subtraktion von $\chi_1(g) \cdot (15.1)$ liefert eine nicht-triviale Relation kleinerer Länge im Widerspruch zur Minimalität von n.
Daher können die χ_i nicht linear abhängig sein. $\square_{15.1.2}$

15.2 Zyklische Erweiterungen

15.2.1 **Proposition und Definition** (Norm)

Seien $K \subseteq E$ eine endliche Galoiserweiterung und $a \in E$.

Dann heißt

$$N_{E/K}(a) := \prod_{\sigma \in \mathrm{Gal}(E/K)} \sigma(a) \in K$$

die *Norm* von a bezüglich E/K.

$$N_{E/K} : E^* \to K^*$$

ist ein Homomorphismus.

Beweis

$$\prod_{\sigma \in \mathrm{Gal}(E/K)} \sigma(a)$$

ist $\mathrm{Gal}\left(E/K\right)$-invariant, und daher ein Element von K.

$$\begin{aligned} N_{E/K}(a \cdot b) = \prod_{\sigma \in \mathrm{Gal}(E/K)} \sigma(ab) = \prod_{\sigma \in \mathrm{Gal}(E/K)} \sigma(a) \cdot \prod_{\sigma \in \mathrm{Gal}(E/K)} \sigma(b) = \\ = N_{E/K}(a) \cdot N_{E/K}(b) \end{aligned}$$

15.2.2 Satz (Hilbert 90)

Seien L/K eine endliche zyklische Galoiserweiterung, $\sigma \in \mathrm{Gal}\left(L/K\right)$ ein erzeugendes Element.
Für ein $b \in L$ ist dann äquivalent:

i) $N_{L/K}(b) = 1$

ii) Es gibt ein $a \in L^*$ mit $b = \frac{a}{\sigma(a)}$.

Beweis

Gilt

$$b = \frac{a}{\sigma(a)}$$

mit $a \in L^*$, so ist:

$$N_{L/K}(b) = \frac{\prod_{\tau \in \mathrm{Gal}(L/K)} \tau(a)}{\prod_{\tau \in \mathrm{Gal}(L/K)} \tau(\sigma(a))} = 1$$

Sei umgekehrt $b \in L$ mit $N_{L/K}$ und $n = [L : K]$.
Wegen 15.1.2 ist

$$\sigma^0 + b\sigma^1 + b\sigma(b)\sigma^2 + \ldots + b\sigma(b) \cdot \ldots \cdot \sigma^{n-2}(b)\sigma^{n-1}$$

als Abbildung $L^* \to L$ nicht die Nullabbildung.
Also gibt es ein $c \in L^*$ mit:

$$a := c + b\sigma(c) + b\sigma(b)\sigma^2(c) + \ldots + b\sigma(b) \cdot \ldots \cdot \sigma^{n-2}(b)\sigma^{n-1}(c) \neq 0$$

Anwenden von σ und Multiplikation mit b ergibt:

$$b \cdot \sigma(a) := b \cdot \sigma(c) + b\sigma(b)\,\sigma^2(c) + \ldots + \underbrace{b\sigma(b) \cdot \ldots \cdot \sigma^{n-1}(b)\,\sigma^n(c)}_{=c} = a$$

Denn es gilt

$$\sigma^n = \mathrm{id}$$

und:

$$b \cdot \sigma(b) \cdot \ldots \cdot \sigma^{n-1}(b) = N_{L/K}(b) = 1$$

Also ist $b = \dfrac{a}{\sigma(a)}$. $\square_{15.2.2}$

15.2.3 **Satz** (zyklische Galoiserweiterung)

Sei L/K eine Körpererweiterung, $n \in \mathbb{N}_{>0}$ mit $\mathrm{char}(K) \nmid n$ und K enthalte eine primitive n-te Einheitswurzel.

i) Ist L/K eine zyklische Galoiserweiterung vom Grad n, so gilt $L = K(a)$ für ein Element $a \in L$, dessen Minimalpolynom über K von der Form $X^n - c$ mit $c \in K$ ist.

ii) Gilt $L = K(\alpha)$ für ein $\alpha \in L$, das Nullstelle eines Polynoms $X^n - c \in K[X]$ ist, so ist L/K eine zyklische Galoiserweiterung von K.
Weiterhin ist $d := [L : K]$ ein Teiler von n und es gilt $a^d \in K$, sodass $X^d - a^d \in K[X]$ das Minimalpolynom von a über K ist.

Beweis

Sei $\zeta \in K$ eine primitive n-te Einheitswurzel.

i) L/K ist zyklisch vom Grad n und wegen $\zeta^{-1} \in K$ und

$$\zeta^{-n} = (\zeta^n)^{-1} = 1^{-1} = 1$$

gilt:

$$N_{L/K}(\zeta^{-1}) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\zeta^{-1}) = \prod_{k=1}^{n} \zeta^{-1} = \zeta^{-n} = 1$$

Aus 15.2.2 folgt, dass es ein $a \in L^*$ mit $\zeta^{-1} = \dfrac{a}{\sigma(a)}$ gibt, also $\sigma(a) = \zeta a$, für einen Erzeuger σ von $\mathrm{Gal}\left(L/K\right)$.
Damit folgt für $i \in \{0, \ldots, n-1\}$:

$$\sigma^i(a) = \zeta^i a$$

Also sind $\sigma^0(a), \ldots, \sigma^{n-1}(a)$ paarweise verschieden und somit $[K(a) : K] \geq n$, also $K(a) = L$.
Es ist $\sigma(a^n) = \sigma(a)^n = \zeta^n a^n = a^n$, also $a^n \in K$ und a ist eine Nullstelle von $X^n - a^n$, weswegen dies das Minimalpolynom von a über K ist. $\square_{\mathrm{i)}}$

ii) ${}^{K(a)}\!/_{K}$ ist galoissch.
TODO: Beweis einfügen (Blatt 13 Aufgabe 4?)

