Algebra 1

UNI HEIDELBERG

Mit Liebe gemacht von:
NIKOLAUS SCHÄFER

Inhaltsverzeichnis

Teil I.

Elementare Gruppentheorie

1. Gruppen und Homomorphismen

Erinnerung an LA: Monoid/Gruppe
Wir schreiben Monoide/Gruppen multiplikativ und bezeichnen das neutrale Element mit e

Definition 1.0.1. M Monoid, $N \subseteq M$
N heißt ein Untermonoid von $M \Leftrightarrow$ es gilt:
(a) $e \in N$
(b) $a,b \in N \Rightarrow ab \in N$

Beispiel 1.0.2. $2\mathbb{N}_0 := \{2a | a \in \mathbb{N}_0\}$ ist ein Untermonoid von $\mathbb{N}_0$ bzgl. "+"

Definition 1.0.3. G Gruppe, $H \subseteq G$
H heißt Untergruppe von $G \Leftrightarrow$ Es gilt:
(a) H ist ein Untermonoid von G
(b) $a \in H \Rightarrow a^{-1} \in H$ (hierbei bezeichne a^{-1} das Inverse zu a)

Beispiel 1.0.4. K Körper $\Rightarrow SL(n,K) := \{A \in GL(n,K) | \det(A) = 1\}$ (spezielle lineare Gruppe) ist eine Untergruppe von GL(n,K) (beachte: $\det(A^{-1}) = \det(A)^{-1}$)

Anmerkung: Ist G eine Gruppe und $H \subseteq G$ eine Untergruppe, dann ist H mit der eingeschränkten Verknüpfung von G eine Gruppe. (analog für (Unter-)monoide).

Bemerkung 1.0.5. (Untergruppenkriterium)
G Gruppe, $H \subseteq G$. Dann sind äquivalent:
(i) H ist eine Untergruppe von G
(ii) $H \neq \emptyset$ und für alle $a,b \in H$ ist $ab^{-1} \in H$

Beispiel 1.0.6. Für jedes $n \in \mathbb{Z}$ ist $n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$, denn:

- $n\mathbb{Z} \neq \emptyset$ wegen $0 \in n\mathbb{Z}$
- $a,b \in n\mathbb{Z} \Rightarrow$ Es existiert $\tilde{a},\tilde{b} \in \mathbb{Z}$ mit $a = n\tilde{a}$, $b = n\tilde{b} \Rightarrow a - b = n\tilde{a} - n\tilde{b} = n(\tilde{a} - \tilde{b}) \in n\mathbb{Z}$

Bemerkung 1.0.7. G Gruppe, $(H_i)_{i \in I}$ Familie von Untergruppen von G
Dann ist $H := \bigcap_{i \in I} H_i$ eine Untergruppe von G

Definition 1.0.8. G Gruppe, $M \subseteq G$ Teilmenge
$< M > := \bigcap_{H \subseteq G \text{ mit } H \supseteq M} H$ heißt die von M erzeugte Untergruppe von G.
Ist $M = \{x_1, \ldots, x_r\}$ endlich, dann schreiben wir auch $< x_1, \ldots, x_r >$ für $< \{x_1, \ldots, x_r\} >$
Existiert ein $x \in G$ mit $G = < x >$, so heißt G zyklisch.

Anmerkung: $< M >$ ist die kleinste Untergruppe von G, die M enthält.

Bemerkung 1.0.9. G Gruppe, $M \subseteq G$. Dann gilt:
$< M > = \{x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n} | n \in \mathbb{N}_0, x_1, \ldots, x_n \in M, \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}\}$

Folgerung 1.0.10. G Gruppe, $x \in G$
Dann gilt: $< x > = \{x^n | n \in \mathbb{Z}\}$
Insbesondere ist $< x >$ abelsch, und jede zyklische Gruppe ist abelsch.

Beispiel 1.0.11. $\mathbb{Z} =< 1 >$, denn: $< 1 >= \{n \cdot 1 | n \in \mathbb{Z}\} = \mathbb{Z}$, insbesondere ist $\mathbb{Z}$ zyklisch.

Erinnerung: an LA: Gruppenhomomorphismus

Bemerkung 1.0.12. G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus. Dann gilt:
(a) $H \subseteq G$ Untergruppe $\Rightarrow \varphi(H) \subseteq G'$ Untergruppe
(b) $H' \subseteq G'$ Untergruppe $\Rightarrow \varphi^{-1}(H') \subseteq G$ Untergruppe

Definition 1.0.13. G, G' Gruppen, e' neutrale Element von G', $\varphi : G \to G'$ Homomorphismus
$\ker(\varphi) := \varphi^{-1}(\{e'\}) = \{a \in G | \varphi(a) = e'\}$ heißt der Kern von φ
$im(\varphi) := \varphi(G) = \{\varphi(a) | a \in G\}$ heißt das Bild von φ

Bemerkung 1.0.14. G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus. Dann gilt:
(a) $\ker(\varphi) \subseteq G$ ist eine Untergruppe
(b) $im(\varphi) \subseteq G'$ ist eine Untergruppe
(c) φ injektiv $\Leftrightarrow \ker(\varphi) = \{e\}$
(d) φ surjektiv $\Leftrightarrow im(\varphi) = G'$

Beispiel 1.0.15. $sgn : S_N \to \{\pm 1\}$
$A_n := \ker(sgn) = \{\pi \in S_n | sgn(\pi) = 1\}$ ist eine Untergruppe von S_n, die alternierende Gruppe.

Definition 1.0.16. G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus
φ heißt:
Monomorphismus $\Leftrightarrow \varphi$ ist injektiv
Epimorphismus $\Leftrightarrow \varphi$ ist surjektiv
Isomorphisms $\Leftrightarrow \varphi$ ist bijektiv
Ist $G = G'$ und φ ein Isomorphismus, dann heißt φ ein Automorphismus von G. Zwei Gruppen heißen isomorph $\Leftrightarrow$ Es gibt einen Isomorphismus zwischen ihnen.

Anmerkung: $\varphi : G \to G'$ Isomorphismus, dann ist die Umkehrabbildung $\varphi^{-1} : G' \to G$ ein Homomorphismus (also auch ein Isomorphismus)

Bemerkung 1.0.17. G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus. Dann sind äquivalent:
(i) φ ist ein Isomorphismus
(i) Es existiert ein Homomorphismus (Isomorphismus) $\psi : G' \to G$ mit $\varphi \circ \psi = id_{G'}$, und $\psi \circ \varphi = id_G$ Insbesondere ist für eine Gruppe G die Menge $Aut(G) := \{\varphi : G \to G | \varphi$ ist ein Automorphismus$\}$ eine Gruppe bzgl. "$\circ$".

Bemerkung 1.0.18. G Gruppe, $a \in G$
Dann ist die Abbildung $\tau_a : G \to G$, $g \mapsto ag$ ("Linkstranslation mit a") bijektiv (aber für $a \neq e$ kein Gruppenhomomorphismus). Insbesondere ist $\tau_a \in S(G)$

Bemerkung 1.0.19. G Gruppe. Dann ist die Abbildung $\varphi : G \to S(G)$, $a \mapsto \tau_a$ ein Monomorphismus

Folgerung 1.0.20. (Satz von Cayley)
G endliche Gruppe mit n Elementen. Dann existiert ein Monomorphismus $G \to S_n$ (d.h. G kann bis auf Isomorphie als Untergruppe der S_n aufgefasst werden.)

Bemerkung 1.0.21. G Gruppe, $a \in G$
Dann ist die Abbildung $\varphi_a : G \to G$, $g \mapsto aga^{-1}$ ("Konjugation mit a")
ist ein Automorphismus von G

2. Normalteiler und Faktorgruppen

In diesem Abschnitt sei G stets ein Gruppe

Bemerkung 2.0.1. $H \subseteq G$ Untergruppe. Durch $a \sim_H b \Leftrightarrow b^{-1}a \in H$ ist eine Äquivalenzrelation auf G erklärt. Die Äquivalenzklasse von $a \in G$ ist durch $aH := \{ah | h \in H\}$ gegeben. Insbesondere gilt für $a,b \in G$: Entweder ist $aH = bH$ oder $aH \cap bH = \emptyset$

Definition 2.0.2. $H \subseteq G$ Untergruppe
Eine Linksnebenklasse von H in G ist eine Teilmenge von G der Gestalt $aH = \{ah | h \in H\}$,
d.h. eine Äquivalenzklasse bzgl. "$\sim_H$". Elemente einer Linksnebenklasse heißen Repräsentanten. Die Menge der Linksnebenklasssen von H in G mit G/H

Satz 2.0.3. $H \subseteq G$ Untergruppe. Dann gilt:
(a) Je zwei Linksnebenklassen von H in G sind gleichmächtig
(b) Je zwei Linksnebenklassen von H in G sind entweder gleich oder disjunkt
(c) G ist die disjunkte Vereinigung der Linksnebenklassen von H in G

Anmerkung: In analoger Weisen zu Linksnebenklassen von H in G sind Rechtsnebenklassen von H in G erklärt, nämlich als Teilmengen der Gestalt: $Ha = \{ha | h \in H\}$
Menge der Rechtsnebenklassen von H in G: $H\backslash G$, $a \in G$
Es ist im Allgemeinen $aH \neq Ha$

Bemerkung 2.0.4. $H \subseteq G$ Untergruppe. Dann gilt:
Die bijektive Abbildung $\psi : G \to G, a \mapsto a^{-1}$ induziert eine bijektive Abbildung $\phi : G/H \to H\backslash G, aH \mapsto Ha^{-1} = \psi(aH)$

Definition 2.0.5. $H \subseteq G$ Untergruppe
Die Ordnung von G ist die Anzahl der Elemente von G, falls diese endlich ist, sonst ∞. Bezeichnung: $ord(G)$
Der Index von H in G ist die Anzahl der Linksnebenklassen von H in G, falls diese endlich sonst ∞. Bezeichnung: $(G : H)$

Anmerkung: Wegen 2.4 stimmt (G:H) mit der Anzahl der Rechtsnebenklassen von H in G überein.

Satz 2.0.6. (Satz von Lagrange) $H \subseteq G$ Untergruppe
Dann gilt: $ord(G) = ord(H) \cdot (G : H)$
Insbesondere ist $ord(H)$ ein Teiler von $ord(G)$

Definition 2.0.7. $H \subseteq G$ Untergruppe
H heißt Normalteiler von G (normale Untergruppe)
$\Leftrightarrow aH = Ha$ für alle $a \in G$ Bezeichnung: $H \trianglelefteq G$
In diesem Fall bezeichnet man die Nebenklasse $aH = Ha$ auch als die Restklasse von a modulo H

Beispiel 2.0.8.
(a) G Gruppe $\Rightarrow \{e\} \trianglelefteq G$, $G \trianglelefteq G$
(b) G abelsche Gruppe $\Rightarrow$ Jede Untergruppe von G ist Normalteiler

Bemerkung 2.0.9. $H \subseteq G$ Untergruppe. Dann sind äquivalent:
(i) $H \trianglelefteq G$
(ii) $aHa^{-1} = H$ für alle $a \in G$
(iii) $aHa^{-1} \subseteq H$ für alle $a \in G$
(iv) $aba^{-1} \in H$ für alle $a \in G, b \in H$

Bemerkung 2.0.10. G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus. Dann gilt:
(a) $H' \trianglelefteq G' \Rightarrow \varphi^{-1}(H') \trianglelefteq G$
(b) $\ker(\varphi) \trianglelefteq G$
(c) $H \trianglelefteq G$ und φ surjektiv $\Rightarrow \varphi(H) \trianglelefteq G'$

Anmerkung: $im(\varphi)$ ist im allgemeinen kein Normalteiler von G'

Beispiel 2.0.11. $A_n \trianglelefteq S_n$, denn $A_n = \ker(sgn)$

Bemerkung 2.0.12. $H \subseteq G$ Untergruppe, mit $(G : H) = 2$. Dann ist $H \trianglelefteq G$

Bemerkung 2.0.13. $H \trianglelefteq G$
Die Menge der Restklassen G/H wird mittels der Verknüpfung:
$G/H \times G/H \to G/H$, $(aH) \cdot (bH) := abH$
zu einer Gruppe, der Faktorgruppe von G modulo H

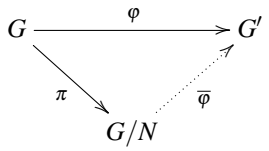
Beispiel 2.0.14.
(a) $G = \mathbb{Z}$, $H = m\mathbb{Z} \rightsquigarrow \mathbb{Z}/m\mathbb{Z}$ mit der Verknüpfung $\overline{a} + \overline{b} = \overline{a+b}$
(b) K Körper, $G = GL(n,K)$, $H = \{aE_n | a \in K^*\} \rightsquigarrow PGL(n,K) := G/H$ heißt die projektive allgemeine lineare Gruppe

Bemerkung 2.0.15. $H \trianglelefteq G$
Dann ist die Abbildung $\pi : G \to G/H$, $a \mapsto aH$ ein Epimorphismus mit $\ker(\pi) = H$
π heißt die kanonische Projektion von G nach G/H

Folgerung 2.0.16. $H \subseteq G$ Untergruppe. Dann sind äquivalent:
(i) $H \trianglelefteq G$
(ii) Es existiert ein Gruppe G', Homomorphismus $\varphi : G \to G'$ mit $\ker(\varphi) = H$

Bemerkung 2.0.17. $H \trianglelefteq G$, $\pi : G \to G/H$ kanonische Projektion. Dann ist die Abbildung
$\phi : \{\text{Untergruppen von } G/H\} \to \{\text{Untergruppen } V \text{ von } G \text{ mit } V \supseteq H\}$, $U \mapsto \pi^{-1}(U)$
ist eine inklusionserhaltende Bijektion, und es gilt: $U \trianglelefteq G/H \Leftrightarrow \phi(U) \trianglelefteq G$

Satz 2.0.18. G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus, $N \trianglelefteq G$ mit $N \subseteq \ker(\varphi)$ Dann existiert ein eindeutig bestimmter Gruppenhomomorphismus. $\overline{\varphi} : G/N \to G'$, so dass folgendes Diagramm kommutiert:



d.h. $\overline{\varphi} \circ \pi = \varphi$. Explizit ist $\overline{\varphi}$ gegeben durch $\overline{\varphi} : G/N \to G'$, $aN \mapsto \varphi(a)$

Satz 2.0.19. (Homomorphiesatz)
G, G' Gruppen, $\varphi : G \to G'$ Homomorphismus
Dann gibt es einen eindeutig bestimmten Isomorphismus $\phi : G/\ker(\varphi) \to im(\varphi)$, sodass folgendes Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & & \uparrow i \\ G/\ker(\varphi) & \xrightarrow[\phi]{\cong} & im(\varphi) \end{array}$$

Hierbei ist π die kanonische Projektion, i die Inklusionsabbildung. Die Abbildung ϕ ist explizit gegeben durch $\phi(a\ker(\varphi)) = \varphi(a)$

Anmerkung: Häufig verwendet man davon nur $G/\ker(\varphi) \cong im(\varphi)$

Definition 2.0.20. $H_1, H_2 \subseteq G$ Untergruppen
$H_1H_2 := \{h_1h_2 | h_1 \in H_1, h_2 \in H_2\}$

Bemerkung 2.0.21. $H_1, H_2 \subseteq G$ Untergruppen. Dann gilt:
(a) $H_1 \trianglelefteq G$ oder $H_2 \trianglelefteq G \Rightarrow H_1H_2 \subseteq G$ Untergruppe
(b) $H_1 \trianglelefteq G$ und $H_2 \trianglelefteq G \Rightarrow H_1H_2 \trianglelefteq G$.

