

Algebra

Vorlesung von
PROF. DR. NIKO NAUMANN
im Wintersemester 2011/2012
Überarbeitung und Textsatz in L^AT_EX von
ANDREAS VÖLKLEIN



Stand: 13. Januar 2012

ACHTUNG

Diese Mitschrift ersetzt *nicht* die Vorlesung.

Es wird daher *dringend* empfohlen, die Vorlesung zu besuchen.

Copyright Notice

Copyright © 2011-2012 ANDREAS VÖLKLEIN

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”.

Disclaimer of Warranty

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING AND TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, **THE COPYRIGHT HOLDERS PROVIDE THE DOCUMENT “AS IS” WITHOUT WARRANTIES OF ANY KIND**, EXPRESSED, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE.

Limitation of Liability

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING **WILL THE COPYRIGHT HOLDERS BE LIABLE TO YOU FOR ANY LOSS** OF REVENUE, PROFIT OR ANYTHING ELSE, **OR FOR ANY DAMAGES**, INCLUDING, BUT NOT LIMITED TO, ANY GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THIS LICENSE OR THE USE OF OR INABILITY TO USE THE DOCUMENT, EVEN IF THE COPYRIGHT HOLDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT WILL THE COPYRIGHT HOLDERS’ LIABILITY TO YOU, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, **EXCEED THE AMOUNT YOU PAID THE COPYRIGHT HOLDERS** FOR THE DOCUMENT UNDER THIS AGREEMENT.

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*, West-view Press, 1994
ISBN 0-201-40751-5, Lokalisierungen: Seite 36-39

Inhaltsverzeichnis

1	Gruppentheorie I	1
1.1	Definition (Gruppenhomomorphismus)	1
1.2	Beispiel	1
1.3	Proposition und Definition (Kern und Bild)	2
1.4	Proposition	2
1.5	Beispiel und Definition (Automorphismengruppe, Konjugation)	2
1.6	Proposition und Definition (Linksnebenklasse, Index)	3
1.7	Korollar (Satz von Lagrange)	4
1.8	Beispiel (Symmetrische und alternierende Gruppe vom Grad 3)	5
1.9	Definition (Normalteiler)	5
1.10	Beispiel	5
1.11	Proposition (Kern ist Normalteiler)	5
1.12	Beispiel und Definition (Zentrum)	6
1.13	Proposition (kanonische Projektionsabbildung)	6
1.14	Beispiel (H ist kein Normalteiler)	7
1.15	Satz (universelle Eigenschaft der Projektionsabbildung π)	7
1.16	Korollar (Isomorphiesatz)	8
1.17	Satz (Primzahlordnung)	8
1.18	Beispiel	8
1.19	Proposition und Definition (erzeugte Untergruppe)	9
1.20	Proposition und Definition (zyklische Gruppe, Erzeuger)	9
1.21	Satz (Klassifizierung zyklischer Gruppen)	9
1.22	Satz (Untergruppe, Kern und Bild zyklischer Gruppen)	10
1.23	Definition (Gruppenordnung)	10
1.24	Beispiel	11
1.25	(kleiner Fermatscher) Satz	11
1.26	Korollar	11
1.27	Proposition (Kriterium für zyklische Gruppen)	12
1.28	Korollar	12
1.29	Bemerkung	13
1.30	Korollar	13
2	Lokalisierungen	14
2.1	Proposition und Definition (multiplikativ abgeschlossen)	14
2.2	Konstruktion und Definition (Quotientenring)	14
2.3	Beispiel (Quotientenkörper)	15
2.4	Proposition (Universelle Eigenschaft von $S^{-1}A$)	16
2.5	Korollar	17
2.6	Beispiel (Lokalisierung)	18
2.7	Konstruktion (Lokalisierung)	18

2.8	Proposition	19
2.9	Proposition	19
2.10	Beispiel	21
3	Der Satz von Gauß	22
3.1	Erinnerung (Primfaktorzerlegung)	22
3.2	Bemerkung	23
3.3	Proposition und Definition (Lemma von Gauß)	23
3.4	Korollar	24
3.5	Beispiel	25
3.6	Beispiel	25
3.7	Proposition und Definition (primitiv)	26
3.8	Satz (von Gauß)	27
3.9	Beispiel	27
3.10	Beispiel und Definition (rationale Funktionen)	28
4	Irreduzibilitätskriterien	30
4.1	Proposition (Äquivalenz von Primelement in R und Q)	30
4.2	Bemerkung	30
4.3	Satz (Reduktionskriterium)	30
4.4	Beispiel	31
4.5	Korollar (Eisensteinkriterium)	32
4.6	Beispiel	32
4.7	Bemerkung	36
5	(Algebraische) Körpererweiterungen	37
5.1	Proposition und Definition (Charakteristik, Primkörper)	37
5.2	Bemerkung und Definition (Körpererweiterung)	37
5.3	Proposition und Definition (Frobenius)	38
5.4	Proposition und Definition (algebraisch, transzendent, Zwischenkörper)	38
5.5	Definition (Grad)	39
5.6	(Grad-)Satz	39
5.7	Korollar	39
5.8	Beispiel (Verfahren von Kronecker)	40
5.9	Definition (algebraische Körpererweiterung)	41
5.10	Beispiel	41
5.11	Bemerkung und Definition (Grad von $\alpha \in E$)	41
5.12	Satz	41
5.13	Proposition und Definition (Polynomring; endlich erzeugte, einfache Körpererweiterung)	42
5.14	Satz	42
5.15	Beispiel	43
5.16	Proposition (endlich \Leftrightarrow endlich erzeugt und algebraisch)	43
5.17	Satz (Transitivität der Algebraizität)	44
5.18	Beispiel	45
6	Der algebraische Abschluss eines Körpers	46
6.1	Proposition und Definition (algebraisch abgeschlossen)	46
6.2	Proposition und Definition (Polynomring)	46
6.3	Das Lemma von Zorn	47

6.3.1	Definition (geordnete Menge, obere Schranke)	47
6.3.2	Beispiel	47
6.3.3	Satz (Lemma von Zorn)	47
6.3.4	Beispiel	48
6.3.5	Satz (Existenz eines maximalen Ideals)	48
6.4	Satz und Definition (algebraischer Abschluss)	48
6.5	Notation und Bemerkung	50
6.6	Lemma	51
6.7	Satz und Definition (Fortsetzung)	51
6.8	Korollar	52
7	Zerfällungskörper	53
7.1	Definition (Zerfällungskörper)	53
7.2	Beispiel	53
7.3	Satz (Existenz und Eindeutigkeit von Zerfällungskörpern)	54
7.4	Satz und Definition (normale Körpererweiterung)	55
7.5	Beispiel	56
7.6	Proposition (algebraischer Abschluss ist normal)	56
7.7	Beispiel	56
7.8	Beispiel (Normalität ist nicht-transitiv)	57
7.9	Definition (normale Hülle)	57
7.10	Satz und Definition (Konjugierte)	58
7.11	Beispiel	58
8	Separabilität	59
8.1	Definition ((formale) Ableitung)	59
8.2	Beispiel	59
8.3	Satz und Definition (mehrfache Nullstelle)	60
8.4	Lemma	60
8.5	Definition (separables Polynom)	61
8.6	Proposition	61
8.7	Beispiel	61
8.8	Definition (separable(s) Element/Körpererweiterung)	62
8.9	Definition (vollkommener Körper)	62
8.10	Beispiel	62
8.11	Definition (Separabilitätsgrad)	62
8.12	Satz (vollkommene Körper)	62
8.13	Lemma	63
8.14	Satz (Separabilitäts-Gradsatz)	63
8.15	Satz	64
8.16	Korollar (Transitivität der Separabilität)	65
8.17	Satz (vom primitiven Element) und Definition	65
9	Endliche Körper	68
9.1	Lemma	68
9.2	Satz und Definition (\mathbb{F}_{p^n})	69
9.3	Bemerkung	69
9.4	Korollar	69
9.5	Satz und Definition (relativer Frobenius)	70

10 Galoistheorie	71
10.1 Definition (galoissche Körpererweiterung, Galoisgruppe)	71
10.2 Beispiel und Definition (Galoisgruppe von f)	71
10.3 Proposition	72
10.4 Proposition	72
10.5 Satz und Definition (Fixkörper)	73
10.6 Beispiel	74
10.7 Korollar	75
10.8 Bemerkung und Beispiel (absolute Galoisgruppe)	76
10.9 Satz (Hauptsatz der Galoistheorie)	76
10.10 Korollar	78
10.11 Definition und Bemerkung (Kompositum)	78
10.12 Satz und Definition (Galoiserweiterung)	78
10.13 Beispiel und Definition (Untergruppen-Diagramm)	80
10.14 Definition (abelsche und zyklische Galoiserweiterung)	81
10.15 Korollar	81
10.16 Satz	82
10.17 Proposition	84
10.18 Beispiel (biquadratische Erweiterung)	85
11 Bestimmung einiger Galoisgruppen	87
11.1 Satz und Definition (Die Permutationsdarstellung)	87
11.2 Quadratische Gleichungen	88
11.3 Kubische Gleichungen	88
11.3.1 Lemma (Normalform)	88
11.3.2 Bestimmung der Galoisgruppe	88
11.3.3 Beispiel	90
11.4 Die allgemeine Gleichung	90
11.4.1 Proposition und Definition (symmetrische rationale Funktionen)	90
11.4.2 Beispiel	90
11.4.3 Definition (elementarsymmetrische Polynome)	91
11.4.4 Definition (algebraische Unabhängigkeit)	91
11.4.5 Beispiel	91
11.4.6 Satz (Hauptsatz über symmetrische Funktionen)	91
11.4.7 Bemerkung	92
11.4.8 Definition (allgemeines Polynom n -ten Grades)	93
11.4.9 Bemerkung	93
11.4.10 Satz	93
11.4.11 Satz (Hilbertscher Irreduzibilitätssatz)	94
12 Kreisteilungskörper (die Galoistheorie der Gleichung $X^n - 1 = 0$)	95
12.1 Proposition und Definition (Gruppe der n -ten Einheitswurzeln)	95
12.2 Definition (primitive Einheitswurzeln)	95
12.3 Beispiel	96
12.4 Proposition	96
12.5 Erinnerung	97
12.6 Proposition	97
12.7 Korollar	98
12.8 Satz	98

12.9	Bemerkung und Definition	99
12.10	Satz (Gauß)	99
12.11	Korollar	101
12.12	Bemerkung	102
12.13	Definition (Kreisteilungspolynom)	102
12.14	Satz	102
12.15	Beispiel	104
12.16	Satz und Definition (Nullstelle modulo p)	104
12.17	Beispiel	105
12.18	Lemma	106
12.19	Satz	106
12.20	Bemerkung	107
 Anhang		109
	GNU Free Documentation License	109

1 Gruppentheorie I

Aus der Linearen Algebra I wird die Kenntnis folgender Objekte 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 $\varphi : G \rightarrow G'$ mit:

$$\forall_{a,b \in G} \varphi(ab) = \varphi(a) \cdot \varphi(b) \quad (1.1)$$

Ferner heißt φ

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

1.2 Beispiel

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

- $\varphi(e) = e'$ mit den neutralen Elementen $e \in G$ und $e' \in G'$.
- $\forall_{a \in G} \varphi(a^{-1}) = \varphi(a)^{-1}$

Beweis

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

□_{i)}

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

□_{1.2}

1.3 Proposition und Definition (Kern und Bild)

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

i) $\ker(\varphi) := \{a \in G \mid \varphi(a) = e'\} \subseteq G$ 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

□_{1.3}

1.4 Proposition

Sei G eine Gruppe. Dann ist die Abbildung

$$\{\varphi \mid \varphi : \mathbb{Z} \rightarrow G \text{ Gruppenhomomorphismus}\} \xrightarrow{\sim} G, \varphi \mapsto \varphi(1) \quad (1.2)$$

bijektiv.

Beweis

Lineare Algebra I

□_{1.4}

1.5 Beispiel und Definition (Automorphismengruppe, Konjugation)

Sei G eine Gruppe. Dann ist $\text{Aut}(G) := \{\varphi \mid \varphi : G \rightarrow G \text{ Automorphismus}\}$ eine Gruppe bezüglich der Komposition \circ mit dem neutralen Element id_G (Nebenbemerkung: im Allgemeinen ist $\text{Aut}(G) \subsetneq \Sigma(G)$ eine echte Untergruppe) und heißt die *Automorphismengruppe von G* .

Die Abbildung $\phi : G \rightarrow \text{Aut}(G)$, definiert durch $\phi(g)(h) = ghg^{-1} \quad \forall g, h \in G$ 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:

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

- $\forall_{g, h \in G} : (\phi(g) \circ \phi(g^{-1}))(h) = g \cdot \phi(g^{-1})(h) \cdot g^{-1} = \underbrace{gg^{-1}}_{=e} h \underbrace{(g^{-1})^{-1}}_{=g} g^{-1} = \underbrace{hg^{-1}}_{=e} = h$

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

- Für $g, g', h \in G$ gilt:

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

Also ist ϕ ein Gruppenhomomorphismus.

□_{1.5}**Beispiel**

$$G = \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}; \text{Aut}(G) \subseteq \Sigma(G) = \Sigma\{\bar{0}, \bar{1}, \bar{2}\} = S_3$$

$$\text{Aut}(G) \cong (\mathbb{Z}/3\mathbb{Z})^* = \{\bar{1}, \bar{2}\}$$

Insbesondere: $|\text{Aut}(G)| = 2, |\Sigma(G)| = 3! = 6$

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

$$\forall_{g, g' \in G} g \sim g' \Leftrightarrow g^{-1}g' \in H \quad (1.3)$$

eine Äquivalenzrelation.

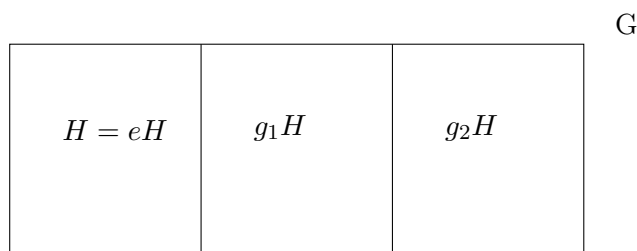
Für $g \in G$ heißt die Äquivalenzklasse

$$[g] = \{g' \in G | g \sim g'\} \stackrel{(1.3)}{=} \{gh | h \in H\} =: gH \subseteq G \quad (1.4)$$

die *Linksnebenklasse* von g bezüglich H . Wir schreiben $G/H := \{gH | g \in G\}$, und $(G : H) := |G/H|$ heißt der *Index* von H in G . Es gelten:

- $\forall_{g, g' \in G} : gH = g'H \Leftrightarrow gH \cap g'H \neq \emptyset \Leftrightarrow g \in g'H \Leftrightarrow g^{-1}g' \in H$
- Für alle $g, g' \in G$ ist die Abbildung $gH \xrightarrow{\sim} g'H, gh \mapsto g'h$ bijektiv.
Für $|H| < \infty$ ist $|gH| = |g'H|$.

$$\text{iii) } G = \dot{\bigcup}_{gH \in G/H} (gH) \quad (\text{disjunkte Vereinigung})$$

Bildchen**Beweis**

Zeige zunächst, dass \sim eine Äquivalenzrelation ist:

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

- \sim ist *symmetrisch*:

$$\forall_{g, g' \in G} g \sim g' \stackrel{(1.3)}{\Rightarrow} g^{-1} \cdot g' \in H \stackrel{H \text{ ist UG}}{\Rightarrow} H \ni (g^{-1} \cdot g')^{-1} = g'^{-1} \cdot g \stackrel{(1.3)}{\Rightarrow} g' \sim g$$

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

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

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

$\square_{1.7}$

1.8 Beispiel (Symmetrische und alternierende Gruppe vom Grad 3)

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

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

und

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

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

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

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:

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

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

Beweis

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

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

□_{1.11}**1.12 Beispiel und Definition (Zentrum)**

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

Beispiel

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

Beweis zu 1.12.0

Für die Abbildung $\phi: G \rightarrow \mathrm{Aut}(G)$ aus 1.5 sieht man leicht, dass $\ker(\phi) = Z(G)$ ist.

Also folgt die Behauptung aus 1.11.

□_{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

$$\pi: G \rightarrow G/N, \pi(g) \mapsto gN \quad (1.8)$$

ein Gruppenhomomorphismus ist.

Es gilt $\ker(\pi) = N$.

Beweis

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

$$\forall_{g, g' \in G} (gN) \cdot (g'N) = \pi(g) \cdot \pi(g') = \pi(gg') = (gg') \cdot N \quad (1.9)$$

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

$$\forall_{g, g', g_1, g'_1 \in G} (gN = g_1N) \wedge (g'N = g'_1N) \quad \Rightarrow \quad (gg')N = (g_1g'_1)N \quad (1.10)$$

Dies ergibt sich aus folgender Überlegung:

Wegen (1.3) in 1.6 betrachte:

$$\begin{aligned} (gg')^{-1} \cdot (g_1 g'_1) &= (g')^{-1} \cdot g^{-1} \cdot g_1 \cdot g'_1 = (g')^{-1} \cdot \underbrace{g'_1 \cdot (g'_1)^{-1}}_{=e} \cdot \underbrace{g^{-1} \cdot g_1}_{=:n \in N, \text{ da } gN=g_1N} \cdot g'_1 = \\ &= \underbrace{(g')^{-1} \cdot g'_1}_{\in N, \text{ da } g'N=g'_1N} \underbrace{(g'_1)^{-1} \cdot n \cdot g'_1}_{\in N, \text{ da } N \trianglelefteq G} \in N \end{aligned}$$

Also gilt $(gg')N = (g_1 g'_1)N$.

Ferner gilt:

$$\ker(\pi) = \left\{ g \in G \mid gN = \pi(g) = e' = eN = N \in G/N \right\} \stackrel{1.6i)}{=} N$$

□_{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 $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus.

Dann sind äquivalent:

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

ii) $\exists! \varphi : G/N \rightarrow G' \text{ Grphom. } \varphi = \bar{\varphi} \circ \pi$

Bildchen

TODO: Abb

Beweis

Übung

□_{1.15}

1.16 Korollar (Isomorphiesatz)

Ist $\varphi : G \rightarrow G'$ ein Epimorphismus, so ist $\bar{\varphi} : G/\ker(\varphi) \rightarrow G'$ wohldefiniert und ein Isomorphismus.

Beweis

Nach 1.15 ist $\bar{\varphi}$ wohldefiniert und ein Gruppenhomomorphismus.

(Wähle in 1.15 $N = \ker(\varphi)$)

Weil φ ein Epimorphismus ist, ist auch $\bar{\varphi}$ ein Epimorphismus.

Aus

$$\ker(\bar{\varphi}) = \ker(\varphi)/N = \ker(\varphi)/\ker(\varphi) = \{e\}$$

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

□_{1.16}

1.17 Satz (Primzahlordnung)

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

$$G \cong \mathbb{Z}/p\mathbb{Z} \quad (1.11)$$

1.18 Beispiel

i) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z}$ (vergleiche Struktursatz für endlich erzeugte abelsche Gruppen).

ii) $S_3 \not\cong \mathbb{Z}/6\mathbb{Z}$ (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 $\varphi : \mathbb{Z} \rightarrow G$ mit $\varphi(1) = g$. Es folgt nach 1.7:

$$1 \neq |\operatorname{im}(\varphi)| \mid |G| = p$$

Weil p eine Primzahl ist, folgt $|\operatorname{im}(\varphi)| = |G|$, 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 $G \cong \mathbb{Z}/p\mathbb{Z}$.

□_{1.17}

1.19 Proposition und Definition (erzeugte Untergruppe)

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

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

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:

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

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

□_{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 $\varphi : \mathbb{Z} \rightarrow G$.

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 $\varphi : \mathbb{Z} \rightarrow G$ mit $\varphi(1) = x$.

ii) \Rightarrow i): Wähle $x := \varphi(1)$.

□_{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 $\varphi : \mathbb{Z} \rightarrow G$, 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:

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

□_{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 $\varphi : G \rightarrow G'$ sind $\ker(\varphi)$ und $\operatorname{im}(\varphi)$ zyklisch.

Beweis

- i) Ohne Einschränkung ist $H \neq \{e\}$. Wähle einen Epimorphismus $\varphi : \mathbb{Z} \rightarrow G$.

Dann ist auch $\psi := \varphi|_{\varphi^{-1}(H)} : \varphi^{-1}(H) \rightarrow H$ 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 $\psi : \mathbb{Z} \rightarrow H$ ein Epimorphismus, das heißt H ist zyklisch.

□_{i)}

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

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

Daher ist $\operatorname{im}(\varphi)$ zyklisch.

Weil $\ker(\varphi) \subseteq G$ eine Untergruppe ist, ist $\ker(\varphi)$ zyklisch nach i).

□_{1.22}

1.23 Definition (Gruppenordnung)

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

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

die Ordnung von x (in G).

1.24 Beispiel

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

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

Man erkennt:

- $\bar{2}$ und $\bar{3}$ sind Erzeuger von G , denn $\text{ord}(x) = 4$.
- Die Ordnung $\text{ord}(x)$ 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 $\text{ord}(x) \mid |G|$ und $x^{|G|} = e$ in G .