$$\varphi : \mathrm{Gal}\left({}^{K(a)}\!/_{K}\right) \hookrightarrow \left\{\zeta^k \middle| k \in \{1,\ldots,n\}\right\} \subseteq K^*$$

Also gilt $d := [L:K] \,|n$ und $\mathrm{Gal}\left({}^{L}\!/_{K}\right)$ ist zyklisch.

Ist $\sigma \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)$ ein Erzeuger, so ist $\varphi(\sigma)$ eine primitive d-te Einheitswurzel und es gilt:

$$\sigma\left(a^d\right) = \sigma(a)^d = \varphi(\sigma)^d a^d = a^d$$

Daher folgt $a^d \in K$ und somit die Behauptung.

$\square_{15.2.3}$

15.3 Auflösbarkeit

Im gesamten Abschnitt betrachten wir nur Körper mit der Charakteristik 0.

15.3.1 **Definition** (Radikale, auflösbar)

i) Eine endliche Körpererweiterung ${}^{L}\!/_{K}$ heißt *durch Radikale auflösbar*, wenn es zu L einen Erweiterungskörper E, sowie eine Körperkette

$$K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_m = E$$

gibt, sodass E_{i+1} jeweils aus E_i durch Adjunktion einer Nullstelle eines Polynoms $X^n - a \in E_i[X]$ entsteht.

ii) Eine endliche Körpererweiterung heißt *auflösbar*, wenn es einen Oberkörper $E \supseteq L$ gibt, sodass ${}^{E}\!/_{K}$ eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe ist.

15.3.2 **Satz** (auflösbar $\Leftrightarrow$ durch Radikale auflösbar)

Eine endliche Körpererweiterung ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Beweis

Sei zunächst ${}^{L}\!/_{K}$ auflösbar. Ohne Einschränkung ist ${}^{L}\!/_{K}$ galoissch mit auflösbarer Galoisgruppe, sonst betrachte einen Erweiterungskörper mit auflösbarer Galoisgruppe.

Sei n das Produkt der Primzahlen, die $[L:K]$ teilen und ${}^{F}\!/_{K}$ entstehe durch Adjunktion der n-ten Einheitswurzeln und ist offenbar durch Radikale auflösbar. Wähle eine Einbettung $L \hookrightarrow \overline{F}$, dann ist ${}^{LF}\!/_{F}$ galoissch.

Da jedes $\sigma \in \mathrm{Gal}\left({}^{LF}\!/_{F}\right)$ die Identität auf F und somit auf K ist und weil ${}^{L}\!/_{K}$ normal ist, ist die Abbildung

$$\begin{aligned} \varphi : \mathrm{Gal}\left({}^{LF}\!/_{F}\right) &\hookrightarrow \mathrm{Gal}\left({}^{L}\!/_{K}\right) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

wohldefiniert und ein Homomorphismus. Wegen $FL = F(L)$ ist

$$\ker(\varphi) = \left\{\sigma \in \mathrm{Gal}\left(LF/F\right) \middle| \sigma|_L = \mathrm{id}_L\right\} = \overset{\sigma|_F = \mathrm{id}_F}{=} \left\{\sigma \in \mathrm{Gal}\left(LF/F\right) \middle| \sigma = \mathrm{id}_{LF} = e\right\} = \{e\}$$

und daher ist φ injektiv und wir können $\mathrm{Gal}\left(LF/F\right)$ als Untergruppe von $\mathrm{Gal}\left(L/K\right)$ auffassen, die wie jede Untergruppe von $\mathrm{Gal}\left(L/K\right)$ auflösbar ist.
Wähle

$$\mathrm{Gal}\left(LF/F\right) = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = \{e\}$$

so, dass $G_i \trianglelefteq G_{i-1}$ und $[G_{i-1} : G_i]$ eine Primzahl ist. Also liegt wegen

$$[G_{i-1} : G_i] \mid \left|\mathrm{Gal}\left(L/K\right)\right| = [L : K]$$

und weil $[G_{i-1} : G_i]$ eine Primzahl ist, also $[G_{i-1} : G_i] \mid n$ gilt, eine $[G_{i-1} : G_i]$-te primitive Einheitswurzeln in F.
Sei

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_m = L \cdot F$$

die entsprechende Körperkette.
Aus 15.2.3 i) folgt, dass F_i/F_{i-1} durch Adjunktion einer Nullstelle eines Polynoms $X^{[G_{i-1}:G_i]} - a$ entsteht.
Außerdem entsteht F aus K durch Adjunktion einer Nullstelle von $X^n - 1$, weswegen LF/K und somit wegen $L \subseteq LF$ auch L/K durch Radikale auflösbar ist.
Sei nun L/K durch Radikale auflösbar. Seien ohne Einschränkung

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_m = L$$

so, dass L_i durch Adjunktion einer n_i-ten Wurzel, genauer einer Nullstelle von $X^{n_i} - a_i \in L_{i-1}[X]$, aus L_{i-1} entsteht.
Sei n das kleinste gemeinsame Vielfache aller n_i, F entstehe aus K durch Adjunktion aller n-ten Einheitswurzeln und wähle eine Einbettung $L \hookrightarrow \overline{F}$.
Für alle $1 \leq i \leq m$ sei E_i eine normale Hülle von $L_i \cdot F$ über K.

