Algebra

gelesen von
Prof. Dr. Niko Naumann
im Wintersemester 2011/12
mitgeschrieben und überarbeitet von
Andreas Völklein

Stand: 24. Dezember 2011

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 Linearer Algebra I wird vorausgesetzt:

- Gruppen,
- die Permutationsgruppe $\Sigma(X)$ (für eine Menge X) und
- Untergruppen (Abkürzung: UG).

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

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

1.2 Beispiel

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

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

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

Beweis

ii)

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

i)

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

$\square_{1.2}$

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:

$$\varphi \text{ Mono} \Leftrightarrow \ker(\varphi) = \{e\}$$

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

Beweis

Übung

$\square_{1.3}$

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

Lineare Algebra I

$\square_{1.4}$

1.5 Beispiel und Definition (Automorphismengruppe, Konjugation)

Sei G eine Gruppe. Dann ist $\text{Aut}(G) := \{\varphi | \varphi : G \to G \text{ Automorphismus}\}$ eine Gruppe bezüglich der Komposition $\circ$ mit dem neutralem Element id_G (Nebenbemerkung: im Allgemeinen ist $\text{Aut}(G) \lneqq \Sigma(G)$ eine echte Untergruppe) und heißt die *Automorphismengruppe von* G.
Die Abbildung $\phi : G \to \text{Aut}(G)$, 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 $\phi(g) \in \text{Aut}(G)$, denn:

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

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

  $\Rightarrow\ \phi(g)\circ\phi\left(g^{-1}\right) = \mathrm{id}_G$; 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) $G = \dot{\bigcup_{gH\in {}^{G}\!/_{H}}}(gH)$ (disjunkte Vereinigung)

TODO: Grafik einfügen: disjunkte Vereinigung

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

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

$\square_{1.7}$

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:
$$(gg')^{-1} \cdot (g_1g_1') = (g')^{-1} \cdot g^{-1} \cdot g_1 \cdot g_1' = (g')^{-1} \cdot \underbrace{g_1' \cdot (g_1')^{-1}}_{=e} \cdot \underbrace{g^{-1} \cdot g_1}_{=:n \in N, \text{ da } gN = g_1N} \cdot g_1' =$$
$$= \underbrace{(g')^{-1} \cdot g_1'}_{\in N, \text{ da } g'N = g_1'N} \underbrace{(g_1')^{-1} \cdot n \cdot g_1'}_{\in N, \text{ da } N \trianglelefteq G} \in N$$
Also gilt $(gg')N = (g_1g_1')N$.
Ferner gilt:
$$\ker(\pi) = \left\{ g \in G | gN = \pi(g) = e' = eN = N \in {}^{G}\!/_{N} \right\} \overset{??\,\mathrm{i)}}{=} N$$

$\square_{1.13}$

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

Bildchen

TODO: Abb

Beweis

Übung

$\square_{1.15}$

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 Struktursatz 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 $|G| = p$.
Nach der Vorlesung lineare Algebra I folgt $\ker(\varphi) = p\mathbb{Z}$, also $G \cong \mathbb{Z}/p\mathbb{Z}$.

$\square_{1.17}$

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

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

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:

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

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 $\bar{1}$ 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.
TODO: Abb einfügen
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).

$\square_{\text{ii)}}$

1.23 **Definition** (Gruppenordnung)

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 $a^{\varphi(n)} \equiv 1 (\operatorname{mod}) n$.
(Hier ist $\varphi(n)$ die Eulersche φ-Funktion.)

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

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

(vergleiche 1.24)

Beweis

i) Wegen $\mathrm{ggT}(a,n)=1$ 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 $\psi(d) := |\{x \in G | \mathrm{ord}(x) = d\}|$.
Aus 1.25 folgt dann:

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

Seien $d|n$ und es gelte $\psi(d) \neq 0$, das heißt es gibt ein $z \in G$ mit $\mathrm{ord}(z) = d$.
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 $\{x \in G | \mathrm{ord}(x) = d\} \subseteq \langle z \rangle \cong \mathbb{Z}/d\mathbb{Z}$.
Es gilt aber:

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

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:

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

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 $\mathrm{ord}(x) = n$, 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 Abschnitt 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:

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

Damit folgt in A:

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

Wegen $tvw \in S$ folgt aus (2.1) schon $(a, s) \sim (c, u)$.

$\square_{\sim \text{ Äquivrel.}}$

Der Rest bleibt als Übung.

$\square_{2.2}$

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 $\psi = f \circ \varphi$.

TODO: Abbildung Homomorphiesatz

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 $\psi(\mathbb{Z} \setminus \{0\}) \subseteq \mathbb{C}^*$.
TODO: Abb Homomorphiesatz ψ

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.

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

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:

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

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:

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

$\square_{\text{ii)}}$

2.5 Korollar

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

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 $s = 0 \in S$.

$\square_{\text{ii)}}$

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 $A \subseteq A_{\mathfrak{p}} \subseteq A_{(0)} = \text{Quot}(A)$.

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 $\frac{m}{s} := [(m, s)] \in S^{-1}M$ für alle $(m, s) \in M \times S$.
Dann ist $S^{-1}M$ ein $S^{-1}A$-Modul vermöge:

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

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

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

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

Beweis

Analog zu 2.2.

$\square_{2.7}$

2.8 Proposition

Sei

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P \tag{2.2}$$

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

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

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 $x = \frac{n}{s}$, 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: (TODO: Formel überprüfen)

$$t := \prod_i s_i \qquad\qquad t_i := \prod_{j=1}^{i} s_j \in S \tag{2.4}$$

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

Folgt aus 2.8 und 2.9.

$\square_{2.10}$

Beweis von 2.10

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

$\square_{???\text{TODO}???}$

3 Der Satz von Gauß

Fixiere in Abschnitt 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)

TODO: ??? Überprüfen

Für alle $p \in \mathcal{P}$ ist

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

$(a \neq 0)$ die *p-adische Bewertung von* $\frac{a}{b}$ und für alle $a \in R \setminus \{0\}$ ist die *Primfaktorzerlegung*

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

($\varepsilon \in R^*$ geeignet) ein Homomorphismus.

TODO: ? obige Aussage überprüfen! Homomorphismus?

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 $q \in \mathbb{Q}^*$ 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

$$\begin{aligned} \pi : R[X] &\to \left(R/(p)\right)[X] \\ \sum_i a_i X^i &\mapsto \sum_i (a_i \,(\mathrm{mod})\, p) X^i \end{aligned}$$

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

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

$\square_{3.2}$

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. ($Q \subseteq Q^*$;TODO: ???).
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: $\forall_{f,g\in\mathbb{Q}[X]} : \nu_p(fg) = \nu_p(f) + \nu_p(g)$

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 $p \in \mathcal{P}$

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

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.

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)

TODO: (1) ??? oder doch 1?

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

i) $\underset{p \in \mathcal{P}}{\forall} : \nu_p(f) = 0 \Leftrightarrow \operatorname{ggT}(a_0, a_1, \ldots) = 1$; 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:

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

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

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

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

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.

$\square_{\text{ii)}}$

Beispiel

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

Dann gilt:

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

ist nicht primitiv, aber

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

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)⇒ii).
Schreibe $f = a \cdot \tilde{f}$ mit $a \in R, \tilde{f} \in R[X]$ primitiv (vgl. 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

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

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

TODO: Überprüfen???

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 $f \in \text{Quot}(R)[Y] = k(X)[Y]$ 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 Abschnitt 4 (Irreduzibilitätskriterien)

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

4.1 Proposition (Äquivalenz von prim in R und Q)

Sei $0 \neq f \in Q[X]$. Dann sind äquivalent:

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

TODO:

i) **??** ii)

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

$\square_{4.2}$

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

ii) TODO: Rest einfügen

iii)

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

Beweis

$f \in \mathbb{Z}[X]$ ist normiert. Wegen **??**3.5 und $f(\pm 1) = 4,2 \neq 0$ folgt:
(1) f besitzt keinen Linearfaktor in $\mathbb{Q}[X]$.
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:

$$\overline{f} = (X+1)\left(X^3 + X + 1\right) \text{in } \mathbb{F}_2[X] \qquad (*) \tag{4.1}$$

Beide Faktoren sind irreduzibel, da sie keine Nullstellen und Grad ≤ 3 haben. Also ist $(*)$ die Primfaktorzerledung von $\overline{f} \in \mathbb{F}_2[X]$.
Wäre nun $f \in \mathbb{Q}[X]$ reduzibel, so wegen **??**3.8 auch $f \in \mathbb{Z}[X]$, und wegen (1) müsste gelten $f = gh$ in $\mathbb{Z}[X]$ mit $\deg(g) = \deg(h) = 2 \Rightarrow \overline{f} = \overline{g} \cdot \overline{h}$ in $\mathbb{F}_2[X]$ mit $\deg(\overline{g}), \deg\left(\overline{h}\right) \leq 2$; wegen $\deg\left(\overline{f}\right) = 4$, also $\deg(\overline{g}) = \deg\left(\overline{h}\right) = 2$. Wegen (*) besitzt aber $\overline{f} \in \mathbb{F}_2[X]$ bis auf Assoziiertheit genau die Teiler $\left\{1, X+1, X^3+X+1, \overline{f}\right\}$, und keines dieser Polynome besitzt Grad 2. $\lightning$ zu Reduzibilitätsannahme.