Satz 2.0.22. (Erster Isomorphiesatz) $H \subseteq G$ Untergruppe, $N \trianglelefteq G$
Dann gilt: Die Inklusion $H \overset{i}{\hookrightarrow} HN$ und die kanonische Projektion $\pi : HN \to HN/N$ induzieren einen Isomorphismus $H/H \cap N \xrightarrow{\cong} HN/N$, $a(H \cap N) \mapsto aN$

Satz 2.0.23. (Zweiter Isomorphiesatz)
$N, H \trianglelefteq G$ mit $N \subseteq H$. Dann ist die Abbildung:

$(G/N)/(H/N) \to G/H$, $(aN)H/N \mapsto aH$
ein Isomorphismus.

3. Zyklische Gruppen

Bemerkung 3.0.1. G Gruppe. Dann sind äquivalent:
(i) G ist zyklisch
(ii) Es gibt ein Epimorphismus $\varphi : \mathbb{Z} \to G$

Satz 3.0.2. Die Untergruppen von $\mathbb{Z}$ sind genau die folgenden:
$\{0\}, n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$, $n \in \mathbb{N}$
Für $n \in \mathbb{N}$ gilt: $n\mathbb{Z} \cong \mathbb{Z}$

Anmerkung: alternatives Argument: Untergruppen von $\mathbb{Z} = \mathbb{Z}$-Untermodul von $\mathbb{Z}$ = Ideale in $\mathbb{Z}$, $\mathbb{Z}$ HIR.

Folgerung 3.0.3. G zyklische Gruppe. Dann gilt:
$$G \cong \begin{cases} \mathbb{Z}, \text{ falls } ord(G) = \infty \\ \mathbb{Z}/n\mathbb{Z}, \text{ falls } ord(G) = n \in \mathbb{N} \end{cases}$$

Satz 3.0.4. G zyklische Gruppe, $H \subseteq G$ Untergruppe. Dann gilt:
(a) H ist zyklisch
(b) G/H ist zyklisch

Definition 3.0.5. G Gruppe, $a \in G$
$ord(a) := min\{n \in \mathbb{N} | a^n = e\}$, falls ein $n \in \mathbb{N}$ existiert mit $a^n = e$
(Andernfalls setzt man $ord(a) := \infty$)
heißt die Ordnung des Elements a.

Bemerkung 3.0.6. G Gruppe, $a \in G$. Dann gilt: $ord(a) = ord(< a >)$

Folgerung 3.0.7. G Gruppe, $a \in G$
Dann gilt: $ord(a) | ord(G)$

Satz 3.0.8. G endliche Gruppe mit $ord(G) = p$, p Primzahl
Dann gilt: G ist zyklisch, insbesondere $G \cong \mathbb{Z}/p\mathbb{Z}$

Satz 3.0.9. (Kleiner Satz von Fermat) G endliche Gruppe, $a \in G$
Dann gilt: $a^{ord(G)} = e$

Definition 3.0.10. $(G_i)_{i \in I}$ Familie von Gruppen
Das kartesische Produkt $\prod_{i \in I} G_i$ wird durch komponentenweise Verknüpfung zu einer Gruppe.
Diese bezeichnet man als das direkte Produkt über die Famile $(G_i)_{i \in I}$

Satz 3.0.11. (Hauptsatz über endlich erzeugte abelsche Gruppen)
G endlich erzeugte abelsche Gruppe (d.h. es existieren $m \in \mathbb{N}$, $x_1, \ldots, x_m \in G$ mit $G =< x_1, \ldots, x_m >$).
Dann existieren eindeutig bestimmte Zahlen $r, s \in \mathbb{N}_0$, $d_1, \ldots, d_s \in \mathbb{N}_{>1}$ mit $d_1 | \ldots | d_s$, sodass
$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z}$.

Beispiel 3.0.12. Bis auf Isomorphie gibt es folgende abelsche Gruppen der Ordnung 24:
$\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Teil II.

Ringe

4. Ringe und Ideale

In diesem Abschnitt sei R stets ein kommutativer Ring.

Bemerkung 4.0.1. $I \subseteq R$ Ideal, $\pi : R \to R/I$ kanonische Projektion
Dann ist die Abbildung:
$\phi : \{$ Ideale in $R/I\} \to \{$ Ideale $\tilde{I}$ in R mit $\tilde{I} \geq I\}$
$J \mapsto \pi^{-1}(J)$
eine inklusionserhaltende Bijektion

Satz 4.0.2. (Homomorphiesatz für Ringe) R' kommutativer Ring, $\varphi : R \to R'$ Ringhomomorphismus
Dann gibt es einen eindeutig bestimmten Ringisomorphismus
$\phi : R/\ker(\varphi) \to im(\varphi)$, sodasss folgendes Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \pi \downarrow & & \uparrow i \\ R/\ker(\varphi) & \xrightarrow[\phi]{\cong} & im(\varphi) \end{array}$$

Hierbei ist π die kanonische Projektion, i die Inklusionsabbildung. Die Abbildung ϕ ist explizit gegeben durch $\phi(a+\ker(\varphi)) = \varphi(a)$ für alle $a \in R$.

Definition 4.0.3. R heißt Körper $\Leftrightarrow R^* = R\backslash\{0\}$

Anmerkung: Insbesondere $R = 0$ kein Körper.

Satz 4.0.4. $R \neq 0$. Dann sind äquivalent:
(i) R ist ein Körper
(ii) (0) und (1) = R sind die einzigen Ideale in R
(iii) Jeder Ringhomomorphismus $\varphi : R \to S$ in einen kommutativen Ring $S \neq 0$ ist injektiv.

Bemerkung 4.0.5. $I, J \subseteq R$ Ideale. Dann sind:
$I+J := \{a+b | a \in I, b \in J\}$, $I \cap J$, $IJ := \{\sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}_0, a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in I\}$ Ideale in R.
Analog für endliche Familie von Idealen, insbesondere $I^n := \underbrace{I \cdots I}_{\text{n-mal}}$ für $n \in \mathbb{N}$.
Konvention: $I^0 := (1) = R$
I, J heißen relativ prim $\Leftrightarrow I + J = (1)$

Anmerkung: Offenbar ist die Multiplikation von Idealen assoziativ, Klammerung nicht notwendig.

Beispiel 4.0.6. $R = \mathbb{Z}$, $I = (2)$, $J = (3)$

- $I + J = (1)$, denn $1 = \underbrace{(-1)\cdot 2}_{\in(2)} + \underbrace{1 \cdot 3}_{\in(3)} \in I + J$
- $I \cap J = (6)$
- $IJ = (6)$

Bemerkung 4.0.7. $I,J,K \subseteq R$ Ideale. Dann gilt:
(a) $I(J+K) = IJ + IK$
(b) $(I \cap J)(I+J) \subseteq IJ \subseteq I \cap J$
(c) $I + J = (1) \Rightarrow I \cap J = IJ$

Bemerkung 4.0.8. $I_1, \ldots, I_n \subseteq R$ paarweise relativ prime Ideale. Dann gilt:
$I_1 \cdot \ldots \cdot I_n = I_1 \cap \ldots \cap I_n$

Bemerkung 4.0.9. $(R_i)_{i \in I}$ Familie von Ringen
Das kartesische Produkt $\prod_{i \in I} R_i$ wird durch komponentenweise Addition und Multiplikation zu einem Ring. Diesen bezeichnet man als das direkte Produkt über die Familie $(R_i)_{i \in I}$.

Satz 4.0.10. (Chinesischer Restsatz)
$I_1, \ldots, I_n \subseteq R$ Ideale, $\varphi : R \to \prod_{i=1}^{n} R/I_i$, $r \mapsto (r + I_1, \ldots, r + I_n)$ (ist offenbar Ringhomomorphismus). Dann gilt:
(a) φ surjektiv $\Leftrightarrow$ Die Ideale $I_1, \ldots, I_n$ sind paarweise relativ prim,
(b) $\ker(\varphi) = \bigcap_{i=1}^{n} I_i$
(c) φ injektiv $\Leftrightarrow \bigcap_{i=1}^{n} I = (0)$
Insbesondere erhalten wir unter der Voraussetzung, dass $I_1, \ldots, I_n$ paarweise relativ prim sind, einen Ringisomorphismus: $R/\bigcap_{i=1}^{n} I_i \cong R/I_1 \times \cdots \times R/I_n$

Beispiel 4.0.11. $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $a \mapsto (a + 2\mathbb{Z}, a + 3\mathbb{Z})$
ist surjektiv wegen $(2) + (3) = (1)$
$\ker(\varphi) = (2) \cap (3) = (6)$ D.h. φ induziert einen Ringisomorphismus $\mathbb{Z}/6\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Folgerung 4.0.12. $m_1, \ldots, m_n \in \mathbb{Z}$ paarweise teilerfremd, $a_1, \ldots, a_n \in \mathbb{Z}$
Dann hat das System von Kongruenzen
$x \equiv a_1 \pmod{m_1}$
$\vdots$
$x \equiv a_n \pmod{m_n}$

eine Lösung. Ist $x \in \mathbb{Z}$ eine Lösung des Systems, dann ist die Menge aller Lösungen gegeben durch $x + m_1 \cdot \ldots \cdot m_n\mathbb{Z}$

Definition 4.0.13. $I \subseteq R$ Ideal. I heißt:
Primideal $\Leftrightarrow I \neq R$ und für alle $x, y \in R$ gilt: $xy \in I \Rightarrow x \in I$ oder $y \in I$
maximales Ideal $\Leftrightarrow I \neq R$ und es existiert kein Ideal $J \subseteq R$ mit $I \subsetneq J \subsetneq R \Leftrightarrow I \neq R$ und für alle Ideale $J \subsetneq R$ gilt: $I \subseteq J \Rightarrow I = J$ (d.h. I ist maximal bzgl. $''\subseteq''$ unter allen Idealen $\neq R$ in R)

Bemerkung 4.0.14. $I \subseteq R$ Ideal. Dann gilt:
(a) I Primideal $\Leftrightarrow R/I$ nullteilerfrei
(b) I maximales Ideal $\Leftrightarrow R/I$ Körper

Folgerung 4.0.15. $I \subseteq R$ maximales Ideal. Dann ist I ein Primideal.

Bemerkung 4.0.16. $n \in \mathbb{N}$. Dann sind äquivalent:
(i) n ist eine Primzahl
(ii) $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei
(iii) $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper

Folgerung 4.0.17.
Primideale in $\mathbb{Z}$: $(0), (p)$ für p Primzahl
maximale Ideale in $\mathbb{Z}$: (p) für p Primzahl

Satz 4.0.18. $R \neq 0$. Dann besitzt R ein maximales Ideal.

Folgerung 4.0.19. Es gilt:
(a) Jedes Ideal $I \subsetneq R$ ist in einem maximalen Ideal von R enthalten.
(b) Jede Nichteinheit in R ist einem maximalen Ideal von R enthalten.

5. Polynomringe

In diesem Abschnitt sei R stets ein kommutativer Ring.

Notation: $n \in \mathbb{N}$
$R[X_1,\ldots,X_n] := \{\sum_{i=(i_1,\ldots,i_n)\in\mathbb{N}_0^n} a_i X_1^{i_1}\cdot\ldots\cdot X_n^{i_n} | a_i \in R \text{ mit } a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0^n\}$ mit üblicher Polynomaddition und multiplikation ist ein kommutativer Ring, der Polynomring über R in den Variablen $X_1,\ldots,X_n$.

Anmerkung:

- für eine präzise Definition vgl. Übung
- Es lassen sich auch Polynomringe $R[X_i|i\in I]$ für beliebige Indexmengen I definieren.
- Offenbar ist R ein Unterring von $R[X_1,\ldots,X_n]$ und $R[X_1,\ldots,X_n] = (R[X_1,\ldots,X_{n-1}])[X_n]$

Satz 5.0.1. (Universelle Eigenschaft von Polynomringen)
R,S kommutative Ringe, $\varphi : R \to S$ Ringhomomorphismus, $\alpha_1,\ldots\alpha_n \in S$
Dann existiert ein eindeutig bestimmter Ringhomomorphismus
$\phi : R[X_1,\ldots,X_n] \to S$ mit $\phi(X_i) = \alpha_i$ für $i = 1,\ldots,n$ und $\phi|_R = \varphi$

Folgerung 5.0.2. $a \in R$
Dann existiert ein surjektiver Ringhomomorphismus $\phi_a : R[X] \to R$ mit $\phi_a|_R = id_R$, $\phi_a(X) = a$ (Einsetzungshomomorphismus)
(explizit: $\phi_a(\sum_{i=0}^{n} b_i X^i) = \sum_{i=0}^{n} b_i a^i$)
Für $f \in R[X]$ setzen wir $f(a) := \phi_a(f)$

Anmerkung: $f \in R[X]$. Dann erhalten wir eine Abbildung $f^* : R \to R$, $a \mapsto f(a)$
Im Allgemeinen ist f durch die Abbildung f^* nicht eindeutig bestimmt:
z.B. $R = \mathbb{Z}/2\mathbb{Z}$, $f_1 = 0$, $f_2 = (X-\overline{1})X$. Dann ist $f_1(\overline{0}) = \overline{0} = f_2(\overline{0})$, $f_1(\overline{1}) = \overline{0} = f_2(\overline{1})$. Dann sind f_1^*, f_2^* die Nullabbildungen, jedoch $f_1 \neq f_2$.

Definition 5.0.3. $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in R[X]$ mit $a_n \neq 0$.
Dann heißt n der Grad von f (Bezeichnung: $\deg(f)$), a_n der Leitkoeffizient von f (Bezeichnung: $l(f)$)
f heißt normiert $\Leftrightarrow l(f) = 1$
$\deg(0) := -\infty, l(0) := 0$

Bemerkung 5.0.4. $f,g \in R[X]$. Dann gilt:
(a) $l(fg) = l(f)l(g)$, falls $l(f)$ oder $l(g)$ kein Nullteiler ist.
(b) $\deg(fg) \leq \deg(f) + \deg(g)$ ("=", falls $l(f)$ oder $l(g)$ kein Nullteiler ist)
(c) $\deg(f+g) \leq max\{\deg(f),\deg(g)\}$ ("=", falls $\deg(f) \neq \deg(g)$)

Bemerkung 5.0.5. R nullteilerfrei. Dann gelten:
(a) $R[X]$ nullteilerfrei
(b) $R[X_1,\ldots,X_n]$ nullteilerfrei
(c) $R[X]^* = R^*$
(d) $(R[X_1,\ldots,X_n])^* = R^*$

Satz 5.0.6. (Division mit Rest)
$f, g \in R[X]$, $l(g) \in R^*$
Dann existieren eindeutig bestimmte Polynome $q, r \in R[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$

Definition 5.0.7. $\alpha \in R$, $f \in R[X]$
α heißt Nullstelle von $f \Leftrightarrow f(\alpha) = 0$.