Behauptung E_i/F hat eine auflösbare Galoisgruppe.

Beweis Führe eine Induktion über i durch:

Induktionsanfang: Da wegen $K = L_0 \subseteq F$ schon $F = L_0 \cdot F$ gilt, ist $E_0 = F$ eine normale Hülle von F und $E_0 = F/F$ hat die triviale Galoisgruppe, die offenbar auflösbar ist.

Induktionsschritt: Angenommen dies wurde für E_{i-1}/F schon gezeigt, so seien $a_i = a_i^1, \ldots, a_i^s$ die Galoiskonjugierten von a_i in E_{i-1} bezüglich $\mathrm{Gal}\left(E_{i-1}/K\right)$. Dann gilt:

$$E_i = E_{i-1}\left(\sqrt[n_i]{a_i^1}, \ldots, \sqrt[n_i]{a_i^s}\right)$$

Daher ist $\mathrm{Gal}\left(E_i/E_{i-1}\right)$ auflösbar und somit auch $\mathrm{Gal}\left(E_i/F\right)$. $\square_{\text{Behauptung}}$

Da $\mathrm{Gal}\left(F/K\right)$ auflösbar ist, ist auch $\mathrm{Gal}\left(E_m/K\right)$ auflösbar und wegen $L \subseteq E_m$ auch L/K.

$\square_{15.3.2}$

15.3.3 Korollar (Erweiterungen bis Grad 4 sind auflösbar)

Es sei L/K eine Körpererweiterung höchstens vom Grad 4.
Dann ist L/K auflösbar und insbesondere auch durch Radikale auflösbar.

Beweis

Nach dem Satz vom primitiven Element gibt es ein $\alpha \in L$ mit $L = K(\alpha)$ und $f := \mathrm{Mipo}_K(\alpha)$.
Sei L' ein Zerfällungskörper von f über K, so gibt es wegen $\deg(f) \leq 4$ eine Einbettung:

$$\mathrm{Gal}\left(L'/K\right) \hookrightarrow S_4$$

Da S_4 nach 13.4.11 auflösbar ist, so ist nach 13.3.3 i) auch $\mathrm{Gal}\left(L'/K\right)$ auflösbar, also auch L'/K und damit L/K. Aus 15.3.2, dass L/K ebenfalls durch Radikale auflösbar ist. $\square_{15.3.3}$

15.3.4 Korollar

Es existieren endliche Körpererweiterungen, die nicht durch Radikale auflösbar sind.
Beispielsweise ist die allgemeine Gleichung n-ten Grades für $n \geq 5$ nicht durch Radikale auflösbar.

Beweis

Die allgemeine Gleichung n-ten Grades, also

$$f(X) := X^n - \mathcal{S}_1 X^{n-1} + \ldots + (-1)^n \mathcal{S}_n = 0$$

mit $f \in k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X]$ für einen Körper k, hat als Galoisgruppe S_n, welche für $n \geq 5$ nach 13.4.11 nicht auflösbar ist.
Deswegen ist auch die dazugehörige Körpererweiterung nicht durch Radikale auflösbar. $\square_{15.3.4}$

15.3.5 Lemma und Definition (transitive Operation)

Für eine Primzahl p sei $G \subseteq S_p$ eine Untergruppe, die *transitiv* auf $\{1, \ldots, p\}$ operiere, dass heißt es gibt genau eine G-Bahn, oder anders ausgedrückt gibt es zu je zwei Elementen $i,j \in \{1, \ldots, p\}$ ein Element $g \in G$ mit $g \cdot i = j$.
Dann enthält G eine Untergruppe H der Ordnung p.
Ist G auflösbar, so ist H eindeutig bestimmt und insbesondere ein Normalteiler in G.

Beweis

Die Operation ist transitiv, hat genau eine G-Bahn Gj, welche p Elemente hat, und daher folgt aus der Bahnengleichung

$$p = \mathrm{ord}(Gj) = (G : G_j) = \frac{|G|}{|G_j|} \qquad \Rightarrow \quad p \mid |G|$$

und wegen

$$p^2 \nmid p! = |S_p|$$

auch schon:

$$p^2 \nmid |G| \mid |S_p|$$

Also hat G eine Untergruppe der Ordnung p, nämlich eine p-Sylowgruppe.
Ist G auflösbar, so gibt es eine Kette

$$G = G_0 \supseteq \ldots \supseteq G_n = \{e\}$$

so, dass $G_i \trianglelefteq G_{i-1}$ und $[G_i : G_{i-1}]$ eine Primzahl ist.

Behauptung G_i operiert auf $\{1,\ldots,p\}$ transitiv für $i < n$.