$\square_{4.4}$

vii) Seien p eine Primzahl und $F_p(X) := (X^p - 1)/(X-1) = X^p + \ldots + 1 \in \mathbb{Z}[X]$ wie in iii).
Für $r \geq 1$ setze $n := p^r$ und $\zeta_{p^r} := \exp\left(\frac{2\pi \mathbf{i}}{n}\right)$. Ferner:

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

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

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 $F_{p^r}(\zeta_{p^r}) = 0$. Offenbar ist F_{p^r} normiert. Zeige nach analog zu iii), dass $f(X) := F_{p^r}(X+1) \in \mathbb{Z}[X]$ Eisenstein bezüglich p ist.

Mit $F_{p^r}(X)$ ist auch $f(X)$ normiert, und für den konstanten Term gilt: $f(0) = F_{p^r}(1) \overset{(*)}{=} F_p(1) \overset{\text{iii)}}{=} p$

Zeige noch, dass alle weiteren Koeffizienten von f durch p teilbar sind; durch Rechnen in $\mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X]$:

$$f(X) \overset{\text{Def.}}{=} F_{p^r}(X+1) \overset{(*)}{=} F_p\left((X+1)^{p^{r-1}}\right) \overset{!}{\equiv} F_p\left(X^{p^{r-1}} + 1\right) \overset{F_p(X+1) \equiv X^{p-1} \text{(iii))}}{\equiv} X^{\left(p^{r-1}\right)(p-1)}\,(p)$$

$\square_{4.4}$

Bemerkung

Für alle $n, m \geq 1$ gilt:

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

Das heißt $\zeta_n := \exp\left(\frac{2\pi \mathbf{i}}{n}\right) \in \mathbb{C}^*$ hat Ordnung n.
TODO: Abb 1

Beweis

$\zeta_n^m = \exp\left(\frac{2\pi\mathbf{i}}{n} \cdot m\right)$. Nach Analysis erfüllt der surjektive Homomorphismus

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

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

$\square_{4.4}$

TODO: Rest einfügen

4.5 ???

5 (Algebraische) Körpererweiterungen

5.1 Proposition und Definition

i) Sei R ein Integritätsring, dann existiert genau ein $p \in \mathbb{N}_{\geq 0}$ mit $\ker\left(\mathbb{Z} \xrightarrow{\varphi} R\right) = (p)$ (hier φ eindeutiger Ringhomomorphismus); 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 $\exists!$ 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) $\mathbb{Z}/(p) \hookrightarrow R$ Unterring $\Rightarrow \mathbb{Z}/(p)$ Integritätsring $\overset{\text{LA II}}{\Rightarrow} p = 0$ oder $p > 0$ Primzahl.

ii) Ist in i) $R = k$ ein Körper, so erhalte Ringhomomorphismus:
TODO: Abb 2
Es ist klar, dass $Q \subseteq k$ der kleinste Teilkörper ist, und man erhält für

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

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

5.2 Definition und Beispiel

Eine *Körpererweiterung* ist ein Ringhomomorphismus $k \hookrightarrow E$, bei dem k und E Körper sind. Es folgt $\operatorname{char}(k) = \operatorname{char}(E)$, denn $k \hookrightarrow E$ ist injektiv.
TODO: Abb 3

Bemerkung 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

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

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

ii) Die Abbildung $\operatorname{Frob}_k : k \hookrightarrow k, \operatorname{Frob}_k(x) := x^p$ ist ein injektiver Ringhomomorphismus, *der Frobenius von* k.

iii) k endlich $\Rightarrow \operatorname{Frob}_k : k \xrightarrow{\sim} k$ Isomorphismus

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

Beweis

i) bekannt

ii) klar sind $\mathrm{Frob}_k(0) = 0, \mathrm{Frob}_k(1) = 1, \mathrm{Frob}_k(x \cdot y) = \mathrm{Frob}_k(x) \cdot \mathrm{Frob}_k(y)$ und $\mathrm{Frob}_k(x+y) = \mathrm{Frob}_k(x) + \mathrm{Frob}_k(y)$ folgt aus i) für $n = 1$. Damit ist $\mathrm{Frob}_k : k \to k$ ein Ringhomomorphismus, und $\mathrm{Frob}_k(x) = x^p = 0 \overset{k \text{ Körper}}{\Leftrightarrow} x = 0 \Rightarrow \mathrm{Frob}_k$ injektiv.

iii) Jede injektive Selbstabbildung, wie zum Beispiel Frob_k, einer endlichen Menge, wie zum Beispiel k, ist surjektiv.

iv) „$\Leftarrow$“: $\forall_{x \in \mathbb{F}_p} : \mathrm{Frob}_{\mathbb{F}_p}(x) - x = x^p - x = x\left(x^{p-1} - 1\right) = 0$ (klar für $x = 0$ und für $x \in \mathbb{F}_p^*$ gilt $x^{p-1} = 1$ nach **??**1.26, *ii*))

„$\Rightarrow$“: Dann ist nach Voraussetzung $\mathrm{char}(k) = p \overset{??5.1}{\Rightarrow} \mathbb{F}_p \subseteq k$ Primkörper. Für alle $x \in k$ folgt: $0 = \mathrm{Frob}_k(x) - x = X^p - x$ und das Polynom $T^p - T \in \mathbb{F}_p[T]$ hat höchstens p Nullstellen in k; jedes $x \in \mathbb{F}_p \subseteq k$ ist aber eine Nullstelle nach Beweis von „$\Leftarrow$“, also gilt $k \subseteq \mathbb{F}_p$.

$\square_{5.3}$

Proposition und Definition Sei $k \subseteq E$ eine Körpererweiterung. Dann ist E insbesondere eine k-Algebra und insbesondere ein k-Vektorraum.

Ein $\alpha \in E$ heißt *algebraisch über* $k :\Leftrightarrow \exists\, 0 \neq f \in k[X] : f(\alpha) = 0$ in E. (sonst heißt α *transzendent über* k) Falls α algebraisch ist, ist $\mathrm{Mipo}_k(\alpha) \in k[X]$ und ist das eindeutige normierte, irreduzible Polynom in $k[X]$, das α annulliert. Ein Körper K mit $k \subseteq K \subseteq E$ heißt *Zwischenkörper* (der Körpererweiterung $k \subseteq E$)

5.4 Definition

Sei $k \subseteq E$ 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 „E über k“)

5.5 (Grad-)Satz

$k \subseteq K \subseteq E$ eine Körpererweiterung $[E : k] = [E : K] \cdot [K : k]$

TOOD Rest

5.6 Beispiel

Es sind $\mathbb{Q} \subseteq \overline{\mathbb{Q}}^{\mathbb{C}} := \{\alpha \in \mathbb{C} | \alpha \text{ ist algebraisch über } \mathbb{Q}\} \subseteq \mathbb{C}$ Körpererweiterung.

Wegen **??**5.14,d)⇒c) ist $\overline{\mathbb{Q}}^{\mathbb{C}}/\mathbb{Q}$ algebraisch. Nach dem Beweis von **??**5.7, *iv*) gilt $\left[\overline{\mathbb{Q}}^{\mathbb{C}} : \mathbb{Q}\right] = \infty$ (N.B.: $\mathbb{Q}\left[2^{\frac{1}{n}}\right] \subseteq \overline{\mathbb{Q}}^{\mathbb{C}}$)

Also ist wegen (**??**5.14, $b) \Rightarrow a)$) $\overline{\mathbb{Q}}^{\mathbb{C}}/\mathbb{Q}$ nicht endlich erzeugt.

6 Der algebraische Abschluss eines Körpers

6.1 Proposition und Definition

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 $f := \mathrm{Mipo}_k(\alpha)$. Wegen f irreduzibel 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 $g \in k[X]$ irreduzibel:

$$g | f \qquad (*) \tag{6.1}$$

Nach **??**5.7 ist $k \subseteq E := k[X]/(g)$ eine endliche (und damit algebraische) Körpererweiterung, und offenbar ist $\alpha := (X + (g)) \in E$ eine Nullstelle von g. Nach iv) gilt $k = E$, also besitzt g, wegen **??**$(*)$ also auch f, eine Nullstelle in k.

$\square_{6.1}$

6.2 Proposition und Definition

Seien $\mathfrak{X}$ eine Menge und für jede endliche Teilmenge $\mathfrak{X} \supseteq \mathfrak{X}' = \{X_1, \ldots, X_n\}$ sei $k[\mathfrak{X}'] := k[X_1, \ldots, X_n]$. Dann heißt

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

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 (**??**+) ist die Abbildung

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

bijektiv, wobei $\varphi_{\mathfrak{X}'} \in \mathrm{Hom}_{k\text{-Alg.}}(k[\mathfrak{X}], A)$.
Wegen **??**5.11 ist folgende Abbildung bijektiv:

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

Es ist klar, dass die Abbildung

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

bijektiv ist, und man prüft dass die resultierende Bijektion $\mathrm{Hom}_{k\text{-Alg.}}(\mathfrak{X}, A) \xrightarrow{\sim} \mathrm{Abb}(\mathfrak{X}, A)$ wie angegeben ist.