Beweis

Nach Definition ist $\text{ord}(x) = |H|$ für die Untergruppe $H := \langle x \rangle \subseteq G$.

Nun folgt $\text{ord}(x) \mid |G|$ aus 1.7.

Klar ist $x^{\text{ord}(x)} = e$, womit folgt:

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

□_{1.25}

1.26 Korollar

- i) Seien $n \geq 1$ und $a \in \mathbb{Z}$ teilerfremd zu n , dann folgt $a^{\varphi(n)} \equiv 1 \pmod{n}$.

(Hier ist $\varphi(n)$ die Eulersche φ -Funktion.)

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

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

(vergleiche 1.24)

Beweis

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

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

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

□_{1.26}

1.27 Proposition (Kriterium für zyklische Gruppen)

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

$$|\{x \in G \mid x^d = e\}| \leq d \quad (1.12)$$

Dann ist G zyklisch.

Beweis

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

Aus 1.25 folgt dann:

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

Seien $d \mid n$ und es gelte $\psi(d) \neq 0$, das heißt es gibt ein $z \in G$ mit $\text{ord}(z) = d$.

Aus 1.25 folgt für alle $g \in \langle z \rangle$ schon $g^d = e$.

Aus $|\langle z \rangle| = d$ und (1.12) folgt damit $\{x \in G \mid x^d = e\} \subseteq \langle z \rangle$ und insbesondere:

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

Es gilt aber:

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

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

$$\psi(d) \leq \varphi(d) \quad (1.14)$$

Denn für $\psi(d) = 0$ ist das trivial.

Die Summation liefert:

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

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

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

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

□_{1.27}

1.28 Korollar

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

Dann ist G zyklisch.

Bemerkung

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

Beweis von 1.28

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

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

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

□_{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 $k = \mathbb{F}_p$.

□_{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, $\varphi : A \rightarrow B$ ein Ringhomomorphismus und $S : \varphi^{-1}(B^*) \subseteq A$.

Dann gelten:

- i) $1 \in S$
- ii) $\forall_{s,t \in S} st \in S$

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

□_{2.1}

Fixiere in Kapitel 2 (Lokalisierungen)

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

2.2 Konstruktion und Definition (Quotientenring)

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

$$\forall_{(a,s),(h,t) \in A \times S} (a,s) \sim (h,t) :\Leftrightarrow \exists_{u \in S} u(at - bs) = 0 \quad (2.1)$$

ist eine Äquivalenzrelation.

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

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

Damit gilt:

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

Die Abbildungen

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

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

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

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

Beweis von 2.2

Die Reflexivität und Symmetrie von \sim sind klar.

Seien $a, b, c \in A$, $s, t, u \in S$ mit $(a, s) \sim (b, t)$ und $(b, t) \sim (c, u)$. gegeben.

Dann folgt aus (2.1), dass es $v, w \in S$ gibt mit:

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

Damit folgt in A :

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

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

□ \sim Äquivrel.

Der Rest bleibt als Übung.

TODO: Rest beweisen

□_{2.2}

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

i) Die Abbildung

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

ist ein Ringhomomorphismus.

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

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

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

TODO: Abbildung Homomorphiesatz

Beispiel

Es gibt genau einen Ringhomomorphismus $\mathbb{Q} \rightarrow \mathbb{C}$, denn:

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

TODO: Abb Homomorphiesatz ψ

Beweis von 2.4

i) $\varphi : A \rightarrow S^{-1}A, a \mapsto \frac{a}{1}$ ist ein Ringhomomorphismus.

Rechne zum Beispiel $\varphi(a) + \varphi(b) = \varphi(a+b)$ nach:

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

Der Rest geht analog.

□_{i)}

ii) b) \Rightarrow a): Es gilt $\varphi(S) \subseteq (S^{-1}A)^*$, 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:

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

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 $s \in S$:

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

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

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

Weil ψ eindeutig ist, folgt in B :

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

□_{2.4}

2.5 Korollar

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

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

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 das in A gilt:

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

□_{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 $s = 0 \in S$.

□_{2.5}

2.6 Beispiel (Lokalisierung)

Seien A ein Integritätsring und $\mathfrak{p} \subseteq A$ ein Primideal.

Dann ist $A \setminus \{\mathfrak{p}\} \subseteq A$ multiplikativ abgeschlossen und

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

heißt *Lokalisierung von A bei \mathfrak{p}* .

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

Für $A = \mathbb{Z}$ und $\mathfrak{p} = (p)$ (für eine Primzahl $p \in \mathbb{Z}$) gilt zum Beispiel:

$$A = \mathbb{Z} \subseteq A_{\mathfrak{p}} = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b \right\} \subseteq A_{(0)} = \mathbb{Q}$$

Einheiten:

$$\{\pm 1\} \subseteq \mathbb{Z}_{(p)}^* \stackrel{(!)}{=} \mathbb{Z}_{(p)} \setminus (p) = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid a, b \right\} \subseteq \mathbb{Q} \setminus \{0\}$$

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:

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

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

□_{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

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

eine Äquivalenzrelation.

Schreibe $S^{-1}M := (M \times S) / \sim$ 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 $\varphi : M \rightarrow N$ A -linear, so ist

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

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

Beweis

Analog zu 2.2.

□_{2.7}

2.8 Proposition

Sei

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P \quad (2.2)$$

eine exakte Folge von A -Moduln, das heißt $\operatorname{im}(\varphi) = \ker(\psi)$.

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: $\operatorname{im}(S^{-1}\varphi) = \ker(S^{-1}\psi)$

„ \subseteq “: Folgt aus:

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

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

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

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 $ts \cdot n \in \ker(\psi) \stackrel{\text{Vor.}}{=} \operatorname{im}(\varphi)$.

Also gibt es ein $m \in M$, für das in N gilt:

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

Damit folgt:

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

□_{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

$$S^{-1}A \times M \rightarrow S^{-1}M$$

$$\left(\frac{a}{s}, m\right) \mapsto \frac{am}{s}$$

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

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

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

Definiere:

$$t := \prod_j s_j \quad t_i := \frac{t}{s_i} = \prod_{j \neq i} s_j \in S \quad (2.4)$$

Damit folgt:

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

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

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

□ Behauptung

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

$$x = \frac{1}{t} \otimes m \quad (2.5)$$

Für geeignete $t \in S$ und $m \in M$.

Damit folgt in $S^{-1}M$:

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

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

$$0 = s \cdot t \cdot m \quad (2.6)$$

Damit ergibt sich:

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

Es folgt $\ker(f) = 0$, also ist f injektiv.

□_{2.9}

2.10 Beispiel

Sei $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ 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 $S = \mathbb{Z} \setminus \{0\}$,)

$$M \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\varphi \otimes \text{id}_{\mathbb{Q}}} N \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\psi \otimes \text{id}_{\mathbb{Q}}} P \otimes_{\mathbb{Z}} \mathbb{Q}$$

exakt.

Beweis

Folgt aus 2.8 und 2.9.

□_{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)

TODO: restlichen Beweis einfügen

Es folgt die Exaktheit der ersten Zeile.

□_{2.10}

3 Der Satz von Gauß

Fixiere in Kapitel 3 (Der Satz von Gauß)

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

Beispiel

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

3.1 Erinnerung (Primfaktorzerlegung)

Für alle $p \in \mathcal{P}$ ist

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

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

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

Die Abbildung

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

ist ein Isomorphismus von Gruppen mit der inversen Abbildung:

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

Für alle $q \in Q^*$ gilt:

$$q \in R \Leftrightarrow \forall_{p \in \mathcal{P}} : \nu_p(q) \geq 0 \quad (3.1)$$

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

3.2 Bemerkung

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

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

$$\text{mit } \varphi[X] \left(\sum_i a_i X^i \right) = \sum_i \varphi(a_i) X^i.$$

Es gilt:

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

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

$$\begin{aligned} \pi : R[X] &\rightarrow (R/(p))[X] \\ \sum_i a_i X^i &\mapsto \sum_i (a_i \pmod{p}) X^i \end{aligned}$$

ein surjektiver Ringhomomorphismus mit:

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

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

Beweis

Betrachte:

TODO: Abb Homomorphiesatz

Es existiert genau ein R -Algebrenhomomorphismus $\varphi[X]$ mit $\varphiX = X$.

Daher gilt:

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

□_{3.2}

3.3 Proposition und Definition (Lemma von Gauß)

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

Zum Beispiel ist:

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

Es gelten:

- i) $f = 0 \Leftrightarrow \forall_{p \in \mathcal{P}} : \nu_p(f) = \infty$
- ii) $f \in R[X] \Leftrightarrow \forall_{p \in \mathcal{P}} : \nu_p(f) \geq 0$
- iii) Lemma von Gauß: $\forall_{f,g \in Q[X]} : \nu_p(fg) = \nu_p(f) + \nu_p(g)$

Beweis

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

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

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:

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

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

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

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

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

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

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

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

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

□_{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 $p \in \mathcal{P}$

$$0 = \nu_p(h) \stackrel{(3.3)}{=} \underbrace{\nu_p(f)}_{\leq 0} + \underbrace{\nu_p(g)}_{\leq 0}$$

gilt, folgt:

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

Daher sind $f, g \in R[X]$.

□_{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 $\alpha|a_0$ 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 .

□_{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:

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

□_{3.6}

3.7 Proposition und Definition (primitiv)

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

- i) $\forall_{p \in \mathcal{P}} : \nu_p(f) = 0 \Leftrightarrow \text{ggT}(a_0, a_1, \dots) = 1$; In diesem Fall heißt f *primitiv*.

Also ist jedes normierte Polynom primitiv, aber auch $3X + 2 \in \mathbb{Z}[X]$.

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

Beweis

- i) Für alle $p \in \mathcal{P}$ gilt:

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

Wendet man

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

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

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

□_{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 $p \in \mathcal{P}$:

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

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

□_{3.7}

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 $\mathbb{Z}[X]$.

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

Beweis von 3.8

ii) \Rightarrow i):

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

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

Also folgt aus dem Isomorphiesatz:

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

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 $q \in R[X]$ 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 $p \in \mathcal{P}$:

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

Daher ist $v_p(h) \geq 0$ 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.

□ii) \Rightarrow i)

Zeige noch:

Jedes

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

(Nebenbemerkung: $R[X]^* = R^*$) ist ein Produkt von Primelementen obiger Gestalt.

Dann folgt sowohl, dass $R[X]$ faktoriell ist, als auch die Implikation i) \Rightarrow ii).

Schreibe $f = a \cdot \tilde{f}$ mit $a \in R$, $\tilde{f} \in R[X]$ primitiv (vergleiche 3.7 ii)). Weil R faktoriell ist, ist a ein Produkt von Primelementen obiger Gestalt, also sei ohne Einschränkung $f = \tilde{f} \in R[X]$ primitiv.

Schreibe in $Q[X]$ mit Primelementen $f_i \in Q[X]$ ($Q[X]$ ist ein Hauptidealring, also faktoriell.)

$$f = \prod_{i=1}^n f_i \stackrel{3.7i)}{=} a \cdot \prod_{i=1}^n \tilde{f}_i \quad (3.6)$$

mit $a \in Q^*$ und primitiven Primelementen $\tilde{f}_i \in R[X]$ in $Q[X]$.

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

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

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

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

Damit ist f ein Produkt von primitiven Faktoren, die Primelemente in $Q[X]$ sind.

□3.8

3.10 Beispiel und Definition (rationale Funktionen)

Sei k ein Körper. Dann heißt

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

der Körper der rationalen Funktionen (in einer Variablen X über k).

Die k -Algebra $k[X, Y] := (k[X])[Y]$ heißt der Polynomring in den Variablen X, Y (über k).

Wegen 3.8 ist $k[X, Y]$ faktoriell.

Behauptung

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

Beweis

Wegen 3.8 „Primelement \Leftrightarrow irreduzibel“ folgt mit $R := k[X]$ und weil $f \in R[Y]$ normiert vom Grad 2 ($f = Y^2 + X^3 \cdot Y^0$), also primitiv ist, dass $f \in R[X, Y]$ ein Primelement ist.

Dies ist äquivalent dazu, dass $f \in \text{Quot}(R)[Y] = k(X)[Y]$ 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:

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

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

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

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

□_{3.10}

4 Irreduzibilitätskriterien

Fixiere in Kapitel 4 (Irreduzibilitätskriterien)

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

4.1 Proposition (Äquivalenz von Primelement in R und Q)

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

- i) Es gibt ein $\alpha \in Q^*$, sodass $\tilde{f} := \alpha f \in R[X]$ primitiv ist.
- ii) Folgende Aussagen sind äquivalent:
 - a) $\tilde{f} \in R[X]$ ist ein Primelement.
 - b) $f \in Q[X]$ ist ein Primelement.

4.2 Bemerkung

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

Beweis von 4.1

- i) Die Aussage wurde bereits in 3.7 ii) bewiesen.
- ii) b) $\xLeftrightarrow{\alpha \in (Q[X])^*} \tilde{f} \in Q[X] \text{ ist ein Primelement} \xLeftrightarrow{3.8, a) \Leftrightarrow b)} \text{a)}$

□_{4.1}

4.3 Satz (Reduktionskriterium)

Seien

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

und $p \in R$ ein Primelement. Es gelte: $p \nmid a_d$ und $d > 0$.

Sei $\pi : R[X] \rightarrow \left(R/(p)\right)[X]$ wie in 3.2.

Ist dann $\pi(f) \in \left(R/(p)\right)[X]$ irreduzibel, so auch $f \in Q[X]$.

Ist f zusätzlich primitiv, so ist $f \in R[X]$ irreduzibel.

(„keine Reduktionshomomorphismen auf $Q[X]$ “!)

4.4 Beispiel

Wähle in 4.3 zum Beispiel:

i) $R = \mathbb{Z}, p = 3, f = 2X \in \mathbb{Z}[X]$

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

ii) $R = \mathbb{Z}, p = 2, f = 2X^2 + X \in \mathbb{Z}[X]$

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

iii) $R = \mathbb{Z}[Y], p = Y, f = 2 \in R[X]$

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

Beweis von 4.3

1. Fall: Sei f primitiv und $\pi(f)$ irreduzibel.

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

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

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

$$\deg(\pi(g)) = \deg(g) > 0 \quad \deg(\pi(h)) = \deg(h) > 0 \quad (4.1)$$

Es folgt in $\left(\frac{R}{(p)}\right)[X]$:

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

und wegen (4.1) gilt:

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

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

□_{1. Fall}

2. (allgemeiner) Fall: Sei nun $f \in R[X]$ mit $p \nmid a_d$ und $d > 0$ beliebig.

Dann gibt es ein $c \in R \setminus \{0\}$ und ein primitives Polynom $\tilde{f} \in R[X]$ mit:

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

Wegen $p \nmid a_d$ gilt $p \nmid c$ in R und $p \nmid \tilde{a}_d$, wobei \tilde{a}_d der höchste Koeffizient von \tilde{f} ist.

Dann gilt in $\left(\frac{R}{(p)}\right)[X]$:

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

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

Nach dem 1. Fall ist dann $\tilde{f} \in R[X]$ irreduzibel und mit 3.8 folgt, dass $\tilde{f} \in Q[X]$ irreduzibel ist.

Weil $c \in Q^* = (Q[X])^*$ ist, ist $f = c\tilde{f} \in Q[X]$ irreduzibel.

□_{4.3}

4.5 Korollar (Eisensteinkriterium)

Sei $p \in R$ ein Primelement und

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

ein primitives Polynom mit:

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

$$(0 \leq i \leq d-1)$$

Dann ist $f \in R[X]$ (und damit nach 3.8 auch $f \in Q[X]$) irreduzibel.

Beweis

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

$$g = \alpha_a X^a + \dots + \alpha_0$$

$$h = \beta_b X^b + \dots + \beta_0$$

$$\deg(g) > 0$$

$$\deg(h) > 0$$

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

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

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

$$\pi(g) = \alpha X^a$$

$$\pi(h) = \beta X^b$$

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

$$a = \deg(\pi(g)) > 0$$

$$b = \deg(\pi(h)) > 0$$

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

Es folgt in R :

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

Dies ist ein Widerspruch zur Voraussetzung $p^2 \nmid a_0$.

□_{4.5}

4.6 Beispiel

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

Beweis

$f(\alpha) = 0$ und f ist normiert.

Zeige noch: f ist in $\mathbb{Q}[X]$ irreduzibel.

Dies folgt sofort aus dem Eisensteinkriterium (Korollar 4.5) mit $R = \mathbb{Z}$ und $p = 2$.

Man sagt: „ f ist Eisenstein bezüglich 2.“

□_{i)}

ii) Seien k ein Körper und $n \in \mathbb{N}_{\geq 1}$.

Dann ist $f(X) := X^n - t \in k(t)[X]$ irreduzibel.

Beweis

$R := k[t]$ ist faktoriell mit $\text{Quot}(R) = k(t)$ und $p := t \in R$ ist ein Primelement.

Die Bedingungen in 4.5 sind erfüllt und f ist primitiv, da es normiert ist.

□_{ii)}

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

Dann gilt:

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

Beweis

f_p ist normiert und erfüllt:

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

Zeige noch, dass $f \in \mathbb{Q}[X]$ irreduzibel ist:

Es existiert genau ein \mathbb{Q} -Algebrenhomomorphismus $\sigma : \mathbb{Q}[X] \xrightarrow{\sim} \mathbb{Q}[X]$ mit $\sigma(X) = X + 1$ (und $\sigma^{-1}(X) = X - 1$) und σ ist ein Automorphismus.

Es genügt also zu zeigen, dass

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

irreduzibel ist.

Rechne:

$$\begin{aligned} g_p(X) &= f_p(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = \frac{1}{X} ((X^p + pX^{p-1} + \dots + pX + 1) - 1) = \\ &= X^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} X^{i-1} + p \in \mathbb{Z}[X] \end{aligned}$$

g_p ist daher normiert.

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

$$\forall_{1 \leq i \leq p-1} \quad p \mid \binom{p}{i}$$

Es gilt:

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

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

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

Insbesondere ist g_p also Eisenstein bezüglich p .

□_{iii)}

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

Beweis

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

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

Rechne:

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

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

□_{iv)}

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

Beweis

Schreibe:

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

Dann ist f primitiv, da bereits a_2 und a_0 in R teilerfremd sind.

$p := Y - 1 \in R$ ist ein Primelement und es gelten:

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

Die Behauptung folgt aus Korollar 4.5.

□_{v)}

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

Beweis

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

Reduktion modulo 2 liefert:

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

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

$$\bar{f} = (X + 1)(X^3 + X + 1) \in \mathbb{F}_2[X] \quad (4.3)$$

Beide Faktoren sind irreduzibel, da sie keine Nullstellen und $\text{Grad} \leq 3$ haben.

Also ist (4.3) die Primfaktorzerlegung von $\bar{f} \in \mathbb{F}_2[X]$.

Wäre nun $f \in \mathbb{Q}[X]$ reduzibel, so wäre wegen 3.8 auch $f \in \mathbb{Z}[X]$ reduzibel, also:

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

Da f keinen Linearfaktor in $\mathbb{Q}[X]$ besitzt, müsste $\deg(g) = \deg(h) = 2$ gelten.

Dann würde $\bar{f} = \bar{g} \cdot \bar{h}$ in $\mathbb{F}_2[X]$ mit $\deg(\bar{g}), \deg(\bar{h}) \leq 2$ folgen und weil $\deg(\bar{f}) = 4$ ist, also schon $\deg(\bar{g}) = \deg(\bar{h}) = 2$.

Wegen (4.3) besitzt aber $\bar{f} \in \mathbb{F}_2[X]$ bis auf Assoziiertheit genau die Teiler $\{1, X + 1, X^3 + X + 1, \bar{f}\}$, und keines dieser Polynome besitzt Grad 2. Dies ist ein Widerspruch zu der angenommenen Reduzibilität.

□_{vi)}

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

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

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

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 Ersetzen von X durch $X^{p^{r-1}}$:

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

Wegen $\zeta_{p^r}^{p^r} = 1$ aber $\zeta_{p^r}^{p^{r-1}} \neq 1$ folgt $F_{p^r}(\zeta_{p^r}) = 0$ und offenbar ist F_{p^r} normiert.

Zeige noch analog zu iii), dass $G_{p^r}(X) := F_{p^r}(X + 1) \in \mathbb{Z}[X]$ Eisenstein bezüglich p ist.