Beweis Führe eine Induktion nach i durch:
Induktionsanfang: $G_0 = G$ operiert nach Voraussetzung transitiv auf $\{1,\ldots,p\}$.
Induktionsschritt: Seien $i \in \mathbb{N}_{\geq 1}$ und $B_1,\ldots,B_r$ Bahnen der Operation von G_i auf $\{1,\ldots,p\}$, so gilt:

$$p = \sum_{j=1}^{r} |B_j|$$

Nach Induktionsvoraussetzung operiert G_{i-1} transitiv auf $\{1,\ldots,p\}$.
Da $G_i \trianglelefteq G_{i-1}$ ist, ergibt sich für $g \in G_{i-1}$ und $x \in \{1,\ldots,p\}$ die Gleichung $g\,(G_i x) = G_i\,(gx)$, also operiert G_{i-1} auf der Menge der Bahnen $\{B_1,\ldots,B_r\}$ transitiv. Damit folgt $|B_j| = |B_k|$ für alle $j,k \in \{1,\ldots,p\}$, und es gilt:

$$p = \sum_{j=1}^{r} |B_j| = r \cdot |B_1|$$

Da p eine Primzahl ist, folgt also $r = 1$ oder $|B_1| = 1$. Für $i < n$ ist $G_i \neq \{e\}$, also $|B_j| > 1$, weswegen schon $r = 1$ gelten muss, das heißt G_i operiert transitiv auf $\{1,\ldots,p\}$. $\square_{\text{Behauptung}}$

Wie oben enthält damit G_i für $i < n$ eine Untergruppe der Ordnung p und daher ist $G_{n-1} \cong \mathbb{Z}/p\mathbb{Z}$.
Für $i \in \{0,1,\ldots,n-2\}$ folgt:

$$p \nmid [G_i : G_{i-1}]$$

Ist nun $H \subseteq G_0$ mit $|H| = p$, so erhält man induktiv $H \subseteq G_i$ für $i \in \{0,1,\ldots,n-1\}$, da die Abbildung

$$H \hookrightarrow G_i \to G_i/G_{i+1}$$

für $i \in \{0,1,\ldots,n-2\}$ trivial ist.
Also ist $H = G_{n-1}$ und somit eindeutig bestimmt.
Dann ist aber H schon invariant unter Konjugation und somit ein Normalteiler von G. $\square_{15.3.5}$

15.3.6 Lemma

Sei G wie in 15.3.5 auflösbar.
Hat $\sigma \in G$ zwei verschiedene Fixpunkte auf $\{1,\ldots,p\}$, so folgt $\sigma = \mathrm{id}$.

Beweis

Nach 15.3.5 gibt es genau eine Untergruppe $H \subseteq G$ mit $|H| = p$ und diese ist insbesondere ein Normalteiler.
H ist zyklisch, also gibt es ein $\pi \in H$ mit $H = \langle\pi\rangle$ und aus der Zykelzerlegung für π und wegen $\mathrm{ord}\,(\pi) = p$ folgt, dass π ein p-Zykel ist.
Ohne Einschränkung sei $\pi = (0,1,\ldots,p-1)$. Wir schreiben jetzt $S_p = \mathrm{Aut}\,(\{0,\ldots,p-1\})$. Hat $\sigma \in G$ zwei verschiedene Fixpunkte, so ist ohne Einschränkung 0 einer von diesen. Dann ist i mit $0 < i < p$ ein weiterer und weil H ein Normalteiler ist, gilt:

$$\sigma \circ \pi \circ \sigma^{-1} = (\sigma\,(0),\ldots,\sigma\,(p-1)) \in H$$

Weil H zyklisch ist, gibt es zudem ein $0 \leq r < p$ mit

$$\sigma \circ \pi \circ \sigma^{-1} = \pi^r$$

also:

$$(\sigma(0), \ldots, \sigma(p-1)) = \left(0, \overline{r \cdot 1}, \ldots, \overline{r \cdot (p-1)}\right)$$

Es folgt unmittelbar:

$$\sigma(0) = 0 \qquad\qquad \sigma(i) = \overline{r \cdot i}$$

Aber i ist ein Fixpunkt, also $\sigma(i) = i$ und wegen $i, r < p$ folgt damit schon $r = 1$, also $\sigma = \mathrm{id}$. $\square_{15.3.6}$

15.3.7 Satz

Sei k ein Körper und $f \in k[X]$ ein irreduzibles Polynom vom Primzahlgrad p. Die zugehörige Galoisgruppe $\mathrm{Gal}(f)$ sei auflösbar.
Ist dann L ein Zerfällungskörper von f über k und sind $\alpha, \beta \in L$ zwei verschiedene Nullstellen von f, so gilt $L = K(\alpha, \beta)$.

Beweis

L/K ist galoissch, denn wegen $\mathrm{char}(k) = 0$ sind alle irreduziblen Polynome separabel.

$$G := \mathrm{Gal}\left(L/K\right)$$

Seien $\alpha_1, \ldots, \alpha_p$ die Nullstellen von f in L. Betrachte die Abbildung.

$$G \hookrightarrow \mathrm{Aut}(\{\alpha_1, \ldots, \alpha_p\}) \cong S_p$$

Da f irreduzibel ist, operiert G transitiv auf $\{\alpha_1, \ldots, \alpha_p\}$.
Weil G auflösbar ist, gilt für alle $\sigma \in G$ schon $\sigma|_{K(\alpha,\beta)} = \mathrm{id}|_{K(\alpha,\beta)}$.
Also ist

$$\mathrm{Gal}\left(L/K(\alpha,\beta)\right) = \{e\}$$

und daher $K(\alpha, \beta) = L$ nach dem Hauptsatz. $\square_{15.3.7}$

15.3.8 Beispiel

Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom und $\deg(f) = p \geq 5$ eine Primzahl.
f besitze mindestens zwei reelle sowie eine nicht-reelle Nullstelle in $\mathbb{C}$.
Angenommen der Zerfällungskörper L von f wäre auflösbar, dann würde nach 15.3.7 schon folgen, dass L aus K durch die Adjunktion der beiden reellen Nullstellen entsteht, also reell ist. Dies ist ein Widerspruch dazu, dass es eine nicht-reelle Nullstelle von f gibt.
Betrachte zum Beispiel für eine Primzahl $p \geq 5$ das Polynom:

$$X^p - 4X + 2 \in \mathbb{Q}[X]$$

Dieses ist Eisenstein bezüglich 2 und somit irreduzibel.
f ist also separabel, da $\mathbb{Q}$ vollkommen ist, das heißt f hat nur einfache Nullstellen.