$\square_{6.2}$

6.3 Das Lemma von Zorn

6.3.1 Definition

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

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 *total geordnet* genau dann, wenn $\underset{x,y \in M}{\forall} x \leq y \vee y \leq x$ gilt.

$x \in M$ heißt *maximales Element* genau dann, wenn $\underset{y \in M}{\forall} : x \leq y \Rightarrow x = y$.

Für eine Teilmenge $N \subseteq M$ heißt $x \in M$ *obere Schranke für* N genau dann, wenn $\underset{y \in N}{\forall} y \leq x$.

6.3.2 Beispiel

Seien R ein kommutativer Ring, $M := \{I | I \subsetneq R \text{ Ideal}\}$ und $I \leq J :\Leftrightarrow I \subseteq J$. Dann ist $(M, \leq)$ teilweise geordnet, aber im Allgemeinen nicht total geordnet, zum Beispiel für $R = \mathbb{Z}, (2), (3) \in M$, 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 Teilfolge $N \subseteq M$ besitze eine obere Schranke. Dann besitzt M ein maximales Element.

(ohne Beweis) äquivalent zum Auswahlaxiom

$$\emptyset \neq I \text{ Menge}, \underset{i \in I}{\forall} : \emptyset \neq X_i \Rightarrow \prod_{i \in I} X_i \neq \emptyset$$

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 ($\Rightarrow J \in M$ ist eine obere Schranke für N)

Beweis

1. $x \in J$ und $a \in R \Rightarrow \underset{I \in N}{\exists} : x \in I \Rightarrow \underset{I \subseteq J}{\exists}$
2. $x, y \in J \Rightarrow \exists_{I_1, I_2 \in N} : x \in I_1, y \in I_2$
   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 $I_1 \subseteq I_2 \Rightarrow x, y \in I_2 \Rightarrow x + y \in I_2 \subseteq J$. Also ist $J \subseteq R$ ein Ideal.

Wäre $J = R$, so folgt $1 \in J = \bigcup_{I \in N} I \Rightarrow \exists_{I \in N} 1 \in I \Rightarrow I = R \lightning$ zu $I \in M$, das heißt $I \subsetneq R$.

Damit erfüllt $(M, \leq)$ alle Voraussetzungen von **??**6.3.3 und es folgt:

6.3.5 6.3.4 Satz

$R \neq \{0\}$ kommutativer Ring $\Rightarrow \exists_{\mathfrak{m} \subseteq R \text{ max. Ideal}}$

6.4 Satz und Definition (algebraischer Abschluss)

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

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

Beweis von ??6.4 (E. Artin) Setze $I := \{f \in k[X] \,|\deg(f) \geq 1\}$, $\mathfrak{X} := \{X_f | f \in I\}$, und betrachte das Ideal

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

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

Beweis Sonst gilt $1 \in I \Rightarrow$

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

mit $n \geq 1$, $g_i \in k[\mathfrak{X}]$ und $f_i \in I$ geeignet. Aus **??**5.7, i) induktiv angewand auf alle irreduziblen Teiler von $f_1, \ldots, f_n$ folgt $\underset{k \subseteq K \text{ endl. KE}}{\exists} \underset{\alpha_1,\ldots,\alpha_n \in K}{\exists}$:

$$f_i(\alpha_i) = 0 \underset{1 \leq i \leq n}{\forall} \qquad (2) \tag{6.4}$$

Wegen **??**6.2 existiert ein k-Algebra-Homomorphismus $\phi : k[X] \to k$ mit (**??**3) $\underset{1 \leq i \leq n}{\forall} \phi(X_{f_I}) = \alpha_i$, und es folgt in K:

$$1 = \phi(1) \overset{(??1)}{=} \sum_{i=1}^{n} \phi(g_i) \cdot \underbrace{\phi(f_i(X_{f_i}))}_{= f_i\left(\underbrace{\phi(X_{f_i})}_{=\alpha_i}\right)} \overset{(??2)}{=} 0 \lightning$$

$\square_{6.4}$

Wegen Behauptung ist ${}^{k[\mathfrak{X}]}\!/_{I} \neq \{0\} \overset{??6.3.4}{\Rightarrow}$ es existiert ein maximales Ideal $\mathfrak{m} \subseteq {}^{k[\mathfrak{X}]}\!/_{I}$. Erhalte eine Körpererweiterung $\overline{k} \supseteq k$ als Komposition $k \hookrightarrow k[\mathfrak{X}] \twoheadrightarrow {}^{k[\mathfrak{X}]}\!/_{I} \twoheadrightarrow \underbrace{{}^{k[\mathfrak{X}]}\!/_{I}\!/_{\mathfrak{m}}}_{=:\overline{k}}$.

Zeige noch:

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

ii) $\overline{k}$ ist algebraisch abgeschlossen.

Beweis Die k-Algebra $\overline{k}$ wird durch die Bilder $\alpha_f \in \overline{k}$ der $X_f\,(f \in I)$ erzeugt. Für jedes $f \in I$ gitl wegen $f(X_f) \in I$:
$f(\alpha_f) = 0$ in $\overline{k}$, das heißt nach Definition von I: Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ besitzt Nullstelle in k.
Damit folgt ii) aus **??**$6.1, i)$. (Nicht ganz!!!TODO:später mehr)
Teil i) folgt aus **??**$5.14, d) \Rightarrow e)$.

6.5 Notation und Bemerkung

Sei $z : K \to L$ ein Körperhomomorphismus. Schreibe für alle $f = \sum a_i X^i \in k[X] : f^\sigma := \sum \sigma(a_i) X^i \in L[X]$.
Dann gilt $\forall_{\alpha \in k} \sigma(f(\alpha)) = \sigma\left(\sum a_i \alpha^i\right) = \sum \sigma(a_i) \cdot \sigma(\alpha)^i = f^\sigma(\sigma(\alpha))$. Insbesondere:

$$\underset{\alpha \in k}{\forall} f(\alpha) = 0 \Rightarrow f^\sigma(\sigma(\alpha)) = 0$$

TODO: Rest

6.6 Lemma

7 Zerfällungskörper

Definition (k-Homomorphismus)

k-Homomorphismus (=: „k-Homomorphismus“) :$\Leftrightarrow$ k-Algebra-Homomorphismus ($\neq$ k-lineare Abbildung)
Fixiere: k Körper, $\emptyset \neq \mathcal{F} \subseteq \{f \in k[X] \,|\deg(f) \geq 1\}$

7.1 Definition (Zerfällungskörper)

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

i) $\underset{f\in\mathcal{F}}{\forall}$ gilt in $E[X]$: $f = \alpha \cdot \prod_{i=1}^{n} (X - \alpha_i)$ mit $n \geq 1$, $\alpha, \alpha_i \in E$ geeignet, das heißt: f zerfällt über E in Linearfaktoren.

ii) $E = k\left(\alpha | \alpha \in E \wedge \underset{f\in\mathcal{F}}{\exists} f(\alpha) = 0\right)$, 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 **??**5.7, i)).
Dann hat f eine Nullstelle in E (nämlich α), und in $E[X]$ gilt:

$$f = (X - \alpha) \cdot \left(X^2 + \alpha X + \alpha^2\right) \qquad (*) \tag{7.1}$$

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

$\overset{\text{??}4.5,iii)}{\Rightarrow}$

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

Wegen $\zeta \in E$ erhalte Körperturm erhalte 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

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

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

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 $\overline{\sigma} : \left(E_1 \xrightarrow{\sim} E_2 \hookrightarrow\right)$.

iii) $E_i \supseteq k$ ist ein Zerfällungskörper von $\mathcal{F}$ $(i = 1, 2) \Rightarrow \underset{k\text{-Iso.}}{\exists} \phi : E_1 \xrightarrow{\sim} E_2$.

Beweis

i) Wähle einen algebraischen Abschluss $\overline{k} \supseteq k$ (**??**?6.4) und setze $E := k\left(\alpha | \alpha \in \overline{k} \wedge \underset{f \in \mathcal{F}}{\exists} f(\alpha) = 0\right)$. Wegen **??**6.1 ii) 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 $\mathcal{N}_i := \left\{\alpha \in E_i \,\middle|\, \underset{f \in \mathcal{F}}{\exists} f(\alpha) = 0\right\}$ 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 $\overline{\sigma}$ ($= \sigma$ in **??**6.7) wie in ii). (N.B.: ${}^{E}\!/_k$ Zerfällungskörper $\Rightarrow {}^{E}\!/_k$ algebraisch)

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 $\overline{\sigma}\left(\overline{E}\right) = E$.

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

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

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

In diesem Fall heißt ${}^{E}\!/_k$ *normal*.