Mit $F_{p^r}(X)$ ist auch $G_{p^r}(X)$ normiert, und für den konstanten Term gilt:

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

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

$$G_{p^r}(X) \stackrel{\text{Def.}}{=} F_{p^r}(X + 1) \stackrel{(4.4)}{=} F_p((X + 1)^{p^{r-1}}) \stackrel{!}{=} F_p(X^{p^{r-1}} + 1) \stackrel{F_p(X+1) \equiv X^{p-1} \pmod{p}}{=} X^{(p^{r-1})(p-1)} \pmod{p}$$

□_{vii)}

4.7 Bemerkung

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

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

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

TODO: Abb 1

Beweis

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

Aus der Analysis folgt, dass der surjektive Homomorphismus

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

folgenden Kern hat:

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

Also gilt:

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

□_{4.7}

5 (Algebraische) Körpererweiterungen

5.1 Proposition und Definition (Charakteristik, Primkörper)

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

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

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

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

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

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

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

Beweis

- i) $\mathbb{Z}/(p) \hookrightarrow R$ ist ein Unterring, also ist $\mathbb{Z}/(p)$ ein Integritätsring, womit aus der linearen Algebra II schon $p = 0$ oder $p > 0$ ist eine Primzahl folgt.
- ii) Ist in i) $R = k$ ein Körper, so erhalte den Ringhomomorphismus:

TODO: Abb 2

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

$$\begin{aligned} p = 0 : Q &\cong \text{Quot}\left(\underbrace{\mathbb{Z}/(p)}_{\cong \mathbb{Z}}\right) \cong \mathbb{Q} \\ p > 0 : Q &\cong \text{Quot}\left(\underbrace{\mathbb{Z}/(p)}_{\cong \mathbb{F}_p}\right) \cong \mathbb{F}_p \end{aligned}$$

Es folgt $\text{char}(k) = \text{char}(E)$, denn $k \hookrightarrow E$ ist injektiv.

TODO: Abb Homsatz 5.1

5.2 Bemerkung und Definition (Körpererweiterung)

Für den Ringhomomorphismus von Integritätsringen $\mathbb{Z} \rightarrow \mathbb{F}_p$ gilt:

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

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

TODO: Abb 3

5.3 Proposition und Definition (Frobenius)

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

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

ii) Die Abbildung

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

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

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

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

Beweis

i) Die Aussage ist bekannt.

TODO: Woher?

ii) Klar sind

$$\text{Frob}_k(0) = 0 \quad \text{Frob}_k(1) = 1 \quad \text{Frob}_k(x \cdot y) = \text{Frob}_k(x) \cdot \text{Frob}_k(y)$$

und

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

folgt aus i) für $n = 1$.

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

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

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

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

Dies ist klar für $x = 0$ und für $x \in \mathbb{F}_p^*$ gilt $x^{p-1} = 1$ nach 1.26 ii).

„ \Rightarrow “: Nach Voraussetzung ist $\text{char}(k) = p$ und nach 5.1 folgt, dass $\mathbb{F}_p \subseteq k$ der Primkörper ist.

Für alle $x \in k$ folgt:

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

und das Polynom $T^p - T \in k[T]$ hat höchstens p Nullstellen in k .

Jedes $x \in \mathbb{F}_p \subseteq k$ ist aber eine Nullstelle nach Beweis von „ \Leftarrow “, also gilt $k = \mathbb{F}_p$.

□_{5.3}

5.4 Proposition und Definition (algebraisch, transzendent, Zwischenkörper)

Sei $E \supseteq k$ eine Körpererweiterung.

Dann ist E insbesondere eine k -Algebra und insbesondere ein k -Vektorraum.

Ein $\alpha \in E$ heißt genau dann *algebraisch über k* , wenn ein $f \in k[X] \setminus \{0\}$ existiert mit $f(\alpha) = 0$ in E , ansonsten heißt α *transzendent über k* .

Falls α algebraisch ist, ist $\text{Mipo}_k(\alpha) \in k[X]$ das eindeutige, normierte, irreduzible Polynom in $k[X]$, das α annulliert.

Ein Körper K mit $k \subseteq K \subseteq E$ heißt *Zwischenkörper (der Körpererweiterung $k \subseteq E$)*.

Beweis

TODO: Wo?

5.5 Definition (Grad)

Sei $E \supseteq k$ eine Körpererweiterung.

Dann heißt

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

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

5.6 (Grad-)Satz

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

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

Beweis

1. Fall: Es gelte:

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

Dann folgt als k -Vektorraum:

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

Damit ergibt sich:

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

Also gilt für die Dimension von E :

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

2. Fall: Ist $[E : k] = \infty$ (oder $[K : k] = \infty$), so existiert eine unendliche k -linear unabhängige Menge $X \subseteq E$ (oder $X \subseteq K \subseteq E$).

In beiden Fällen ist $X \subseteq E$ schon k -linear unabhängig und es folgt $[E : k] = \infty$.

□_{5.6}**5.7 Korollar**

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

Beweis

TODO: Einfügen

5.8 Beispiel (Verfahren von Kronecker)

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

Dann liefert die Komposition

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

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

Das Element $\alpha := \pi(X) = X + (f) \in E$ erfüllt in E :

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

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

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

Beachte

Es gibt zwei \mathbb{Q} -Algebrenhomomorphismen

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

nämlich:

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

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

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

Beweis

Jede endliche Erweiterung von \mathbb{Q} ist eine abzählbare Menge! \mathbb{R} ist jedoch überabzählbar.

Alternativ: Seien $n \in \mathbb{N}_{\geq 1}$ und $\alpha \in \mathbb{R}$ mit $\alpha^n = 2$.

Schreibe:

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

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

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

(vergleiche 4.6 i)) ist

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

ein Körper mit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ (vergleiche 5.8 i)).

Aus $\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{R}$ und 5.6 folgt $n \mid [\mathbb{R} : \mathbb{Q}]$.

Weil dabei $n \in \mathbb{N}_{\geq 1}$ beliebig groß gewählt werden kann, folgt $[\mathbb{R} : \mathbb{Q}] = \infty$.

□_{iv)}

5.9 Definition (algebraische Körpererweiterung)

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

5.10 Beispiel

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

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

Seien $E \supseteq k$ eine Körpererweiterung und $\alpha \in E$.

Dann erhält man eine k -Algebra $k \subseteq k[\alpha] \subseteq E$ und es gilt:

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

Damit folgt

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

und $[k(\alpha) : k] := [k[\alpha] : k]$ heißt *der Grad von α über k* .

Ist α transzendent über k , so ist der Einsetzungshomomorphismus

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

ein k -Algebrenisomorphismus.

Beweis

Übung.

TODO: Beweis ergänzen.

□_{5.11}

5.12 Satz

Jede endliche Körpererweiterung ist algebraisch.

Beweis

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

TODO: Beweis ergänzen

□_{5.12}

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

Sei k ein Körper.

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

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

den Polynomring in den Variablen X_1, \dots, X_n über k .

Dann ist für jede kommutative k -Algebra A die Abbildung von Mengen

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

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

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

Dann ist

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

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

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

$$k(\alpha_1, \dots, \alpha_n) := k(\{\alpha_1, \dots, \alpha_n\}) = \text{Quot}(k[\alpha_1, \dots, \alpha_n])$$

wobei

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

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

- iv) Eine Körpererweiterung $E \supseteq k$ heißt genau dann *endlich erzeugt*, wenn endlich viele $\alpha_1, \dots, \alpha_n \in E$ existieren mit $E = k(\alpha_1, \dots, \alpha_n)$.
- v) Eine Körpererweiterung $E \supseteq k$ heißt genau dann *einfach*, wenn ein $\alpha \in E$ existiert mit $E = k(\alpha)$.

Beweis

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

- ii) Übung.

TODO: Ergänzen

- iii) Übung.

TODO: Ergänzen

□_{5.13}

5.14 Satz

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

Dann gelten:

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

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

Beweis

Induktion über $n \geq 1$:

$n = 1$: Siehe 5.11.

$n > 1$: Nach Induktionsvoraussetzung ist $E' := k[\alpha_1, \dots, \alpha_{n-1}] \supseteq k$ eine endliche Körpererweiterung.

Da α_n algebraisch über k ist, ist es insbesondere algebraisch über E' und nach 5.11 ist $E'[\alpha_n] \supseteq E'$ eine endliche Körpererweiterung.

Mit 5.6 für $k \subseteq E' \subseteq E'[\alpha_n]$ folgt, dass $E'[\alpha_n] = k[\alpha_1, \dots, \alpha_n] \supseteq k$ eine endliche Körpererweiterung ist.

Insbesondere ist $k[\alpha_1, \dots, \alpha_n]$ ein Körper und somit $E = k(\alpha_1, \dots, \alpha_n) = k[\alpha_1, \dots, \alpha_n]$.

Es folgten i) und ii).

□_{5.14}**5.15 Beispiel**

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

Beweis

Nach Euler gilt:

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

Außerdem ist

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

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

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

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

□_{5.15}**Problem**

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

5.16 Proposition (endlich \Leftrightarrow endlich erzeugt und algebraisch)

Sei $E \supseteq k$ eine Körpererweiterung.

i) Es sind äquivalent:

- a) E/k ist endlich.
- b) E/k ist endlich erzeugt und algebraisch.

ii) Es sind äquivalent:

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

Beweis

- i) a) \Rightarrow b): Ist E/k endlich, so offenbar auch endlich erzeugt und nach 5.12 algebraisch.
 b) \Rightarrow a): Dies wurde in 5.14 ii) gezeigt.
- ii) a) \Rightarrow b): Wähle $X = E$.
 b) \Rightarrow a): $I := \{X' \mid X' \subseteq X \text{ ist endlich}\}$
 Damit folgt:

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

Seien nun $\alpha \in E$, dann gibt es ein $X' \in I$ mit $\alpha \in k(X')$.

Wegen 5.14 ist $k(X') \supseteq k$ endlich und nach 5.12 ist $\alpha \in k(X')$ algebraisch über k .

Weil dabei $\alpha \in E$ beliebig ist, folgt, dass E/k algebraisch ist.

□_{5.16}**5.17 Satz** (Transitivität der Algebraizität)

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

- i) Ist $\alpha \in E$ algebraisch über K und K/k algebraisch, dann ist α algebraisch über k .
 ii) Sind E/K und K/k algebraisch, so ist auch E/k algebraisch.

Beweis

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

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

Mit 5.14 ii) folgt:

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

Mit 5.6 folgt insgesamt:

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

Nach 5.12 ist dann α algebraisch über k .

□_{i)}

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

□_{5.17}

5.18 Beispiel

Es sind

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

Körpererweiterung.

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

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

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

6 Der algebraische Abschluss eines Körpers

6.1 Proposition und Definition (algebraisch abgeschlossen)

Für einen Körper k sind folgende Aussagen äquivalent:

- i) Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in k .
- ii) Jedes irreduzible $f \in k[X]$ ist linear.
- iii) Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ ist ein Produkt linearer Polynome.
- iv) Für alle algebraischen Körpererweiterungen E/k gilt $E = k$.

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

Beweis

i) \Rightarrow ii) \Rightarrow iii) sind klar, iii) \Rightarrow iv): Seien $\alpha \in E$ und $f := \text{Mipo}_k(\alpha)$.

Weil f irreduzibel ist, folgt aus iii) $\deg(f) = 1$, also $\alpha \in k$.

iv) \Rightarrow i): Sei $f \in k[X]$ mit $\deg(f) \geq 1$. Es existiert ein irreduzibles $g \in k[X]$ mit:

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

Nach 5.6 ist $E := k[X]/(g) \supseteq k$ eine endliche (und damit algebraische) Körpererweiterung, und nach 5.8 i) ist $\alpha := (X + (g)) \in E$ eine Nullstelle von g .

Nach iv) gilt $k = E$, also besitzt g und wegen (6.1) auch f , eine Nullstelle in k .

□_{6.1}

6.2 Proposition und Definition (Polynomring)

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

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

Dann heißt

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

der *Polynomring in den Variablen \mathfrak{X} über k* .

Er besitzt folgende universelle Eigenschaft:

Für jede kommutative k -Algebra A ist die Abbildung von Mengen

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

bijektiv.

Beweis

Wegen (6.2) ist die Abbildung

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

bijektiv, wobei $\varphi_{\mathfrak{X}'} \in \mathrm{Hom}_{k\text{-Alg.}}(k[\mathfrak{X}], A)$.

Wegen 5.13 ist folgende Abbildung bijektiv:

$$\mathrm{Hom}_{k\text{-Alg.}}(k[\mathfrak{X}], A) \xrightarrow{\sim} \left\{ (f_{\mathfrak{X}'})_{\mathfrak{X}' \subseteq \mathfrak{X} \text{ endl.}} \left| \begin{array}{c} f_{\mathfrak{X}'} : \mathfrak{X}' \rightarrow A; \\ \forall \mathfrak{X}' \subseteq \mathfrak{X}'' \subseteq \mathfrak{X} \text{ endl.} \\ f_{\mathfrak{X}''}|_{\mathfrak{X}'} = f_{\mathfrak{X}'} \end{array} \right. \right\} =: \Sigma$$

Es ist klar, dass die Abbildung

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

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.

□_{6.2}

6.3 Das Lemma von Zorn**6.3.1 Definition (geordnete Menge, obere Schranke)**

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

- i) $x \leq x$
- ii) $(x \leq y \wedge y \leq z) \Rightarrow (x \leq z)$
- iii) $(x \leq y \wedge y \leq x) \Rightarrow (x = y)$

(M, \leq) heißt genau dann *total geordnet*, wenn für alle $x, y \in M$ schon $x \leq y$ oder $y \leq x$ gilt.

$x \in M$ heißt genau dann *maximales Element*, wenn für alle $y \in M$ aus $x \leq y$ schon $x = y$.

Für eine Teilmenge $N \subseteq M$ heißt $x \in M$ genau dann *obere Schranke für N* , wenn für alle $y \in N$ schon $y \leq x$.

6.3.2 Beispiel

Seien R ein kommutativer Ring, $M := \{I \mid I \subsetneq R \text{ ist ein Ideal}\}$ und $I \leq J \Leftrightarrow I \subseteq J$.

Dann ist (M, \leq) teilweise geordnet, aber im Allgemeinen nicht total geordnet, zum Beispiel ist für $R = \mathbb{Z}$ schon $(2), (3) \in M$ und weder $(2) \leq (3)$ noch $(3) \leq (2)$.

6.3.3 Satz (Lemma von Zorn)

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

Dann besitzt M ein maximales Element.

(ohne Beweis)

Diese Aussage ist äquivalent zum Auswahlaxiom:

Sei $I \neq \emptyset$ eine Menge. Für alle $i \in I$ gilt:

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

6.3.4 Beispiel

Sei (M, \leq) wie in 6.3.2 für $R \neq \{0\}$.

Dann ist $\{0\} \in M$, also $M \neq \emptyset$.

Sei $N \subseteq M$ total geordnet.

Behauptung

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

Beweis

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

Also ist $J \subseteq R$ ein Ideal.

Wäre $J = R$, so würde $1 \in J = \bigcup_{I \in N} I$ folgen. Dann müsste ein $I \in N$ existieren mit $1 \in I$, also $I = R$ im Widerspruch zu $I \in M$, das heißt $I \subsetneq R$.

□ Behauptung

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

6.3.5 Satz (Existenz eines maximalen Ideals)

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

Beweis

Siehe 6.3.4.

□_{6.3}

6.4 Satz und Definition (algebraischer Abschluss)

Sei k ein Körper.

Dann existieren eine algebraische Körpererweiterung $\bar{k} \subseteq k$, die algebraisch abgeschlossen ist.

Jedes solches \bar{k} heißt *ein algebraischer Abschluss von k* .

Bemerkung

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

Beweis von 6.4 (EMIL ARTIN)

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

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

Behauptung

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

Beweis

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

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

Dabei ist $n \in \mathbb{N}_{\geq 1}$, $g_i \in k[\mathfrak{X}]$ und $f_i \in I$ geeignet.

Aus 5.8 i) induktiv angewendet auf alle irreduziblen Teiler von f_1, \dots, f_n folgt, dass es eine endliche Körpererweiterung $K \supseteq k$ und $\alpha_1, \dots, \alpha_n \in K$, sodass für alle $1 \leq i \leq n$ gilt:

$$f_i(\alpha_i) = 0 \quad (6.4)$$

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

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

gilt, und es folgt in K :

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

□_{6.4}

Wegen der Behauptung ist $k[\mathfrak{X}]/I \neq \{0\}$ und wegen 6.3.5 existiert ein maximales Ideal $\mathfrak{m} \subseteq k[\mathfrak{X}]/I$.

Erhalte eine Körpererweiterung $\alpha(k) \supseteq k$ als Komposition $k \hookrightarrow k[\mathfrak{X}] \twoheadrightarrow k[\mathfrak{X}]/I \twoheadrightarrow \underbrace{k[\mathfrak{X}]/I/\mathfrak{m}}_{=: \alpha(k)}$.

Zeige noch:

- i) $\alpha(k)/k$ ist algebraisch.
- ii) $\bar{k} := \bigcup_{n \geq 1} \alpha^n(k)$ ist algebraisch über k .
- iii) \bar{k}/k ist algebraisch abgeschlossen.

Beweis

i) Die k -Algebra $\alpha(k)$ wird durch die Bilder $\alpha_f \in \alpha(k)$ der X_f ($f \in I$) erzeugt.

Für jedes $f \in I$ gilt wegen $f(X_f) \in I$: $f(\alpha_f) = 0$ in $\alpha(k)$.

Teil i) folgt aus 5.16 ii) b) \Rightarrow a).

Nach Definition von I folgt auch: Jedes $f \in k[X]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in $\alpha(k)$.

□_{i)}

ii) Betrachte nun den Körperturm:

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

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

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

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

□_{ii)}

iii) Sei $f \in \bar{k}[X]$ nicht konstant.

Da f nur endlich viele Koeffizienten hat, folgt, dass ein $n \in \mathbb{N}_{\geq 0}$ existiert mit $f \in \alpha^n(k)[X]$.

Also hat f eine Nullstelle in $\alpha^{n+1}(k) \subseteq \bar{k}$. Damit folgt aus 6.1 i) die Behauptung.

□_{6.4}**6.5 Notation und Bemerkung**

Sei $z: K \rightarrow L$ ein Körperhomomorphismus.

Schreibe für alle $f = \sum_i a_i X^i \in k[X]$:

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

Dann gilt für alle $\alpha \in k$:

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

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

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

6.6 Lemma

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

Dann ist die Abbildung

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

wohldefiniert und bijektiv.

Insbesondere gilt:

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

TODO: Abb einfügen

Beweis

Die erste Aussage folgt aus der universellen Eigenschaft von $k \hookrightarrow k[X]$ und $k[X] \twoheadrightarrow k[X]/(f) \cong k(\alpha)$.

Die zweite Aussage folgt aus $\deg(f^\sigma) = \deg(f) = [k(\alpha) : k]$.

□_{6.6}

6.7 Satz und Definition (Fortsetzung)

Seien $k' \supseteq k$ eine algebraische Körpererweiterung und $\sigma : k \hookrightarrow L = \bar{L}$ eine Körpererweiterung und L algebraisch abgeschlossen.

Dann existiert ein k -Algebrenhomomorphismus $\sigma' : k' \rightarrow L$. Man nennt diesen eine *Fortsetzung von σ auf k'* .

Sind zusätzlich k' algebraisch abgeschlossen und L algebraisch über $\sigma(k) \subseteq L$, so ist jedes solche σ' ein Isomorphismus.

Beweis

Betrachte die Menge:

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

Wegen $(k, \sigma) \in M$ ist $M \neq \emptyset$.

Setze für alle $(K, \tau), (K', \tau') \in M$:

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

Dann ist (M, \leq) eine teilweise geordnete Menge und jede total geordnete Teilmenge besitzt eine obere Schranke in M , nämlich die Vereinigung aller Elemente der total geordneten Teilmenge.

Nach 6.3.3 existiert ein maximales Element in $(K, \sigma') \in M$.

Zeige nun $K = k'$:

Angenommen $K \subsetneq k'$.

Wähle $\alpha \in k' \setminus K$, dann besitzt das Minimalpolynom $\text{Mipo}_K(\alpha) \in K[X] \subseteq L[X]$ wegen $L = \bar{L}$ eine Nullstelle in L .

Nach 6.6 besitzt $\sigma' : K \hookrightarrow L$ eine Fortsetzung $\sigma'' : K(\alpha) \hookrightarrow L$.

Wegen $\sigma''|_k = \sigma'|_k$ ist $(K(\alpha), \sigma'') \in M$, was wegen $K \subsetneq K(\alpha)$ der Maximalität von $(K, \sigma) \in M$ widerspricht.

Damit ist $\sigma' : k \hookrightarrow L$ eine Fortsetzung von σ .

Seien nun zusätzlich k' algebraisch abgeschlossen und $L/\sigma(k)$ algebraisch.

Dann ist auch $L/\sigma'(k)$ algebraisch, da $\sigma'(k') \supseteq \sigma(k)$ ist.

Weil $\sigma'(k') \cong k'$ algebraisch abgeschlossen ist, folgt nach 5.9 iv) schon $L = \sigma'(k')$, das heißt $\sigma' : k' \twoheadrightarrow L$ ist surjektiv, also ein Isomorphismus.

□_{6.7}

6.8 Korollar

Seien k ein Körper und $\bar{k}_i \supseteq k$ (für $i \in \{1, 2\}$) algebraische Abschlüsse von k .

Dann existiert ein k -Algebrenhomomorphismus $\bar{k}_1 \xrightarrow{\sim} \bar{k}_2$ und jeder solche ist ein Isomorphismus.