Behauptung: f hat genau 3 reelle Nullstellen.

Beweis: Die Ableitung ist:

$$f'(X) = pX^{p-1} - 4$$

Nach dem Zwischenwertsatz gibt es ein $t \in \mathbb{R}$ mit $f'(t) = 0$, denn $f'(0) = -4 < 0$ und $f' \overset{X\to\infty}{\longrightarrow} \infty$. Dies ist äquivalent zu

$$t^{p-1} = \frac{4}{p}$$

und dies wiederum zu:

$$t = \pm \sqrt[p-1]{\frac{4}{p}}$$

Also hat f höchstens 3 verschiedene reelle Nullstellen. $\square_{\text{Behauptung}}$
TODO: Wieso folgt „genau“ 3?

Also ist die Galoisgruppe eines Zerfällungskörpers von f nicht auflösbar.

15.4 Gleichungen vom Grad 3 und 4

Seien k ein Körper, $f \in K[X]$ normiert ${}^{L}\!/_{K}$ ein Zerfällungskörper von f und $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f, also:

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

15.4.1 Proposition und Definition (Diskriminante)

i) Der Ausdruck

$$\Delta(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \in K$$

heißt die *Diskriminante von* f.

ii) Für

$$\delta(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \in L$$

gilt:

a) $\sigma(\delta(f)) = \operatorname{sgn}(\sigma) \cdot \delta(f)$ (Benutze hierbei $\operatorname{Gal}\left({}^{L}\!/_{K}\right) \hookrightarrow S_n$.)

b) $\operatorname{Gal}\left({}^{L}\!/_{K}\right) \subseteq A_n \Rightarrow \delta(f) \in K$
Die Umkehrung gilt, falls f separabel ist.

c) Ist f separabel, so ist $K(\delta(f))$ der Fixkörper von $\operatorname{Gal}\left({}^{L}\!/_{K}\right) \cap A_n$.

Beweis

i) ${}^{L}\!/_{K}$ ist galoissch und $\Delta(f)$ ist invariant unter $\operatorname{Gal}\left({}^{L}\!/_{K}\right)$. Also ist $\Delta(f) \in K$. $\square_{\text{i)}}$

ii) a) Dies ist klar nach der Definition von sgn und $\delta(f)$.

b) Diese Aussage folgt direkt aus a).

c) Dies ist klar, falls $\mathrm{Gal}\left(L/K\right) \subseteq A_n$ ist, denn dann ist $\delta(f) \in K$ und somit:

$$K(\delta(f)) = K = L^{\mathrm{Gal}(L/K)}$$

Ist $\mathrm{Gal}\left(L/K\right) \not\subseteq A_n$, so gilt:

$$\left[\mathrm{Gal}\left(L/K\right) : \mathrm{Gal}\left(L/K\right) \cap A_n\right] = 2$$

Aber es gilt:

$$[K(\delta(f)) : K] = 2$$

Damit folgt die Behauptung aus dem Hauptsatz, denn $K(\delta(f)) \subseteq L^{\mathrm{Gal}(L/K)\cap A_n}$, da für jedes Element $\sigma \in A_n$ gilt:

$$\sigma(\delta(f)) = \mathrm{sgn}(\sigma) \cdot \delta(f) \overset{\sigma \in A_n}{=} \delta(f)$$

$\square_{15.4.1}$

15.4.2 Proposition

Für $f = X^3 + pX + q \in k[X]$ gilt:

$$\Delta(f) = -27q^2 - 4p^3$$

Siehe 11.3.

Beweis

Seien L ein Zerfällungskörper von f und $\alpha_1,\alpha_2,\alpha_3 \in L$ die Nullstellen von f, also:

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

Für alle i,j,k mit $\{i,j,k\} = \{1,2,3\}$ kann einerseits die Produktregel anwenden und andererseits das Polynom direkt ableiten und erhält:

$$(\alpha_i - \alpha_j)(\alpha_i - \alpha_k) = f'(\alpha_i) = 3\alpha_i^2 + p = \frac{1}{\alpha_i}\left(3\alpha_i^3 + p\alpha_i\right) =$$
$$\overset{\alpha_i^3 = -p\alpha_i - q}{=} -\frac{1}{\alpha_i}(-3p\alpha_i - 3q + p\alpha_i) = \frac{2p}{\alpha_i}\left(-\frac{3q}{2p} - \alpha_i\right)$$