Beweis von 7.4

- i) $\Rightarrow$ iii): Da f über $\overline{E}$ in Linearfaktoren zerfällt, zeige nur: $\beta \in \overline{E}, f(\beta) = 0 \Rightarrow \beta \in E$.
  Wegen f irreduzibel und ohne Einschränkung normiert ist $f = \mathrm{Mipo}_k(\alpha) = \mathrm{Mipo}_k(\beta) \overset{??5.7\ \mathrm{i})}{\Rightarrow} \exists_{k\text{-Iso}}\, \varphi : k(\alpha) \xrightarrow{\sim} k(\beta), \varphi(\alpha) = \beta$.
  Betrachte $k(\alpha) \xrightarrow{\sim} k(\beta) \subseteq E$ TODO: Abb1
  Es folgt $\beta = \varphi(\alpha) \overset{(*)}{=} \sigma(\alpha) \in \sigma(E) \overset{\mathrm{i})}{=} E$.

$\square_{7.4}$

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

  1. $f \in \mathcal{F} \overset{\mathrm{Def.}}{\Rightarrow} \exists_{\alpha \in E} f(\alpha) = 0 \overset{\mathrm{iii})}{\Rightarrow} f$ zerfällt in Linearfaktoren über E.
  2. Wegen $E/_k$ algebraisch gilt: $\forall_{\alpha \in E}$ ist $f := \mathrm{Mipo}_k(\alpha) \in \mathcal{F}$ und $f(\alpha) = 0$. Also wird $E/_k$ von allen Nullstellen aller $f \in \mathcal{F}$ erzeugt.

- 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))

$\square_{7.4}$

7.5 Beispiel

Wegen 7.2 und 7.4 iii) ist die algebraische Körpererweiterung $E := \mathbb{Q}\left(2^{\frac{1}{3}}\right)/_k := \mathbb{Q}$ 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 $k \subseteq E = \overline{E}$ eine algebraische Körpererweiterung mit E algebraisch abgeschlossen(, 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 $E/_K$). ($k \subseteq E \subseteq \overline{k}$!)

Beweis

i) Prüfe 7.4 iii): Sei $f \in k[X]$ irreduzibel mit $\exists_{\alpha \in E} : f(\alpha) = 0$.
$\overset{[E:k]=2}{\Rightarrow} \deg(f) = [k(\alpha) : k] \overset{k \subseteq k(\alpha) \subseteq E}{\in} \{1, 2\}$. Der Fall $\deg(f) = 1$ ist trivial. Sei $\deg(f) = 2$ und ohne Einschränkung f normiert:

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

$$\Rightarrow \text{in } E[X]: f(X) = (X-\alpha)\left(X - \underbrace{(-\alpha + a)}_{\in E}\right)$$

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

ii) Klar nach 7.4 ii).

$\square_{\text{ii)}}$

7.8 **Beispiel** („normal ist nicht-transitiv“)

In dem Körperturm $k := \mathbb{Q} \overset{2}{\subseteq} K := \mathbb{Q}\left[\sqrt{2}\right] \overset{2}{\subseteq} E := \mathbb{Q}\left(\sqrt{[4]2}\right)$. ($K \subseteq E$, da $(\left(\sqrt{[4]2}\right)^2)^2 = 2$, also $\left(\sqrt{[4]2}\right)^2 = \sqrt{2}$) sind beide Erweiterungen vom Grad 2(=: *quadratisch*), insbesondere normal, aber $E/_k$ ist nicht normal. (vergleiche mit **??**5.15)

Beweis $X^2 - 2, X^4 - 2 \in \mathbb{Q}[X]$ sind irreduzibel, da Eisenstein bezüglich 2, und aus der Gradformel 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 von $i: \mathbb{Q}\left[\sqrt{[4]2}\right] \hookrightarrow \mathbb{R}, \sqrt{[4]2} \to \alpha$ und $j: \mathbb{Q}\left[\sqrt{[4]2}\right] \hookrightarrow \mathbb{C}, \sqrt{[4]2} \to \beta$. 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 normale Hülle $E'/_k$ von $E/_k$, eindeutig bis auf Isomorphie.

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

iii) Ist $k \subseteq E \subseteq L$ ein Körperturm mit $L/_k$ normal (zum Beispiel $L = \overline{k}$,7.6), so ist $E' = k(\sigma(E) \,|\, \sigma: E \to L$ ist k-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 $\mathcal{F} := \{f \in k[X] \,|\, \deg(f) \geq 1 \text{ und } \exists_{\alpha \in E} f(\alpha) = 0\}$ über k leistet das Gewünschte. (vergleiche 7.3)

ii) Dann kann in i) $|\mathcal{F}| < \infty$ gewählt werden und aus **??**5.14, i) b)⇒a) folgt $[E':k] < \infty$.

iii) Übung (mit 6.6).

$\square_{7.10}$

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 ist

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

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:

$$\left(\alpha\zeta^i\right)^3 = \alpha^3 \cdot \left(\zeta^3\right)^i = 2 \cdot 1 = 2 \quad \underset{i \in \mathbb{Z}}{\forall}$$

Und weil $\mathrm{ord}\,(\zeta \in \mathbb{C}^*) = 3$ (Bemerkung zu **??**4.5) sind $\alpha, \alpha\zeta, \alpha\zeta^2 \in \mathbb{C}$ paarweise verschieden, also *alle* Nullstellen von $X^3 - 2$ in $\mathbb{C}$.

TODO: Abb 2

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 $[E' : \mathbb{Q}] = 6$:

TODO: Abb3

8 Separabilität

Sei k ein Körper.

8.1 Definition ((formale) Ableitung)

Die Abbildung $k[X] \to k[X], f = \sum_{i=0} a_i X^i \mapsto f' := \sum_{i=1} i \cdot a_i X^{i-1}$ 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 $f = X^m, g = X^n$ $(n, m \geq 0)$ angenommen werden).

$\square_{8.1}$

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 Übung

$\square_{8.2}$

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 *mehrfache Nullstelle* genau dann, wenn $r \geq 2$ (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:

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

$\square_{8.3}$

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 $0 \neq f \in k[X] \subseteq \overline{k}[X]$ 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)

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 $f'(\alpha) = 0$.
   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)

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

8.6 Proposition

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

Beweis

Wegen $\mathrm{char}(k) = 0$ 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 4.5 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:

$$\mathrm{Hom}_{k\text{-Alg.}}\left(E, \overline{k}\right) \underset{6.6}{\simeq} \left\{\beta \in \overline{k} | \beta^p = t\right\} \overset{??5.3}{=} \{\alpha\}$$

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:

$$1 = \left|\mathrm{Hom}_{k\text{-Alg.}}\left(E, \overline{k}\right)\right| < [k(\alpha) = E : k] = p$$

(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 $\mathrm{Mipo}_k(\alpha)$ in $k[X]$ separabel ist.

ii) E/k heißt *separabel über k*, wenn $\mathrm{Mipo}_k(\alpha)$ in $k[X]$ 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 (Stabilitätsgrad)

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 Stabilitätsgrad von E/k.

8.12 Satz

i) Im Fall $\operatorname{char}(k) = p > 0$ gilt:

$$h \text{ vollkommen} \Leftrightarrow \operatorname{Frob}_k : k \xrightarrow{\sim} k \text{ ist ein Isomorphismus}$$

ii) Jeder endliche Körper ist vollkommen.

Beweis

i) „⇒“: Zeige $\operatorname{Frob}_k : k \twoheadrightarrow k$ ist surjektiv.

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 $g = \operatorname{Mipo}_k(\beta)$: $g | f$

Weil nun h vollkommen ist, ist g separabel, womit folgt $g = X - \beta \in h[X]$, also $\beta \in k$ und $\alpha = \beta^p = \operatorname{Frob}_k(\beta)$.

„⇐“: Sonst existiert ein $f \in k[X]$ irreduzibel und nicht separabel, 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 $k[X]$:

$$f(X) = g(X^p) = \sum a_i (X^p)^i = \sum b_i^p (X^p)^i = \sum \left(b_i X^i\right)^p = \left(\sum b_i X^i\right)^p$$

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 $k \subseteq E = k(\alpha)$ eine einfache algebraische Körpererweiterung.

i) $[k(\alpha) : k]_S = \left|\left\{\beta \in \overline{k} | \operatorname{Mipo}_k(\alpha)(\beta) = 0\right\}\right|$ (Anzahl der Nullstellen des Minimalpolynoms)

ii) α ist genau dann separabel über k, wenn $[k(\alpha) : k] = [k(\alpha) : k]_S$.

Beweis

i) $[k(\alpha) : k]_S \overset{8.11}{=} |\operatorname{Hom}_{k\text{-Alg.}}(k(\alpha), k)| \overset{6.6}{=} \left|\left\{\beta \in \overline{k} | \operatorname{Mipo}_k(\alpha)(\beta) = 0\right\}\right|$

ii) $f := \operatorname{Mipo}_k(\alpha) \in k[X]$ 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, das heißt f separabel ist.