Bemerkung 5.0.8. $f \in R[X]$, $\alpha \in R$ Nullstelle von f
Dann existiert ein $q \in R[X]$ mit $f = (X - \alpha)q$

Folgerung 5.0.9. R nullteilerfrei, $f \in R[X], f \neq 0$, $n := \deg(f)$
Dann besitzt f in R höchstens n Nullstellen.

Beispiel 5.0.10. $R = \mathbb{Z}/8\mathbb{Z}$ (nicht nullteilerfrei: $\overline{0} = \overline{2} \cdot \overline{4}$), $f = X^2 - \overline{1}$ f hat die Nullstellen $\overline{1}, \overline{3}, \overline{5}, \overline{7}$ (obwohl $\deg(f) = 2$).

6. Primfaktorzerlegung

In diesem Abschnitt sei R stets ein nullteilerfreier kommutativer Ring.

Definition 6.0.1. $\pi \in R\backslash(R^* \cup \{0\})$
π heißt Primelement $\Leftrightarrow$ Aus $\pi|ab$ mit $a,b \in R$ folgt $\pi|a$ oder $\pi|b$
π heißt irreduzibel $\Leftrightarrow$ Aus $\pi = ab$ mit $a,b \in R$ folgt stets $a \in R^*$ oder $b \in R^*$

Anmerkung:

- In LA2 gezeigt π Primelement $\Rightarrow$ π irreduzibel
- Es gibt Beispiele für irreduzible Elemente, die keine Primelemente sind

Bemerkung 6.0.2. $\pi \in R\backslash(R^* \cup \{0\})$. Dann sind äquivalent:
(i) π ist irreduzibel
(ii) (π) ist maximal bzgl. "$\subseteq$" in $\{I \subsetneq R | I \text{ ist Hauptideal}\}$

Satz 6.0.3. R HIR. $\pi \in R\backslash(R^* \cup \{0\}$. Dann sind äquivalent:
(i) π ist irreduzibel
(ii) π ist Primelement
(iii) (π) ist maximales Ideal in R

Bemerkung 6.0.4.
$a \in R$ habe Zerlegungen $a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$
Dann ist $r = s$ und nach Umnummerieren ist $p_i \hat{=} q_i$ für $i = 1, \ldots r$

Satz 6.0.5. Es sind äquivalent:
(i) Jedes $a \in R\backslash(R^* \cup \{0\})$ lässt sich eindeutig bis auf Reihenfolge und Assoziiertheit als Produkt irreduzibler Elemente aus R schreiben.
(ii) Jedes $a \in R\backslash(R^* \cup \{0\})$ lässt sich als Produkt von Primelementen aus R schreiben.
In diesem Fall heißt R ein faktorieller Ring.

Folgerung 6.0.6. R faktorieller Ring, $\pi \in R\backslash(R^* \cup \{0\})$. Dann sind äquivalent:
(i) π irreduzibel
(ii) π Primelement
Insbesondere lässt sich in R jedes Element aus $R\backslash(R^* \cup \{0\})$ eindeutig bis auf Reihenfolge und Assoziiertheit als Produkt von Primelementen schreiben.

Satz 6.0.7. R HIR. Dann ist R faktoriell.

Bemerkung 6.0.8. R faktorieller Ring. $\mathbb{P}$ Vertretersystem von Primelementen von R modulo "$\hat{=}$", $a \in R\backslash\{0\}$. Dann existieren eindeutig bestimmte $v_p(a) \in \mathbb{N}_0$ für $p \in \mathbb{P}$, $\varepsilon \in R^*$ mit $v_p(a) = 0$ für fast alle $p \in \mathbb{P}$, sodass:
$a = \varepsilon \prod_{p \in \mathbb{P}} p^{v_p(a)}$

Beispiel 6.0.9. $R = \mathbb{Z}$, wähle $\mathbb{P} = \{p \in \mathbb{N} | p \text{ Primelement}\}$. Jedes $a \in \mathbb{Z}\backslash\{0\}$ lässt sich eindeutig als $a = \varepsilon \prod_{p \in \mathbb{P}} p^{v_p(a)}$, $\varepsilon \in \{\pm 1\}$ schreiben.
z.B. $90 = 2 \cdot 3^2 \cdot 5$, d.h. $v_2(90) = 1$, $v_3(90) = 1$, $v_5(90) = 1$, $v_p(90) = 0$ für $p \in \mathbb{P}\backslash\{2,3,5\}, \varepsilon = 1$

Bemerkung 6.0.10. R HIR, $a_1,\ldots,a_n \in R$ Dann gilt:
(a) $GGT(a_1,\ldots,a_n) \neq \emptyset$
(b) $d \in GGT(a_1,\ldots,a_n) \Leftrightarrow (d) = (a_1,\ldots,a_n)$

Folgerung 6.0.11. R HIR, $a,b \in R$, $d \in GGT(a,b)$
Dann existiert $u,v \in R$ mit $d = ua + vb$

Bemerkung 6.0.12. R faktorieller Ring, $\mathbb{P}$ Vertretersystem von Primelementen von R modulo "$\hat{=}$", $a_1,\ldots,a_n \in R\backslash\{0\}$ mit $a_i = \varepsilon_i \prod_{p\in\mathbb{P}} p^{v_p(a_i)}$, $\varepsilon_i \in R^*$, $i = 1,\ldots,n$
Dann gilt:
$GGT(a_1,\ldots,a_n) \neq \emptyset$, und es ist $\prod_{p\in\mathbb{P}} p^{min\{v_p(a_1),\ldots v_p(a_n)\}} \in GGT(a_1,\ldots,a_n)$.

Anmerkung: In faktoriellen Ringen existieren GGTs, 6.10(b), 6.11 sind jedoch im Allgemeinen nicht erfüllt.

Satz 6.0.13. R euklidischer Ring. Dann ist R ein HIR.

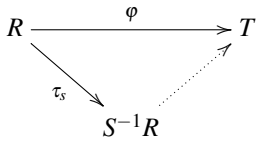
Folgerung 6.0.14. R euklidischer Ring. Dann ist R faktoriell.

7. Lokalisierung

In diesem Abschnitt sei R stets ein kommutativer Ring

Satz 7.0.1. $S \subseteq R$ Untermonoid bzgl. "$\cdot$", dann gilt:
(a) Aus $R \times S$ ist durch $(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow$ Es existiert ein $t \in S$ mit $tr_2s_1 = tr_1s_2$ eine Äquivalenzrelation gegeben. Wir setzen $S^{-1}R = (R \times S)/\sim$ (Menge der Äquivalenzklassen), $\frac{r}{s}$ bezeichnet die Äquivalenzklasse von $(r,s) \in R \times S$
(b) $S^{-1}R$ ist ein Ring via
$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1s_2+r_2s_1}{s_1s_2}$, $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1r_2}{s_1s_2}$
$S^{-1}R$ heißt der Quotientenring (Bruchring) von R nach der Nennermenge S.
(c) Die Abbildung $\tau_s : R \to S^{-1}R$, $r \mapsto \frac{r}{1}$ ist ein Ringhomomorphismus.
(d) τ_s injektiv $\Leftrightarrow$ S enthält keinen Nullteiler.

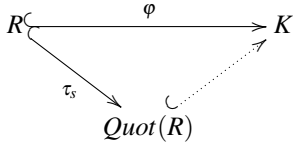
Satz 7.0.2. $S \subseteq R$ Untermonoid bzgl. "$\cdot$". Dann gilt:
Für jeden kommutativen Ring T und jeden Ringhomomorphismus $\varphi : R \to T$ mit $\varphi(S) \subseteq T^*$ gibt es genau einen Ringhomomorphismus $\psi : S^{-1}R \to T$ mit $\psi \circ \tau_s = \varphi$:



Explizit ist ψ gegeben durch $\psi(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$ für $r \in R, s \in S$

Bemerkung 7.0.3. R nullteilerfrei. Dann gilt:
(a) $Quot(R) := (R\backslash\{0\})^{-1}R$ ist ein Körper, der Quotientenkörper von R.
(b) In $Quot(R)$ ist $\frac{r_1}{s_1} = \frac{r_2}{s_2} \Leftrightarrow r_1s_2 = r_2s_1$ (für alle $r_1, r_2 \in R$, $s_1, s_2 \in R\backslash\{0\}$)
(c) Die Abbildung $R \to Quot(R)$, $r \mapsto \frac{r}{1}$ ist ein injektiver Ringhomomorphismus.

Folgerung 7.0.4. R nullteilerfrei, K Körper, $\varphi : R \hookrightarrow K$ injektiver Ringhomomorphismus. Dann existiert ein eindeutig bestimmter Körperhomomorphismus $\psi : Quot(R) \hookrightarrow K$, sodass das folgende Diagramm kommutiert:



(d.h. $\psi \circ \tau = \varphi$)

Anmerkung: Körperhomomorphismen sind immer injektiv (denn: $\varphi : K \to L$ Körperhomomorphismus $\Rightarrow \ker(\varphi) \subseteq K$ ist ein Ideal, somit $\ker(\varphi) = (0)$ oder $\ker(\varphi) = (1)$ und es ist $\varphi(1) = 1 \neq 0$, d.h. $1 \notin \ker(\varphi)$. Also $\ker(\varphi) = (0)$).
Philosophie hinter 7.0.4: $Quot(R)$ ist der kleinste Körper, in den R eingebettet werden kann.

Bemerkung 7.0.5. R faktorieller Ring, $\mathbb{P}$ Vertretersystem von Primelementen von R modulo "$\doteq$", $x \in Quot(R), x \neq 0$.
Dann existieren eindeutig bestimmte $v_p(x) \in \mathbb{Z}$ für $p \in \mathbb{P}$ mit $v_p(x) = 0$ für fast alle $p \in \mathbb{P}$ und $\varepsilon \in R^*$ mit
$x = \varepsilon \prod_{p \in \mathbb{P}} p^{v_p(x)}$

Es gilt: $x \in R \Leftrightarrow v_p(x) \geq 0$ für alle $p \in \mathbb{P}$.
Konvention: $v_p(0) := \infty$

Beispiel 7.0.6. $R = \mathbb{Z}$, $\mathbb{P}$ Menge aller Primzahlen in $\mathbb{N}$
$v_2(\frac{2}{9}) = v_2(\frac{2^1}{3^2}) = v_2(2^1 \cdot 3^{-2}) = 1$, $v_3(\frac{2}{9}) = -2$, $v_p(\frac{2}{9}) = 0$ für alle Primzahlen $p \neq 2,3$.

Bemerkung 7.0.7. R faktorieller Ring, $x, y \in Quot(R)$. Dann gilt:
(a) p Primelement in $R \Rightarrow v_p(xy) = v_p(x) + v_p(y)$
(b) Ist $v_p(x) = 0$ für alle Primelemente $p \in R \Rightarrow x \in R^*$

8. Primfaktorzerlegung in Polynomringen

In diesem Abschnitt sei R stets ein faktorieller Ring.
Ziel $R[T]$ ist faktoriell.

Definition 8.0.1. $f = a_r T^r + \ldots + a_1 T + a_0 \in Quot(R)[T]$, $p \in R$ Primelement
Wir setzen $v_p(f) := \min\limits_{i=0,\ldots,r} v_p(a_i)$

Bemerkung 8.0.2. $f \in Quot(R)[T]$. Dann gilt:
(a) Ist $\mathbb{P}$ ein Vertretersystem von Primelementen von R, dann ist $v_p(f) = 0$ für fast alle $p \in \mathbb{P}$.
(b) $f \in R[T] \Leftrightarrow v_p(f) \geq 0$ für fast alle $p \in \mathbb{P}$

Satz 8.0.3. $p \in R$ Primelement, $f, g \in Quot(R)[T]$. Dann gilt:
$v_p(fg) = v_p(f) + v_p(g)$

Folgerung 8.0.4. $h \in R[T]$ normiert. Es sei $h = fg$ mit normierten Polynomen $f, g \in Quot(R)[T]$
Dann gilt: $f, g \in R[T]$

Definition 8.0.5. $f = a_n T^n + \ldots + a_1 T + a_0 \in R[T]$
f heißt primitiv $\Leftrightarrow 1 \in GGT(a_0, \ldots, a_n) \Leftrightarrow v_p(f) = 0$ für alle Primelemente $p \in R$

Beispiel 8.0.6.

- Jedes normierte Polynom aus $R[T]$ ist primitiv
- $R = \mathbb{Z}$: $f = 5T^2 + 3T + 9 \in \mathbb{Z}[T]$ ist primitiv

Bemerkung 8.0.7. $0 \neq f \in Quot(R)[T]$
Dann exisitert ein $a \in Quot(R), a \neq 0$ und ein primitives Polynom $\tilde{f} \in R[T]$ mit $f = a\tilde{f}$.

Satz 8.0.8. (Satz von Gauß) Es gilt:
(a) $R[T]$ ist faktoriell
(b) Ein Polynom $q \in R[T]$ ist genau dann ein Primelement in $R[T]$, wenn gilt:

(i) $q \in R$ und q ist Primelement in R

oder

(ii) q ist primitiv in $R[T]$ und Primelement in $Quot(R)[T]$

Folgerung 8.0.9. $f \in R[T]$ primitiv. Dann sind äquivalent:
(i) f ist Primelement in $R[T]$
(ii) f ist Primelement in $Quot(R)[T]$

Folgerung 8.0.10. $n \in \mathbb{N}$. Dann ist $R[T_1, \ldots, T_n]$ faktoriell.

Beispiel 8.0.11.
(a) K Körper $\Rightarrow K[T_1, \ldots, T_n]$ faktoriell
(b) $\mathbb{Z}[T_1, \ldots, T_n]$ faktoriell

Anmerkung: $R[T]$ und $Quot(R)[T]$ sind faktorielle Ringe, d.h. "Primelemente" und "irreduzible Elemente" sind äquivalent. Im Folgenden werden wir immer von irreduziblen Polynomen sprechen.

Bemerkung 8.0.12. $f \in Quot(R)[T]$ mit $\deg(f) \geq 1$. Sei $f = c\tilde{f}$ mit $c \in Quot(R)^*$, $\tilde{f} \in R[T]$ primitiv. Dann sind äquivalent:
(i) f ist irreduzibel in $Quot(R)[T]$
(ii) $\tilde{f}$ ist irreduzibel in $Quot(R)[T]$
(iii) $\tilde{f}$ ist irreduzibel in $R[T]$

Ziel: Kritierien, wann ein Polynom irreduzibel ist.