Beweis

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

□_{6.8}

7 Zerfällungskörper

Fixiere in Kapitel 7 (Zerfällungskörper)

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

Definition (k -Homomorphismus)

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

7.1 Definition (Zerfällungskörper)

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

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

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

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

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

7.2 Beispiel

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

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

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

Mit 4.6 iii) folgt:

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

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

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

Also ist (7.1) die Primfaktorzerlegung von f in $E[X]$, denn:

$g \in E[X]$ ist irreduzibel, sonst gäbe es ein $\beta \in E$ mit $g(\beta) = 0$, woraus $\beta = \alpha = 0$ und der Widerspruch

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

folgt (siehe oben).

Insbesondere zerfällt f über E nicht in Linearfaktoren, das heißt E ist kein Zerfällungskörper von

7.3 Satz (Existenz und Eindeutigkeit von Zerfällungskörpern)

- i) Es existiert ein Zerfällungskörper $E \supseteq k$ von \mathcal{F} .
- ii) Seien $E_1 \supseteq k$, $E_2 \supseteq k$ Zerfällungskörper von \mathcal{F} und $\bar{\sigma} : E_1 \hookrightarrow \bar{E}_2$ ein k -Homomorphismus.
Dann gilt $\bar{\sigma}(E_1) = E_2$, also $\bar{\sigma} : (E_1 \xrightarrow{\sim} E_2 \hookrightarrow \bar{E}_2)$.
- iii) Sind $E_i \supseteq k$ Zerfällungskörper von \mathcal{F} ($i \in \{1, 2\}$), dann gibt es einen k -Isomorphismus:

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

Beweis

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

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

Wegen 6.1 i) ist dann E_i/k ein Zerfällungskörper von \mathcal{F} .

□_{i)}

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

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

für $i \in \{1, 2\}$:

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

Damit folgt:

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

Behauptung

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

Beweis

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

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

Daher ist $\bar{\sigma}(\alpha) \in \mathcal{N}_2$.

□ Behauptung

Dabei ist $f^{\bar{\sigma}} = f$, da $f \in k[X]$ und $\bar{\sigma}|_k = \text{id}_k$.

Es folgt:

$$k \subseteq \bar{\sigma}(E_1) \stackrel{(7.3)}{=} k(\bar{\sigma}(N_1)) \stackrel{(7.4)}{\subseteq} k(N_2) \stackrel{(7.2)}{=} E_2$$

Und da sowohl $\bar{\sigma}(E_1)/_k$, als auch $E_2/_k$ Zerfällungskörper von \mathcal{F} sind, gilt sogar $\bar{\sigma}(E_1) = E_2$.

□ ii)

iii) Nach 6.7 mit $k' := E_1$ und $L := \bar{E}_2$ existiert ein $\bar{\sigma}$ ($= \sigma$ in 6.7) wie in ii).

Nebenbemerkung: Ist $E/_k$ Zerfällungskörper, so ist $E/_k$ algebraisch.

□ 7.3

7.4 Satz und Definition (normale Körpererweiterung)

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

- i) Jeder k -Homomorphismus $\bar{\sigma} : E \rightarrow \bar{E}$ erfüllt $\bar{\sigma}(E) = E$.
- ii) Es existiert eine nicht-leere Teilmenge $\mathcal{F} \subseteq \{f \in k[X] \mid \deg(f) \geq 1\}$ so, dass $E/_k$ ein Zerfällungskörper von \mathcal{F} ist.
- iii) Für alle irreduziblen Polynome $f \in k[X]$ gilt:

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

In diesem Fall heißt $E/_k$ *normal*.

Beweis von 7.4

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

$$(\beta \in \bar{E} \wedge f(\beta) = 0) \Rightarrow \beta \in E$$

Weil f irreduzibel und ohne Einschränkung normiert ist, gilt:

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

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

Betrachte $k(\alpha) \xrightarrow{\sim} k(\beta) \subseteq E$:

TODO: Abb1

Es folgt:

$$\beta = \varphi(\alpha) \stackrel{(*)}{=} \bar{\sigma}(\alpha) \in \bar{\sigma}(E) \stackrel{i)}{=} E$$

□ i) \Rightarrow iii)

- 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. $f \in \mathcal{F} \stackrel{\text{Def.}}{\Rightarrow} \exists_{\alpha \in E} f(\alpha) = 0 \stackrel{\text{iii)}}{\Rightarrow} f$ zerfällt in Linearfaktoren über E .

□_{iii) \Rightarrow ii)}

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

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

□_{7.4}

7.5 Beispiel

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

7.6 Proposition (algebraischer Abschluss ist normal)

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

Beweis

Folgt aus 7.4 iii) und 6.1 iii).

□_{7.6}

7.7 Beispiel

- i) Sei $E \supseteq k$ eine Körpererweiterung mit $[E : k] = 2$. Dann ist E/k normal.
ii) Seien $E \supseteq K \supseteq k$ algebraische Körpererweiterungen mit E/k normal. Dann ist E/K normal (aber im Allgemeinen nicht K/k). ($k \subseteq E \subseteq \bar{k}$ (!))

Beweis

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

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

Der Fall $\deg(f) = 1$ ist trivial, denn dann ist $k(\alpha) = k$.

Sei $\deg(f) = 2$ und ohne Einschränkung f normiert:

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

Dann gilt in $E[X]$:

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

□_{i)}

ii) Klar nach 7.4 ii).

□_{7.7}

7.8 Beispiel (Normalität ist nicht-transitiv)

Betrachte den Körperturm:

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

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

Beide Erweiterungen sind vom Grad 2 (man nennt sie *quadratisch*) und insbesondere normal, aber E/k ist nicht normal. (vergleiche mit 5.17)

Beweis

$X^2 - 2, X^4 - 2 \in \mathbb{Q}[X]$ sind irreduzibel, da Eisenstein bezüglich 2, und aus dem Gradsatz folgt die erste Aussage.

Nun existieren $\alpha \in \mathbb{R}$ und $\beta \in \mathbb{C} \setminus \mathbb{R}$ mit $\alpha^4 = \beta^4 = 2$. Erhalte \mathbb{Q} -Homomorphismen:

$$\begin{aligned} i : \mathbb{Q}[\sqrt[4]{2}] &\hookrightarrow \mathbb{R}, \sqrt[4]{2} \mapsto \alpha \\ j : \mathbb{Q}[\sqrt[4]{2}] &\hookrightarrow \mathbb{C}, \sqrt[4]{2} \mapsto \beta \end{aligned}$$

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.

□_{7.8}

7.9 Definition (normale Hülle)

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

- i) E'/k ist normal.
- ii) Ist $E \subseteq K \subseteq E'$ ein Zerfällungskörper mit K/k normal, so folgt $K = E'$.

7.10 Satz und Definition (Konjugierte)

Sei $E \supseteq k$ eine algebraische Körpererweiterung.

- i) Es existiert eine bis auf Isomorphie eindeutige normale Hülle E'/k von E/k .
- ii) $[E : k] < \infty \Rightarrow [E' : k] < \infty$
- iii) Ist $k \subseteq E \subseteq L$ ein Körperturm und L/k normal (zum Beispiel $L = \bar{k}$, 7.6), so ist

$$E' = k(\sigma(E) \mid \sigma : E \rightarrow L \text{ ist } k\text{-Homomorphismus})$$

eine normale Hülle von E/k , die *normale Hülle von E in L/k* .

Die Zerfällungskörper von $k \subseteq \sigma(E) \subseteq L$ heißen die *Konjugierten von E in L* .

Beweis

- i) Ein Zerfällungskörper E' von $\mathcal{F} := \{f \in k[X] \mid \deg(f) \geq 1 \text{ und } \exists_{\alpha \in E} f(\alpha) = 0\}$ über k leistet das Gewünschte. (vergleiche 7.3)
- ii) Dann kann in i) $|\mathcal{F}| < \infty$ gewählt werden und aus 5.16 i) b) \Rightarrow a) folgt $[E' : k] < \infty$.
- iii) Übung (mit 6.6).

□_{7.10}

7.11 Beispiel

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

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

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

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

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

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

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

TODO: Abb 2

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

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

(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

$$k[X] \rightarrow k[X]$$

$$f = \sum_{i=0} a_i X^i \mapsto f' := \sum_{i=1} i \cdot a_i X^{i-1}$$

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 $f = X^m, g = X^n$ für $n, m \geq 0$ angenommen werden.)

TODO: Rechnung einfügen

□_{8.1}

8.2 Beispiel

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

Beweis

Übung

TODO: Beweis einfügen

□_{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:

$$f(X) = (X - \alpha)^r \cdot g(X) \quad (1) \quad (8.1)$$

mit $g(\alpha) \neq 0$ und $r \geq 1$, da $f(\alpha) = 0$.

Hierbei heißt r die *Vielfachheit der Nullstelle* α und α heißt genau dann *mehrfache Nullstelle*, wenn $r \geq 2$ ist, sonst *einfache Nullstelle*.

Zeige also:

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

Rechne:

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

Wegen $r \geq 1$ folgt:

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

□_{8.3}

8.4 Lemma

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

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

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

ii) Ist f irreduzibel, so sind äquivalent:

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

Beweis

i) Wegen $f \in k[X] \setminus \{0\} \subseteq \bar{k}[X] \setminus \{0\}$ folgt a) \Leftrightarrow b) aus 8.3. Dann gilt:

$$\text{b) } \Leftrightarrow (X - \alpha) \mid f, f' \text{ in } \bar{k}[X] \Leftrightarrow (X - \alpha) \mid \text{ggT}(f, f') \text{ in } \bar{k}[X] \Leftrightarrow \text{ggT}(f, f')(\alpha) = 0 \Leftrightarrow \text{c)}$$

□_{i)}

ii) a) \Rightarrow b):

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

$$f = \text{Mipo}_k(\alpha) \quad (8.2)$$

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 \bar{k} algebraisch abgeschlossen und f nicht konstant ist, existiert ein $\alpha \in \bar{k}$ mit $f(\alpha) = 0$.

Wegen $f'(\alpha) = 0$ ($\alpha = 0$ und i) b) \Rightarrow a) ist α eine mehrfache Nullstelle von f .

□_{8.4}

8.5 Definition (separables Polynom)

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

8.6 Proposition

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

Beweis

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

□_{8.6}

8.7 Beispiel

Sei $k := \mathbb{F}_p(t)$ und $f(X) = X^p - t \in k[X]$.

Dann ist f irreduzibel nach 4.6 iii).

In $k[X]$ gilt:

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

Also ist f nach 8.4 ii) nicht separabel, genauer gilt:

Setze $k \subseteq E := k(\alpha)$ mit $0 = f(\alpha) = \alpha^p - t$.

Dann gilt in $E[X]$:

$$f(X) = X^p - t = X^p - \alpha^p = (X - \alpha)^p$$

Damit ist E/k ein Zerfällungskörper von f und es folgt:

$$\text{Hom}_{k\text{-Alg.}}(E, \bar{k}) \underset{6.6}{\cong} \{\beta \in \bar{k} \mid \beta^p = t\} \stackrel{5.4}{=} \{\alpha\}$$

Denn aus $\beta \in \bar{k}$ 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 \bar{k} , das heißt $\alpha = \beta$.

Insbesondere folgt:

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

(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 $\text{Mipo}_k(\alpha)$ in $k[X]$ separabel ist.
- ii) E/k heißt *separabel über k* , wenn jedes $\alpha \in E$ separabel ist.

8.9 Definition (vollkommener Körper)

k heißt *vollkommen*, wenn jede algebraische Körpererweiterung von k separabel ist.

8.10 Beispiel

- i) Jeder Körper der Charakteristik 0 ist vollkommen. (folgt aus 8.6)
- ii) $\mathbb{F}_p(t)$ ist nicht vollkommen, denn nach 8.7 ist $\alpha \in \overline{\mathbb{F}_p}(t)$ mit $\alpha^p = t$ nicht separabel über $\mathbb{F}_p(t)$.
- iii) Jeder endliche Körper ist vollkommen.

8.11 Definition (Separabilitätsgrad)

Sei $E \supseteq k$ eine algebraische Körpererweiterung, so heißt

$$[E : h]_S := |\text{Hom}_{k\text{-Alg.}}(E, \bar{k})| \in \mathbb{N} \cup \{\infty\}$$

der *Separabilitätsgrad* von E/k .

8.12 Satz (vollkommene Körper)

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

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

- ii) Jeder endliche Körper ist vollkommen.

Beweis

- i) „ \Rightarrow “: Zeige, dass $\text{Frob}_k : k \rightarrow k$ surjektiv ist.

Sei $\alpha \in k$ und E/k der Zerfällungskörper von $f(X) = X^p - \alpha \in k[X]$.

In $E[X]$ gilt $f(X) = (X - \beta)^p$ für ein geeignetes $\beta \in E$.

Vergleiche 8.7 für $g = \text{Mipo}_k(\beta)$ mit $g|f$.

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

Daher ist Frob_k schon ein Isomorphismus, da er als Körperhomomorphismus schon injektiv ist.

„ \Leftarrow “: Sonst existiert ein irreduzibles und nicht separables $f \in k[X]$, woraus mit 8.4 ii) schon $f' = 0$ in $k[X]$ folgt und sich aus 8.2 schon $f(X) = g(X^p)$ mit einem geeigneten $g = \sum a_i X^i \in k[X]$ ergibt.

Weil Frob_k surjektiv ist, folgt $a_i = b_i^p$ für geeignete $b_i \in k$. Es folgt in $k[X]$:

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

□_{i)}

Dies ist wegen $p \geq 2$ ein Widerspruch dazu, dass f irreduzibel ist.

ii) Dies folgt aus i) und 5.3 iii).

□_{8.12}

8.13 Lemma

Sei $E =: k(\alpha) \supseteq k$ eine einfache algebraische Körpererweiterung.

- i) $[k(\alpha) : k]_S = |\{\beta \in \bar{k} \mid \text{Mipo}_k(\alpha)(\beta) = 0\}|$ (Anzahl der Nullstellen des Minimalpolynoms)
- ii) α ist genau dann separabel über k , wenn $[k(\alpha) : k] = [k(\alpha) : k]_S$.

Beweis

- i) $[k(\alpha) : k]_S \stackrel{8.11}{=} |\text{Hom}_{k\text{-Alg.}}(k(\alpha), k)| \stackrel{6.6}{=} |\{\beta \in \bar{k} \mid \text{Mipo}_k(\alpha)(\beta) = 0\}|$
- ii) $f := \text{Mipo}_k(\alpha) \in k[X]$ zerfällt über k in Linearfaktoren, also gilt:

$$[k(\alpha) : k] = \deg(f) \geq |\{\beta \in \bar{k} \mid f(\beta) = 0\}| = [k(\alpha) : k]_S$$

Zudem gilt Gleichheit genau dann, wenn alle Nullstellen in \bar{k} einfach sind, also f separabel ist.

□_{8.13}

8.14 Satz (Separabilitäts-Gradsatz)

Seien $E \supseteq K \supseteq k$ algebraische Körpererweiterungen, dann gilt:

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

Beweis

Sei $\bar{k} \supseteq E$ ein algebraischer Abschluss.

Weil E/K und K/k algebraisch sind, sind \bar{k}/K und \bar{k}/k algebraische Abschlüsse und nach Definition gilt:

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

Für jedes $\sigma \in \text{Hom}_{k\text{-Alg.}}(K, \bar{k})$ existiert nach 6.7 ein k -Isomorphismus $\bar{\sigma} : \bar{k} \rightarrow \bar{k}$ mit:

$$\bar{\sigma}|_K = \sigma \tag{8.3}$$

Es ist nun klar, dass 8.14 aus folgender Behauptung folgt:

Behauptung: Die Abbildung

$$\text{Hom}_{K\text{-Alg.}}(E, \bar{k}) \times \text{Hom}_{k\text{-Alg.}}(K, \bar{k}) \rightarrow \text{Hom}_{k\text{-Alg.}}(E, \bar{k}), (\tau, \sigma) \mapsto \bar{\sigma} \circ \tau$$

ist wohldefiniert und bijektiv.

Beweis: Die Abbildung ist wohldefiniert, da τ ein k -Homomorphismus ist.

Injektivität: Gelte:

$$\bar{\sigma}_1 \circ \tau_1 = \bar{\sigma}_2 \circ \tau_2 \quad (8.4)$$

Dabei sind $\sigma_i \in \text{Hom}_{k\text{-Alg.}}(k, \bar{k})$, $\tau_i \in \text{Hom}_{k\text{-Alg.}}(E, \bar{k})$ und $i \in \{1, 2\}$.

Damit folgt:

$$\begin{array}{ccc} (\bar{\sigma}_1 \circ \tau_1)|_k & = & (\bar{\sigma}_2 \circ \tau_2)|_k \\ \parallel & & \parallel \\ \bar{\sigma}_1|_k & & \bar{\sigma}_2|_k \\ \parallel & & \parallel \\ \sigma_1 & = & \sigma_2 \end{array}$$

Damit folgt $\sigma_1 = \sigma_2$, also $\bar{\sigma}_1 = \bar{\sigma}_2$ und mit (8.4) ergibt sich $\tau_1 = \tau_2$.

□_{injektiv}

Surjektivität: Sei $\alpha \in \text{Hom}_{k\text{-Alg.}}(E, \bar{k})$, $\sigma := \alpha|_K \in \text{Hom}_{k\text{-Alg.}}(K, \bar{k})$ und $(\bar{\sigma}^{-1} \circ \alpha)|_K = \text{id}$.

Also gilt $\tau = \bar{\sigma}^{-1} \circ \alpha \in \text{Hom}_{k\text{-Alg.}}(E, \bar{k})$. Es folgt:

$$\bar{\sigma} \circ \tau = \bar{\sigma} \circ (\bar{\sigma}^{-1} \circ \alpha) = \alpha$$

□_{8.14}

8.15 Satz

Für eine endliche Körpererweiterung $E \supseteq k$ sind äquivalent:

- i) E/k ist separabel.
- ii) Es gibt $\alpha_1, \dots, \alpha_n \in E$, die separabel über k sind mit:

$$E = k(\alpha_1, \dots, \alpha_n)$$

- iii) $[E : k]_S = [E : k]$

Beweis

i) \Rightarrow ii) ist trivial.

ii) \Rightarrow iii): Wegen den Gradsätzen 8.14 und 5.6 kann man durch Induktion $n = 1$ annehmen und dann folgt die Behauptung aus 8.13 ii) „ \Rightarrow “.

iii) \Rightarrow i): Sei $\alpha \in E$ beliebig. Da E endlich ist, ist es insbesondere endlich erzeugt, also $E = k(\alpha_1 := \alpha, \dots, \alpha_n)$.

Sei $K_m := k(\alpha_1, \dots, \alpha_m)$, also $K_n = E$ und $K_0 = k$.

Dann gilt wegen den Gradsätzen 8.14 und 5.6:

$$\begin{array}{ccc} [E : k] & = & \prod_{m=1}^n [K_m : K_{m-1}] \\ \parallel & & \vee \\ [E : k]_S & = & \prod_{m=1}^n [K_m : K_{m-1}]_S \end{array}$$

Daher folgt schon:

$$[K_m : K_{m-1}] = [K_m : K_{m-1}]_S$$

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

Es folgt insbesondere:

$$[K_1 = k(\alpha) : K_0 = k]_S = [K_1 = k(\alpha) : K_0 = k]$$

Also ist α separabel über k (nach 8.13 iii) „ \Leftarrow “).

□_{8.15}

8.16 Korollar (Transitivität der Separabilität)

Für eine algebraische Körpererweiterung $E \supseteq K \supseteq k$ sind äquivalent:

- i) E/k ist separabel.
- ii) E/K und K/k sind separabel.

Beweis

i) \Rightarrow ii): K/k separabel ist trivial.

Sei $\alpha \in E$, dann folgt $\text{Mipo}_K(\alpha) | \text{Mipo}_k(\alpha)$, also ist mit $\text{Mipo}_k(\alpha)$ auch $\text{Mipo}_K(\alpha)$ separabel, das heißt α ist separabel über K .

ii) \Rightarrow i): Sei $\alpha \in E$, $f := \text{Mipo}_K(\alpha) = \sum_{i=0}^n a_i X^i \in K[X]$ und $K' := k(a_i | 0 \leq i \leq n) \subseteq K$.

Dann folgt:

1. K'/k ist endlich und separabel (8.15 ii) \Rightarrow i)).
2. $f \in K'[X]$ ist separabel (da E/k separabel ist).

Es folgt:

$$\begin{aligned} \infty &\stackrel{1.}{>} [K'(\alpha) : k] \stackrel{5.6}{=} [K'(\alpha) : K'] \cdot [K' : k] \stackrel{1., 2.}{=}_{8.15 \text{ i) } \Leftrightarrow \text{ ii)}} [K'(\alpha) : K']_S \cdot [K' : k]_S = \\ &\stackrel{8.14}{=} [K'(\alpha) : k]_S \end{aligned}$$

Daher ist $K'(\alpha)/k$ separabel, also α separabel über k .

□_{8.16}

8.17 Satz (vom primitiven Element) und Definition

Sei $k \subseteq E = k(\alpha_1, \dots, \alpha_n)$ eine endliche Körpererweiterung und seien $\alpha_2, \dots, \alpha_n$ 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 $k := \text{Frob}_E(E) \subseteq E$, dann ist $[E : k] = p^2$ und E/k ist nicht einfach (ohne Beweis).