$\square_{8.13}$

8.14 Satz

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 auch $\overline{k}/K$ und $\overline{k}/k$ algebraische Abschlüsse und nach Definition gilt:

$$\begin{aligned}[E:k]_S &= \left|\mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)\right| \\ [E:K]_S &= \left|\mathrm{Hom}_{K\text{-Alg.}}\left(E,\overline{k}\right)\right| \\ [K:k]_S &= \left|\mathrm{Hom}_{k\text{-Alg.}}\left(K,\overline{k}\right)\right|\end{aligned}$$

Für jedes $\sigma \in \mathrm{Hom}_{k\text{-Alg.}}\left(K,\overline{k}\right)$ 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

$$\mathrm{Hom}_{K\text{-Alg.}}\left(E,\overline{k}\right) \times \mathrm{Hom}_{k\text{-Alg.}}\left(K,\overline{k}\right) \to \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right), (\tau,\sigma) \mapsto \overline{\sigma} \circ \tau$$

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 ist $\sigma_i \in \mathrm{Hom}_{k\text{-Alg.}}\left(k,\overline{k}\right)$, $\tau_i \in \mathrm{Hom}_{k\text{-Alg.}}\left(E,\overline{k}\right)$ 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 8.14 und **??**5.5 (Gradsätze) 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, dann gilt:

$$\begin{array}{ccc} [E:k] & \overset{k\subseteq k(\alpha)\subseteq E}{=} & [E:k(\alpha)] \\ \| & & \vee| \\ [E:k]_S & = & [E:k(\alpha)]_S \end{array}$$

$$[k(\alpha):k] \geq [k(\alpha):k]_S$$

Dabei folgen die Ungleichungen aus dem Beweis von 8.13 ii).

Es folgt $[k(\alpha):k]_S = [k(\alpha):k]$, also ist α separabel über k (nach 8.13 iii) „$\Leftarrow$“).

$\square_{8.15}$

8.16 Korollar

Für eine algebraische Körpererweiterung $k \subseteq K \subseteq E$ 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 $\alpha \in E$, $f := \mathrm{Mipo}_K(\alpha) = \sum a_i X^i \in K[X]$ und $K' := k(a_i) \subseteq K$.
Dann folgt:

1. ${}^{K'}\!/_{k}$ ist endlich und separabel (**??**8.15, ii) $\Rightarrow$ i)).
2. $f \in K'[X]$ ist separabel $\Big(\text{da } {}^{E}\!/_{k} \text{ separabel ist}\Big)$.

Es folgt:

$$\infty \overset{1.}{>} [K'(\alpha):k] \overset{(??)5.5}{=} [K'(\alpha):K'] \cdot [K':k] \underset{??8.15,\ \mathrm{i)} \Leftrightarrow \mathrm{ii)}}{\overset{1.,\ 2.}{=}} [K'(\alpha):K']_S \cdot [K':k]_S = \overset{(??8.14)}{=} [K'(\alpha):k]_S$$

Daher ist ${}^{K'(\alpha)}\!/_{k}$ separabel, also α separabel über k.

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 $k := \mathrm{Frob}_E(E) \subseteq\Rightarrow [E:k] = p^2$ und E/k ist nicht einfach (ohne Beweis).

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 $P(X) := \prod_{\substack{1\le i,j\le n \\ i\neq j}} \left(\left(\sigma_i(\alpha_1) - \sigma_j(\alpha_1)\right) + X\left(\sigma_i(\alpha_2) - \sigma_j(\alpha_2)\right)\right) \in \overline{k}[X]$

Behauptung: $P(X) \neq 0$ in $\overline{k}[X]$

Beweis: Sonst existieren $1 \le i,j \le n$, $i \neq j$ mit $\sigma_i(\alpha_k) = \sigma_j(\alpha_k)$, $k \in \{1,2\}$. Damit folgt $\sigma_i = \sigma_j$ im Widerspruch zu $i \neq j$.

$\square_{\text{Behauptung}}$

Wegen $P(X) \neq 0$ und k unendlich 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 $\sigma(\alpha_1), \ldots, \sigma(\alpha_1) \in \overline{k}$ parrweise verschieden sind, denn:

$$0 \neq P(\beta) = \prod_{\substack{1\le i,j\le n \\ i\neq j}} \left(\underbrace{\left(\sigma_i(\alpha_1) - \sigma_j(\alpha_1)\right) + \beta \cdot \left(\sigma_i(\alpha_2) - \sigma_j(\alpha_2)\right)}_{\overset{\beta\in k}{=} (\sigma_i(\alpha) - \sigma_j(\alpha))} \right)$$

Für $k \subseteq E' := k(\alpha) \subseteq E$ folgt:

$$[E':k]_S \ge n = [E:k]_S$$

Da die $\sigma_i|_{E'} \in \mathrm{Hom}_{k\text{-Alg.}}\left(E', \overline{k}\right)$ paarweise verschieden sind.
Wegen $E' \subseteq E$ folgt:

$$[E:k]_S = [E':k]_S \tag{8.5}$$

Behauptung: $E = E'\,(= k(\alpha)$, also folgt die Behauptung von (**??**)8.17)

Beweis: Aus α_2 separabel über k folgt mit (**??**)8.15:

$$\alpha_2 \text{ ist separaber über } E' \tag{8.6}$$

Und damit folgt:

$$[E'(\alpha_2) : E']_S = [E'(\alpha_2) : E']$$

Ferner gilt:

$$[E:k]_S \overset{((??)8.14)}{\ge} [E'(\alpha_2):E']_S \cdot [E':k]_S \overset{(8.5),\,(8.6)}{=} [E'(\alpha_2):E'] \cdot [E:k]_S$$

Daraus folgt $[E'(\alpha_2):E'] = 1$, also $\alpha_2 \in E'$. Wegen $\alpha_1 = \alpha - \beta\alpha_2$ damit auch $\alpha_1 \in E'$ und gesamt:

$$E' \supseteq k(\alpha_1, \alpha_2) = E$$

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) Sonst müssten $\operatorname{char}(k) = 0$ gelten, also $\mathbb{Q} \subseteq k$ im Widerspruch zu $|k| < \infty$. (vergleiche **??**5.1)

ii) $|k| < \infty$, also folgt $n < \infty$ und aus $k \cong \mathbb{F}_p^n$ als $\mathbb{F}_p$-Vektorraum folgt $|k| = p^n$.

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:

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_{p^n} \Leftrightarrow n = 1$$

Beweis von 9.2

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 $\mathbb{F}_{p^n} \big/ \mathbb{F}_p$ normal ist, gilt für jeden $\mathbb{F}_p$-Homomorphismus $i : \mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p : i(\mathbb{F}_{p^n}) = \tilde{\mathbb{F}}_{p^n}$.
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

„$\Rightarrow$“: Schreibe $m = xn$, $x \in \mathbb{N}$ geeignet und sei $\alpha \in \mathbb{F}_{p^n}$, dann folgt:

$$\alpha^{p^n} = \mathrm{Frob}_{\overline{F}_p}^{nx}(\alpha) = \underbrace{\mathrm{Frob}_{\overline{F}_p}^n(\alpha) \circ \ldots \circ \mathrm{Frob}_{\overline{F}_p}^n(\alpha)}_{x\text{-mal}} \overset{\alpha^{p^n}=\alpha}{=} a$$

Also ist $\alpha \in \mathbb{F}_{p^m}$.

„$\Leftarrow$“: Aus $m = [\mathbb{F}_{p^m} : \mathbb{F}_p] \overset{\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}}{=} \underbrace{\left[\overline{\mathbb{F}}_{p^m} : \mathbb{F}_{p^n}\right]}_{\in\mathbb{N}} \cdot \underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{=n}$ folgt $n|m$.

$\square_{9.4}$

9.5 Satz und Definition

Seien p eine Primzahl und $1 \leq n|m$, $q := p^n$, $q' := p^m$, also $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q'} \subseteq \overline{\mathbb{F}}_p$.

i) $F_q := \mathrm{Frob}_{\overline{\mathbb{F}}_p}^n \in \mathrm{Aut}_{\mathbb{F}_q}\left(\overline{\mathbb{F}}_p, \overline{\mathbb{F}}_p\right)$ heißt *der relative Frobenius über F_q*.

ii) Die Gruppe $\mathrm{Aut}_{\mathbb{F}_q\text{-Alg.}}(\mathbb{F}_{q'}, \mathbb{F}_{q'})$ ist zyklisch von Ordnung $\frac{m}{n} = [\mathbb{F}_{q'} : \mathbb{F}_q]$ 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:

$$\left|\mathrm{Aut}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \mathbb{F}_{q'}\right)\right| \overset{(\text{Übung})}{=} \left|\mathrm{Hom}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \mathbb{F}_{q'}\right)\right| \overset{\mathbb{F}_{q'}/\mathbb{F}_q \text{ normal}}{=} \left|\mathrm{Hom}_{\mathbb{F}_q\text{-Alg.}}\left(\mathbb{F}_{q'}, \overline{\mathbb{F}}_p\right)\right| =$$
$$\overset{\text{Def.}}{=} [\mathbb{F}_{q'} : \mathbb{F}_q]_S \overset{??8.12,\ \text{ii)}}{=} [\mathbb{F}_{q'}; \mathbb{F}_q] = \frac{m}{n} =: k$$

Weil $\mathbb{F}_{q'}/\mathbb{F}_q$ normal ist, folgt $\sigma(\mathbb{F}_{q'}) = \mathbb{F}'_q \subseteq \overline{\mathbb{F}}_p$, also $\sigma \in \mathrm{Aut}_{\mathbb{F}_q\text{-Alg.}}(\mathbb{F}_{q'}, \mathbb{F}_{q'})$.
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:

$$\underset{\alpha \in \mathbb{F}_{q'}}{\forall} \alpha = \sigma^a(\alpha) = \alpha^{q^a} = \alpha p^{n \cdot a}$$

Es gilt aber:

$$\left|\left\{\alpha \in \overline{\mathbb{F}}_p | \alpha = \alpha p^{n \cdot a}\right\}\right| \leq p^{na} \overset{a<k}{<} p^{nk} = p^m = (q')^{q'}$$

Dies wird zu $|\mathbb{F}_{q'}| = q'$.