Satz 8.0.13. (Reduktionskriterium) $p \in R$ Primelement, $f \in R[T], f \neq 0$, $p \nmid l(f)$
Wir betrachten den Ringhom. $\varphi : R[T] \to R/(p)[T]$, $\sum_{i=0}^{n} a_i T^i \mapsto \sum_{i=0}^{n} \bar{a}_i T^i$ (Koeffizientenprojektion)
Dann gilt:
(a) Ist $\varphi(f)$ irreduzibel in $R/(p)\ [T]$, dann ist f irreduzibel in $Quot(R)[T]$
(b) Ist $\varphi(f)$ irreduzibel in $R/(p)\ [T]$, und ist f primitiv, dann ist f irreduzibel in $R[T]$

Anmerkung:

- Satz (drüber) wird häufig angewendet, wenn R HIR, p Primelement in R. Dann ist (p) nach 6.3 maximales Ideal in R, also $R/(p)$ Körper, $R/(p)\ [T]$ faktoriell
- andere Anwendung: $R = K[T_1, \ldots, T_n]$, K Körper, $p = T_n$ (ist Primelement) $\Rightarrow R/(p) = K[T_1, \ldots, T_{n-1}]$, Problem um eine Variable reduziert.

Beispiel 8.0.14. $R = \mathbb{Z}$, $f = X^3 + 7X^2 + 4X - 5 \in \mathbb{Z}[X]$ ist irreduzibel in $\mathbb{Z}[X]$ und in $\mathbb{Q}[X]$ denn: Reduktionskriterium mit $p = 2 : \varphi(f) = X^3 + X^2 + \bar{1} \in \mathbb{F}_2[X]$ ist irreduzibel (andernfalls hätte $\varphi(f)$ wegen $\deg(\varphi(f)) = 3$ einen Teiler vom Grad 1, also eine Nullstelle in $\mathbb{F}_2 : \varphi(f)(\bar{0}) = \bar{1}, \varphi(f)(\bar{1}) = \bar{1}$)

Satz 8.0.15. (Eisensteinisches Irreduzibilitästkriterium)
$f = a_n T^n + \ldots + a_0 \in R[T]$ primitiv mit $\deg(f) \geq 1$
$p \in R$ Primelement mit $p \nmid a_n$, $p | a_i$ für $0 \leq i < n$, $p^2 \nmid a_0$
Dann ist f irreduzibel in $R[T]$ und in $Quot(R)[T]$.

Beispiel 8.0.16.
(a) $f = T^3 + 5T^2 + 5 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$ und in $\mathbb{Q}[T]$ (Eisenstein mit $p = 5$)
(b) p Primzahl. Dann ist $f = T^{p-1} + T^{p-2} + \ldots + 1 = \frac{T^p - 1}{T - 1}$ irreduzibel in $\mathbb{Z}[T]$ und in $\mathbb{Q}[T]$.
f irreduzibel $\Leftrightarrow f(T+1)$ irreduzibel (vgl. Blatt 7, A2)
$f(T+1) = \frac{(T+1)^p - 1}{T+1-1} = \frac{T^p + \binom{p}{1} T^{p-1} + \ldots + \binom{p}{p-1} T^2 + \binom{p}{p-1} T}{T} = T^{p-1} + \binom{p}{1} T^{p-2} + \ldots + \binom{p}{p-2} T + \binom{p}{p-1}$.
Es gilt: $p | (p_i) = \frac{p!}{(p-i)!i!}$ für $i = 1, \ldots, p-1$, $p^2 \nmid \binom{p}{p-1} = p$
$\Rightarrow f(T+1)$ irreduzibel nach Eisenstein-Kriterium $\Rightarrow f$ irreduzibel.
(c) k Körper, $R = k[t]$, $K := Quot(R) =: k(t)$ (Körper der rationalen Funktionen über k in der Variablen t)
Sei $f = T^n - t \in R[T]$.
R ist faktoriell, t ist Primelement in R. $\Rightarrow f$ irreduzibel in $R[T]$ und in $K[T]$ (nach Eisenstein).

Teil III.

Algebraische Körpererweiterungen

9. Die Charakteristik

In diesem Abschnitt sei R stets ein kommutativer Ring

Bemerkung 9.0.1. Es gilt:
(a) Es gibt genau einen Ringhomomorphismus $\phi_R : \mathbb{Z} \to R$. Für diesen gilt:

$$\varphi_R(n) = n \cdot 1_R := \begin{cases} \underbrace{1_R + \ldots + 1_R}_{n\text{-mal}}, & \text{falls } n \in \mathbb{N} \\ 0_R, & \text{falls } n = 0 \\ -(\underbrace{1_R + \ldots + 1_R}_{(-n)\text{-mal}}), & \text{falls } -n \in \mathbb{N} \end{cases}$$

(b) R nullteilerfrei $\Rightarrow \ker(\varphi_R) \subseteq \mathbb{Z}$ Primideal, insbesondere ist $\ker(\varphi) = \begin{cases} (0) & \text{oder} \\ (p) & \text{für eine Primzahl } p \in \mathbb{N} \end{cases}$

Definition 9.0.2. R nullteilerfrei, $\mathbb{P}$ Menge der Primzahlen in $\mathbb{N}$
Das eindeutig bestimmte $n \in \mathbb{P} \cup \{0\}$ mit $\ker(\varphi_R) = (n)$ heißt die Charakteristik von R. Bezeichnung: $char(R)$.

Anmerkung: Offenbar ist $char(R) = \min\{n \in \mathbb{N} | n \cdot 1_R = 0\}$, falls dieses existiert, sonst $= 0$

Beispiel 9.0.3.
(a) $char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0$
(b) p Primzahl, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \Rightarrow char(\mathbb{F}_p) = p$ (hier ist $\varphi_{\mathbb{Z}/p\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $n \mapsto \bar{n}$ mit $\ker(\varphi_{\mathbb{Z}/p\mathbb{Z}}) = p\mathbb{Z}$)

Bemerkung 9.0.4. R nullteilerfrei, S nullteilerfreier kommutativer Ring
(a) Existiert ein injektiver Ringhomomorphismus $i : R \hookrightarrow S$, dann ist $char(R) = char(S)$
(b) R, S Körper mit $char(R) \neq char(S) \Rightarrow$ Es existiert kein Körperhomomorphismus von R nach S.

Folgerung 9.0.5. R nullteilerfrei. Dann ist $char(R) = char(Quot(R))$

Beispiel 9.0.6.
p Primzahl, $K = \mathbb{F}_p(t) = Quot(\mathbb{F}_p[t])$ ist ein Körper mit $char(K) = p$ (und unendlich vielen Elementen)

Definition 9.0.7. K Körper. Der Durchschnitt aller Teilkörper (Unterringe von K, die selbst Körper sind) von K heißt der Primkörper von K

Anmerkung: Dies ist selbst ein Körper, der kleinste Teilkörper von K

Bemerkung 9.0.8. K Körper, $P \subseteq K$ Primkörper von K. Dann gilt:
(a) $charK = 0 \Leftrightarrow P \cong \mathbb{Q}$
(b) $charK = p > 0 \Leftrightarrow P \cong \mathbb{F}_p$

Definition 9.0.9. K Körper mit $char(K) = p > 0$.
Die Abbildung $\sigma_K : K \to K$, $a \mapsto a^p$ heißt der Frobeniushomomorphismus von K.

Bemerkung 9.0.10. K Körper mit $char(K) = p > 0$. Dann gilt:
(a) σ_K ist ein Körperhomomorphismus
(b) K endlicher Körper $\Rightarrow \sigma_K$ ist Körperautomorphismus.

Bemerkung 9.0.11. K Körper mit $char(K) = p > 0$, P Primkörper von K.
Dann gilt: $P = \{a \in K | \sigma_K(a) = a\}$

10. Endliche und algebraische Körpererweiterungen

Definition 10.0.1. L Körper, $K \subseteq L$ Teilkörper
Sprechweise: L ist Erweiterungskörper von K, $L|K$ ist eine Körpererweiterung.
Vermöge $K \times L \to L$, $(x,y) \mapsto xy$ als skalare Multiplikation wird L zu einem K-Vektorraum.
$[L:K] := dim_K L \in N \cup \{\infty\}$ heißt der Grad der Körpererweiterung $L|K$
$L|K$ heißt endlich, falls $[L:K]$ endlich ist.

Beispiel 10.0.2.
(a) $\mathbb{C}|\mathbb{R}$ ist eine Körpererweiterung mit $[\mathbb{C}:\mathbb{R}] = 2$
(b) $\mathbb{R}|\mathbb{Q}$ ist eine Körpererweiterung mit $[\mathbb{R}:\mathbb{Q}] = \infty$, denn: Falls $[\mathbb{R}:\mathbb{Q}] = n \in \mathbb{N}$, dann wäre $\mathbb{R} \cong \mathbb{Q}^n$ abzählbar. $\lightning$
(c) K Körper, $K(t) = Quot(K[t]) \Rightarrow K(t)|K$ ist eine Körpererweiterung mit $[K(t):K] = \infty$, denn: $(t^i)_{i\in\mathbb{N}_0}$ ist K-linear unabhängig (und unendlich).

Bemerkung 10.0.3. $L|K$ Körpererweiterung. Dann sind äquivalent:
(i) $[L:K] = 1$
(ii) $L = K$

Satz 10.0.4. (Gradsatz) $M|L|K$ Körpererweiterung. Dann gilt:
$[M:K] = [M:L][L:K]$

Anmerkung: Ist $(x_i)_{i\in I}$ Basis von M als L-Vektorraum und $(y_j)_{j\in J}$ Basis von L als K-Vektorraum $\Rightarrow (x_i y_j)_{(i,j)\in I\times J}$ ist Basis von M als K-Vektorraum.

Folgerung 10.0.5. $M|L|K$ Körpererweiterung, $[M:K]$ Primzahl.
Dann ist: $L = K$ oder $L = M$

Definition 10.0.6. $L|K$ Körpererweiterung, $\alpha_1,\ldots,\alpha_n \in L$
Die Familie $(\alpha_1,\ldots,\alpha_n)$ heißt algebraisch unabhängig (transzendent) über K
$\Leftrightarrow$ Der Ringhomomorphismus $\phi : K[X_1,\ldots,X_n] \to L, f \mapsto f(\alpha_1,\ldots,\alpha_n)$ ist injektiv
$\Leftrightarrow$ Es existiert kein $f \in K[X_1,\ldots,X_n]$, $f \neq 0$ mit $f(\alpha_1,\ldots,\alpha_n) = 0$
Andernfalls heißt die Familie algebraisch abhängig über K.
$n = 1$: $\alpha \in L$ heißt algebraisch über K
$\Leftrightarrow (\alpha)$ ist algebraisch abhängig über K
$\Leftrightarrow$ Der Ringhomomorphismus. $\phi : K[X] \to L$, $f \mapsto f(\alpha)$ ist nicht injektiv
$\Leftrightarrow$ Es existiert ein $f \in K[X]$, $f \neq 0$ mit $f(\alpha) = 0$
Andernfalls heißt α transzendent über K.

Beispiel 10.0.7.
(a) $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn für $f = X^2 - 2 \in \mathbb{Q}[X]$ ist $f(\sqrt{2}) = 0$
(b) π ist transzendent über $\mathbb{Q}$ (Satz von Lindemann)
(c) (π, π^2) ist algebraisch abhängig über $\mathbb{Q}$, denn für $f = X_1^2 - X_2 \in \mathbb{Q}[X_1,X_2]$ ist $f(\pi,\pi^2) = 0$
(d) π ist algebraisch über $\mathbb{R}$, denn für $f = X - \pi \in \mathbb{R}[X]$ ist $f(\pi) = 0$
(e) Ist (e,π) transzendent über $\mathbb{Q}$? Ungelöst

Definition 10.0.8. $L|K$ heißt algebraisch $\Leftrightarrow$ Jedes Element aus L ist algebraisch über K.

Beispiel 10.0.9.
(a) $\mathbb{C}|\mathbb{R}$ ist algebraisch, denn $\alpha = a+ib \in \mathbb{C}$ mit $a,b \in \mathbb{R}$ ist eine Nullstelle von $X^2 - 2aX + (a^2+b^2) \in \mathbb{R}[X]$
(b) K Körper, $K(t)$ Körper der rationalen Funktionen über K in der Variablen t
$K(t)|K$ ist nicht algebraisch, denn: $t \in K(t)$ ist nicht algebraisch über K:
Die Abbildung: $\phi : K[X] \to K(t)$, $f \mapsto f(t)$ ist injektiv (genauer: ein Isomorphismus von $K[X]$ auf dem Unterring $K[t] \subseteq K(t)$).

Bemerkung 10.0.10. $L|K$ Körpererweiterung, $\alpha \in L$ algebraisch über K, $\phi : K[X] \to L$, $g \mapsto g(\alpha)$. Dann gilt:
(a) Es gibt genau ein normiertes Polynom kleinsten Grades $f \in K[X]$ mit $f(\alpha) = 0$
(b) f ist irreduzibel
(c) $\ker(\phi) = (f)$
f heißt das Minimalpolynom von α über K.

Bemerkung 10.0.11. $L|K$ Körpererweiterung, $\alpha \in L$. Dann gilt:
$K[\alpha] := \{c_0 + c_1\alpha + \ldots + c_n\alpha^n | n \in \mathbb{N}_0, c_1, \ldots, c_n \in K\} = im(\phi)$ für $\phi : K[X] \to L$, $g \mapsto g(\alpha)$ ist der kleinste Teilring von L, der K und α umfasst und heißt der von α über K erzeugte Teilring von L.
$K(\alpha) := Quot(K[\alpha]) \subseteq L$ ist der kleinste Teilkörper von L, der K und α umfasst und heißt der von α über K erzeugte Teilkörper von L ("K adjungiert α")

Satz 10.0.12. $L|K$ Körpererweiterung, $\alpha \in L$ algebraisch über K, $f \in K[X]$ Minimalpolynom von α über K.
Dann gilt:
(a) $K[\alpha]$ ist ein Körper, d.h. $K[\alpha] = K(\alpha)$
(b) Der Homomorphismus $\phi : K[X] \to L$, $g \mapsto g(\alpha)$ induziert einen Isomorphismus $\overline{\phi} : K[X]/(f) \xrightarrow{\sim} K(\alpha)$
(c) $[K(\alpha) : K] = \deg(f)$, insbesondere ist $K(\alpha)|K$ eine endliche Körpererweiterung.