Also:

$$\Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 =$$
$$= (-1)^3 f'(\alpha_1) f'(\alpha_2) f'(\alpha_3) = \frac{-8p^3}{\alpha_1\alpha_2\alpha_3} f\left(\frac{-3q}{2p}\right) =$$
$$\overset{-\alpha_1\alpha_2\alpha_3 = q}{=} \frac{8p^3}{q}\left(-\left(\frac{3q}{2p}\right)^3 - \frac{3}{2}q + q\right) = -27q^2 - 4p^3$$

$\square_{15.4.2}$

15.4.3 Lösungsformel für allgemeine Polynome 3. Grades

Betrachte:

$$g = X^3 + t_1 X^2 + t_2 X + t_3 \in E[X]$$

Dabei ist $E = k(t_1, \ldots, t_3)$ und t_i Unbestimmte.
Sei L ein Zerfällungskörper und $\beta_1, \beta_2, \beta_3 \in L$ die Nullstellen von g, also $L = (\beta_1, \beta_2, \beta_3)$ und:

$$g = (X - \beta_1)(X - \beta_2)(X - \beta_3)$$

Betrachte das Polynom

$$f(X) = g\left(X - \frac{t_1}{3}\right) = X^3 + pX + q \in E[X]$$

mit:

$$p = t_2 - \frac{t_1^2}{3}$$
$$q = \frac{2t_1^3}{27} - \frac{t_1 t_2}{3} + t_3$$

Dann sind $\alpha_i = \beta_i + \frac{t_1}{3}$ sind die Nullstellen von f. Die Diskrimante von f ist:

$$\Delta(f) = -27q^2 - 4p^3$$

K enthalte eine primitive 3. Einheitswurzel ζ und es sei:

$$\sigma = (123) \in A_3 \subseteq S_3 = \mathrm{Gal}\left(L/K\right)$$

Definiere:

$$a := \alpha_1 + 3\sigma(\alpha_1) + \zeta^2$$

Es gilt:

$$\sigma^2(\alpha_1) = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 \neq 0$$

TODO: Wieso gilt das?
Denn die α_i sind linear unabhängig über K.
Sei $\tau = (23)$, so gilt:

$$b = \tau(a) = \alpha_1 + \zeta\alpha_3 + \zeta^2\alpha_2 \neq 0$$

$$\sigma(a) = \zeta^{-1}a \qquad \sigma(b) = \zeta^2 b$$

TODO: Wieso gilt das?
Es folgt:

$$a^3, b^3 \in F := L^{A_3}$$

TODO: Wieso gilt das?
Wegen $\alpha_1 + \alpha_2 + \alpha_3 = 0$ und $1 + \zeta + \zeta^2 = 0$ gilt $a + b = 2\alpha_1 - \zeta\alpha_1 - \zeta^2\alpha_1 = 3\alpha_1$.
Analog folgt $\zeta^2 a + \zeta b = 3\alpha_2$ und $\zeta a + \zeta^2 b = 3\alpha_3$.
Also genügt es, um α_1, α_2 und α_3 zu bestimmen, a und b zu bestimmen.

Wegen $\tau(a) = b$, $\tau^2 = \mathrm{id}$ und $S_3 = \langle \sigma, \tau \rangle$ sind a^3 und b^3 Wurzeln des Polynoms:

$$h(X) := \left(X - a^3\right)\left(X - b^3\right) = X^2 - \left(a^3 + b^3\right)X + a^3b^3 \in E[X]$$

Nun gilt:

$$\begin{aligned} ab &= \left(\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3\right) \cdot \left(\alpha_1 + \zeta\alpha_3 + \zeta^2\alpha_2\right) = \\ &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \left(\zeta + \zeta^2\right)\left(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1\right) = \\ &= \left(\alpha_1 + \alpha_2 + \alpha_3\right)^2 - \zeta\left(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1\right) = -3p \end{aligned}$$

Die Wurzeln von $X^3 + 1$ sind $-1, -\zeta, -\zeta^2$ also $X^3 + 1 = (X+1)(X+\zeta)\left(X+\zeta^2\right)$.
Die Wahl $X = \dfrac{a}{b}$ und Multiplikation mit b^3 liefert:

$$a^3 + b^3 = (a+b)(a+\zeta b)\left(a+\zeta^2 b\right) = \zeta\alpha_1\zeta\alpha_2\zeta\alpha_3 = -27q$$

Also ist

$$h = X^2 + 27qX - 27p^3$$

und damit:

$$a^3, b^3 = -\frac{27}{2} \pm \sqrt{\left(\frac{27}{2}\right)^2 q^2 + 27p^3}$$

Aus dieser Gleichung und aus

$$\begin{aligned} a + b &= 3\alpha_1 \\ \zeta^2 a + \zeta b &= 3\alpha_2 \\ \zeta a + \zeta^2 b &= 3\alpha_3 \end{aligned}$$

ergeben sich die Lösungsformeln:

$$\left(\frac{a}{3}\right)^3, \left(\frac{b}{3}\right)^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

$\square_{15.4.3}$

15.4.4 **Satz** (Cardano)

Seien

$$u, v = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

wobei die 3. Wurzeln so gewählt sind, dass $u \cdot v = -\dfrac{p}{3}$ gilt.
Dann sind die Lösungen der Gleichung

$$X^3 + pX + q \in K[X]$$

gegeben durch:

$$\begin{aligned} \alpha_1 &= u + v \\ \alpha_2 &= \zeta^2 u + \zeta v \\ \alpha_3 &= \zeta u + \zeta^2 v \end{aligned}$$

Beweis

Dies wurde in 15.4.3 gezeigt. $\square_{15.4.4}$

15.4.5 Lösungsformel für allgemeine Polynome 4. Grades

Betrachte die allgemeine Gleichung 4. Grades:

$$g(X) = X^4 + t_1X^3 + t_2X^2 + t_3X + t_4 \in E[X]$$

$$E := K(t_1,t_2,t_3,t_4)$$

Betrachte

$$f(X) := g\left(X - \frac{t_1}{4}\right) = X^4 + pX^2 + qX + r$$

mit:

$$p =$$
$$q =$$
$$r =$$

TODO: p,q,r angeben.