$\square_{9.5}$

TODO: Rest

10 Galoistheorie

10.1 Definition (galoissche Körpererweiterung, 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 ${}^{E}\!/_{k}$.

10.2 Beispiel und Definition

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 kan 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 $[E : k]$
   [TODO: Was bedeutet folgende Zeile?]
   erzeugt von $(\mathbb{F}_q)\Big|_E = \mathrm{Gal}\left({}^{E}\!/_{k}\right)$.

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).

$\square_{\text{ii)}}$

10.3 Proposition

Seien $E \supseteq K \supseteq k$ Körpererweiterungen und ${}^{E}\!/_{k}$ galoissch.
Dann gelten:

i) ${}^{E}\!/_{K}$ ist galoissch und

$$\mathrm{Gal}\left({}^{E}\!/_{K}\right) = \left\{\delta \in \mathrm{Gal}\left({}^{E}\!/_{k}\right) \mid \delta|_K = \mathrm{id}_K\right\} \subseteq \mathrm{Gal}\left({}^{E}\!/_{k}\right)$$

ist eine Untergruppe.

ii) Ist zusätzlich ${}^{K}\!/_{k}$ galoissch, dann ist die Abbildung

$$\begin{aligned} \pi : \mathrm{Gal}\left({}^{E}\!/_{k}\right) &\twoheadrightarrow \mathrm{Gal}\left({}^{K}\!/_{k}\right) \\ \sigma &\mapsto \sigma|_K \end{aligned}$$

wohldefiniert und ein surjektiver Gruppenhomomorphismus mit:

$$\ker(\pi) = \mathrm{Gal}\left({}^{E}\!/_{K}\right) \trianglelefteq \mathrm{Gal}\left({}^{E}\!/_{k}\right)$$

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 heißt

$$\bigvee_{\sigma \in \mathrm{Gal}\left({}^{E}\!/_{k}\right)} : \sigma(K) \subseteq K$$

und daher $\sigma|_K \in \mathrm{Gal}\left({}^{K}\!/_{k}\right)$.
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).

$\square_{\text{ii)}}$

10.4 Proposition

Sei $E \supseteq k$ eine endliche normale Körpererweiterung.
Dann gelten:

i) $|\mathrm{Aut}(E)| = [E : k]_s \leq [E : k]$

ii) $(|\mathrm{Aut}_k(E)| = [E : k]) \Leftrightarrow {}^{E}\!/_{k}$ 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) $k := E^G := \{\alpha \in E | \forall_{B \in G} : \sigma(\alpha) = \alpha\}$ ist ein TK(TODO???) und heißt *der Fixkörper von E unter G.*

ii) Aus $|G| < \infty$ folgt, dass E/k galoissch ist und dass gelten: (TODO: Gleichung überprüfen)

   - Mit $\operatorname{Aut}_k(E)$ definiert als die Gruppe der Automorphismen von E, die auf k die Identiät 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 endlich), so ist E/k galoissch und $G \subseteq \operatorname{Gal}\left(E/k\right)$ ist eine Untergruppe.

10.6 Beispiel

10.7 Korollar

10.8 Bemerkung und Beispiel

10.9 Satz (Hauptsatz der Galoistheorie)

Seien $E \supseteq k$ eine endliche galoissche Körpererweiterung und $G := \operatorname{Gal}\left(E/k\right)$. Dann gelten:

i) Die Abbildung

$$\phi : \{H | H \subseteq G \text{ Untergruppe}\} \rightleftarrows \{K | k \subseteq K \subseteq E \text{ Zwischenkörper}\} : \psi$$

$$\phi(H) := E^H \qquad\qquad \psi(K) := \operatorname{Gal}\left(E/k\right) \subseteq G$$

   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

$$\begin{aligned} \operatorname{Gal}\left(E/k\right) = G &\twoheadrightarrow \operatorname{Gal}\left(E^H/k\right) \\ \sigma &\mapsto \sigma|_{E^H} \end{aligned}$$

   ein surjektiver Gruppenhomomorphismus, der einen Isomorphismus

$$\operatorname{Gal}\left(E/k\right)/\operatorname{Gal}\left(E/E^H\right) \xrightarrow{\sim} \operatorname{Gal}\left(E^H/k\right)$$

   induziert.

Beweis

i) Die Wohldefiniertheit von ϕ ist klar und die von ψ folgt aus 10.3 i).

- $\phi \circ \psi = \mathrm{id}$

  Zeige: $k \subseteq K \subseteq E$ Zwischenkörper $\Rightarrow K = \phi(\psi(K)) = E^{\mathrm{Gal}\left(E/K\right)}$.
  Dies folgt aus **??**10.7 ii) für die Körpererweiterung $E \subseteq K$.
- $\psi \circ \phi = \mathrm{id}$

  Zeige: $H \subseteq G$ Untergruppe $\Rightarrow \mathrm{Gal}\left(E/E^H\right) = H$ in G.
  Dies gilt nach 10.5 ii).

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

ii) b) $\Rightarrow$ a) und zweite Aussage: 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.
Dazu nach **??**7.4 i):
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 $\overline{\sigma} \in \mathrm{Aut}_k(E) = G$.
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, 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 mit

$$G := \mathrm{Gal}\left(E'/k\right)$$

endlich, genauer $|G| = [E' : k] < \infty$.
G besitzt nur endlich viele Untergruppen, also besitzt nach 10.9 i) E'/k 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.

$\square_{10.10}$

10.11 Definition und Bemerkung

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

Seien $E \supseteq k$ eine endliche Galoiserweiterung (das ist definiert als endliche Körpererweiterung, die galoissch ist), $k \subseteq K_1, K_2 \subseteq E$ 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.

Bildchen

TODO: Abb1

Bemerkung

Ist ${}^{E}\!/_{k}$ endlich separabel und ${}^{E'}\!/_{k}$ normale Hülle von ${}^{E}\!/_{k}$, dann ist ${}^{E'}\!/_{k}$ endlich separabel (und normal).

Beweis

Aus **??**8.17 ergibt sich:

$$\underset{\alpha \in E}{\exists} E = k(\alpha)$$

Wähle $E \hookrightarrow \overline{E} = \overline{k}$.
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:

$$[E':k'] < \infty \text{**??**??}$$

Für alle σ gilt $\mathrm{Mipo}_k(\sigma(\alpha)) \overset{(!)}{=} \mathrm{Mipo}_k(\alpha) \in k[X]$ ist separabel, also ist ${}^{E'}\!/_{k}$ separabel. (nach **??**??)

Beweis von 10.12

i) „⇒“: $H_2 = \mathrm{Aut}_{K_2}(E) \overset{K_1 \subseteq K_2}{\subseteq} \mathrm{Aut}_{K_1}(E) = H_1$
„⇐“: $K_1 \overset{??10.9\,i)}{=} E^{H_1} \overset{H_2 \subseteq H_1}{\subseteq} E^{H_2} \overset{??10.9\,i)}{=} K_2$

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

ii) $K_1 \cdot K_2 = E^{H_1} \cdot E^{H_2} \overset{\text{i)}}{\subseteq} \left(E^{H_1 \cap H_2}\right) \cdot \left(E^{H_1 \cap H_2}\right) = E^{H_1 \cap H_2}$
Ferner gilt:

$$\mathrm{Gal}\left(E/K_1 \cdot K_2\right) \overset{K_i \subseteq K_1 \cdot K_2}{\subseteq} \mathrm{Aut}_{K_1}(E) \cap \mathrm{Aut}_{K_2}(E) = H_1 \cap H_2$$

Damit folgt mit i):

$$E^{H_1 \cap H_2} \subseteq K_1 \cdot K_2$$

$\square_{\text{ii)}}$

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.)