Beispiel 10.0.13. $L|K$ Körpererweiterung, $\alpha \in L$ algebraisch über K, $\alpha \neq 0$. Wie findet man $\alpha^{-1} \in K[\alpha]$?
Sei $f = X^n + c_{n-1}X^{n-1} + \ldots + c_0 \in K[X]$ Minimalpolynom über K
$n = 1$: $f = X + c_0$, $f(\alpha) = 0 \Rightarrow \alpha + c_0 = 0 \Rightarrow \alpha = -c_0 \in K^* \Rightarrow \alpha^{-1} = -c_0^{-1} \in K \subseteq K[\alpha]$
$n \geq 2 : c_0 \neq 0$, da f irreduzibel.
$\Rightarrow 0 = \alpha^{-1}f(\alpha) = \alpha^{-1}(\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_0)$
$\Rightarrow -c_0\alpha^{-1} = \alpha^{n-1} + c_{n-1}\alpha^{n-2} + \ldots + c_1$
$\Rightarrow \alpha^{-1} = -c_0^{-1}(\alpha^{n-1} + c_{n-1}\alpha^{n-2} + \ldots + c_1) \in K[\alpha]$

Bemerkung 10.0.14. $L|K$ algebraische Körpererweiterung, $[L : K] < \infty$, $\alpha \in L$, $h_\alpha : L \to L$, $b \mapsto \alpha b$ (ist ein K-VR-Endomorphismus.) Dann stimmt das Minimalpolynom von α über K mit dem Minimalpolynom von h_α überein.

Satz 10.0.15. $L|K$ endliche Körpererweiterung. Dann ist $L|K$ algebraisch.

Anmerkung: Es gibt eine algebraische Körpererweiterungen, die nicht endlich sind (vgl. Bsp. 10.24)

Folgerung 10.0.16. $L|K$ Körpererweiterung, $\alpha \in L$ algebraisch über K.
Dann ist $K(\alpha)|K$ algebraisch.

Bemerkung 10.0.17. $L|K$ Körperweiterung, $S \subseteq L$. Dann gilt:
(a) $K[S] := \{f(\alpha_1, \ldots, \alpha_n) | n \in \mathbb{N}_0, f \in K[X_1, \ldots, X_n], \alpha_1, \ldots, \alpha_n \in S\}$ ist der kleinste Teilring von L, der K und S umfasst.
(b) $K(S) := Quot(K[S])$ ist der kleinste Teilkörper von L, der K und S umfasst.
(c) $K(S) = \bigcup_{T \subseteq S \text{ endl.}} K(T)$
Ist $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich, so schreiben wir $K[S] = K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) | f \in K[X_1, \ldots, X_n]\}$
$K(S) = K(\alpha_1, \ldots, \alpha_n) = Quot(K[\alpha_1, \ldots, \alpha_n])$

Definition 10.0.18. $L|K$ Körpererweiterung
Für $\alpha \in L$ heißt $[K(\alpha) : K]$ der Grad von α über K.
$L|K$ heißt einfach $\Leftrightarrow$ Es existiert ein $\alpha \in L$ mit $L = K(\alpha)$.
$L|K$ heißt endlich erzeugt $\Leftrightarrow$ Es existiert ein $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$.

Beispiel 10.0.19. $\mathbb{C}|\mathbb{R}$ ist einfach wegen $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$

Satz 10.0.20. $L|K$ Körpererweiterungen, $\alpha_1, \ldots, \alpha_n \in L$ algebraisch über K, $L = K(\alpha_1, \ldots, \alpha_n)$
Dann gilt:
(a) $L = K[\alpha_1, \ldots, \alpha_n]$
(b) $L|K$ endlich, insbesondere algebraisch

Folgerung 10.0.21. $L|K$ Körpererweiterung. Dann sind äquivalent:
(i) $L|K$ ist endlich.
(ii) L wird über K von endlich vielen algebraischen Elementen erzeugt, d.h. es existieren $\alpha_1, \ldots, \alpha_n \in L$, $\alpha_1, \ldots, \alpha_n$ algebraisch über K mit $L = K(\alpha_1, \ldots, \alpha_n)$
(iii) $L|K$ ist eine endlich erzeugte algebraische Körpererweiterung, d.h. $L|K$ algebraisch und es existieren $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$

Folgerung 10.0.22. $L|K$ Körpererweiterung. Dann sind äquivalent:
(i) $L|K$ ist algebraisch
(ii) L wird über K von algebraischen Elementen erzeugt.

Folgerung 10.0.23. $L|K$ Körpererweiterung, $M := \{\alpha \in L | \alpha \text{ ist algebraisch über } K\}$. Dann gilt:
(a) M ist eine Teilkörper von L, der sogenannte algebraische Abschluss von K in L
(b) $M|K$ ist algebraisch

Beispiel 10.0.24. $K = \mathbb{Q}$, $L = \mathbb{C}$
$\mathbb{Q}^{alg} := \{\alpha \in \mathbb{C} | \alpha \text{ ist algebraisch über } \mathbb{Q}\}$ = algebraischer Abschluss von $\mathbb{Q}$ in $\mathbb{C}$ ist eine algebraische Erweiterung von $\mathbb{Q}$.

1. $[\mathbb{Q}^{alg} : \mathbb{Q}] = \infty$, denn:
   Sei $n \in \mathbb{N}$, p Primzahl $\Rightarrow f := X^n - p \in \mathbb{Q}[X]$ irreduzibel von Grad n wegen dem Eisensteinkriterium, es existieren $\alpha \in \mathbb{C}$ mit $f(\alpha) = 0 \Rightarrow \alpha \in \mathbb{Q}^{alg}$, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}^{alg}$
   Wegen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = n$ folgt $[\mathbb{Q}^{alg} : \mathbb{Q}] \geq n$

2. $\mathbb{Q}^{alg}$ ist abzählbar, denn:
   $P := \{f \in \mathbb{Q}[X] | f \text{ irreduzibel, normiert}\}$ ist abzählbar, denn$\mathbb{Q}[X]$ ist abzählbar. $\mathbb{Q}^{alg}$ ist als Menge aller NS in $\mathbb{C}$ aller Polynome aus P dann auch abzählbar. Insbesondere existiert in $\mathbb{C}$ überabzählbar viele Elemente, die transzendent über $\mathbb{Q}$ sind.

Satz 10.0.25. $M|L|K$ Körpererweiterung, $\alpha \in M$. Dann gilt:
(a) α algebraisch über L und $L|K$ algebraisch $\Rightarrow \alpha$ algebraisch über K
(b) $M|K$ algebraisch $\Leftrightarrow M|L$ algebraisch und $L|K$ algebraisch

11. Algebraischer Abschluss

Satz 11.0.1. K Körper, $f \in K[X]$, $\deg(f) \geq 1$
Dann existiert eine endliche Körpererweiterung $L|K$, sodass f eine Nullstelle in L hat.

Definition 11.0.2. K Körper
K heißt algebraisch abgeschlossen
$\Leftrightarrow$ Jedes $f \in K[X]$, $\deg(f) \geq 1$ besitzt eine Nullstelle in K
$\Leftrightarrow$ Jedes $f \in K[X], f \neq 0$ kann in der Form $f = c(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$ mit $n = \deg(f)$, $c \in K^*$, geschrieben werden.

Bemerkung 11.0.3. K Körper. Dann sind äquivalent:
(i) K ist algebraisch abgeschlossen
(ii) Es gibt keine echte algebraische Erweiterung $L|K$
(iii) Es gibt keine echte endliche Erweiterung $L|K$

Satz 11.0.4. K Körper. Dann existiert ein algebraisch abgeschlossener Erweiterungskörper von K

Folgerung 11.0.5. K Körper
Dann existiert ein algebraisch abgeschlossener Erweiterungskörper $\bar{K}$ von K, sodass $\bar{K}|K$ algebraisch ist. Mann nennt $\bar{K}$ einen algebraischen Abschluss von K

Beispiel 11.0.6. $\mathbb{Q}^{alg}$ aus Bsp 10.24 ist ein algebraischer Abschluss von $\mathbb{Q}$.
Aber: $\mathbb{C}$ ist kein algebraischer Abschluss von $\mathbb{Q}$

Ziel: Je zwei algebraische Abschlüsse von K sind isomorph.

Definition 11.0.7. K, L Körper, $\sigma : K \to L$ Körperhomomorphismus, $f = a_n X^n + \ldots + a_0 \in K[X]$
$f^\sigma := \sigma(a_n)X^n + \ldots + \sigma(a_0) \in L[X]$

Bemerkung 11.0.8. K, L Körper, $K'|K$ einfache algebraische Körpererweiterung, etwa $K' = K(\alpha)$, $f \in K[X]$ Minimalpolynom von α über K, $\sigma : K \to L$ Körperhomomorphismus. Dann gilt:
(a) Ist $\sigma' : K' \to L$ Körperhomomorphismus, der σ fortsetzt, d.h. $\sigma'|_K = \sigma$, dann ist $\sigma'(\alpha)$ eine Nullstelle von $f^\sigma \in L[X]$
(b) Zu jeder Nullstelle $\beta \in L$ von f^σ gibt es genau eine Fortsetzung $\sigma' : K' \to L$ von σ mit $\sigma'(\alpha) = \beta$.
Insbesondere ist die Anzahl der Fortsetzungen σ' von σ nach K' gleich der Anzahl der verschiedenen Nullstellen von f^σ in L, also $\leq \deg(f)$.

Satz 11.0.9. $K'|K$ algebraische Körpererweiterung, L algebraisch abgeschlossener Körper, $\sigma : K \to L$ Körperhomomorphismus. Dann gilt:
(a) σ besitzt eine Forsetzung $\sigma' : K' \to L$
(b) Ist K' algebraisch abgeschlossen und $L|\sigma(K)$ algebraisch, dann ist jede Fortsetzung von σ nach K' ein Isomorphismus.

Folgerung 11.0.10. K Körper, $\bar{K}_1, \bar{K}_2$ algebraische Abschlüsse von K.
Dann existiert ein Isomorphismus $\bar{K}_1 \xrightarrow{\sim} \bar{K}_2$, der $id_K : K \to K$ fortsetzt.

Anmerkung: Dieser Isomorphismus existiert, es gibt aber keine kanonische Wahl: Man sagt: $\bar{K}_1, \bar{K}_2$ sind unterkanonisch isomorph.

12. Normale Körpererweiterungen

In diesem Abschnitt sei K stets ein Körper.

Definition 12.0.1. $L|K, L'|K$ Körpererweiterungen, $\sigma : L \to L'$ Körperhomomorphismus
σ heißt K-Homomorphismus $\Leftrightarrow \sigma|_K = id_K$

Definition 12.0.2. $F = (f_i)_{i\in I}$ Familie nichtkonstanter Polynome mit Koeffizienten in K.
Ein Erweiterungskörper L von K heißt ein Zerfällungskörper der Familie F über K, wenn gilt:
(a) Jedes f_i zerfällt über L vollständig in Linearfaktoren und
(b) $L|K$ wird von den Nullstellen der f_i, $i \in I$ in L erzeugt.

Anmerkung

- $F = (f)$, $f \in K[X]$ nichtkonstant, $\bar{K}$ ein algebraischer Abschluss von K, $\alpha_1, \ldots, \alpha_n$ Nullstellen von f in $\bar{K} \Rightarrow L := K(\alpha_1, \ldots, \alpha_n)$ ein Zerällungskörper von F über K (kurz: Zerfällungskörper von f über K)
- $F = (f_1, \ldots, f_n) \Rightarrow$ Zerfällungskörper von F ist ein Zerfällungskörper von $f_1 \cdot \ldots \cdot f_n$ und umgekehrt
- $F = (f_i)_{i\in I}$: Man erhält einen Zerfällungskörper, indem man sämtliche Nullstellen der f_i, $i \in I$ in einem festen algebraischen Abschluss von K zu K adjungiert.

Somit: Existenz von Zerällungskörper ist stets gesichert.

Beispiel 12.0.3. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist ein Zerfällungskörper der Familie $(X^2 - 2, X^2 - 3)$ über $\mathbb{Q}$.

Satz 12.0.4. $F = (f_i)_{i\in I}$ Familie nicht-konstanter Polynome mit Koeffizienten in K, L_1, L_2 Zerfällungskörper von F. $\bar{L_2}$ ein algebraischer Abschluss von L_2.
Dann gilt: Jeder K-Homomorphismus $\bar{\sigma} : L_1 \to \bar{L_2}$ beschränkt sich zu einem K-Isomorphismus $\sigma : L_1 \xrightarrow{\sim} L_2$ (d.h. $\sigma(L_1) = L_2$)

Folgerung 12.0.5. F Familie nicht konstanter Polynome über K
Dann sind je zwei Zerfällungskörper von F über K (unkanonisch) K-isomorph.

Satz 12.0.6. $L|K$ algebraische Körpererweiterung. Dann sind äquivalent:
(i) Jeder K-Homomorphismus $\tau : L \to \bar{L}$ in einen algebraischen Abschluss $\bar{L}$ von L schränkt sich zu einem Automorphismus von L ein, d.h. $\tau(L) = L$.
(ii) L ist Zerfällungskörper einer Familie von Polynomen über K.
(iii) Jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle hat, zerfällt in $L[X]$ vollständig in Linearfaktoren.
$L|K$ heißt normal, wenn eine der obigen Bedingungen erfüllt ist.

Anmerkung: zu (i): Ein algebraischer Abschluss $\bar{L}|L$ ist eine Körpererweiterung, d.h. kommt mit einer Einbettung $L \hookrightarrow \bar{L}$ daher. Es gibt aber im Allgemeinen mehr K-Homomorphismen von L nach $\bar{L}$ als diesen einen.

Beispiel 12.0.7.
(a) $\bar{K}$ ein algebraischer Abschluss von $K \Rightarrow \bar{K}|K$ normal, denn: Bedingung (iii) ist erfüllt.
(b) $K = \mathbb{Q}$, $\alpha = \sqrt[3]{2} \in \mathbb{R}$ (d.h. die eindeutig bestimmte reelle Nullstelle von $f = X^3 - 2 \in \mathbb{Q}[X]$)

$L = \mathbb{Q}(\alpha)$, $\bar{L} = \mathbb{Q}^{alg}$ ist ein algebraischer Abschluss von L
Wir betrachten den eindeutig bestimmten $\mathbb{Q}$-Hom. $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}^{alg}$ mit $\sigma(\alpha) = \alpha e^{2\pi i/3}$
(beachte: $f(\alpha^{2\pi i/3}) = (\alpha e^{2\pi i/3})^3 - 2 = \alpha^3 \cdot 1 - 2 = 0$
Dies ist wohldefiniert, denn $\sigma(\alpha) = \alpha e^{2\pi i/3}$ ist eine Nullstelle von f in $\mathbb{Q}^{alg}$.
Es ist $\sigma(\mathbb{Q}(\alpha)) \neq \mathbb{Q}(\alpha)$, denn: $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, $\sigma(\alpha) \notin \mathbb{R}$
Also ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ nicht normal, da (i) verletzt.
Alternatives Argument: $f = X^3 - 2 \in \mathbb{Q}[X]$ (irreduzibel nach Eisenstein) besitzt die Nullstelle $\alpha = \sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$.
Wäre $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ normal, so würde f in $\mathbb{Q}(\sqrt[3]{2})[X]$ als auch in $\mathbb{R}[X]$ in Linearfaktoren zerfallen $\lightning$ (also auch (iii) verletzt).

Folgerung 12.0.8. $M|L|K$ Körpererweiterung, $M|K$ normal. Dann ist auch $M|L$ normal.