TODO: Beweis einfügen

Beweis von 8.17

1. Fall: k ist endlich, also ist E endlich und nach 1.30 i) existiert ein $\alpha \in E^*$ mit $E^* = \langle \alpha \rangle$, womit sich sofort $E = k(\alpha)$ ergibt.
2. Fall: k ist unendlich. Induktiv kann man $n = 2$ annehmen.
Schreibe $\text{Hom}_{k\text{-Alg.}}(E, \bar{k}) = \{\sigma_1, \dots, \sigma_n\}$, das heißt $n := [E : k]_S$.
Setze:

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

Behauptung

In $\bar{k}[X]$ gilt:

$$P(X) \neq 0$$

Beweis:

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

□Behauptung

Weil $P(X) \neq 0$ und k unendlich ist, gibt es ein $\beta \in k$ mit $P(\beta) \neq 0$.

Darum folgt, dass für $\alpha := \alpha_1 + \beta\alpha_2 \in E$ die Elemente $\sigma(\alpha_1), \dots, \sigma(\alpha_1) \in \bar{k}$ paarweise verschieden sind, denn:

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

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

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

Da die $\sigma_i|_{E'} \in \text{Hom}_{k\text{-Alg.}}(E', \bar{k})$ paarweise verschieden sind.

Wegen $E' \subseteq E$ folgt:

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

□Behauptung

Behauptung

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

Beweis

Weil α_2 separabel über k ist, folgt mit 8.15:

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

Und damit folgt:

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

Ferner gilt:

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

Daraus folgt $[E'(\alpha_2) : E'] = 1$, also $\alpha_2 \in E'$.

Wegen $\alpha_1 = \alpha - \beta\alpha_2$ folgt damit auch $\alpha_1 \in E'$ und insgesamt:

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

Also ist $E = E'$.

□_{8.17}

9 Endliche Körper

9.1 Lemma

Sei k ein endlicher Körper. Dann gelten:

- i) $p := \text{char}(k) > 0$ und $\mathbb{F}_p \subseteq k$ ist der Primkörper.
- ii) $n := \dim_{\mathbb{F}_p}(k) < \infty$ und $|k| = p^n$.
- iii) k ist der Zerfällungskörper von

$$X^{(p^n)} - X \in \mathbb{F}_p[X]$$

über \mathbb{F}_p .

Beweis

- i) Andernfalls müsste $\text{char}(k) = 0$ gelten, also $\mathbb{Q} \subseteq k$ im Widerspruch zu $|k| < \infty$. (vergleiche 5.1)

□_{i)}

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

□_{ii)}

- iii) **Behauptung**

$$X^{(p^n)} - X = \prod_{\alpha \in k} (X - \alpha) \quad (9.1)$$

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 $G = k^*$):

$$\alpha^{p^n-1} = 1 \quad \Rightarrow \quad \alpha^{p^n} = \alpha$$

□_{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

Die Eindeutigkeit folgt aus 9.1 iii) und 7.3.

Sei $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ ein algebraischer Abschluss.

Behauptung

$\mathbb{F}_{p^n} := \{ \alpha \in \overline{\mathbb{F}}_p \mid \alpha^{p^n} = \alpha \} \subseteq \overline{\mathbb{F}}_p$ ist ein Teilkörper.

Beweis

$\text{Frob}_{\overline{\mathbb{F}}_p}^n = \underbrace{\text{Frob}_{\overline{\mathbb{F}}_p} \circ \dots \circ \text{Frob}_{\overline{\mathbb{F}}_p}}_{n\text{-mal}} : \overline{\mathbb{F}}_p \rightarrow \overline{\mathbb{F}}_p$ ist ein Körperisomorphismus mit:

$$\tilde{\mathbb{F}}_{p^n} = \{ \alpha \in \overline{\mathbb{F}}_p \mid \text{Frob}_{\overline{\mathbb{F}}_p}^n(\alpha) = \alpha \}$$

Daraus folgt die Behauptung.

□ Behauptung

Es ist klar, dass $\tilde{\mathbb{F}}_{p^n}$ ein Zerfällungskörper von $X^{p^n} - X \in \mathbb{F}_p[X]$ ist.

Wegen $(X^{p^n} - X)' = -1$ und 8.3 ist $X^{p^n} - X \in \mathbb{F}_p[X]$ separabel, und es folgt $|\tilde{\mathbb{F}}_{p^n}| = p^n$.

□ 9.2

9.3 Bemerkung

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

Schreibe daher auch $\mathbb{F}_{p^n} = \tilde{\mathbb{F}}_{p^n}$ und fasse im Folgenden alle \mathbb{F}_{p^n} als Teilkörper eines festen algebraischen Abschlusses $\overline{\mathbb{F}}_p$ auf:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_{p^n}$$

9.4 Korollar

Für alle $n, m \geq 1$ gilt: $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n|m$.

Beweis

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

$$\alpha^{p^m} = \text{Frob}_{\mathbb{F}_p}^{nx}(\alpha) = \underbrace{\text{Frob}_{\mathbb{F}_p}^n(\alpha) \circ \dots \circ \text{Frob}_{\mathbb{F}_p}^n(\alpha)}_{x\text{-mal}} \stackrel{\alpha^{p^n} = \alpha}{=} \alpha$$

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

„ \Rightarrow “: Aus

$$m = [\mathbb{F}_{p^m} : \mathbb{F}_p] \stackrel{\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}}{=} \underbrace{[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]}_{\in \mathbb{N}} \cdot \underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{=n}$$

folgt $n|m$.

□_{9.4}**9.5 Satz und Definition (relativer Frobenius)**

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

- i) $F_q := \text{Frob}_{\mathbb{F}_p}^n \in \text{Aut}_{\mathbb{F}_q}(\overline{\mathbb{F}_p}, \overline{\mathbb{F}_p})$ heißt *der relative Frobenius über \mathbb{F}_q* .
- ii) Die Gruppe $\text{Aut}_{\mathbb{F}_q\text{-Alg.}}(\mathbb{F}_{q'}, \mathbb{F}_{q'})$ 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 $F_q|_{\mathbb{F}_q} = \text{id}$.

Ist $\alpha \in \mathbb{F}_q$ so folgt $F_q(\alpha) = \alpha^q \stackrel{9.2}{=} \alpha$

□_{i)}

- ii) Es gilt:

$$\begin{aligned} |\text{Aut}_{\mathbb{F}_q\text{-Alg.}}(\mathbb{F}_{q'}, \mathbb{F}_{q'})| &\stackrel{(\text{Übung})}{=} |\text{Hom}_{\mathbb{F}_q\text{-Alg.}}(\mathbb{F}_{q'}, \mathbb{F}_{q'})| \stackrel{\mathbb{F}_{q'}/\mathbb{F}_q \text{ normal}}{=} |\text{Hom}_{\mathbb{F}_q\text{-Alg.}}(\mathbb{F}_{q'}, \overline{\mathbb{F}_p})| = \\ &\stackrel{\text{Def.}}{=} [\mathbb{F}_{q'} : \mathbb{F}_q]_S \stackrel{8.12 \text{ ii)}}{=} [\mathbb{F}_{q'} : \mathbb{F}_q] = \frac{m}{n} =: k \end{aligned}$$

TODO: Übung beweisen

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

Zeige noch: $\text{ord}(\sigma) = k$.

Zunächst ist $\sigma^k = F_q^k = F_{q'} = \text{id}_{\mathbb{F}_{q'}}$ klar.

Wäre nun $a := \text{ord}(\sigma) < k$, so wäre $\sigma^a = F_q^a = \text{id}_{\mathbb{F}'_q}$, dass heißt für alle $\alpha \in \mathbb{F}_{q'}$ würde gelten:

$$\alpha = \sigma^a(\alpha) = \alpha^{q^a} = \alpha^{p^{n \cdot a}}$$

Es gilt aber:

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

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

□_{9.5}

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

$$\mathrm{Gal}(E/k) := \mathrm{Aut}_{k\text{-Alg.}}(E) \stackrel{\text{Blatt 8 Aufgabe 2}}{=} \mathrm{Hom}_{k\text{-Alg.}}(E, E)$$

die *Galoisgruppe* von E/k .

TODO: Beweis von Blatt 8 Aufgabe 2 einfügen

10.2 Beispiel und Definition (Galoisgruppe von f)

i) Für eine endliche Körpererweiterung $E \supseteq k$ sind äquivalent:

- a) E/k ist galoissch.
- b) E/k ist ein Zerfällungskörper eines separablen Polynoms $f \in k[X]$.

In diesem Fall kann f in b) irreduzibel gewählt werden und $\mathrm{Gal}(E/k) =: \mathrm{Gal}(f)$ 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:

$\mathrm{Gal}(E/k)$ ist zyklisch mit Ordnung $[E : k]$ und wird von $F_q|_E$ erzeugt, also $\mathrm{Gal}(E/k) = \langle F_q|_E \rangle$.

Beweis

i) a) \Rightarrow b): 8.17 impliziert:

$$\exists_{\alpha \in E} : E = k(\alpha)$$

Weil E/k normal ist, folgt aus 7.4 iii), dass E/k ein Zerfällungskörper von

$$f := \mathrm{Mipo}(\alpha) \in k[X]$$

und f separabel und irreduzibel ist.

b) \Rightarrow a): 7.4 ii) impliziert, dass E/k normal ist.

Weil $f \in k[X]$ separabel ist, folgt mit 7.10 iii) und 8.15 i) \Rightarrow ii), dass E/k separabel ist.

Zusammen bedeutet das, dass E/k galoissch ist.

□_{i)}

ii) Folgt aus 9.1 iii), 8.12 ii) und 9.5 ii).

□_{10.2}

10.3 Proposition

Seien $E \supseteq K \supseteq k$ Körpererweiterungen und E/k galoissch.

Dann gelten:

i) E/K ist galoissch und

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

ist eine Untergruppe.

ii) Ist zusätzlich K/k galoissch, dann ist die Abbildung

$$\begin{aligned} \pi : \text{Gal}(E/k) &\rightarrow \text{Gal}(K/k) \\ \sigma &\mapsto \sigma|_K \end{aligned}$$

wohldefiniert und ein surjektiver Gruppenhomomorphismus mit:

$$\ker(\pi) = \text{Gal}(E/K) \trianglelefteq \text{Gal}(E/k)$$

Beweis

i) Wegen 7.7 ii) und 8.16 i) \Rightarrow ii) ist E/K galoissch.

Der Rest ist klar.

□_{i)}

ii) π ist, weil K/k normal ist, und wegen 7.4 i) wohldefiniert, das heißt für alle $\sigma \in \text{Gal}(E/k)$ ist

$$\sigma(K) \subseteq K$$

und daher ist $\sigma|_K \in \text{Gal}(K/k)$.

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).

□_{10.3}

10.4 Proposition

Sei $E \supseteq k$ eine endliche normale Körpererweiterung.

Dann gelten:

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

$$\text{ii) } |\text{Aut}_k(E)| = [E : k] \Leftrightarrow E/k \text{ ist galoissch.}$$

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

$$G \subseteq \text{Aut}(E) := \left\{ \varphi : E \xrightarrow{\sim} E \mid \varphi \text{ ist ein Körperisomorphismus} \right\}$$

eine Untergruppe. Dann gelten:

- i) $k := E^G := \{ \alpha \in E \mid \forall \sigma \in G : \sigma(\alpha) = \alpha \}$ ist ein Teilkörper und heißt *der Fixkörper von E unter G* .
- ii) Aus $|G| < \infty$ folgt, dass E/k galoissch ist und dass gelten:
 - Mit $\text{Aut}_k(E)$ definiert als die Gruppe der Automorphismen von E , die auf k die Identität sind, gilt:

$$\text{Aut}_k(E) = \text{Gal}(E/k) = G \subseteq \text{Aut}(E)$$

$$– [E : k] = |G|$$

- iii) Ist E/k algebraisch (aber nicht notwendigerweise $|G| < \infty$, beziehungsweise G endlich), so ist E/k galoissch und $G \subseteq \text{Gal}(E/k)$ ist eine Untergruppe.

Beweis

i) ist klar.

ii) und iii): Zeige zunächst, dass E/k separabel ist:

Sei $\alpha \in E$ und $G\alpha := \{ \sigma(\alpha) \mid \sigma \in G \} \subseteq E$.

Dann gilt für alle $\sigma \in G$:

$$\text{Mipo}_k(\alpha)(\sigma(\alpha)) = \underbrace{(\text{Mipo}_k(\alpha))^\sigma}_{\in k[X] = E^G[X]}(\alpha) = \text{Mipo}_k(\alpha)(\alpha) = 0$$

Damit folgt $|G\alpha| \leq \deg(\text{Mipo}_k(\alpha)) < \infty$ und

$$f(X) := \prod_{\beta \in G\alpha} (X - \beta) \in E[X]$$

ist ein separables Polynom mit $f(\alpha) = 0$, da $\alpha \in G\alpha$ ist.

Zeige noch, dass $f \in k[X]$ ist, denn dann ist α separabel über k :

Weil die Abbildung

$$\begin{aligned} \sigma : G\alpha &\rightarrow G\alpha \\ \beta &\mapsto \sigma(\beta) \end{aligned}$$

bijektiv mit der Umkehrabbildung σ^{-1} ist, gilt für alle $\sigma \in G$:

$$f^\sigma(X) = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\beta \in G\alpha} (X - \beta) = f(X)$$

Daher hat $f \in E[X]$ Koeffizienten in $E^G = k$.

□_{separabel}

Zeige nun, dass E/k normal ist:

E/k ist ein Zerfällungskörper aller obigen Polynome $f \in k[X]$ (für $\alpha \in E$ variabel).

□_{normal}

Insgesamt ist also E/k galoissch.

Es ist klar, dass

$$G \subseteq \text{Gal}(E/k)$$

eine Untergruppe ist.

Sei nun $n := |G| < \infty$.

Dann folgt aus

$$\deg(f) = |G\alpha| \leq |G| = n$$

für alle $\alpha \in E$:

$$[k(\alpha) : k] \leq n$$

Wegen 8.17 angewendet auf die endlichen Zwischenkörper von E/k folgt damit:

$$[E : k] \leq n$$

Dies ist klar, wenn $E \supseteq k$ endlich ist, da dann E insbesondere ein endlicher Zwischenkörper $k(\alpha)$ ist.

Wäre E nicht endlich, so gäbe es für jedes $m \in \mathbb{N}$ einen Zwischenkörper $k \subseteq K = k(\alpha) \subseteq E$ mit $[E : K] > m$, denn E ist das Kompositum aller endlichen Zwischenkörper. Dies ist ein Widerspruch zu $[K = k(\alpha) : k] \leq n$. Also ist E endlich.

TODO: Beweis für diese Aussage einfügen

Insgesamt ergibt sich:

$$n = |G| \leq |\text{Gal}(E/k)| \stackrel{10.4}{\leq} [E : k] \leq n$$

Es folgt:

$$|G| = |\text{Gal}(E/k)|$$

Wegen $G \subseteq \text{Gal}(E/k)$ folgt schon:

$$G = \text{Gal}(E/k)$$

□_{10.5}

10.6 Beispiel

Seien p eine Primzahl, $E = \overline{\mathbb{F}}_p$, $\sigma := \text{Frob}_{\overline{\mathbb{F}}_p}$ und $G := \langle \text{Frob}_{\overline{\mathbb{F}}_p} \rangle \subseteq \text{Aut}(E)$.

Dann gilt:

- i) $G \cong \mathbb{Z}$
- ii) $k := E^G = \mathbb{F}_p$
- iii) $G \subsetneq \text{Gal}(E/k)$ ist eine echte Untergruppe (vergleiche 10.5 ii)).

Beweis

Übung

TODO: Beweis einfügen von Zusatzaufgabe Blatt 9

□_{10.6}**10.7 Korollar**Seien $E \supseteq k$ eine normale Körpererweiterung und $G := \text{Aut}_k(E)$.

Dann gelten:

- i) E/E^G ist galoissch mit $\text{Gal}(E/E^G) = G$.
- ii) Ist E/k galoissch, so gilt $E^G = k$.

Beweis

- i) Nach 10.5 ist E/E^G galoissch und es gilt:

$$\text{Gal}(E/E^G) = \text{Aut}_{E^G}(E) \stackrel{*}{=} \text{Aut}(E/k) = G$$

Zeige *:

„ \subseteq “ ist klar wegen $k \subseteq E^G$.„ \supseteq “: Für $\sigma \in \text{Aut}_k(E) = G$ gilt:

$$\sigma|_{E^G} = \text{id}_{E^G}$$

Damit folgt $\sigma \in \text{Aut}_{E^G}(E)$.□_{i)}

- ii) Klar sind $k \subseteq E^G \subseteq E$.

Behauptung

$$[E^G : k]_S = 1$$

BeweisSeien $\sigma \in E^G \hookrightarrow \bar{k}$ eine k -Homomorphismus und $\bar{\sigma} : \bar{k} \rightarrow \bar{k}$ eine Fortsetzung von σ (vergleiche 6.7).Nach 7.4 i) gilt, weil E/k normal ist:

$$\tau := (\bar{\sigma}|_E : E \rightarrow E) \in \text{Aut}_k(E) = G$$

Damit folgt:

$$\sigma = \tau|_{E^G} \stackrel{\tau \in G}{=} \text{id}_{E^G}$$

Es folgt:

$$1 = |\text{Hom}_{k\text{-Alg.}}(E^G, \bar{k})| = [E^G : k]_S$$

□_{Behauptung}

Weil nach Voraussetzung E/k galoissch, also insbesondere separabel ist, ist auch E^G/k separabel nach 8.16 i) \Rightarrow ii), also gilt:

$$1 = [E^G : k]_S \stackrel{8.15 \text{ i)} \Rightarrow \text{ii)}}{=} [E^G : k]$$

Also gilt $E^G = k$.

□_{10.7}

10.8 Bemerkung und Beispiel (absolute Galoisgruppe)

i) Aus 10.7 folgt insbesondere:

$$E/k \text{ ist galoissch} \Rightarrow E^{\text{Gal}(E/k)} = k$$

Das heißt für alle $\alpha \in E \setminus k$ gibt es ein $\sigma \in \text{Gal}(E/k)$ mit $\sigma(\alpha) \neq \alpha = \text{id}(\alpha)$, also separieren die Automorphismen von E/k die Elemente $\alpha \in E/k$.

ii) Ist k ein vollkommener Körper, so ist $\bar{k} \supseteq k$ galoissch (vergleiche 6.1 und 8.9) und

$$G_k := \text{Gal}(\bar{k}/k)$$

heißt *die absolute Galoisgruppe von k* .

iii) Seien $p \in \mathcal{P}$ eine Primzahl und $k := \mathbb{F}_p(t) \subseteq k(\alpha)$ mit $\alpha^p = t$.

Dann ist E/k nach 8.7 normal und:

$$G := \text{Aut}_k(E) = \{\text{id}\}$$

Insbesondere ist also $E^G = E \supsetneq k$ und:

$$[E : k] = p \neq 1$$

(vergleiche 10.7 ii))

10.9 Satz (Hauptsatz der Galoistheorie)

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

i) Die Abbildung

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

$$\phi(H) := E^H$$

$$\psi(K) := \text{Gal}(E/K) \subseteq G$$

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

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

ein surjektiver Gruppenhomomorphismus, der einen Isomorphismus

$$\text{Gal}(E/k) / \text{Gal}(E/E^H) \xrightarrow{\sim} \text{Gal}(E^H/k)$$

induziert.

Beweis

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

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

Für den Zwischenkörper $k \subseteq K \subseteq E$ folgt aus 10.7 ii):

$$K = \phi(\psi(K)) = E^{\text{Gal}(E/K)}$$

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

Für die Untergruppe $H \subseteq G$ gilt nach 10.5 ii) in G :

$$\text{Gal}(E/E^H) = H$$

□_{i)}

ii) b) \Rightarrow a) und zweite Aussage folgen aus 10.3 ii).

a) \Rightarrow b): Wegen 8.16 i) \Rightarrow ii) ist mit E/k auch E^H/k separabel.

Zeige also noch, dass E^H/k normal ist und dazu nach 7.4 i):

Behauptung

Für jeden k -Homomorphismus $\sigma : E^H \hookrightarrow \bar{E}$ gilt $\sigma(E^H) \subseteq E^H$.

Beweis

Für eine Fortsetzung $\bar{\sigma} : E \hookrightarrow \bar{E}$ von σ gilt, weil E/k normal ist, $\bar{\sigma}(E) = E$, also ist $\bar{\sigma} \in \text{Aut}_k(E) = G$.

Seien nun $\alpha \in E^H$ und $\omega \in H$ beliebig, dann folgt:

$$\omega(\sigma(\alpha)) = (\omega \circ \bar{\sigma})(\alpha)$$

Rechne:

$$\omega \circ \bar{\sigma} = \bar{\sigma} \circ \underbrace{\bar{\sigma}^{-1} \circ \omega \circ \bar{\sigma}}_{=: \omega' \in H, \text{ da } H \trianglelefteq G}$$

Also ist:

$$\omega(\sigma(\alpha)) = \bar{\sigma}\left(\underbrace{\omega'(\alpha)}_{=\alpha, \text{ da } \omega' \in H, \alpha \in E^H}\right) = \bar{\sigma}(\alpha) = \sigma(\alpha)$$

Weil α und ω beliebig sind, folgt $\sigma(E^H) \subseteq E^H$.