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.
Genauer: $\alpha \in \mathbb{C} : \alpha^3 = 2$ 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 Gruppehnisomorphismus.
Aus der linearen Algebra I ist folgendes *Untergruppen-Diagramm* der S_3 bekannt:
TODO: abb2
$A_3 \trianglelefteq S_3$ 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 ?)
Außerdem können der Durchschnitt und die Erzeugerrelation abgelesen werden, zum Beispiel $\langle A_3, H_i \rangle = S_3$ und $H_i \cap A_3 = \{e\}$ für alle $0 \leq i \leq 2$.

$$E = E^{\{e\}} = \mathbb{Q}(\alpha, \zeta)$$

Aus 10.9 und 10.12 folgt daraus folgendes Diagramm von Zwischenkörpern.
TODO: Abb 4

$$(\mathbb{Q}(\zeta) = E^{A_3})$$

Weil $H_i \subseteq S_3$ nicht normal ist, ist $\mathbb{Q}(\alpha\zeta^i)/\mathbb{Q}$ nicht normal (vergleiche **??**7.2).
Weil $A_3 \trianglelefteq S_3$ ist $\mathbb{Q}(3)/\mathbb{Q}$ galoissch mit:

$$\mathrm{Gal}\left(\mathbb{Q}(3)/\mathbb{Q}\right) \cong S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$

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 $\text{Mipo}_{\mathbb{Q}}(\zeta) = X^2 + X + 1$ ist, also folgt $E^{A_3} = \mathbb{Q}(\zeta)$.
2. Für $\text{id} \neq \tau_i \in H_i$ $(0 \leq i \leq 2)$ gilt $\tau_i\left(\alpha\zeta^i\right) = \alpha\zeta^i$, also $\alpha\zeta^i \in E^{H_i}$.
Wegen $\left[\alpha\zeta^i : \mathbb{Q}\right] = 3$, da $\text{Mipo}_{\mathbb{Q}}\left(\alpha\zeta^i\right) = X^3 - 2$, und $\left[E^{H_i} : \mathbb{Q}\right] = \left[E^{H_i} : E^{S_3}\right] = [S_3 : H_i] = 3$ folgt $E^{H_i} = \mathbb{Q}\left(\alpha\zeta^i\right)$ $(0 \leq i \leq 2)$.

Bemerkung

Seien $E \supseteq k$ endlich und galoissch, $G := \text{Gal}\left(E/k\right)$, $H \subseteq G$ eine Untergruppe und $K := E^H$.
Dann gilt:

a) $\left[E : E^H\right] = [G : H]$

b) $\left[E^H : k\right] = [G : H]$

Beweis

$\text{Gal}\left(E/k\right) = H$
Aus 10.3 folgt damit a).
Dann gilt:
$$[E : k] = [G : H] \cdot |H| \overset{\text{a)}}{=} [G : H] \cdot \left[E : E^H\right]$$
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 $\text{Gal}\left(E/k\right)$ 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

$G := \text{Gal}\left(E/k\right)$ ist abelsch und damit folgt, dass $H := \text{Gal}\left(E/K\right) \trianglelefteq G$ gilt.
Aus 10.9 ii) folgt damit, dass K/k galoissch ist und $\text{Gal}\left(K/k\right) \cong G/H$ endlich zyklisch (beziehungsweise zyklisch nach 1.22 ii)) ist.

$\square_{10.15}$

10.16 Satz

Seien $E \supseteq k$ eine Körpererweiterung und $k \subseteq K_1, K_2 \subseteq E$ Zwischenkörper mit K_i/k endlich galoissch $(i = 1, 2)$.
Dann gilt:

i) Das Kompositum $K_1 \cdot K_2$ ist endlich galoissch und die Abbildung

$$\varphi : \mathrm{Gal}\left(K_1 \cdot K_2 / K_1\right) \xrightarrow{\sim} \mathrm{Gal}\left(K_1 \cap K_2 / k\right)$$
$$\sigma \mapsto \sigma|_{K_2}$$

ist wohldefiniert und ein Gruppenisomorphismus.

ii) Die Abbildung

$$\psi : \mathrm{Gal}\left(K_1 \cdot K_2 / k\right) \hookrightarrow \mathrm{Gal}\left(K_1 / k\right) \times \mathrm{Gal}\left(K_2 / k\right)$$
$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

ist wohldefiniert und ein injektiver Gruppenhomomorphismus.
Im Fall $K_1 \cap K_2 = k$ ist ψ ein Isomorphismus.

Beweis

i) Es existiert separable $f_i \in k[X]$ so, dass K_i/k der Zerfällungskörper von f_i ist $(i = 1, 2)$, siehe 10.2 a) $\Rightarrow$ b).
Dann ist $K_1 \cdot K_2/k$ der Zerfällungskörper des separablen Polynoms $f_1 f_2$, also endlich und galoissch.
φ ist wohldefiniert, da $\left(\sigma|_{K_1} = \mathrm{id} \Rightarrow (\sigma|_{K_2})\big|_{K_1 \cap K_2} = \mathrm{id}\right)$ gilt, und 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:

$$K_2^{\mathrm{im}(\varphi)} \overset{\text{Def. von } \varphi}{=} (K_1 \cdot K_2)^{\mathrm{Gal}\left(K_1 \cdot K_2 / K_1\right)} \cap K_2 \overset{??10.9i)}{=} K_1 \cap K_2 = K_2^{\mathrm{Gal}\left(K_2 / K_1 \cap K_2\right)}$$

Mit 10.9 i) folgt:

$$\mathrm{im}(\varphi) = \mathrm{Gal}\left(K_2 / K_1 \cap K_2\right)$$

Also ist φ surjektiv.

ii) Wohldefiniertheit und Gruppenhomomorphismus sind klar.
Aus $\sigma \in \ker(\psi)$ folgt $\sigma|_{K_i} = \mathrm{id}$ $(i = 1, 2)$ und damit folgt $\sigma = \sigma|_{K_1 \cdot K_2} = \mathrm{id}$, weswegen ψ injektiv ist.
Gelte nun $K_1 \cap K_2 = k$ und sei $(\sigma, \sigma') \in \mathrm{Gal}\left(K_1/k\right) \times \mathrm{Gal}\left(K_2/k\right)$ beliebig.
Aus i) folgt damit, dass es ein $\tilde{\sigma} \in \mathrm{Gal}\left(K_1 \cdot K_2 / K_2\right)$ mit $\tilde{\sigma}|_{K_1} = \sigma$ gibt, und ebenso ein $\tilde{\sigma}' \in \mathrm{Gal}\left(K_1 \cdot K_2 / K_1\right)$ mit $\tilde{\sigma}'|_{K_2} = \mathrm{id}$.
Dann gilt:

$$\psi(\tilde{\sigma}' \cdot \tilde{\sigma}) = (\tilde{\sigma}' \cdot \tilde{\sigma}|_{K_1}, \tilde{\sigma}' \cdot \tilde{\sigma}|_{K_2}) = (\mathrm{id} \cdot \sigma, \sigma' \cdot \mathrm{id}) = (\sigma, \sigma')$$

Daher ist ψ surjekiv.

$\square_{10.16}$

Beweis

Nach **??**8.17 gibt es ein $\alpha_i \in K_i$ mit $K_i = k(\alpha_i)$ $(i = 1, 2)$.
Es gilt $\text{Mipo}_{K_1}(\alpha_2) | \text{Mipo}_k(\alpha_2)$, da $\text{Mipo}_k(\alpha_2) \in K_1[X]$ schon α_2 annuliert.
Mit $\text{Mipo}_k(\alpha_2)$ ist damit auch $\text{Mipo}_{K_1}(\alpha_2)$ 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 **??**6???).

Bemerkung

1. $f_1, f_2 \in k[X]$ separable $\not\Rightarrow f_1 \cdot f_2 \in k[X]$ separabel, zum Beispiel $f_1 = f_2 = X$.
2. $k \subseteq K_1, K_2 \subseteq E$ Zwischenkörper mit ${}^{K_i}\!/_k$ endlich und separabel. Damit folgt ${}^{K_1 \cdot K_2}\!/_k$ endlich und separabel.

10.17 Proposition

Seien k ein Körper, $f \in k[X]$ separabel, ${}^{E}\!/_k$ ein Zerfällungskörper von f, $G := \text{Gal}\left({}^{E}\!/_k\right)$ (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:

$$0 = \sigma(\underbrace{f(\alpha)}_{=0}) = f^\sigma(\sigma(t\alpha)) \overset{f=f^\sigma,\ \text{da } f \in k[X]}{=} f(\sigma(\alpha))$$

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 $\tilde{\sigma} : \overline{k} \to \overline{k}$ mit $\tilde{\sigma}(\alpha) = \beta$. (Blatt 8, A3,d) $\Rightarrow$ a))
Weil ${}^{E}\!/_k$ normal ist, ist $\sigma := \tilde{\sigma}|_E \in G$ und es gilt $\sigma(\alpha) = \tilde{\sigma}(\alpha) = \beta$.
ii) $\Rightarrow$ i):
Für $g := \text{Mipo}_k(\alpha)$ gelten $g | f$ in $k[X]$ und:

$$\underset{\beta \in \mathcal{N}}{\forall} \underset{\sigma \in G}{\exists} : \sigma(\alpha) = \beta \Rightarrow 0 = \sigma(\underbrace{g(\alpha)}_{=0}) = g^\sigma(\sigma(\alpha)) = g(\beta)$$

Also:

$$g|_{\mathcal{N}} = 0 \tag{10.1}$$

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

Mit $k := \mathbb{Q} \subseteq K_1 := \mathbb{Q}(\alpha_1), K_2 := \mathbb{Q}(\alpha_2) \subseteq E = K_1 \cdot K_2$ ist klar, dass K_i/k 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), und 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 $i = 1, 2$ gilt $\mathrm{Gal}\left(K_i/k\right) = \{1, \tau_i\}$, wobei $\tau_i : K_i \xrightarrow{\sim} K_i$ 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

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

$$p : \mathrm{Gal}\left(E/k\right) \hookrightarrow \sum(\mathcal{N}) \left(\tilde{=} \text{ nach Wahl einer Nummerierung } \mathcal{N} = \{\alpha_1, \ldots, \alpha_n\}\right)$$

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 galoissch nach **??**10.2 b) $\Rightarrow$ a).
Die Aussagen über p folgen wie in Aufgabe 2, ii) auf Blatt 7.
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 gilt: $f \in k[X]$ ist nicht separabel $\overset{f \text{ irreduzibel}}{\Leftrightarrow}$ in $k[X]$ gilt: $0 = f(X) = 2X + a \Leftrightarrow (\mathrm{char}(k) = 2$ und $a = 0)$
Gelte nun ($\mathrm{char}(k) \neq 2$ oder $a \neq 0$).
Dann ist E/k galoissch mit $\mathrm{Gal}\left(E/k\right) \tilde{=} \mathbb{Z}/2\mathbb{Z}$ und das eindeutige $1 \neq \sigma \in \mathrm{Gal}\left(E/k\right)$ 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.
Betrachte (ähnlich wie quadratische Ergänzung): (TODO: restliche Terme)

$$\begin{aligned} f(X) := F\left(X - \frac{A}{3}\right) &= X^3 + X^2\left(-3 \cdot \frac{A}{3} + \alpha\right) + \ldots (TODO) = \\ &= X^3 + aX + b \end{aligned}$$

(Hier geht $\operatorname{char}(k) \neq 3$ ein.)