Bemerkung 12.0.9. $L|K$ Körpererweiterung mit $[L : K] = 2$. Dann ist $L|K$ normal.

Beispiel 12.0.10. Normalität ist nicht transitiv in Köpertürmen $M|L|K$
Sei $f = X^4 - 2 \in \mathbb{Q}[X] \overset{\text{Eisenstein}}{\Rightarrow} f$ irreduzibel in $\mathbb{Q}[X]$.
Sei $\alpha = \sqrt[4]{2} \in \mathbb{Q}^{alg}$ die eindeutig bestimmte positive reelle Nullstelle von f, setze $M := \mathbb{Q}(\alpha) \Rightarrow [M : \mathbb{Q}] = \deg(f) = 4$
$M|\mathbb{Q}$ ist nicht normal, denn: Für $\beta = i\alpha \in \mathbb{Q}^{alg}$ ist $f(\beta) = 0$, aber $\beta \notin M$ wegen $M \subseteq \mathbb{C}\backslash\mathbb{R}$, $\beta \in \mathbb{R}$
$\alpha^2 = \sqrt{2}$ ist Nullstelle von $X^2 - 2 \in \mathbb{Q}[X] \overset{X^2-2 \text{ irred.}}{\Longrightarrow} [\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$,
$4 = [M : \mathbb{Q}] = [\underbrace{M : \mathbb{Q}(\alpha^2)}_{=2}][\underbrace{\mathbb{Q}(\alpha^2) : \mathbb{Q}}_{=2}] \overset{12.9}{\Rightarrow} M|\mathbb{Q}(\alpha^2), \mathbb{Q}(\alpha^2)|\mathbb{Q}$ normal, aber $M|\mathbb{Q}$ nicht normal.

Definition 12.0.11. $L|K$ algebraischer Körpererweiterung. Eine Körpererweiterung $L'|K$ mit $L' \supseteq L$ heißt normale Hülle von $L|K$, wenn gilt:
(a) $L'|K$ normal
(b) Kein echter Zwischenkörper $L \subsetneq M \subsetneq L'$ ist normal über K.

Satz 12.0.12. $L|K$ algebraische Körpererweiterung. Dann gilt:
(a) Es gibt zu $L|K$ eine normale Hülle $L'|K$, diese ist bis auf (unkanonsiche) L-Isomorphie eindeutig bestimmt.
(b) $L|K$ endlich $\Rightarrow L'|K$ endlich
(c) Ist $M|L$ algebraisch, $M|K$ normal, dann kann man $L \subseteq L' \subseteq M$ wählen. Als Teilkörper von M ist L' eindeutig betimmt: Ist $(\sigma_j)_{j\in J}$ die Familie aller K-Homomorphismen von L nach M, so ist $L' = K((\sigma_j(L))_{j\in J})$
Mann nennt L' die normale Hülle von L in M.

13. Separable Körpererweiterungen

In diesem Abschnitt sei K stets ein Körper.

Definition 13.0.1. $\bar{K}$ ein algebraischer Abschluss von K, $f \in K[X], \alpha \in \bar{K}$ mit $f(\alpha) = 0$
α heißt eine Nullstelle der Vielfachheit r von $f \Leftrightarrow$ In $\bar{K}[X]$ gilt $(X-\alpha)^r | f, (X-\alpha)^{r+1} \nmid f$
α heißt mehrfache Nullstelle von $f \Leftrightarrow$ Die Vielfachheit von α ist > 1
f heißt separabel $\Leftrightarrow$ f hat keine mehrfachen Nullstellen von $\bar{K}$
Andernfalls heißt f inseparabel.

Anmerkung: Die (In-)separabilität von f ist unabhängig von der Wahl von $\bar{K}$ (da je zwei algebraische Abschlüsse von K stets K-isomorph sind).

Definition 13.0.2. $f = a_n X^n + \ldots + a_0 \in K[X]$
Dann heißt $f' = n a_k X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + a_1 \in K[X]$ die formale Ableitung von f.

Bemerkung 13.0.3. $f, g \in K[X]$. Dann gilt:
(a) $(f+g)' = f' + g'$
(b) $(fg)' = f'g + fg'$

Bemerkung 13.0.4. $L|K$ Körpererweiterung, $f, g \in K[X]$. Dann gilt:
$ggT_{K[X]}(f,g) = ggT_{L[X]}(f,g)$

Bemerkung 13.0.5. $f \in K[X], \deg(f) \geq 1$
Dann gilt: Die mehrfache Nullstelle von f in einem algebraischen Abschluss $\bar{K}$ von K sind genau die gemeinsamen Nullstellen von f und f' in $\bar{K}$, d.h. die Nullstellen von $ggT_{K[X]}(f,f')$ in $\bar{K}$.

Bemerkung 13.0.6. $f \in K[X]$ irreduzibel, $\deg(f) \geq 1$. Dann sind äquivalent:
(i) f ist separabel
(ii) $f' \neq 0$

Anmerkung: ohne die Voraussetzung "f irred." wird $(ii) \Rightarrow (i)$ falsch: (z.B. $f = X^2 \in \mathbb{Q}[X]$ hat $f' = 2X \neq 0$, aber $f = X^2$ ist inseparabel)

Folgerung 13.0.7. $char(K) = 0$, $f \in K[X]$ irreduzibel
Dann ist f separabel.

Beispiel 13.0.8. $f = X^p - t \in \mathbb{F}_p(t)[X]$ ist irreduzibel nach Bsp 8.0.16(c), aber f inseparabel wegen $f' = pX^{p-1} = 0$

Bemerkung 13.0.9. $char(K) = p > 0$, $a \in K$, $r \in \mathbb{N}$
Dann existiert in $\bar{K}$ genau eine p^r-te Wurzel aus a (d.h. genau ein $\beta \in \bar{K}$ mit $\beta^{p^r} = a$).

Satz 13.0.10. $char(K) = p > 0$. $f \in K[X]$ irreduzibel, $\bar{K}$ ein algebraischer Abschluss von K
$r := max\{m \in \mathbb{N}_0 |$ Es ex. $h \in K[X]$ mit $f(X) = h(X^{p^m})\}$, $g \in K[X]$ mit $f(X) = g(X^{p^r})$.
Dann gilt:
(a) Jede Nullstelle von f in $\bar{K}$ hat Vielfache p^r
(b) g ist irreduzibel und separabel
(c) Die Nullstelle von f in $\bar{K}$ sind genau die p^r-ten Wurzeln der Nullstellen von g in $\bar{K}$

Beispiel 13.0.11. $f = X^p - t \in \mathbb{F}_p(t)[X]$ (vgl. Bsp. 13.0.8). Hier ist $r = 1, g = X - t$ (dann $f = g(X^p)$)

Definition 13.0.12. $L|K$ algebraische Körpererweiterung, $\alpha \in L$
α heißt separabel über $K \Leftrightarrow$ Es gibt ein separables Polynom $f \in K[X]$ mit $f(\alpha) = 0 \Leftrightarrow$ Das Minimalpolynom von α über K ist separabel
$L|K$ heißt separabel $\Leftrightarrow$ Jedes Element $\alpha \in L$ ist separabel über K
K heißt vollkommen (perfekt) $\Leftrightarrow$ Jede algebraische Erweiterung von K ist separabel.

Folgerung 13.0.13. $char(K) = 0$. Dann ist K vollkommen.

Beispiel 13.0.14. $\alpha \in \overline{\mathbb{F}_p(t)}$ Nullstelle von $X^p - t \in \mathbb{F}_p(t)[X]$
$\Rightarrow$ Die Erweiterung $\mathbb{F}_p(t)(\alpha)|\mathbb{F}_p(t)$ ist nicht separabel, da $X^p - t \in \mathbb{F}_p(t)[X]$ (Minimalpolynom von α, da irreduzibel) inseparabel. Insbesondere ist $\mathbb{F}_p(t)$ nicht vollkommen.

Definition 13.0.15. $L|K$ algebraische Körpererweiterung, $\bar{K}$ ein algebraischer Abschluss von K
$[L : K]_s := \#Hom_K(L, \bar{K})$ heißt der Separabilitätsgrad von L über K.

Anmerkung: Die ist unabhängig von der Wahl von $\bar{K}$ (da je zwei algebraische Abschlüsse von K K-isomorph sind)

Bemerkung 13.0.16. $\bar{K}$ ein algebraischer Abschluss von K, $\alpha \in \bar{K}$, $f \in K[X]$ Minimalpolynom von α über K
Dann gilt:
(a) $[K(\alpha) : K]_s$ = Anzahl der verschiedenen Nullstellen von $f \in \bar{K}$
(b) α separabel über $K \Leftrightarrow [K(\alpha) : K]_s = [K(\alpha) : K]$
(c) Gilt $char(K) = p > 0$, und ist p^r die Vielfachheit der Nullstelle von α von f, so ist $[K(\alpha) : K] = p^r[K(\alpha) : K]_s$

Satz 13.0.17. $M|L|K$ algebraische Körpererweiterung. Dann gilt:
$[M : K]_s = [M : L]_s[L : K]_s$

Satz 13.0.18. $L|K$ endliche Körpererweiterung. Dann gilt:
(a) Falls $char(K) = 0$, dann $[L : K] = [L : K]_s$
(b) Falls $char(K) = p > 0$, dann existiert ein $r \in \mathbb{N}_0$ mit $[L : K] = p^r[L : K]_s$
Insbesondere gilt stets: $[L : K]_s | [L : K]$

Satz 13.0.19. $L|K$ endliche Körpererweiterung. Dann sind äquivalent:
(i) $L|K$ separabel
(ii) Es gibt über K separable Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$
(iii) $[L : K]_s = [L : K]$

Folgerung 13.0.20. $L|K$ endliche Körpererweiterung, $char(K) = p > 0$, $p \nmid [L : K]$
Dann ist $L|K$ separabel.

Folgerung 13.0.21. $L|K$ algebraisch. Dann sind äquivalent:
(i) $L|K$ separabel
(ii) L wird über K von separablen Elementen erzeugt.
Ist eine der Bedingungen erfüllt, dann $[L : K] = [L : K]_s$

Folgerung 13.0.22. $M|L|K$ algebraische Körpererweiterung. Dann sind äquivalent:
(i) $M|K$ separabel
(ii) $M|L$ separabel und $L|K$ separabel

Definition 13.0.23. K heißt separabel abgeschlossen $\Leftrightarrow$ Es existiert keine nichttriviale separable Erweiterung von K

Beispiel 13.0.24. K algebraisch abgeschlossen $\Leftrightarrow$ K separabel abgeschlossen.

Satz 13.0.25. Es gibt einen separablen abgeschlossenen Erweiterungskörper K^{sep} von K, sodass $K^{sep}|K$ algebraisch und separabel ist. Man nennt K^{sep} einen separablen Abschluss von K. K^{sep} ist bis auf (unkan.) K-Isomorphie eindeutig bestimmt.

Beispiel 13.0.26. K vollkommen $\Rightarrow$ Jeder algebraische Abschluss von K ist auch ein separabler Abschluss von K.

Satz 13.0.27. (Satz vom primitiven Element)
$L|K$ endlich separable Körpererweiterung. Dann existiert ein $\alpha \in L$ mit $L = K(\alpha)$, d.h. $L|K$ ist einfach. Man nennt α ein primitives Element von $L|K$.

Anmerkung: Beweis hat gezeigt: Für $\#K = \infty$ sind fast alle Elemente $a + \lambda b$, $\lambda \in K$ primitive Elemente von $K(a,b)$ (für a,b separabel über K).

Beispiel 13.0.28. $a,b \in \mathbb{Q} \Rightarrow \sqrt{a} + \sqrt{b}$ ist ein primitives Element von $\mathbb{Q}(\sqrt{a},\sqrt{b})|\mathbb{Q}$, denn: $\mathbb{Q}(\sqrt{a}+\sqrt{b}) = \mathbb{Q}(\sqrt{a},\sqrt{b})$
$''\subseteq''$ klar
$''\supseteq'' \underbrace{a-b}_{\in\mathbb{Q}} = (\sqrt{a}-\sqrt{b})(\underbrace{\sqrt{a}+\sqrt{b}}_{\mathbb{Q}(\sqrt{a}+\sqrt{b})}) \Rightarrow \sqrt{a}-\sqrt{b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$
Es ist $\sqrt{a} = \frac{1}{2}((\sqrt{a}+\sqrt{b})+(\sqrt{a}-\sqrt{b})) \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$
analog für $\sqrt{b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$

14. Endliche Körper

Bemerkung 14.0.1. $\mathbb{F}$ endlicher Körper. Dann gilt:
(a) $char(\mathbb{F}) = p$ für eine Primzahl p
(b) Der Primkörper von $\mathbb{F}$ ist kanonisch isomorph zu $\mathbb{F}_p$
(c) $\mathbb{F}$ enthält genau $q = p^n$ Elemente, $n = [\mathbb{F} : \mathbb{F}_p]$
(d) $\mathbb{F}$ ist Zerällungskörper des Polynom $X^q - X$ über $\mathbb{F}_p$
(e) $\mathbb{F}|\mathbb{F}_p$ ist eine normale Körpererweiterung

Satz 14.0.2. p Primzahl. Dann gilt:
(a) Zu jedem $n \in \mathbb{N}$ existiert ein Erweiterungskörper $\mathbb{F}_q|\mathbb{F}_p$ mit $q = p^n$ Elementen. Dieser ist als Zerfällungskörper des separablen Polynoms $X^q - X \in \mathbb{F}_p[X]$ eindeutig bis auf (unkanonische) Isomorphie bestimmt. $\mathbb{F}_q$ besteht aus den q Nullstellen von $X^q - X \in \mathbb{F}_p[X]$ in einem algebraischen Abschluss von $\mathbb{F}_p$
(b) $\mathbb{F}$ endlicher Körper der Charakteristik $p \Rightarrow$ Es existieren eindeutig bestimmte $n \in \mathbb{N}$, sodass $\mathbb{F} \cong \mathbb{F}_{p^n}$

Anmerkung: Es gilt zwar $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, aber für $n > 1$ gilt stets $\mathbb{F}_{p^n} \ncong \mathbb{Z}/p^n\mathbb{Z}$ (rechts steht ein nicht-nullteilerfreier Ring).