□_{10.9}

10.10 Korollar

Ist E/k eine endliche separable Körpererweiterung, so besitzt E/k nur endlich viele Zwischenkörper.

1. Beweis

Die normale Hülle E'/k ist endlich (nach 7.10 ii)), normal und separabel, also galoissch, und

$$G := \text{Gal}(E'/k)$$

ist endlich, genauer $|G| = [E' : k] < \infty$.

G besitzt nur endlich viele Untergruppen, also besitzt E'/k nach 10.9 i) nur endlich viele Zwischenkörper.

Jeder Zwischenkörper von E/k ist aber insbesondere einer von E'/k .

□_{1. Beweis}

2. Beweis

Nach 8.17 existiert ein $\alpha \in E$ mit $E = k(\alpha)$.

Dann folgt die Aussage aus Blatt 6, Aufgabe 4.

TODO: Beweis einfügen

□_{10.10}

10.11 Definition und Bemerkung (Kompositum)

Seien $E \supseteq k$ eine Körpererweiterung und $k \subseteq K_1, K_2 \subseteq E$ Zwischenkörper.

Dann ist $K_1 \cdot K_2 := K_1(K_2) = K_2(K_1) \subseteq E$ der kleinste Zwischenkörper von E/k , der K_1 und K_2 enthält und heißt *das Kompositum von K_1 und K_2 (in E)*.

10.12 Satz und Definition (Galoiserweiterung)

Sei $E \supseteq k$ eine endliche *Galoiserweiterung*, das heißt eine Körpererweiterung, die galoissch ist.

Seien $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ Zwischenkörper und

$$H_i := \text{Gal}(E/K_i) \subseteq G := \text{Gal}(E/k)$$

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 und separabel und E'/k normale Hülle von E/k , dann ist E'/k endlich, separabel und normal.

Beweis

Aus 8.17 gibt es ein $\alpha \in E$ mit:

$$E = k(\alpha)$$

Wähle einen algebraischen Abschluss \bar{k} :

$$E \hookrightarrow \bar{E} = \bar{k}$$

Nach 7.10 folgt:

$$E' = k(\sigma(\alpha) \mid \sigma \in \text{Hom}_{k\text{-Alg.}}(E, \bar{E}))$$

Aus

$$|\text{Hom}_{k\text{-Alg.}}(E, \bar{E})| = [E : k]_S = [E : k] < \infty$$

folgt nach 7.10 ii):

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

Für alle $\sigma \in \text{Hom}_{k\text{-Alg.}}(E, \bar{E})$ ist

$$\text{Mipo}_k(\sigma(\alpha)) \stackrel{!}{=} \text{Mipo}_k(\alpha) \in k[X]$$

separabel, also ist E'/k nach 8.15 separabel.

Beweis von 10.12

$$\begin{aligned} \text{i) } „\Rightarrow“: H_2 = \text{Aut}_{K_2}(E) &\stackrel{K_1 \subseteq K_2}{\subseteq} \text{Aut}_{K_1}(E) = H_1 \\ „\Leftarrow“: K_1 &\stackrel{10.9 \text{ i)}}{=} E^{H_1} \stackrel{H_2 \subseteq H_1}{\subseteq} E^{H_2} \stackrel{10.9 \text{ i)}}{=} K_2 \end{aligned}$$

□_{i)}

$$\text{ii) } K_1 \cdot K_2 = E^{H_1} \cdot E^{H_2} \stackrel{\text{i)}}{\subseteq} (E^{H_1 \cap H_2}) \cdot (E^{H_1 \cap H_2}) = E^{H_1 \cap H_2}$$

Ferner gilt:

$$\text{Gal}(E/K_1 \cdot K_2) \stackrel{K_i \subseteq K_1 \cdot K_2}{\subseteq} \text{Aut}_{K_1}(E) \cap \text{Aut}_{K_2}(E) = H_1 \cap H_2$$

Daraus folgt mit i):

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

□_{ii)}

$$\text{iii) } E^{\langle H_1, H_2 \rangle} = E^{H_1} \cap E^{H_2} = K_1 \cap K_2$$

(Da jedes Element von $\langle H_1, H_2 \rangle$ ein Produkt von Elementen aus H_1 oder H_2 ist.)

□_{10.12}

10.13 Beispiel und Definition (Untergruppen-Diagramm)

Nach Blatt 7, Aufgabe 2 ist die Galoisgruppe von $f := X^3 - 2 \in \mathbb{Q}[X]$ isomorph zu S_3 .

TODO: Beweis einfügen

Genauer: Seien $\alpha \in \mathbb{C}$ mit $\alpha^3 = 2$ und $\zeta := \exp\left(\frac{2\pi i}{3}\right) \in \mathbb{C}$.

Dann ist $E := \mathbb{Q}(\alpha, \zeta)/\mathbb{Q}$ ein Zerfällungskörper von f und die Abbildung

$$\begin{aligned} \text{Gal}\left(E/\mathbb{Q}\right) &\simeq \sum \underbrace{\{\alpha, \alpha\zeta, \alpha\zeta^2\}}_{=: \mathcal{N}} \\ \sigma &\mapsto \sigma|_{\mathcal{N}} \end{aligned}$$

ist wohldefiniert und ein Gruppenisomorphismus.

Aus der linearen Algebra I ist folgendes *Untergruppen-Diagramm* der S_3 bekannt:

TODO: Abb2 einfügen

$A_3 \trianglelefteq S_3$ ist der einzige nicht-triviale Normalteiler und es gilt:

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$

Die H_i sind alle von Ordnung 2 und nicht normal. (vergleiche Übungsaufgabe ?)

TODO: Beweis einfügen

Außerdem können der Durchschnitt und die Erzeugerrelation abgelesen werden, zum Beispiel

$$\begin{aligned} \langle A_3, H_i \rangle &= S_3 \\ H_i \cap A_3 &= \{e\} \end{aligned}$$

für alle $0 \leq i \leq 2$.

Außerdem gilt:

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

Aus 10.9 und 10.12 folgt daraus folgendes Diagramm von Zwischenkörpern:

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, ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoissch mit:

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

Zur Bestimmung der Fixkörper:

1. $\sigma := \begin{pmatrix} \alpha & \alpha\zeta & \alpha\zeta^2 \end{pmatrix} \in A_3$ ist ein Erzeuger und es gilt:

$$\sigma(\zeta) = \sigma\left(\frac{\alpha\zeta}{\alpha}\right) = \frac{\alpha\zeta^2}{\alpha\zeta} = \zeta$$

Daher ist $\zeta \in E^{A_3}$.

Wegen $[E^{A_3} : \mathbb{Q}] = 2$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, da das Minimalpolynom

$$\text{Mipo}_{\mathbb{Q}}(\zeta) = X^2 + X + 1$$

Grad 2 hat, folgt also $E^{A_3} = \mathbb{Q}(\zeta)$.

2. Für $\text{id} \neq \tau_i \in H_i$ mit $0 \leq i \leq 2$ gilt:

$$\tau_i(\alpha\zeta^i) = \alpha\zeta^i$$

Also gilt:

$$\alpha\zeta^i \in E^{H_i}$$

Wegen $[\alpha\zeta^i : \mathbb{Q}] = 3$, da

$$\text{Mipo}_{\mathbb{Q}}(\alpha\zeta^i) = X^3 - 2$$

Grad 3 hat, und

$$[E^{H_i} : \mathbb{Q}] = [E^{H_i} : E^{S_3}] = [S_3 : H_i] = 3$$

folgt $E^{H_i} = \mathbb{Q}(\alpha\zeta^i)$ für $0 \leq i \leq 2$.

Bemerkung

Seien $E \supseteq k$ eine endliche und galoissche Körpererweiterung, $G := \text{Gal}(E/k)$ und $H \subseteq G$ eine Untergruppe.

Dann gilt:

a) $[E : E^H] = [G : H]$

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

Beweis

$$\text{Gal}(E/E^H) = H$$

Aus 10.3 folgt damit a).

Dann gilt:

$$[E : E^H] \cdot [E^H : k] = [E : k] = [G : H] \cdot |H| \stackrel{\text{a)}}{=} [G : H] \cdot [E : E^H]$$

Und damit folgt:

$$[E^H : k] = [G : H]$$

□Bemerkung

10.14 Definition (abelsche und zyklische Galoiserweiterung)

Eine Galoiserweiterung E/k heißt genau dann *abelsch* (beziehungsweise *zyklisch*), wenn $\text{Gal}(E/k)$ 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

$G := \text{Gal}(E/k)$ ist abelsch und damit folgt, dass $H := \text{Gal}(E/K) \trianglelefteq G$ gilt.

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

□_{10.15}**10.16 Satz**

Seien $E \supseteq k$ eine Körpererweiterung, $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ Zwischenkörper und K_i/k endlich und galoissch für $i \in \{1, 2\}$.

Dann gilt:

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

$$\begin{aligned} \varphi : \text{Gal}(K_1 \cdot K_2/K_1) &\xrightarrow{\sim} \text{Gal}(K_2/K_1 \cap K_2) \\ \sigma &\mapsto \sigma|_{K_2} \end{aligned}$$

ist wohldefiniert und ein Gruppenisomorphismus.

- ii) Die Abbildung

$$\begin{aligned} \psi : \text{Gal}(K_1 \cdot K_2/k) &\hookrightarrow \text{Gal}(K_1/k) \times \text{Gal}(K_2/k) \\ \sigma &\mapsto (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

ist wohldefiniert und ein injektiver Gruppenhomomorphismus.

Im Fall $K_1 \cap K_2 = k$ ist ψ ein Isomorphismus.

Beweis

- i) Es existieren separable $f_i \in k[X]$ so, dass

$$K_i/k$$

Zerfällungskörper von f_i für $i \in \{1, 2\}$ sind (siehe 10.2 a) \Rightarrow b)).

Nach 8.17 gibt es $\alpha_i \in K_i$ mit $K_i = k(\alpha_i)$ für $i \in \{1, 2\}$.

Es gilt $\text{Mipo}_{K_1}(\alpha_2) | \text{Mipo}_k(\alpha_2)$, da $\text{Mipo}_{K_1}(\alpha_2) \in K_1[X]$ schon α_2 annulliert.

Mit $\text{Mipo}_k(\alpha_2)$ ist damit auch $\text{Mipo}_{K_1}(\alpha_2)$ separabel.

Also gilt

$$k \stackrel{\text{endlich, separabel}}{\subseteq} K_1 \stackrel{\text{endlich, separabel}}{\subseteq} K_1(\alpha_2) = K_1(k(\alpha_2)) = K_1(K_2) = K_1 \cdot K_2$$

nach der Gradformel und Transitivität der Separabilität (vergleiche 5.6, 8.14 und 8.16).

Dann ist

$$K_1 \cdot K_2/k$$

also endlich und galoissch.

φ ist wohldefiniert, da aus

$$\sigma|_{K_1} = \text{id}$$

schon

$$(\sigma|_{K_2})|_{K_1 \cap K_2} = \text{id}$$

folgt. Außerdem ist φ offenbar ein Gruppenhomomorphismus.

Für $\sigma \in \ker(\varphi)$ gilt:

$$\begin{aligned} \text{id} &= \sigma|_{K_2} = \sigma|_{K_1} \\ \Rightarrow \quad \sigma|_{K_1 \cdot K_2} &= \sigma = \text{id} \end{aligned}$$

Also ist φ injektiv.

Ferner gilt:

$$K_2^{\text{im}(\varphi)} \stackrel{\text{Def. von } \varphi}{=} (K_1 \cdot K_2)^{\text{Gal}(K_1 \cdot K_2 / K_1)} \cap K_2 \stackrel{10.9 \text{ i)}}{=} K_1 \cap K_2 = K_2^{\text{Gal}(K_2 / K_1 \cap K_2)}$$

Mit 10.9 i) folgt:

$$\text{im}(\varphi) = \text{Gal}(K_2 / K_1 \cap K_2)$$

Also ist φ surjektiv.

ii) Wohldefiniertheit und, dass ψ ein Gruppenhomomorphismus ist, sind klar.

Aus $\sigma \in \ker(\psi)$ folgt für $i \in \{1, 2\}$ schon

$$\sigma|_{K_i} = \text{id}$$

und damit ergibt sich:

$$\sigma = \sigma|_{K_1 \cdot K_2} = \text{id}$$

Deswegen ist ψ injektiv.

Gelte nun $K_1 \cap K_2 = k$ und sei

$$(\sigma, \sigma') \in \text{Gal}(K_1 / k) \times \text{Gal}(K_2 / k)$$

beliebig.

Aus i) folgt damit, dass es ein

$$\tilde{\sigma} \in \text{Gal}(K_1 \cdot K_2 / K_2)$$

mit $\tilde{\sigma}|_{K_1} = \sigma$ gibt, und ebenso ein

$$\tilde{\sigma}' \in \text{Gal}(K_1 \cdot K_2 / K_1)$$

mit $\tilde{\sigma}'|_{K_2} = \text{id}$.

Dann gilt:

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

Daher ist ψ surjektiv.

□_{10.16}

Bemerkung

1. $f_1, f_2 \in k[X]$ separabel $\not\Rightarrow f_1 \cdot f_2 \in k[X]$ separabel, zum Beispiel $f_1 = f_2 = X$.
2. Sind $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ Zwischenkörper und K_i/k endlich und separabel für $i \in \{1, 2\}$.
Dann ist $K_1 \cdot K_2/k$ endlich und separabel.

10.17 Proposition

Seien k ein Körper, $f \in k[X]$ separabel, E/k ein Zerfällungskörper von f , $G := \text{Gal}(E/k)$ (vergleiche 10.2 ii)) und $\mathcal{N} := \{\beta \in E \mid f(\beta) = 0\}$.

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:

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

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 $\bar{k} \supseteq E$ ein algebraischer Abschluss, so existiert ein $\tilde{\sigma} : \bar{k} \rightarrow \bar{k}$ mit $\tilde{\sigma}(\alpha) = \beta$. (Blatt 8, A3,d) \Rightarrow a))

TODO: Beweis einfügen

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 für alle $\beta \in \mathcal{N}$ gibt es ein $\sigma \in G$ mit:

$$\sigma(\alpha) = \beta \quad \Rightarrow \quad 0 = \underbrace{\sigma(g(\alpha))}_{=0} = g^\sigma(\sigma(\alpha)) = g(\beta)$$

Also gilt:

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

Weil f separabel ist, gilt:

$$|\mathcal{N}| = \deg(f)$$

Aus (10.1) folgt:

$$\deg(g) \geq \deg(f)$$

Wegen $g|f$ sind damit f und g in $k[X]$ assoziiert, also ist mit g auch f irreduzibel.

□_{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:

$$\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\beta := \alpha_1 + \alpha_2$$

$$E = \mathbb{Q}(\beta)$$

$$\text{Mipo}_{\mathbb{Q}}(\beta) = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$$

Beweis

Seien $k := \mathbb{Q}$, $K_1 := \mathbb{Q}(\alpha_1)$, $K_2 := \mathbb{Q}(\alpha_2)$ und $E = K_1 \cdot K_2$.

Mit $k \subseteq K_1 \subseteq E$ und $k \subseteq K_2 \subseteq E$ ist klar, dass K_i/k für $i \in \{1, 2\}$ galoissch vom Grad 2 ist, also folgt:

$$\text{Gal}(K_i/k) \cong \mathbb{Z}/2\mathbb{Z}$$

Man kann zeigen, dass $K_1 \cap K_2 = k$ gilt (Übung).

TODO: Beweis einfügen

Nach 10.16 ii) ist

$$\begin{aligned} \varphi : \text{Gal}(E/k) &\xrightarrow{\sim} \text{Gal}(K_1/k) \times \text{Gal}(K_2/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \varphi(\sigma) &:= (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

ein Isomorphismus.

Für $i \in \{1, 2\}$ gilt:

$$\text{Gal}(K_i/k) = \{1, \tau_i\}$$

Dabei $\tau_i : K_i \xrightarrow{\sim} K_i$ durch $\tau_i(\alpha_i) = -\alpha_i$ eindeutig bestimmt ist.

Nach Definition von φ folgt:

$$\text{Gal}(E/k) = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$$

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:

$$\begin{aligned} f(X) &:= \prod_{\sigma \in \text{Gal}(E/k)} (X - \sigma(\beta)) = \\ &\stackrel{\text{Tabelle}}{=} (X - (\alpha_1 + \alpha_2))(X + (\alpha_1 + \alpha_2))(X - (\alpha_1 - \alpha_2))(X + (\alpha_1 - \alpha_2)) = \\ &= (X^2 - (\alpha_1 + \alpha_2)^2)(X^2 - (\alpha_1 - \alpha_2)^2) = (X^2 - (5 + 2\alpha_1\alpha_2))(X^2 - (5 - 2\alpha_1\alpha_2)) = \\ &= X^4 - 10X^2 + (5 + 2\alpha_1\alpha_2)(5 - 2\alpha_1\alpha_2) = X^4 - 10X^2 + 25 - 24 = \\ &= X^4 - 10X^2 + 1 \in \mathbb{Q}[X] \end{aligned}$$

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 $f = \text{Mipo}_k(\beta)$.

□_{10.18}

11 Bestimmung einiger Galoisgruppen

Fixiere in Kapitel 11 (Bestimmung einiger Galoisgruppen)

Sei k ein Körper.

11.1 Satz und Definition (Die Permutationsdarstellung)

Seien $f \in k[X]$ separabel, $n := \deg(f) > 0$, $E \supseteq k$ ein Zerfällungskörper von f und

$$\mathcal{N} := \{\alpha \in E \mid f(\alpha) = 0\}$$

mit $|\mathcal{N}| = n$.

Dann ist die Abbildung

$$p : \text{Gal}(E/k) \hookrightarrow \sum (\mathcal{N}) \left(\begin{array}{c} \text{nach Wahl} \\ \cong \\ \text{einer Nummerierung} \end{array} \mathcal{N} = \{\alpha_1, \dots, \alpha_n\} \right)$$

mit

$$p(\sigma)(\alpha) = \sigma(\alpha)$$

für alle $\alpha \in \mathcal{N}$ und $\sigma \in \text{Gal}(E/k)$ wohldefiniert und ein injektiver Gruppenhomomorphismus.

p heißt *die Permutationsdarstellung von $\text{Gal}(E/k)$* .

Es gelten:

$$f \in k[X] \text{ irreduzibel} \stackrel{\text{a)}}{\Leftrightarrow} \left(\forall_{\alpha, \beta \in \mathcal{N}} \exists_{\sigma \in \text{Gal}(E/k)} : p(\sigma)(\alpha) = \beta \right) \stackrel{\text{b)}}{\Leftrightarrow} p \text{ ist ein Isomorphismus}$$

Beweis

E/k ist endlich und galoissch nach 10.2 b) \Rightarrow a).

Die Aussagen über p folgen wie in Aufgabe 2, ii) auf Blatt 7.

TODO: Beweis einfügen

a) ist 10.17 i) \Leftrightarrow ii).

b) ist klar.

□_{11.1}

11.2 Quadratische Gleichungen

$f = X^2 + aX + b \in k[X]$ besitze keine Nullstelle in k .

Dann ist $E := k(\alpha)/k$ für $f(\alpha) = 0$ ein Zerfällungskörper von f , und in $E[X]$ gilt nach 7.1 i):

$$f(X) = (X - \alpha) \cdot (X - (-\alpha - a))$$

Weiter ist die Separabilität von $f \in k[X]$, weil f irreduzibel ist, äquivalent zu folgender Äquivalenz in $k[X]$:

$$0 = f'(X) = 2X + a \Leftrightarrow (\text{char}(k) = 2 \wedge a = 0)$$

Gelte nun $\text{char}(k) \neq 2$ oder $a \neq 0$.

Dann ist E/k galoissch mit $\text{Gal}(E/k) \cong \mathbb{Z}/2\mathbb{Z}$ und das eindeutige $\sigma \in \text{Gal}(E/k) \setminus \{1\}$ ist durch $\sigma(\alpha) = -\alpha - a$ eindeutig bestimmt.

11.3 Kubische Gleichungen

Es gelte $\text{char}(k) \neq 2, 3$ und $F(X) = X^3 + AX^2 + BX + C \in k[X]$ besitze keine Nullstellen in k .

Dann ist $F \in k[X]$ irreduzibel.

11.3.1 Lemma (Normalform)

Jede kubische Gleichung der Form $F(X)$ lässt sich reduzieren auf:

$$f(X) =: X^3 + aX + b$$

Beweis

Betrachte ähnlich der quadratischen Ergänzung:

$$\begin{aligned} f(X) &:= F\left(X - \frac{A}{3}\right) = X^3 + X^2\left(-3 \cdot \frac{A}{3} + A\right) + \left(B - \frac{A^2}{3}\right)X + \frac{2A^3}{27} - \frac{AB}{3} + C = \\ &=: X^3 + aX + b \end{aligned}$$

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

Da $k[X] \xrightarrow{\sim} k[X], X \mapsto X - \frac{A}{3}$ ein Isomorphismus ist, folgt die Behauptung.