Seien L/E ein Zerfällungskörper von f und $\alpha_1,\ldots,\alpha_4$ die Nullstellen von f in L. Es gilt:

$$L = K(\alpha_1,\ldots,\alpha_4)$$
$$\mathrm{Gal}\left(L/E\right) \cong S_4$$

Betrachte $1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ und die zugehörige Körperkette sei $E = L_0 \subseteq L_1 \subseteq L_2 \subseteq L_3 = L$ und die Elemente:

$$z_1 := (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$z_2 := (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$z_3 := (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

Diese Elemente bleiben fest unter V_4, und liegen daher in $L_2 = E^{V_4}$.
Außerdem bleiben z_1,z_2,z_3 bei keinem weiteren Elemente aus $S_4 \setminus V_4$ sämtlich fixiert.
Also folgt:

$$L_2 = L_0(z_1,z_2,z_3)$$

Das Polynom

$$h := (X - z_1)(X - z_2)(X - z_3)$$

ist symmetrisch in $\alpha_1,\ldots,\alpha_4$. Also ist $h \in L_0[X]$.
Eine längere Rechnung liefert:

$$\begin{aligned} h(X) &= X^3 - (-z_1 - z_2 - z_3)X^2 + (z_1z_2 + z_2z_3 + z_3z_1)X - z_1z_2z_3 = \\ &= X^3 - 2 \cdot \sum_{1 \le i \le j \le 4} \alpha_i\alpha_j X^2 + \ldots = \\ &= X^3 - 2pX^2 + \left(p^2 - 4r\right)X + q^2 \end{aligned}$$

Dies ist ein Polynom dritten Grades, weswegen man z_1,z_2,z_3 mit Hilfe der Cardanoschen Formel bestimmen kann.
V_4 hat die nicht-trivialen Untergruppen $\langle (12)(34)\rangle, \langle (13)(24)\rangle, \langle (14)(23)\rangle$. Die dazugehörige Zwischenkörper werden über L_2 erzeugt $u_1 = \alpha_1 + \alpha_2$, $u_2 = \alpha_1 + \alpha_3$ und $u_3 = \alpha_1 + \alpha_4$.
Wegen $\sum_i \alpha_i = 0$ gilt:

$$\begin{aligned} u_1^2 &= (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_2) = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -z_1 \\ u_2^2 &= -z_2 \\ u_3^2 &= -z_3 \end{aligned}$$

Außerdem folgt aus diesem linearen Gleichungssystem:

$$\begin{aligned} \alpha_1 &= \frac{1}{2}(u_1 + u_2 + u_3) \\ \alpha_2 &= \frac{1}{2}(u_1 - u_2 - u_3) \\ \alpha_3 &= \frac{1}{2}(-u_1 - u_2 + u_3) \end{aligned}$$

Dabei sind die Wurzeln u_1,u_2,u_3 so zu wählen, dass $u_1u_2u_3 = -q$ ist, denn:

$$\begin{aligned} u_1u_2u_3 &= (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4) = \\ &= \underbrace{\alpha_1^3 + \alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_1^2\alpha_4}_{=0} + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3 + \alpha_2\alpha_3\alpha_4 = -q \end{aligned}$$

Dies liefert Lösungen von f.

15.5 Positive Charakteristik (Ausblick)

Hier lassen wir die Voraussetzung $\operatorname{char}(K) = 0$ fallen.

15.5.1 Proposition und Definition (Spur)

Seien ${}^{L}\!/_{K}$ eine endliche Galoiserweiterung und $a \in L$.
Dann heißt

$$\operatorname{Sp}_{{}^{L}\!/_{K}}(a) := \sum_{\sigma \in \operatorname{Gal}({}^{L}\!/_{K})} \sigma(a) \in K$$

die *Spur* von a bezüglich ${}^{L}\!/_{K}$.

$$\operatorname{Sp}_{{}^{L}\!/_{K}} : L \to K$$

ist ein Homomorphismus abelscher Gruppen.
TODO: L und K sind Körper und keine Gruppen!?

Beweis

Sei $\tau \in \operatorname{Gal}\left({}^{L}\!/_{K}\right)$, so gilt:

$$\tau\left(\sum_{\sigma \in \operatorname{Gal}({}^{L}\!/_{K})} \sigma(a)\right) = \sum_{\sigma \in \operatorname{Gal}({}^{L}\!/_{K})} (\tau \circ \sigma)(a) = \operatorname{Sp}_{{}^{L}\!/_{K}}(a)$$

Also ist $\operatorname{Sp}_{{}^{L}\!/_{K}} \in K$.
Dass $\operatorname{Sp}_{{}^{L}\!/_{K}}$ ein Homomorphismus ist, kann man direkt an der Definition ablesen. $\square_{15.5.1}$

15.5.2 **Satz** (Hilbert 90-Analogon für Spur)

Sei L/K eine endliche zyklische Galoiserweiterung und $\sigma \in \mathrm{Gal}\left(L/K\right)$ ein Erzeuger.
Für $b \in L$ ist dann äquivalent:

i) $\mathrm{Sp}_{L/K}(b) = 0$

ii) Es gibt ein $a \in L$ mit $b = a - \sigma(a)$.