Folgerung 14.0.3. p Primzahl. Man bette die Körper $\mathbb{F}_q, q = p^n$, $n \in \mathbb{N}$ ein einen festen algebraischen Abschluss $\bar{\mathbb{F}_p}$ von $\mathbb{F}_p$ ein. Dann gelten:
(a) $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ mit $q = p^n$, $q' = p^{n'} \Leftrightarrow n|n'$
(b) Die Erweiterung des Typs $\mathbb{F}_{q'}|\mathbb{F}_q$ sind bis auf Isomorphie die einzigen Erweiterungen zwischen endlichen Körpern der Charakteristik p

Folgerung 14.0.4. K endlicher Körper. Dann gilt:
(a) Ist $L|K$ eine algebraische Erweiterung, dann ist $L|K$ normal und separabel
(b) K ist vollkommen

Satz 14.0.5. p Primzahl, $r \in \mathbb{N}$, $q = p^r$, $\mathbb{F}_{q'}|\mathbb{F}_q$ endliche Körpererweiterungen von Grad n. Dann ist $Aut_{\mathbb{F}_q}(\mathbb{F}_{q'})$ eine zyklische Gruppe der Ordnung n, erzeugt vom relativen Frobeniusautomorphismus $\sigma = \sigma^r_{\mathbb{F}_{q'}} : \mathbb{F}_{q'} \to \mathbb{F}_{q'}$, $a \mapsto a^q$
(hierbei ist $\sigma_{\mathbb{F}_{q'}} : \mathbb{F}_{q'} \to \mathbb{F}_{q'}$, $a \mapsto a^p$ der Frobeniusautomorphismus aus 9.0.9)

Satz 14.0.6. R nullteilerfreier kommutativer Ring, $H \subseteq R^*$ endliche Untergruppe.
Dann ist H zyklisch.

Folgerung 14.0.7. p Primzahl, $n \in \mathbb{N}$, $q = p^n$. Dann ist $\mathbb{F}_q^*$ eine zyklische Gruppe der Ordnung $q - 1$.

Teil IV.

Galoistheorie

Idee:

K Körper, $f \in K[X]$, L ein Zerfällungskörper von f über K. Wir studieren die Nullstellen von f mit Hilfe der gruppentheoretischen Eigenschaften von $Aut_{K(L)}$.

In diesem Kapitel sei K stets ein Körper.

15. Galoiserweiterungen

Definition 15.0.1. $L|K$ algebraische Körpererweiterung
$L|K$ heißt galoisch (Galoiserweiterung): $\Leftrightarrow L|K$ normal und separabel. In diesem Fall heißt $Gal(L|K) := Aut_K(L)$ die Galoisgruppe von $L|K$.

Beispiel 15.0.2.
(a) $f \in K[X]$ separabel, L Zerfällungskörper von $f \Rightarrow L|K$ galoisch
(b) p Primzahl, $r \in \mathbb{N}$, $q = p^r \Rightarrow$ Jede algebraische Erweiterung $\mathbb{F}|\mathbb{F}_q$ ist galoisch (Folgerung 14.0.4(a)). Ist $\mathbb{F}_{q'}|\mathbb{F}_q$ eine endliche Erweiterung mit $q' = q^n$, dann ist $Gal(\mathbb{F}_{q'}|\mathbb{F}_q)$ zyklisch von der Ordnung n. Ein Erzeuger ist der relative Frobenius $\mathbb{F}_{q'} \to \mathbb{F}_{q'}$, $a \mapsto a^q$ (Satz 14.0.5)

Bemerkung 15.0.3. $L|K$ endlich normale Körpererweiterung. Dann gilt:
(a) $ord(Aut_K(L)) \leq [L:K]$
(b) $L|K$ galoisch $\Leftrightarrow ord(Aut_K(L)) = [L:K]$

Beispiel 15.0.4. $\mathbb{C}|\mathbb{R}$ ist galoisch $[\mathbb{C}:\mathbb{R}] = 2 \Rightarrow ord((Gal(\mathbb{C}|\mathbb{R})) = 2$. Das nichttriviale Element ist die komplexe Konjugation.

Bemerkung 15.0.5. $L|K$ Galoiserweiterung. E Zwischenkörper vom $L|K$ (d.h. $K \leq E \leq L$). Dann gilt:
(a) $L|E$ ist galoisch und $Gal(L|E)$ ist in natürlich Weise eine Untergruppe von $Gal(L|K)$
(b) Ist $E|K$ galoisch, so beschränkt sich jeder K-Automorphismus von L zu einem K-Automorphismus von E und $\pi : Gal(L|K) \to Gal(E|K)$, $\sigma \mapsto \sigma|_E$ ist eine surjektiver Gruppenhomorphismus mit $\ker(\pi) = Gal(L|E)$

Satz 15.0.6. L Körper, $G \leq Aut(L)$ Untergruppe.
$L^G := \{a \in L | \sigma(a) = a$ für alle $\sigma \in G\}$ heißt Fixkörper L unter G (insbesondere ist L^G ein Körper!). Es gilt:
(a) Ist G endlich, oder $L|L^G$ algebraisch, dann ist $L|L^G$ galoisch.
(b) Ist G endlich, dann ist $L|L^G$ endlich galoisch mit $Gal(L|L^G) = G$
(c) Ist $L|L^G$ algebraisch und G nicht endlich, dann ist $L|L^G$ eine unendliche Galoiserweiterung und $Gal(L|L^G)$ enthält G als Untergruppe.

Folgerung 15.0.7. $L|K$ normale Körpererweiterung $G = Aut_K(L)$. Dann gilt:
(a) $L|L^G$ ist eine Galoiserweiterung mit Galoisgruppe G.
(b) Ist $L|K$ separabel, dann ist $K = L^G$

Satz 15.0.8. (Hauptsatz der Galoistheorie)
$L|K$ endliche Galoiserweiterung, $G = Gal(L|K)$. Dann gilt:
(a) Die Abbildungen:

$$\{\text{Untergruppen von } G\} \xrightarrow{\phi} \text{Zwischenkörper von } L|K$$
$$\xleftarrow[\psi]{}$$
$$H \longmapsto L^H$$
$$Gal(L|E) \longmapsfrom E$$

sind (inklusionsumkehrend), bijektiv und invers zueinander.
(b) $L^H|K$ normal (d.h. galoisch) $\Leftrightarrow H \trianglelefteq G$

In diesem Fall induziert die Einschränkungsabbildung

$$G \to Gal(L^H|K), \quad \sigma \mapsto \sigma|_{L^H}$$

einen Isomorphismus $G/H \xrightarrow{\cong} Gal(L^H|K)$.

Anmerkung: Der Beweis von (a) zeigt: Ist $L|K$ unendlich, so ist immer noch $\phi \circ \psi = id$, insbesondere ist ψ injektiv (aber im Allgemeinen nicht mehr surjektiv).

Folgerung 15.0.9. $L|K$ endlich separable Körpererweiterung $\Rightarrow L|K$ hat nur endlich viele Zwischenkörper.

Anmerkung: Es gibt endlich inspeparable Erweiterungen mit unendlich vielen Zwischenkörpern.

Definition 15.0.10. L Körper, $E, E' \leq L$ Teilkörper
$EE' := E(E') = E'(E)$ heißt das Kompositum von E und E'.

Anmerkung: EE' ist der kleinste Teilkörper von L, der E und E' enthält.

Beispiel 15.0.11.
$L = \mathbb{R}$, $E = \mathbb{Q}(\sqrt{2})$, $E' = \mathbb{Q}(\sqrt{5})$, $EE' = \mathbb{Q}(\sqrt{2}, \sqrt{5})$

Folgerung 15.0.12. $L|K$ endliche Galoiserweiterung, EE' Zwischenkörper von $L|K$, $H = Gal(L|E)$, $H' = Gal(L'|E)$ (sind Untergruppen von $Gal(L|K)$). Dann gilt:
(a) $E \subseteq E' \Leftrightarrow H \supseteq H'$ (d.h. ϕ, ψ aus 15.0.8 sind inklusionsumkehrend)
(b) $EE' = L^{H \cap H'}$
(c) $E \cap E' = L^{<H,H'>}$

Definition 15.0.13. $L|K$ endliche Galoiserweiterung
$L|K$ heißt abelsch (bzw. zyklisch) $\Leftrightarrow Gal(L|K)$ ist abelsch (bzw. zyklisch)

Folgerung 15.0.14. $L|K$ endlich abelsche (bzw. zyklische) Galoiserweiterung. Dann gilt:
Für jeden Zwischenkörper E von $L|K$ sind $L|E$ und $E|K$ endliche abelsche (bzw. zyklische) Galoiserweiterung.

Satz 15.0.15. $L|K$ Körpererweiterung, E, E' Zwischenkörper, sodass $E|K$ und $E'|K$ endlich galoisch. Dann gilt:
(a) (Translationssatz) $EE'|K$ ist eine endliche Galoiserweiterung, und der Homomorphismus

$$\varphi : Gal(EE'|E) \to Gal(E'|E \cap E'), \quad \sigma \mapsto \sigma|_{E'}$$

ist ein Isomorphismus
(b) Der Homomorphismus $\psi : Gal(EE'|K) \to Gal(E|K) \times Gal(E'|K)$, $\sigma \mapsto (\sigma|_E, \sigma|_{E'})$ ist injektiv.
Gilt $E \cap E' = K$, ist ψ auch surjektiv, d.h. ein Isomorphismus.

Bemerkung 15.0.16. $L|K$ endlich Galoiserweiterung, $a \in L$ mit $L = K(a)$, $H \subseteq Gal(L|K)$ Untergruppe.
Wir setzen $f_H := \prod_{\sigma \in H} (X - \sigma(a)) = \sum_{i=0}^{m} c_i X^i \in L[X]$, $m = ord(H)$. Dann gilt:
(a) f_H ist das Minimalpolynom von a über L^H
(b) $L^H = K(c_0, \ldots c_{m-1})$

16. Galoisgruppe von Polynomen

Definition 16.0.1. $f \in K[X]$ separabel, $\deg f \geq 1$, L Zerfällungskörper von f über K
$Gal(f) := Gal(L|K)$ heißt die Galoisgruppe von f über K.

Satz 16.0.2. $f \in K[X]$ separabel, $\deg(f) \geq 1$, L Zerfällungskörper von f über K, $\alpha_1, \ldots, \alpha_n$, die Nullstelle von f in L. Dann gilt:
(a) Die Abbildung $\varphi : Gal(L|K) \to S(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n$, $\sigma \mapsto \sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$ ist ein injektiver Gruppenhomomorphismus, d.h. man kann $Gal(L|K)$ als Untergruppe von S_n auffassen.
(b) $[L : K] = ord(Gal(L|K))|n!$
(c) f irreduzibel $\Leftrightarrow$ $Gal(L|K)$ operiert transitiv auf $\{\alpha_1, \ldots, \alpha_n\}$, d.h. für alle $1 \leq i, j \leq n$ existiert $\sigma \in Gal(L|K)$ mit $\sigma(\alpha_i) = \alpha_j$

Folgerung 16.0.3. $L|K$ endliche Galoiserweiterung, $[L : K] = n$
Dann lässt sich $Gal(L|K)$ als Untergruppe der S_n auffassen.

Beispiel 16.0.4. $char(K) \neq 2$, $f = X^2 + aX + b \in K[X]$ habe keine Nullstellen in K.
$\Rightarrow f$ irreduzibel, $f' = 2X + a \neq 0 \Rightarrow f$ separabel
Sei $\overline{K}$ ein algebraischer Abschluss von K, $\alpha, \beta \in \overline{K}$ Nullstellen von $f \Rightarrow \alpha\beta = b \Rightarrow \beta = \frac{b}{\alpha}$
$\Rightarrow K(\alpha)$ ist Zerfällungskörper von f über K, $[K(\alpha) : K] = 2$
$\Rightarrow Gal(f) = Gal(K(\alpha)|K)$ zyklische Gruppe der Ordnung 2, erzeugt von $\sigma : K(\alpha) \to K(\alpha)$, $\alpha \mapsto \beta$

Definition 16.0.5. $f \in K[X]$, $\overline{K}$ algebraischer Abschluss von K, $n = \deg(f)$, $\alpha_1, \ldots, \alpha_n$ Nullstelle von f in $\overline{K}$
$\Delta_f := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$ heißt die Diskriminante von f

Bemerkung 16.0.6. $f \in K[X]$. Dann gilt:
(a) $f = X^2 + aX + b \Rightarrow \Delta_f = a^2 - 4b$
(b) $f = X^3 + aX + b \Rightarrow \Delta_f = -4a^3 - 27b^2$

Bemerkung 16.0.7. $f \in K[X]$. Dann gilt:
(a) f separabel $\Leftrightarrow \Delta_f \neq 0$
(b) $\Delta_f \in K$. Insbesondere ist Δ_f unabhängig von der Wahl von $\bar{K}$

Bemerkung 16.0.8. $char(K) \neq 2$, $f \in K[X]$ separabel, $\alpha_1, \ldots, \alpha_n$ Nullstellen von f in $\bar{K}$, $L := K(\alpha_1, \ldots, \alpha_n)$
$\varphi : Gal(L|K) \to S_n$ wie in 16.0.2. Dann sind äquivalent:
(i) Δ_f ist ein Quadrat in K
(ii) $\varphi(Gal(L|K)) \subseteq A_n$

Anmerkung: Ist $\beta_1, \ldots, \beta_n$ eine Umnummerierung von $\alpha_1, \ldots, \alpha_n$ etwa $\beta_i = \alpha_{\pi(i)}$ für ein $\pi \in S_n$, ist $\psi : Gal(L|K) \hookrightarrow S_n$ die Abbildung aus 16.0.2 zu $\beta_1, \ldots, \beta_n$, dann gilt für $Gal(L|K)$, $i \in \{1, \ldots, n\} : \beta_{\psi(\sigma)(i)} = \sigma(\beta_i) = \sigma(\alpha_{\pi(i)} = \alpha_{\varphi(\sigma)(\pi(i))} = \beta_{\pi^{-1}(\varphi(\sigma)(\pi(i)))}$, d.h. $\psi(\sigma) = \pi^{-1}\varphi(\sigma)\pi$, insbesondere ist $sgn(\psi(\sigma)) = sgn(\varphi(\sigma))$.
Insbesondere macht es Sinn, $sgn(\sigma) := sgn(\varphi(\sigma))$ und von "$Gal(f) \subseteq A_n$" zu sprechen.