□_{11.3}

11.3.2 Bestimmung der Galoisgruppe

Betrachte im Folgenden $f(X)$.

Es gilt $f'(X) = 3X^2 + a \neq 0$, da $3 \neq 0$ wegen $\text{char}(k) \neq 3$, also ist $f \in k[X]$ separabel nach 8.4 ii), und der Zerfällungskörper E/k von f ist galoissch.

Nummeriere:

$$\mathcal{N} := \{\alpha \in E \mid f(\alpha) = 0\} = \{\alpha_1, \alpha_2, \alpha_3\}$$

Nach 11.1 existiert genau ein Gruppenhomomorphismus $\varrho : \text{Gal}(E/k) \hookrightarrow S_3$ mit:

$$\forall_{\sigma \in \text{Gal}(E/k), 1 \leq i \leq 3} : \sigma(\alpha_i) = \alpha_{\varrho(\sigma)(i)} \quad (11.1)$$

Weil f irreduzibel ist, folgt $[E : k] \geq 3$ und aus der bekannten Untergruppenstruktur von S_3 (vergleiche 10.13) folgt:

$$\text{Gal}(E/k) \cong \text{im}(\varrho) = \begin{cases} A_3 \\ S_3 \end{cases}$$

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 $\sigma \in \text{Gal}(E/k)$ gilt in E^* :

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

Beweis

Die Behauptung ist klar wegen (11.1), der Definition von σ und δ und der Definition von $\text{sgn}(\varrho(\sigma))$ als Anzahl der Fehlstände.

□ Behauptung

Es folgt in \mathbb{Z} :

$$\text{im}(\varrho) = A_3 \xLeftrightarrow{\text{Definition von } A_3} \forall_{\sigma \in \text{Gal}(E/k)} : \text{sgn}(\varrho(\sigma)) = 1 \xLeftrightarrow[\text{char}(k) \neq 2]{\text{Behauptung}} \forall_{\sigma \in \text{Gal}(E/k)} : \sigma(\delta) = \delta$$

Dies ist äquivalent zu $\delta \in E^{\text{Gal}(E/k)} = k$.

Ferner gilt mit $\Delta := \delta^2$ für alle $\sigma \in \text{Gal}(E/k)$:

$$\sigma(\Delta) = (\pm\delta)^2 = \Delta$$

Damit folgt $\Delta \in k$.

Später wird noch gezeigt:

$$\Delta = -4a^3 - 27b^2$$

Damit gilt für die Galoisgruppe der irreduziblen Gleichung $X^3 + aX + b$:

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

□_{11.3}

11.3.3 Beispiel

Seien $k = \mathbb{Q}$ und $f(X) := X^3 - X + 1 \in \mathbb{Q}[X]$.

Wegen $f(\pm 1) \neq 0$ besitzt f keine Nullstelle in \mathbb{Q} (benutzt, dass ein ganzzahliges Polynom ohne Nullstellen in \mathbb{Z} keine Nullstellen in \mathbb{Q} hat und eine ganzzahlige Nullstelle eines normierten Polynoms den letzten Koeffizienten teilt).

Außerdem gilt hier:

$$\Delta = -4 \cdot (-1)^3 - 27 \cdot 1^2 = -23 \notin (\mathbb{Q}^*)^2$$

Also hat die Gleichung $X^3 - X + 1 = 0$ über \mathbb{Q} die Galoisgruppe S_3 .

Ferner gilt mit dem Zerfällungskörper E von f für den eindeutigen Zwischenkörper $\mathbb{Q} \subseteq K \subseteq E$ mit $[K : \mathbb{Q}] = 2$ (vergleiche 10.13):

$$K = \mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{-23})$$

11.4 Die allgemeine Gleichung

Sei $n \geq 1$ fixiert und $E := k(t_1, \dots, t_n)$.

Dann existiert genau eine Abbildung

$$\varrho : S_n \rightarrow \text{Aut}(E)$$

für die für alle $\sigma \in S_n$ mit $1 \leq i \leq n$ gilt:

$$\varrho(\sigma)(t_i) = t_{\sigma(i)}$$

Benutze zum Beweis die universelle Eigenschaft des Polynomrings und des Quotientenkörpers.

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

TODO: Beweis einfügen

11.4.1 Proposition und Definition (symmetrische rationale Funktionen)

Die Körpererweiterung $K := E^{S_n} \subseteq E$ ist galoissch mit $\text{Gal}(E/K) = S_n$.

K heißt der Körper der symmetrischen rationalen Funktionen (in den Variablen t_1, \dots, t_n über k).

Beweis

Folgt aus 10.7 i).

□_{11.4}

11.4.2 Beispiel

Sei $n = 2$, betrachte also $S_2 = \{1, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} =: \sigma\}$.

Wegen

$$\sigma(t_1 + t_2) = t_2 + t_1 = t_1 + t_2$$

ist $t_1 + t_2 \in k(t_1, t_2)^{S_2}$, aber, falls $\text{char}(k) \neq 2$ ist, ist wegen

$$\sigma(t_1 - t_2) = t_2 - t_1 = -(t_1 - t_2) \neq t_1 - t_2$$

das Polynom $t_1 - t_2 \notin k(t_1, t_2)^{S_2}$, da $1 \neq -1$.

11.4.3 Definition (elementarsymmetrische Polynome)

Die in der Entwicklung

$$k[t_1, \dots, t_n][X] \ni f(X) := \prod_{i=1}^n (X - t_i) =: \sum_{j=0}^n (-1)^j \cdot s_j(t_1, \dots, t_n) \cdot X^{n-j}$$

auftretenden $s_j \in k[t_1, \dots, t_n]$ ($0 \leq j \leq n$) heißen die *j-ten elementarsymmetrischen Polynome* (in t_1, \dots, t_n über k).

Es gilt für alle $0 \leq k \leq n$:

$$s_k(t_1, \dots, t_n) = \sum_{1 \leq j_1 < \dots < j_k \leq n} (t_{j_1} \cdot t_{j_2} \cdot \dots \cdot t_{j_k})$$

Zum Beispiel: $s_0 = 1$, $s_1 = t_1 + \dots + t_n$, $s_n = t_1 \cdot \dots \cdot t_n$.

11.4.4 Definition (algebraische Unabhängigkeit)

Seien A eine k -Algebra und I eine Menge und für alle $i \in I$ sei $a_i \in A$.

Dann heißt $(a_i)_{i \in I}$ genau dann *algebraisch unabhängig über k* , wenn der eindeutige k -Algebrenhomomorphismus $k[I] \rightarrow A$ 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

$$a_1 := X^2$$

$$a_2 := X^3$$

in $A := k[X]$ sind transzendent über k (vergleiche Blatt 6 Aufgabe 1 iii)), aber (a_1, a_2) ist nicht algebraisch unabhängig über k , da für $0 \neq f(X, Y) := X^3 - Y^2 \in k[X, Y]$ gilt $f(a_1, a_2) = 0$.

TODO: Beweis einfügen

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

11.4.6 Satz (Hauptsatz über symmetrische Funktionen)

Es gelten:

- i) $K = E^{S_n} \subseteq E$ ist ein Zerfällungskörper von $f(X) = \prod_{i=1}^n (X - t_i) \in K[X]$.
- ii) Hauptsatz über symmetrische Funktionen:

$$K = k(s_1, \dots, s_n)$$

- iii) $(s_1, \dots, s_n) \subseteq K$ ist algebraisch unabhängig über k (und damit ist $K = E^{S_n}$ ein rationaler Funktionenkörper über k in den Variablen s_1, \dots, s_n).

Insbesondere gilt für alle $f, g \in k(T_1, \dots, T_n)$:

$$f(s_1, \dots, s_n) = g(s_1, \dots, s_n) \Rightarrow f = g$$

11.4.7 Bemerkung

i) Sei $\text{char}(k) \neq 2$. 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:

$$E^{A_n} = K(\delta) \stackrel{11.4.6 \text{ ii)}}{=} k(s_1, \dots, s_n, \delta)$$

Es ist ein offenes Problem, ob $f_1, \dots, f_n \in E^{A_n}$ existieren, die $E^{A_n} = k(f_1, \dots, f_n)$ erfüllen.

ii) **Vermutung**

Für jede endliche Gruppe G existiert eine Galoiserweiterung E/\mathbb{Q} mit $\text{Gal}(E/\mathbb{Q}) \cong G$.

Beweis von 11.4.6

i) Zunächst gilt für alle $\sigma \in S_n$:

$$f^\sigma(X) = \prod_{i=1}^n (X - t_{\sigma(i)}) = f(X)$$

Also ist $f \in K[X]$.

Wegen $E = k(t_1, \dots, t_n) = K(t_1, \dots, t_n)$ ist klar, dass E/k ein Zerfällungskörper von f ist.

□_{i)}

ii) Wir haben $k(s_1, \dots, s_n) \stackrel{\text{i)}}{\subseteq} K = E^{S_n} \subseteq E$ und nach 11.4.3 gilt sogar $f(X) \in k(s_1, \dots, s_n)[X]$, und damit folgt wegen $\deg(f) = n$ und i):

$$[E : k(s_1, \dots, s_n)] \leq n!$$

Aus $[E : E^{S_n}] = |S_n| = n!$ (siehe 11.4.1) folgt $K = k(s_1, \dots, s_n)$.

□_{ii)}

iii) Seien $k(S_1, \dots, S_n) \subseteq \tilde{L}$ ein Zerfällungskörper von

$$\tilde{f}(X) := \sum_{i=0}^n (-1)^i \cdot \mathcal{S}_i \cdot X^{n-i} \in k(S_1, \dots, S_n)[X]$$

mit $\mathcal{S}_0 := 1$ und seien $T_1, \dots, T_n \in \tilde{L}$ die Nullstellen von \tilde{f} in \tilde{L} (gelistet mit Vielfachheit).

Dann gilt:

$$\tilde{L} = k(S_1, \dots, S_n)(T_1, \dots, T_n) \stackrel{(11.2)}{=} k(T_1, \dots, T_n)$$

Denn es gilt für alle i :

$$\mathcal{S}_i = s_i(T_1, \dots, T_n) \in k(T_1, \dots, T_n) \quad (11.2)$$

Für den eindeutigen k -Algebrenhomomorphismus

$$\varphi : k[t_1, \dots, t_n] \rightarrow k[T_1, \dots, T_n]$$

mit $\varphi(t_i) = T_i$ gilt

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

für alle $1 \leq i \leq n$.

Da $\{\mathcal{S}_1, \dots, \mathcal{S}_n\} \subseteq k[\mathcal{S}_1, \dots, \mathcal{S}_n]$ algebraisch unabhängig über k ist, ist $\{s_1, \dots, s_n\} \subseteq k[s_1, \dots, s_n]$ algebraisch unabhängig über k .

□_{11.4.6}

11.4.8 Definition (allgemeines Polynom n -ten Grades)

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

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

11.4.9 Bemerkung

Seien $F \supseteq k$ eine Körpererweiterung und

$$f = X^n + \sum_{i=1}^n a_i X^{n-i} \in F[X]$$

mit $a_i \in F$ für $1 \leq i \leq n$ ein normiertes Polynom vom Grad n .

Dann existiert genau ein k -Algebrenhomomorphismus

$$\varphi : k(\mathcal{S}_1, \dots, \mathcal{S}_n) \rightarrow F$$

mit

$$\begin{aligned} \varphi[X] : k(\mathcal{S}_1, \dots, \mathcal{S}_n)[X] &\rightarrow F[X] \\ \varphi[X](p(X)) &= f(X) \end{aligned}$$

also mit $\varphi(\mathcal{S}_i) = a_i$ für $1 \leq i \leq n$.

11.4.10 Satz

$p(X) \in k(\mathcal{S}_1, \dots, \mathcal{S}_n)[X]$ ist irreduzibel und separabel und es gilt:

$$\text{Gal}(p(X)) \cong S_n$$

(vergleiche 10.2 i))

Beweis

Wegen 11.4.6 ii) existiert ein k -Isomorphismus

$$\varphi : k(\mathcal{S}_1, \dots, \mathcal{S}_n) \xrightarrow{\sim} k(s_1, \dots, s_n)$$

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.

□_{11.4}

11.4.11 Satz (Hilbertscher Irreduzibilitätssatz)

Für $n \geq 1$ existieren unendlich viele Tupel $(q_1, \dots, q_n) \in \mathbb{Q}^n$, sodass

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

irreduzibel und separabel ist und es gilt:

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

(ohne Beweis)

Beispiel

Obiges gilt nicht für alle q_i .

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

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

Fixiere in 12 (Kreisteilungskörper (die Galoistheorie der Gleichung $X^n - 1 = 0$))

Sei k ein Körper und $n, m \in \mathbb{N}_{\geq 1}$ entweder mit $\text{char}(k) = 0$ oder $\text{char}(k) \nmid n, m$.

12.1 Proposition und Definition (Gruppe der n -ten Einheitswurzeln)

Die Teilmenge

$$U_n := U_n(k) := \{\zeta \in \bar{k}^* \mid \zeta^n = 1\} \subseteq \bar{k}^*$$

ist eine zyklische Untergruppe der Ordnung n , die Gruppe der n -ten Einheitswurzeln (Abkürzung: EW) (in k).

Beweis

Es ist klar, dass $U_n \subseteq \bar{k}^*$ eine Untergruppe ist.

Für $\zeta \in U_n$ gelten:

$$\begin{aligned} (X^n - 1)(\zeta) &= 0 \\ (X^n - 1)'(\zeta) &= n\zeta^{n-1} \neq 0 \end{aligned}$$

Denn es gilt $\zeta \neq 0$ und $n \neq 0$, da $\text{char}(k) \nmid n$.

Damit ist $X^n - 1 \in k[X]$ separabel und es folgt:

$$|U_n| = \deg(X^n - 1) = n$$

Insbesondere ist $U_n \subseteq \bar{k}^*$ endlich, also zyklisch nach 1.28.

□_{12.1}

Bemerkung

Sei p eine Primzahl und $n \in \mathbb{N}_{\geq 1}$, dann folgt:

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

12.2 Definition (primitive Einheitswurzeln)

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

12.3 Beispiel

Seien $k = \mathbb{C}$ und $U_6 = \left\langle \zeta_6 := \exp\left(\frac{2\pi i}{6}\right) \right\rangle \subseteq \mathbb{C}^*$.

Dann sind genau $\zeta_6, \zeta_6^5 = \zeta_6^{-1} \in U_6$ primitiv:

TODO: Abb1

Es gilt:

$$\begin{aligned} \text{ord}(\zeta_6^2) &= \text{ord}(\zeta_6^4) = 3 \\ \text{ord}(\zeta_6^3) &= 2 \\ \text{ord}(\zeta_6^0) &= 1 \end{aligned}$$

12.4 Proposition

Sind n, m teilerfremd (und $\text{char}(k) \nmid n, m$), so ist die Abbildung

$$f : U_n \times U_m \rightarrow U_{nm}$$

wohldefiniert und ein Gruppenisomorphismus.

Sind $\zeta \in U_n$ und $\psi \in U_m$ primitiv, so auch $\zeta \cdot \psi \in U_{n \cdot m}$.

Beweis

Dass f wohldefiniert und ein Gruppenhomomorphismus ist, ist klar.

Wegen 12.1 gilt:

$$|U_n \times U_m| = |U_{nm}| = nm \quad (12.1)$$

Gelte:

$$f(\zeta \cdot \xi) = \zeta \cdot \xi = 1 \quad (12.2)$$

Da n, m teilerfremd sind, existieren $a, b \in \mathbb{Z}$ mit $1 = an + bm$. Dann folgt:

$$\zeta = \zeta^1 = \left(\underbrace{\zeta^n}_{=1} \right)^a \cdot \left(\zeta^m \right)^b \stackrel{(12.2)}{=} \left(\underbrace{\zeta^m}_{=1} \right)^b = 1$$

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:

$$\text{ord}((\zeta, \xi)) = \text{kgV}(\text{ord}(\zeta), \text{ord}(\xi))$$

Sind nun $\zeta \in U_n$ und $\xi \in U_m$ primitiv, dann gilt:

$$\text{ord}((\zeta, \xi)) = \text{kgV}(n, m) \stackrel{\text{ggT}(n, m)=1}{=} n \cdot m$$

Da f ein Isomorphismus ist, folgt:

$$\text{ord}(f((\zeta, \xi))) = \text{ord}(\zeta \xi) = nm$$

Also ist $\zeta \xi \in U_{nm}$ primitiv.

□_{12.4}

Bemerkung

Die Teilerfremdheit von n und m wird gebraucht:

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

12.5 Erinnerung

Für alle $n \geq 1$ sei die „Eulersche φ -Funktion“ definiert als:

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

Es gelten:

$$\text{i) } \left(\mathbb{Z}/n\mathbb{Z} \right)^* = \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(a, n) = 1 \right\}$$

Insbesondere gilt:

$$\varphi(n) = |\{0 \leq a < n-1 \mid \text{ggT}(a, n) = 1\}|$$

ii) φ ist multiplikativ, das heißt für alle $n, m \in \mathbb{N}_{\geq 1}$ gilt:

$$\text{ggT}(n, m) = 1 \Rightarrow \varphi(n) \cdot \varphi(m) = \varphi(nm)$$

iii) Ist $p > 0$ eine Primzahl und $r \in \mathbb{N}_{\geq 1}$, dann folgt:

$$\varphi(p^r) = (p-1)p^{r-1}$$

12.6 Proposition

Für alle $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ gilt:

$$\bar{a} \text{ erzeugt } \left(\mathbb{Z}/n\mathbb{Z}, + \right) \Leftrightarrow \bar{a} \in \left(\mathbb{Z}/n\mathbb{Z} \right)^*$$

Beweis

„ \Rightarrow “: Es gibt ein $k \in \mathbb{Z}_{\geq 1}$ mit:

$$\bar{1} = \underbrace{\bar{a} + \dots + \bar{a}}_{k \text{ mal}} = \bar{a} \cdot \bar{k} \in \mathbb{Z}/n\mathbb{Z}$$

Also ist $\bar{a} \in \left(\mathbb{Z}/n\mathbb{Z} \right)^*$.

„ \Leftarrow “: Es gibt ein $b \in \mathbb{Z}_{\geq 1}$ mit

$$\bar{a} \cdot \bar{b} = \underbrace{\bar{a} + \dots + \bar{a}}_{b \text{ mal}} = \bar{1}$$

in $\mathbb{Z}/n\mathbb{Z}$.

Also ist $\bar{1} \in \langle \bar{a} \rangle \subseteq \left(\mathbb{Z}/n\mathbb{Z}, + \right)$.

Wegen $\langle \bar{1} \rangle = \left(\mathbb{Z}/n\mathbb{Z}, + \right)$ folgt:

$$\langle \bar{a} \rangle = \left(\mathbb{Z}/n\mathbb{Z}, + \right)$$

□_{12.6}

12.7 Korollar

Für $n \in \mathbb{N}_{\geq 1}$ gelten mit $(\text{char}(k) \nmid n)$:

- i) $|\{\zeta \in U_n \mid \zeta \text{ ist primitiv}\}| = \varphi(n)$
- ii) Für ein primitives $\zeta \in U_n$ und $r \in \mathbb{Z}$ gilt:

$$\zeta^r \in U_n \text{ ist primitiv} \Leftrightarrow \bar{r} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \left(\stackrel{12.5 \text{ i)}}{\Leftrightarrow} \text{ggT}(r, n) = 1 \right)$$

Beweis

$$\begin{aligned} \text{i)} \quad |\{\zeta \in U_n \mid \zeta \text{ ist primitiv}\}| &\stackrel{12.1}{=} \left| \left\{ a \in \left(\mathbb{Z}/n\mathbb{Z}, +\right) \mid \langle a \rangle = \left(\mathbb{Z}/n\mathbb{Z}, +\right) \right\} \right| = \\ &\stackrel{12.2}{=} \left| \left(\mathbb{Z}/n\mathbb{Z}\right)^* \right| \stackrel{12.5}{=} \varphi(n) \end{aligned}$$

□_{i)}

- ii) Aus der Primitivität von $\zeta \in U_n$ folgt:

$$\begin{aligned} \left(\mathbb{Z}/n\mathbb{Z}, +\right) &\xrightarrow{\sim} U_n \\ \bar{a} &\mapsto \zeta^a \end{aligned}$$

Also gilt für alle $r \in \mathbb{Z}$:

$$\zeta^r \in U_n \text{ ist primitiv} \Leftrightarrow \langle \bar{r} \rangle = \left(\mathbb{Z}/n\mathbb{Z}, +\right) \stackrel{12.5}{=} \bar{r} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

□_{12.7}

12.8 Satz

Seien $n \in \mathbb{N}_{\geq 1}$ und $\zeta_n \in \bar{k}$ eine primitive n -te Einheitswurzel. Dann gelten:

- i) $k(\zeta)/k$ ist endlich und abelsch.
- ii) Die Abbildung

$$\begin{aligned} \psi : \text{Gal}\left(k(\zeta_n)/k\right) &\hookrightarrow \text{Aut}(U_n) \\ \psi(\sigma) &:= \sigma|_{U_n} \end{aligned}$$

ist wohldefiniert und ein injektiver Gruppenhomomorphismus.