Beweis

Ähnlich wie der Beweis von 15.2.2. $\square_{15.5.2}$

15.5.3 **Satz** (Artin-Schreier)

Es sei L/K eine Körpererweiterung und $\mathrm{char}(K) = p > 0$.

i) Ist L/K eine zyklische Galoiserweiterung vom Grad p, so gilt

$$L = K(a)$$

für ein $a \in L$, dessen Minimalpolynom über K von der Form $X^p - X - c \in K[X]$ mit $c \in K$ ist.

ii) Gilt umgekehrt $L = K(a)$ für ein $a \in L$, das Nullstelle eines Polynoms der Form $X^p - X - c \in K[X]$ ist, so ist L/K eine zyklische Galoiserweiterung.
Es zerfällt $X^p - X - c$ über K entweder vollständig in Linearfaktoren, oder aber dieses Polynom ist irreduzibel. In letzteren Fall ist L/K eine zyklische Galoiserweiterung vom Grad p.

Beweis

i) Für $c \in K$ gilt:

$$\mathrm{Sp}_{L/K}(c) = \sum_{\sigma \in \mathrm{Gal}(L/K)} c = pc = 0$$

Insbesondere ist $\mathrm{Sp}_{L/K}(1) = 0$.
Aus 15.5.2 folgt, dass es ein $a \in L$ mit

$$\sigma(a) - a = 1$$

wobei $\sigma \in \mathrm{Gal}\left(L/K\right)$ ein Erzeuger ist.
Also folgt:

$$\sigma^i(a) = a + i$$

für $i \in \{0, \ldots, p-1\}$.
$\sigma^0(a), \ldots, \sigma^{p-1}(a)$ sind paarweise verschieden, weswegen gilt:

$$[K(a) : K] \geq p$$

Daher ist $L = K(a)$.
Weiter gilt

$$\sigma(a^p - a) = \sigma(a)^p - \sigma(a) = (a+1)^p - (a+1) = a^p - a$$

und damit:

$$c := a^p - a \in K$$

Daher ist a eine Nullstelle des Polynoms:

$$X^p - X - c \in K[X]$$

Da dieses Polynom Grad p hat, muss es aus Gradgründen schon das Minimalpolynom von a sein. $\square_{\text{i)}}$

ii) Ist $L = K(a)$ und a eine Nullstelle von $f = X^p - X - c \in K[X]$.

Dann sind $(a+1), (a+2), \ldots, (a+(p-1)) \in L$ ebenfalls Nullstellen von f und diese sind paarweise verschieden, also sind es alle Nullstellen von f.

Hat f eine Nullstelle in K, so liegen daher alle Nullstellen in K.

L ist ein Zerfällungskörper des separablen Polynoms f, denn für die Ableitung gilt:

$$f'(X) = pX^{p-1} - 1 = -1 \neq 0$$

Also ist L/K galoissch.

Falls $L = K$ ist, so ist diese Erweiterung auch zyklisch.

Habe f keine Nullstelle in K, so gilt:

Behauptung: f ist irreduzibel.

Beweis: Wäre $f = gh \in K[X]$ und g,$h \in K[X]$ nicht-konstante, normierte Polynome.
Es gilt:

$$f = \prod_{i=0}^{p-1} \underbrace{(X - a - i)}_{\in L[X]}$$

Sei $d := \deg(g)$. Der Koeffizient von X^{d-1} in g ist von der Form:

$$-da + j \in K$$

mit $j \in \mathbb{F}_p$. Aus $p \not| d$ folgt $a \in K$, was ein Widerspruch ist. $\square_{\text{Behauptung}}$

Wähle ein $\sigma \in \text{Gal}\left(L/K\right)$ mit $\sigma(a) = a + 1$. Dann ist $\text{ord}(\sigma) \geq p$. Also ist L/K zyklisch vom Grad p.

$\square_{15.5.3}$

Mit Hilfe von 15.5.3 lässt sich die Theorie von auflösbaren und durch Radikale auflösbaren Erweiterungen auf beliebige Charakteristik ausdehnen.

Es gilt dann wieder, dass auflösbar äquivalent zu durch Radikale auflösbar ist.

Für durch Radikale aufläsbar nimmt man Erweiterungen von der Form $K(a)/K$, wobei $\text{Mipo}_K(a) = X^p - X - c \in K[X]$ ist, hinzu.

Anhang

Danksagungen

Mein besonderer Dank geht an Professor Naumann, der diese Vorlesung hielt und es mir gestattete, diese Vorlesungsmitschrift zu veröffentlichen.

Außerdem möchte ich mich ganz herzlich bei allen bedanken, die durch aufmerksames Lesen Fehler gefunden und mir diese mitgeteilt haben.

Andreas Völklein

GNU Free Documentation License

0. Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. Applicability and definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain

any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "**publisher**" means any person or entity that distributes copies of the Document to the public.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. Verbatim copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. Copying in quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. Combining documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. Collections of documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. Aggregation with independent works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. Future revisions of this license

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `https://www.gnu.org/copyleft/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. Relicensing

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

Addendum: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation;

> with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
>
> A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.