Da $k[X] \xrightarrow{\sim} k[X], X \mapsto X - \frac{A}{3}$ ein Isomorphismus ist, 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 $\mathcal{N} := \{\alpha \in E | f(\alpha) = 0\} = \{\alpha_1, \alpha_2, \alpha_2\} \overset{??11.1}{\Rightarrow}$ Es 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 $\sigma \in \operatorname{Gal}\left(E/k\right)$ gilt in E^*:

$$\sigma(\delta) = \operatorname{sgn}(\varrho(\sigma)) \cdot \delta$$

Beweis

Klar wegen (11.1), Definition von σ und δ und Definition von $\operatorname{sgn}(\varrho(\sigma))$ als Anzahl der Fehlstände.

$\square_{\text{Behauptung}}$

Es folgt in $\mathbb{Z}$: $\operatorname{im}(\varrho) = A_3 \overset{\text{Definition von } A_3}{\Leftrightarrow} \forall_{\sigma \in \operatorname{Gal}(E/k)} : \operatorname{sgn}(\varrho(\sigma)) = 1 \overset{\text{Behauptung}}{\underset{\operatorname{char}(k) \neq 2}{\Leftrightarrow}} \forall_{\sigma \in \operatorname{Gal}(E/k)} : \sigma(\delta) = \delta$.

Dies ist äquivalent zu $\delta \in E^{\operatorname{Gal}(E/k)} = k$.
Ferner gilt mit $\Delta := \delta^2 : \forall_{\sigma \in \operatorname{Gal}(E/k)} : \sigma(\Delta) = (\pm\delta)^2 = \Delta$ und damit folgt $\Delta \in k$.

Später wird noch gezeigt: $\Delta = -4a^3 - 27b^2$.
Damit gilt für die Galoisgruppe der irreduziblen Gleichung $X^3 + aX + b$:

$$\operatorname{Gal}\left(E/k\right) \cong \begin{cases} A_3 & \Delta = -3a^3 - 27b^2 \in (k^*)^2 \\ S_3 & \text{sonst} \end{cases}$$

11.3.1 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 $\mathbb{Z}$ hat keine Nullstellen in $\mathbb{Q}$“ und „eine ganzzahlige Nullstelle eines normierten Polynoms teilt den letzten Koeffizienten“).

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, $E := k(t_1, \ldots, t_n)$.

Dann existiert genau eine Abbildung

$$\varrho : S_n \to \mathrm{Aut}(E)$$

mit:

$$\underset{\sigma \in S_n, 1 \leq i \leq n}{\forall} : \varrho(\sigma)(t_i) = t_{\sigma(i)}$$

(benutze zum Beweis die universelle Eigenschaft des Polynomrings und des Quotientenkörpers)

und ϱ ist ein injektiver Gruppenhomomorphismus, vermöge dessen wir $S_n \subseteq \mathrm{Aut}(E)$ als Untergruppe auffassen.

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

(**??**)10.7 i)

$\square_{11.4}$

11.4.2 Beispiel

$n = 2 \Rightarrow S_2 = \left\{1, \begin{pmatrix} 1 & 2 \end{pmatrix} =: \sigma\right\}$, also $t_1 + t_2 \in k(t_1, t_2)^{S_2}$, da $\sigma(t_1 + t_2) = t_2 + t_1 = t_1 + t_2$, aber, falls $\mathrm{char}(k) \neq 2$, $t_1 - t_2 \notin k(t_1, t_2)^{S_2}$, da $\sigma(t_1 - t_2) = t_2 - t_1 = -(t_1 - t_2) \neq t_1 - t_2$, da $1 \neq -1$.

11.4.3 Definition

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, 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 $a_1 := X^2, a_s := X^3 \in A := k[X]$ 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 $f(a_1, a_2) = 0$.

(Beachte: (a_1, a_2) sind in A aber k-linear unabhängig.)

11.4.6 **Satz**

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 $\mathrm{char}(k) \neq 2$. 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 $E^{A_n} = K(\delta) \overset{??11.4.6ii)}{=} k(s_1, \ldots, s_n, \delta)$.

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 $\mathrm{Gal}\left(E/\mathbb{Q}\right) \cong G$.

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 $\varphi(t_i) = T_i$ für alle $1 \leq i \leq n$ gilt für alle $1 \leq i \leq n$:

$$\varphi(s_i) \overset{(11.2)}{=} \mathcal{S}_i$$

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.

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

11.4.8 Definition

$$p(X) := X^n + \mathcal{S}_i X^{n-1} + \ldots + \mathcal{S}_n = X^n + \sum_{i=1}^{n} \mathcal{S}_i \cdot X^{n-i} \in k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X]$$

heißt das *allgemeine Polynom n-ten Grades über k.*

11.4.9 Bemerkung

Seien $k \subseteq F$ eine Körpererweiterung und $f \in F[X]$ ein normiertes Polynom vom Grad n.
Dann existiert genau ein k-Algebrenhomomorphismus

$$\varphi : k(\mathcal{S}_1, \ldots, \mathcal{S}_n) \to F$$

mit

$$\varphi[X](p(X)) = f$$

(nämlich $\varphi(\mathcal{S}_i) = (n-i)$-ter Koeffizient von f).

11.4.10 Satz

$p(X) \subseteq k(\mathcal{S}_1, \ldots, \mathcal{S}_n)[X]$ ist irreduzibel, 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.

$\square_{11.4}$

11.4.11 Satz (Hilbertscher Irreduzibilitätssatz)

Für $n \geq 1$ existieren unendlich viele Tupel $(q_1, \ldots, q_n) \in \mathbb{Q}^n$ so, dass für

$$f(X) = X^n + \sum_{i=1}^{n} q_i X^{n-i} \in \mathbb{Q}[X]$$

ist $f(X) \in \mathbb{Q}[X]$ irreduzibel, separabel und es gilt:

$$\mathrm{Gal}(f) = S_n$$

(ohne Beweis)

Beispiel

$q_i = 0$, dann ist $f(X) = X^n$ mit der trivialen Galoisgruppe und nicht S_n.

12 Kreisteilungskörper (die Galoistheorie von $X^n - 1 = 0$)

Fixiere

Sei k ein Körper und $n, m \geq 1$ mit $\mathrm{char}(k) \nmid n, m$ (im Fall $\mathrm{char}(k) = 0$ seien $n, m \geq 1$ beliebig).

12.1 Proposition und Definition

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 $(X^n - 1)(\zeta) = 0$ und $(X^n - 1)'(\zeta) = n\zeta^{n-1} \neq 0$, da $\zeta \neq 0$ 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 $n \geq 1$, dann folgt:

$$\left\{\zeta \in \overline{\mathbb{F}_p} | \zeta^{p^n} = 1\right\} = \{1\}$$

12.2 Definition

Eine n-te Einheitswurzel $\zeta \in U_n$ heißt genau dann *primitiv*, wenn $\langle\zeta\rangle = U_n$.

12.3 Beispiel

$k = \mathbb{C}$, $U_6 = \left\langle \zeta_6 := \exp\left(\frac{2\pi\mathbf{i}}{6}\right)\right\rangle \subseteq \mathbb{C}^*$ und genau $\zeta_6, \zeta_6^5 = \zeta_6^{-1} \in U_6$ sind primitiv:
TODO: Abb1
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

Für $n, m \geq 1$ sind $(n, m) = 1$ (und $\operatorname{char}(k) \nmid n, m$) ist die Abbildung $f : U_n \times U_m \to U_{nm}$ ist 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

$(n,m) = 1$ wird gebraucht:
$\zeta := \mathbf{i} \in U_4(\mathbb{C}), \xi := \mathbf{i} \in U_4(\mathbb{C})$ sind primitiv, aber $\zeta \cdot \xi = -1 \in U_{16}(\mathbb{C})$ hat Ordnung $2 \neq 16$, ist also nicht primitiv.

Anhang

GNU Free Documentation License

Version 1.3, 3 November 2008

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 (C) 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.