- iii) Die Abbildung

$$\begin{aligned} \left(\mathbb{Z}/n\mathbb{Z}\right)^* &\xrightarrow{\sim} \text{Aut}(U_n) \\ \bar{a} &\mapsto (\zeta \mapsto \zeta^a) \end{aligned}$$

ist wohldefiniert und ein Gruppenisomorphismus.

Beweis

Weil ζ_n primitiv ist, folgt:

$$U_n = \langle \zeta_n \rangle = \{ \zeta_n^a \mid a \in \mathbb{Z} \} \subseteq k(\zeta_n) \quad (12.3)$$

Also ist $k(\zeta_n)/k$ ein Zerfällungskörper von $X^n - 1 \in k[X]$.

Weil aus $\zeta^n = 1$ schon $(X^n - 1)'(\zeta) = n\zeta^{n-1} \neq 0$ folgt, ist $X^n - 1 \in k[X]$ separabel, also ist $k(\zeta_n)/k$ endlich und galoissch.

Für $\zeta \in U_n$ und $\sigma \in \text{Gal}(k(\zeta_n)/k)$ gilt:

$$[\sigma(\zeta)]^n = \sigma(\zeta^n) = \sigma(1) = 1$$

Also ist $\sigma(\zeta) \in U_n$.

Ferner ist die Abbildung

$$\begin{aligned} U_n &\rightarrow U_n \\ \zeta &\mapsto \sigma(\zeta) \end{aligned}$$

Wegen $\sigma(\zeta \cdot \xi) = \sigma(\zeta) \cdot \sigma(\xi)$ ein Gruppenhomomorphismus mit Inversen $\sigma^{-1}|_{U_n}$.

Damit ist ψ in ii) wohldefiniert und ein Gruppenhomomorphismus. Wegen (12.3) ist ψ injektiv.

□_{ii)}

iii) folgt, da U_n nach 12.1 ein freier $(\mathbb{Z}/n\mathbb{Z})$ -Modul vom Rang 1 ist.

Zu i): Wegen ii) und iii) ist $\text{Gal}(k(\zeta_n)/k)$ abelsch.

□_{12.8}

12.9 Bemerkung und Definition

In der Situation von 12.8 gilt:

$$\text{i) } [k(\zeta_n) : k] \mid \left| \text{Gal}(k(\zeta_n)/k) \right| = \varphi(n)$$

ii) Für $k = \mathbb{Q}$ in 12.8 heißt $\mathbb{Q}(\zeta_n)$ der n -te Kreisteilungskörper.

12.10 Satz (Gauß)

Seien $n \geq 1$ und $\zeta_n \in \overline{\mathbb{Q}}$ eine primitive n -te Einheitswurzel.

Dann ist der Gruppenhomomorphismus

$$\psi : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^*$$

mit der Eigenschaft, dass für alle $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ und $\zeta \in U_n(\mathbb{Q})$ schon

$$\sigma(\zeta) = \zeta^{\psi(\sigma)}$$

(vergleiche 3.8 ii))

TODO: Verweis überprüfen 2.8 ii) ?

gilt, ein Isomorphismus.

Insbesondere gilt:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

Beweis

$$f := \text{Mipo}_{\mathbb{Q}}(\zeta_n) \quad (12.4)$$

Also gilt:

$$f | X^n - 1 \in \mathbb{Q}[X]$$

Weil f normiert ist und mit 3.4 mit $h = X^n - 1$ und $R = \mathbb{Z}$ folgt $f \in \mathbb{Z}[X]$ und

$$X^n - 1 = f \cdot h \in \mathbb{Z}[X] \quad (12.5)$$

für ein geeignetes $h \in \mathbb{Z}[X]$.

Behauptung 1 Ist $p > 0$ eine Primzahl mit $p \nmid n$, dann ist $f(\zeta_n^p) = 0$ und $\zeta_n^p \in U_n$ ist primitiv.

Beweis Die zweite Aussage folgt aus 12.7 ii).

Angenommen $f(\zeta_n^p) \neq 0$, dann würde wegen $(\zeta_n^p)^n = 1$ und (12.5) gelten:

$$h(\zeta_n^p) = 0$$

Also gilt:

$$h(X^p)(\zeta_n) = 0$$

Wegen 3.4 folgt:

$$f | h(X^p) \in \mathbb{Z}[X]$$

Das heißt $h(X^p) = f \cdot g \in \mathbb{Z}[X]$ für geeignetes $g \in \mathbb{Z}[X]$.

Also gilt in $\mathbb{F}_p[X]$:

$$\bar{h}^p \stackrel{(+)}{\underset{\text{siehe unten}}{=}} \overline{h(X^p)} = \bar{f} \cdot \bar{g}$$

Damit folgt $\text{ggT}(\bar{h}, \bar{f}) \neq 1$ in $\mathbb{F}_p[X]$.

Also besitzt $\overline{X^n - 1} = \bar{f} \cdot \bar{h} \in \mathbb{F}_p[X]$ eine mehrfache Nullstelle in $\overline{\mathbb{F}_p}$.

Dies ist ein Widerspruch zur Separabilität von $X^n - 1$ in $\mathbb{F}_p[X]$, da $p \nmid n$. (vergleiche mit dem Beweis von 8.4 i))

Zu (+):

$$\bar{h} = \sum_i a_i X^i \quad a_i \in \mathbb{F}_p$$

Dann gilt:

$$\overline{h(X^p)} = \sum_i a_i (X^p)^i \stackrel{a_i \in \mathbb{F}_p}{=} \sum_i a_i^p (X^i)^p = \left(\sum_i a_i X^i \right)^p = \bar{h}^p$$

□ Behauptung 1

Behauptung 2 Ist $\zeta \in U_n$ primitiv, so ist $f(\zeta) = 0$.

Beweis Nach 12.7 ii) gibt es ein $r \in \mathbb{Z}$ mit $\text{ggT}(r, n) = 1$ und $\zeta = \zeta_n^r$.

Dann ist $r = p_1 \cdot \dots \cdot p_m$ ein endliches Produkt von Primzahlen p_i mit $p_i \nmid n$ für alle $1 \leq i \leq m$.

Aus Behauptung 1 folgt induktiv:

$$f(\zeta_n^{p_1}) = 0$$

und $\zeta_n^{p_1} \in U_n$ ist primitiv.

Dann folgt aus der Behauptung 1 für $\zeta_n^{p_2}$, dass

$$(\zeta_n^{p_1})^{p_2} = \zeta_n^{p_1 \cdot p_2} \in U_n$$

primitiv ist und gilt:

$$f(\zeta_n^{p^1 \cdot p^2}) = 0$$

Dann folgt:

$$0 = f(\zeta_n^r) = f(\zeta)$$

□ Behauptung 2

Nach 12.8 ii) ist

$$\psi : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

injektiv.

Zeige also nur:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \geq |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$$

Beweis

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \stackrel{(12.4)}{=} \deg(f) \stackrel{\text{Beh. 2}}{\geq} |\{\zeta \in U_n \mid \zeta \text{ ist primitiv}\}| \stackrel{?? \text{ i)}}{=} \varphi(n)$$

□_{12.10}

12.11 Korollar

Seien $n, m \geq 1$ teilerfremd und $\zeta_n, \zeta_m \in \overline{\mathbb{Q}}$ primitive n -te (beziehungsweise m -te) Einheitswurzeln.

Dann gelten:

- i) $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n \cdot \zeta_m)$
- ii) $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$
- iii) Die Abbildung

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}) &\rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ \sigma &\mapsto (\sigma|_{\mathbb{Q}(\zeta_n)}, \sigma|_{\mathbb{Q}(\zeta_m)}) \end{aligned}$$

ist ein Gruppenisomorphismus.

Beweis

- i) Da $\zeta_n \cdot \zeta_m$ nach 12.4 eine primitive (nm) -te Einheitswurzel ist, gelten $\zeta_n, \zeta_m \in \mathbb{Q}(\zeta_n \cdot \zeta_m)$, denn $U_n, U_m \subseteq U_{nm}$.

Der Rest ist klar.

□_{i)}

ii) Wir haben folgendes Körperdiagramm:

TODO: Abbildung Körperdiagramm

Dabei gelten die Grade nach 12.10.

Aus der Gradformel für $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{nm})$ folgt:

$$[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_m)] = \varphi(n) \leq [\mathbb{Q}(\zeta_n) : E] \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \stackrel{12.10}{=} \varphi(n)$$

Also folgt:

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : E] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

Also folgt wegen $\mathbb{Q} \subseteq E$ schon $E = \mathbb{Q}$.

□_{ii)}

iii) Dies folgt aus i), ii) und 10.16 ii).

□_{12.11}

12.12 Bemerkung

In der Situation von 12.11 ist das Diagramm

TODO: Abb1 einfügen

kommutativ.

Beweis

TODO: Beweis einfügen (als Übung)

12.13 Definition (Kreisteilungspolynom)

Seien $n \in \mathbb{N}_{\geq 1}$ und $\{\zeta_1, \dots, \zeta_{\varphi(n)}\} \subseteq U_n \subseteq \bar{k}^*$ die primitiven n -ten Einheitswurzeln (vergleiche 12.7 i)). Dann heißt

$$\phi_n(X) := \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \bar{k}[X]$$

das n -te Kreisteilungspolynom über k .

12.14 Satz

Für $n \geq 1$ (und $\text{char}(k) \nmid n$) gelten:

- i) $\phi_n(X) \in k[X]$ ist separabel und normiert mit $\deg(\phi_n) = \varphi(n)$.
- ii) Aus $k = \mathbb{Q}$ folgt, dass $\phi_n(X) \in \mathbb{Z}[X]$ und irreduzibel ist.
- iii) $X^n - 1 = \prod_{0 < d|n} \phi_d(X) \in k[X]$

Beweis

i) Nach 12.13 ist klar, dass $\phi_n(X) \in \bar{k}[X]$ normiert, separabel und vom Grad $\varphi(n)$ ist.

Zeige also nur:

$$\phi_n(X) \in k[X]$$

Für

$$E := k(\zeta_n) = k(\zeta | \zeta \in U_n)$$

ist $\phi_n(X) \in E[X]$ und E/k ist endlich und galoissch nach 12.8 ii).

Für jedes $\sigma \in \text{Gal}(E/k)$ und jedes primitive $\zeta \in U_n$ ist auch $\sigma(\zeta) \in U_n$ primitiv, womit nach 12.13 folgt:

$$\phi_n^\sigma(X) = \phi_n(X)$$

Also folgt mit dem Hauptsatz der Galoistheorie:

$$\phi_n(X) \in \left(E^{\text{Gal}(E/k)}\right)[X] = k[X]$$

□_{i)}

ii) $\phi_n(X) \subseteq \mathbb{Q}[X]$ ist irreduzibel, denn genauer gilt für ein primitives $\zeta \in U_n(\mathbb{Q})$:

$$\begin{aligned} [\zeta_n : \mathbb{Q}] &\stackrel{12.10}{=} \varphi(n) \\ \deg(\phi_n(X)) &\stackrel{12.13}{=} \varphi(n) \\ \phi_n(\zeta_n) &\stackrel{12.13}{=} 0 \end{aligned}$$

Also gilt sogar:

$$\phi_n(X) = \text{Mipo}_{\mathbb{Q}}(\zeta_n)$$

Weil $\phi_n(X)$ normiert ist, folgt $\phi_n(X) | X^n - 1$ in $\mathbb{Q}[X]$ und mit 3.4 folgt $\phi_n(X) \in \mathbb{Z}[X]$.

□_{ii)}

iii) Für alle $0 < d|n$ gilt:

$$P_d := \{\zeta \in U_n | \text{ord}(\zeta) = d\}$$

Damit folgt:

$$U_n = \bigcup_{0 < d|n} P_d \quad (12.6)$$

Daher gilt in $\bar{k}[X]$:

$$X^n - 1 \stackrel{\text{klar}}{=} \prod_{\zeta \in U_n} (X - \zeta) \stackrel{(12.6)}{\stackrel{12.3}{=}} \prod_{0 < d|n} \phi_d(X)$$

Beachte auch, dass für alle Teiler d von n schon $U_d \subseteq U_n$ gilt.

□_{12.14}

12.15 Beispiel

Sei $k = \mathbb{Q}$. Mit 12.14 iii) kann man $\phi_n(X) \in \mathbb{Z}[X]$ durch Induktion über die Anzahl der Primfaktoren von n explizit berechnen:

- i) Für eine Primzahl $p > 0$ folgt mit 12.14 iii):

$$X^p - 1 = \underbrace{\phi_1(X)}_{X-1} \cdot \phi_p(X)$$

Daher gilt:

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \dots + 1 = \text{Mipo}_{\mathbb{Q}}(\zeta_p)$$

(vergleiche 4.5 iii))

- ii) Seien $p, q > 0$ Primzahlen mit $p \neq q$, so folgt mit 12.14 iii):

$$X^{pq} - 1 = \phi_1(X) \cdot \phi_p(X) \cdot \phi_q(X) \cdot \phi_{pq}(X)$$

Damit folgt nach i):

$$\phi_{pq}(X) = \frac{(X^{pq} - 1)(X - 1)(X - 1)}{(X - 1)(X^p - 1)(X^q - 1)} = \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}$$

Zur Einübung:

$$\begin{aligned} \deg(\phi_{pq}) &= \varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) = \\ &= \deg\left(\frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}\right) = pq + 1 - p - q \end{aligned}$$

Zum Beispiel gilt für $p = 2$ und $q = 3$:

$$\phi_6(X) = X^2 - X + 1 = \text{Mipo}_{\mathbb{Q}}\left(\zeta_6 = e^{\frac{\pi i}{3}}\right)$$

12.16 Satz und Definition (Nullstelle modulo p)

Seien \mathbb{F}_q ein endlicher Körper (vergleiche 9.1), $n \in \mathbb{N}_{\geq 1}$ eine natürliche Zahl mit $\text{ggT}(n, q) = 1$ und $\zeta_n \in \overline{\mathbb{F}_p}$ eine primitive n -te Einheitswurzel. Dann gilt:

- i) Der surjektive Gruppenhomomorphismus $\psi : \text{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\right) \hookrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ (vergleiche 12.8 ii) und iii)) erfüllt:

$$\psi(\text{Frob}_q) = \bar{q}$$

(vergleiche 9.5 i))

Insbesondere induziert ψ einen Isomorphismus:

$$\text{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\right) \xrightarrow{\sim} \langle \bar{q} \rangle \subseteq \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

- ii) $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \text{ord}\left(\bar{q} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$
 iii) $\phi_n(X) \in \mathbb{F}_q[X]$ ist genau dann irreduzibel, wenn $\langle \bar{q} \rangle = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.
 iv) Ist $q = p$ eine Primzahl, so gilt:

$$p \equiv 1 \pmod{n} \quad \Leftrightarrow \quad \zeta_n \in \mathbb{F}_p \subseteq \overline{\mathbb{F}_p}$$

Letzteres ist äquivalent dazu, dass $\phi_n(X) \in \mathbb{Z}[X]$ eine Nullstelle modulo p besitzt, das heißt:

$$\exists_{x \in \mathbb{Z}} : \phi_n(x) \equiv 0 \pmod{p}$$

Beweis

$$\text{i) } \zeta_n^{\psi(\text{Frob}_q)} \stackrel{12.10}{=} \text{Frob}_q(\zeta_n) \stackrel{\text{Def.}}{=} \zeta_n^q$$

Also folgt wegen $\text{ord}(\zeta_n) = n$ schon:

$$\psi(\text{Frob}_q) \equiv \bar{q}(n)$$

Die zweite Aussage folgt aus:

$$\text{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\right) = \langle \text{Frob}_q \rangle$$

(vergleiche 9.5 ii))

□_{i)}

$$\text{ii) } [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \left| \text{Gal}\left(\mathbb{F}_q(\zeta_n)/\mathbb{F}_1\right) \right| \stackrel{\text{i)}}{=} |\langle \bar{q} \rangle| = \text{ord}\left(\bar{q} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$$

□_{ii)}

iii) Die Irreduzibilität von $\phi_n(X) \in \mathbb{F}_q[X]$ ist äquivalent zu folgenden Aussagen:

$$\Leftrightarrow \phi_n(X) = \text{Mipo}_{\mathbb{F}_q}(\zeta_n)$$

$$\Leftrightarrow [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \varphi(n)$$

$$\Leftrightarrow \psi \text{ in i) ist surjektiv.}$$

$$\stackrel{\text{i)}}{\Leftrightarrow} \langle \bar{q} \rangle = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

□_{iii)}

$$\begin{aligned} \text{iv) } \quad p \equiv 1 \pmod{n} &\Leftrightarrow \langle \bar{p} \rangle = \{\tau\} \subseteq \left(\mathbb{Z}/n\mathbb{Z}\right)^* \\ &\stackrel{\text{i)}}{\Leftrightarrow} \text{Gal}\left(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p\right) = \{1\} \\ &\stackrel{\phi_n(\zeta_n)=0}{\Leftrightarrow} \phi_n \text{ besitzt eine Nullstelle in } \mathbb{F}_p. \end{aligned}$$

□_{12.16}

12.17 Beispiel

Sei $n = 4$, so folgt:

$$\phi_n(X) = \phi_n(X) \stackrel{\text{vergleiche 12.15 iii)}}{=} X^2 + 1$$

$p \nmid n$	3	5	7	11	13	...
Nullstelle von $X^2 + 1 \pmod{p}$	/	2	/	/	8	...
$p \pmod{n}$	-1	1	-1	-1	1	...

12.18 Lemma

Sei $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$ und setze:

$$P(f) := \{p | p > 0 \text{ ist eine Primzahl} \wedge f \text{ besitzt eine Nullstelle (mod } p)\}$$

Dann gilt:

$$|P(f)| = \infty$$

Beweis

Offenbar ist:

$$P(f) = \left\{ p \in \mathbb{Z}_{>0} \mid p \text{ ist eine Primzahl} \wedge \exists_{z \in \mathbb{Z}} : p | f(z) \text{ in } \mathbb{Z} \right\}$$

Schreibe $f = a_n X^n + \dots + a_0$ mit $a_i \in \mathbb{Z}$ und $a_n \neq 0$.

Ist $a_0 = 0$, so gilt $p | f(p)$ für alle Primzahlen p von \mathbb{Z} .

Sei also ohne Einschränkung $a_0 \neq 0$, dann folgt:

$$f(a_0 X) = a_0 \cdot \underbrace{(a_n a_0^{n-1} X^n + \dots + 1)}_{=: g(X)}$$

Damit folgt $P(g) \subseteq P(f)$.

Zeige also nur noch $|P(g)| = \infty$.

Angenommen dies wäre nicht so, dann sei:

$$P(g) = \{p_1, \dots, p_m\}$$

Dann existiert ein $\alpha \in \mathbb{Z}_{\geq 1}$ so, dass $0, \pm 1 \neq g(\alpha, p_1, \dots, p_m) =: N$, da $\deg(g) \geq 1$ ist.

TODO: Was ist $g(\alpha, p_1, \dots, p_n)$?

$$N \stackrel{\text{Def. von } g}{\equiv} 1 \pmod{p_i} \quad \forall_{1 \leq i \leq m} \quad (12.7)$$

Daher gibt es eine Primzahl q mit:

$$q | N \quad \Rightarrow \quad q \in P(g)$$

Damit folgt

$$N \equiv 0 \pmod{q}$$

und:

$$N \equiv 1 \not\equiv 0 \pmod{q}$$

Dies ist ein Widerspruch zur Endlichkeit von $P(g)$.

□_{12.18}

12.19 Satz

Für jede Zahl $n \geq 1$ existieren unendlich viele Primzahlen p mit $p \equiv 1 \pmod{n}$.

Beweis

12.16 iv) und 12.18 mit $f = \phi_n(X)$.

□_{12.19}

12.20 Bemerkung

Allgemeiner gilt der Satz von DIRICHLET:

Für $a, n \in \mathbb{N}_{\geq 1}$ mit $\text{ggT}(a, n) = 1$, gibt es unendlich viele Primzahlen p mit $p \equiv a \pmod{n}$.

(vergleiche JEAN-PIERRE SERRE, „A Course in Arithmetics“)

Anhang

GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.

`<https://fsf.org/>`

Everyone is permitted to copy and distribute verbatim copies of this license document,
but changing it is not allowed

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. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “**Document**”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “**you**”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “**Modified Version**” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “**Secondary Section**” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain

any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “**Invariant Sections**” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “**Cover Texts**” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “**Transparent**” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “**Opaque**”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, \LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “**Title Page**” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “**publisher**” means any person or entity that distributes copies of the Document to the public.

A section “**Entitled XYZ**” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “**Acknowledgements**”, “**Dedications**”, “**Endorsements**”, or “**History**”.) To “**Preserve the Title**” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.

- I. Preserve the section Entitled “History”, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <https://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation;

with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.