Bemerkung 16.0.9. $char(K) \neq 2, 3$, $f = X^3 + aX + b \in K[X]$ irreduzibel. Dann gilt:
(a) f ist separabel
(b) $Gal(f) \cong \begin{cases} A_3, \text{ falls } \Delta_f = -4a^3 - 27b^2 \text{ ein Quadrat in } K \text{ ist} \\ S_3, \text{ falls } \Delta_f = -4a^3 - 27b^2 \text{ kein Quadrat in } K \text{ ist} \end{cases}$

Beispiel 16.0.10.
(a) $f = X^3 - X + 1 \in \mathbb{Q}[X]$ ist irreduzibel, $\Delta_f = -4(-1)^3 - 27 = -23$ kein Quadrat in $\mathbb{Q} \Rightarrow Gal(f) \cong S_3$
(b) $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel, $\Delta_f = -4(-3)^3 - 27 = 81 = 9^2 \Rightarrow Gal(f) \cong A_3$

Bemerkung 16.0.11. $T_1, \ldots, T_n$ Variablen, k Körper, $L = k(T_1, \ldots, T_n) = Quot(k[T_1, \ldots, T_n])$. Dann gilt:
(a) Jedes Element $\pi \in S_n$ induziert einen Automorphismus von L:

$$\frac{g(T_1, \ldots, T_n)}{h(T_1, \ldots, T_n)} \longmapsto \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})},$$

dadurch erhalten wir eine Inklusion $S_n \subseteq Aut(L)$
$K := L^{S_n}$ heißt der Körper der symmetrischen rationalen Funktionen in n Variablen $T_1, \ldots, T_n$ mit Koeffizienten in k.
(b) $L|K$ ist eine Galoiserweiterung mit $Gal(L|K) \cong S_n$, insbesondere ist $[L : K] = n!$

Definition 16.0.12. $T_1, \ldots, T_n$ Variablen, k Körper. Wir definieren Polynome $s_0(T_1, \ldots, T_n), \ldots, s_n(T_1, \ldots, T_n) \in k[T_1, \ldots, T_n]$ durch:

$$\prod_{i=1}^{n}(X - T_i) = \sum_{j=0}^{n}(-1)^j s_j(T_1, \ldots, T_n)X^{n-j} \in k[T_1, \ldots, T_n][X]$$

$s_j(T_1, \ldots, T_n)$ heißt das j-te elementarsymmetrische Polynome in $T_1, \ldots, T_n$.
Ist die Anzahl der Variablen aus dem Kontext klar, schreibt man kurz s_j

Beispiel 16.0.13.
$n = 1 : X - T_1 \stackrel{!}{=} s_0(T_1)X - s_1(T_1) \Rightarrow s_0(T_1) = 1, s_1(T_1) = T_1$
$n = 2 : (X - T_1)(X - T_2) = X^2 - (T_1 + T_2)X + T_1T_2 \stackrel{!}{=} s_0(T_1, T_2)X^2 - s_1(T_1, T_2)X + s_2(T_1, T_2)$
$\Rightarrow s_0(T_1, T_2) = 1, s_1(T_1, T_2) = T_1 + T_2, s_2(T_1, T_2) = T_1T_2$
allgemein: $s_0(T_1, \ldots, T_n) = 1, s_1(T_1, \ldots, T_n) = T_1 + \ldots + T_n, s_2(T_1, \ldots, T_n) = T_1T_2 + T_1T_3 + \ldots + T_{n-1}T_n, s_n(T_1, \ldots, T_n) = T_1 \cdot \ldots \cdot T_n$

Bemerkung 16.0.14. $T_1, \ldots, T_n$ Variablen k Körper, $L = k(T_1, \ldots, T_n)$, $K = L^{S_n}$, $f = \prod_{i=1}^{n}(X - T_i) \in L[X]$. Dann gilt:
(a) $s_j \in K$ für $j = 1, \ldots, n$, insbesondere $f \in K[X]$
(b) $k(s_1, \ldots, s_n) \subseteq K$
(c) L ist Zerfällungskörper von f über K
(d) f ist irreduzibel in $K[X]$
(e) f ist separabel
(f) $Gal(f) \cong S_n$ (über K)

Satz 16.0.15. (Hauptsatz über symmetrisch rationale Funktionen)
$T_1, \ldots, T_n$ Variablen, k Körper, $L = k(T_1, \ldots, T_n)$, $K = L^{S_n}$. Dann gilt:
(a) $K = k(s_1, \ldots, s_n)$
(b) $s_1, \ldots, s_n$ sind algebraisch unabhängig über k
Insbesondere lässt sich jede symmetrisch rationale Funktion eindeutig als rationale Funktion in den elementarsymmetrischen Polynomen darstellen, d.h. für alle $f \in K$ existieren eindeutig bestimmte $g \in k(T_1, \ldots, T_n)$, sodass $f(T_1, \ldots, T_n) = g(s_1, \ldots, s_n)$

Definition 16.0.16. $T_1, \ldots, T_n$ Variablen, k Körper
$p(X) = X^n + T_1X^{n-1} + \ldots, T_{n-1}X + T_n \in k(T_1, \ldots, T_n)[X]$
heißt das allgemeine Polynom n-ten Grades über k.
Die Gleichung $p(X) = 0$ heißt die allgemeine Gleichung n-ten Grades über k.

Satz 16.0.17. k Körper, $T_1, \ldots, T_n$ Variablen. Dann gilt:
(a) Das allgemeine Polynom n-ten Grades $p(X) \in k(T_1, \ldots, T_n)[X]$ ist irreduzibel und separabel
(b) $Gal(p(X)) \cong S_n$

17. Einheitswurzeln

Bemerkung 17.0.1. $n \in \mathbb{N}$. Dann sind äquivalent:
(i) $f = X^n - 1 \in K[X]$ ist separabel
(ii) $char(K) \nmid n$

Definition 17.0.2. $n \in \mathbb{N}$ mit $char(K) \nmid n$, $\bar{K}$ ein algebraischer Abschluss von K. Ein Element $\zeta \in \bar{K}$ heißt eine n-te Einheitswurzel (EW) $\Leftrightarrow \zeta^n = 1$.
Die Menge der n-ten Einheitswurzel in $\bar{K}$ wir mit μ_n bezeichnet und ist offenbar eine Untergruppe von $\bar{K}^*$

Satz 17.0.3. $n \in \mathbb{N}$ mit $char(K) \nmid n$
Dann ist μ_n eine zyklische Gruppe der Ordnung n

Definition 17.0.4. $n \in \mathbb{N}$ mit $char(K) \nmid n$
$\zeta \in \mu_n$ heißt eine primitive n-te Einheitswurzel $\Leftrightarrow \zeta$ ist ein Erzeuger der zyklischen Gruppe μ_n.

Beispiel 17.0.5. $K = \mathbb{C}$, $\zeta_n = e^{2\pi i/n}$ ist eine primitive n-te Einheitswurzel.

Definition 17.0.6. Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$, $n \mapsto ord((\mathbb{Z}/n\mathbb{Z})^*)$ heißt die Eulersche φ-Funktion.

Bemerkung 17.0.7. $n \in \mathbb{N}$. Dann gilt:
(a) $\varphi(n) = \#\{a \in \mathbb{N}_0 | 0 \le a < n, ggT(a,n) = 1\}$
(b) $m,n \in \mathbb{N}$ teilerfremd $\Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$
(c) p Primzahl, $r \in \mathbb{N} \Rightarrow \varphi(p^r) = \varphi^{r-1}(p-1)$
(d) $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ Primfaktorzerlegung von $n \Rightarrow \varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = n \prod_{p \text{ PZ mit } p|n} (1 - \frac{1}{p})$

Bemerkung 17.0.8. $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Dann sind äquivalent:
(i) $\bar{a}$ erzeugt die additive zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$
(ii) $\bar{a}$ ist Einheit im Ring $\mathbb{Z}/n\mathbb{Z}$
(iii) $ggT(a,n) = 1$
Insbesondere enthält $\mathbb{Z}/n\mathbb{Z}$ genau $\varphi(n)$ Elemente, die $\mathbb{Z}/n\mathbb{Z}$ erzeugen.

Bemerkung 17.0.9. $n \in \mathbb{N}$ mit $char(K) \nmid n$, $\zeta \in \bar{K}$ primitive n-te Einheitswurzel. Dann gilt:
(a) Es gibt genau $\varphi(n)$ primitive n-te Einheitswurzeln in $\bar{K}$.
(b) Die primitiven n-ten Einheitswurzeln in $\bar{K}$ sind genau von der Form ζ^r mit $1 \le r < n$, $ggT(r,n) = 1$

Bemerkung 17.0.10. $n \in \mathbb{N}$ mit $char(K) \nmid n$, $\zeta \in \mu_n$ primitive n-te Einheitswurzel
Dann ist $K(\mu_n) = K(\zeta)|K$ eine endliche Galoiserweiterung.

Satz 17.0.11. $n \in \mathbb{N}$ mit $char(K) \nmid n$, $\zeta_n \in \bar{K}$ primitive n-te Einheitswurzel. Dann gilt:
(a) $K(\zeta_n)|K$ ist eine endliche abelsche Galoiserweiterung mit Grad $\le \varphi(n)$
(b) Es existiert ein injektiver Gruppenhomomorphismus

$$\chi : Gal(K(\zeta_n)|K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*,$$

sodass für jede n-te Einheitswurzel $\zeta \in K(\zeta_n)$ und jedes $\sigma \in Gal(K(\zeta_n)|K)$ gilt: $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ (hierbei ist $\zeta^{\bar{a}} := \zeta^a$ für $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$).
χ heißt der zyklotomische Charakter.

Ziel: Für $K = \mathbb{Q}$ ist χ ein Isomorphismus.

Definition 17.0.12. $n \in \mathbb{N}, \zeta_n \in \bar{\mathbb{Q}}$ primitive n-te Einheitswurzel
$\mathbb{Q}(\zeta_n)$ heißt n-ter Kreisteilungskörper
$\phi_n = \prod_{\zeta \text{ prim. } n\text{-te Einheitswurzel in } \bar{\mathbb{Q}}} (X - \zeta) \in \mathbb{Q}(\zeta_n)[X]$ heißt das n-te Kreisteilungspolynom.

Bemerkung 17.0.13. $n \in \mathbb{N}$. Dann gilt:
(a) $\phi_n \in \mathbb{Q}[X]$
(b) $\deg(\phi_n) = \varphi(n)$
(c) p Primzahl $\Rightarrow \phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$

Anmerkung: (a) zeigt insbesondere, dass ϕ_n unabhängig von der Wahl von $\bar{\mathbb{Q}}$

Satz 17.0.14. $n \in \mathbb{N}$. Dann gilt:
(a) $\phi_n \in \mathbb{Z}[X]$
(b) ϕ_n ist irreduzibel in $\mathbb{Z}[X]$

Folgerung 17.0.15. $n \in \mathbb{N}$, ζ_n primitive n-te Einheitswurzel in $\bar{\mathbb{Q}}$. Dann gilt:
(a) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$
(b) Der zyklotomische Charakter $\chi : Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ aus 17.0.11(b) ist (für $K = \mathbb{Q}$) ein Isomorphismus.

Definition 17.0.16. K Körper, $n \in \mathbb{N}$ mit $char(K) \nmid n$, $\bar{K}$ ein algebraischer Abschluss von K.
$\phi_{n,K} := \prod_{\zeta \text{prim. n-te EW in } \bar{K}} (X - \zeta) \in K[X]$ heißt das n-te Kreisteilungspolynom über K.

Anmerkung: $\phi_{n,K} \in K[X]$ folgt analog zu 17.0.13(a)

Bemerkung 17.0.17. K Körper, $n \in \mathbb{N}$ mit $char(K) \nmid n$, $\psi : \mathbb{Z} \to K$ kanonischer Homomorphismus (vgl. 9.0.1(a))
Dann gilt: $\phi_{n,K} = \phi_n^{\psi}$

Satz 17.0.18. q Primzahlpotenz, $n \in \mathbb{N}$ mit $ggT(q,n) = 1$, $\psi : \mathbb{Z} \to \mathbb{F}_q$ kanonischer Homomorphismus, $\zeta \in \bar{\mathbb{F}_q}$ primitive n-te Einheitswurzel $\sigma \in Gal(\mathbb{F}_q(\zeta_n)|\mathbb{F}_q)$ relativer Frobeniusautomorphismus (vgl. 14.0.15), $\chi : Gal(\mathbb{F}_q(\zeta_n)|\mathbb{F}_q) \to (\mathbb{Z}/n\mathbb{Z})^*$ zyklotomischer Charakter. Dann gilt:
(a) $\chi(\sigma) = \bar{q}$
(b) χ induziert einen Isomorphismus zwischen $Gal(\mathbb{F}_q(\zeta_n)|\mathbb{F}_q)$ und der von $\bar{q}$ erzeugten Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$
(c) $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = ord_{(\mathbb{Z}/n\mathbb{Z})^*}(\bar{q})$
(d) $\phi_{n,\mathbb{F}_q} = \phi_n^{\psi}$ ist irreduzibel in $\mathbb{F}_q[X] \Leftrightarrow \bar{q}$ erzeugt $(\mathbb{Z}/n\mathbb{Z})^*$

Teil V.

Fortführung der Gruppentheorie

18. Gruppenoperationen

Definition 18.0.1. G Gruppe (im Folgenden stets multiplikativ geschrieben), M Menge. Eine Operation (Aktion, Wirkung) von G auf M ist eine Abbildung

$$G \times M \to M, \quad (g,x) \mapsto gx$$

sodass gilt:
(a) $1x = x$ für alle $x \in M$
(b) $(gh)x = g(hx)$ für alle $g,h \in G$, $x \in M$

Beispiel 18.0.2.
(a) Die Multiplikation $G \times G \to G$, $(g,h) \mapsto gh$ ist eine G-Operation auf $M = G$, die Linkstranslation.
(b) Durch $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$ ist eine Operation von G auf $M = G$ gegeben, die Konjugation.
(c) $L|K$ Galoiserweiterung $\Rightarrow G = Gal(L|K)$ operiert auf $M = L$ (bzw. $M = L^*$) via $G \times L \to L$, $(\sigma,x) \mapsto \sigma(x)$ (bzw. $G \times L^* \to L^*$, $(\sigma,x) \mapsto \sigma(x)$)

Bemerkung 18.0.3. G Gruppe, M Menge. Dann gilt: Die Abbildungen

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{Gruppenhom.}\\ G \to S(M)\end{array}\right\} & \longrightarrow & \left\{\begin{array}{c}\text{Operationen von } G\\ \text{auf } M\end{array}\right\} \\ \left\{\begin{array}{c}\\ \end{array}\right. & \longleftarrow & \left.\begin{array}{c}\\ \end{array}\right\} \\ \varphi : G \to S(M) & \longmapsto & G \times M \to M,\ (g,x) \mapsto \varphi(g) \\ G \to S(M),\ g \mapsto \tau_g & \longmapsto & G \times M \to M,\ (g,x) \mapsto gx \end{array}$$

mit $\tau_g : M \to M$, $x \mapsto gx$
sind bijektiv und invers zueinander.

Bemerkung 18.0.4. G Gruppe. Wir setzen für $g \in G$: $int_g : G \to G$, $h \mapsto ghg^{-1}$
Dann gilt:
(a) $int_g \in Aut(G) \subseteq S(G)$ für alle $g \in G$
(b) Die Abbildung $int : G \to Aut(G)$, $g \mapsto int_g$ ist ein Gruppenhomomorphismus

Definition 18.0.5. G Gruppe, $int : G \to Aut(G)$ wie in 18.0.4
$int(G) \subseteq Aut(G)$ heißt die Gruppe der inneren Automorphismen von G.
$Z(G) := \ker(int) = \{g \in G | int_g = id_G\} = \{g \in G | int_g(h) = ghg^{-1} = h\ \forall h \in G\} = \{g \in G | gh = hg\ \forall h \in G\}$
heißt das Zentrum von G.

Beispiel 18.0.6. $Z(S_3) = \{id\}$

Bemerkung 18.0.7. G Gruppe. Dann gilt:
(a) $Z(G) \trianglelefteq G$, $Z(G)$ abelsch
(b) $G/Z(G) \cong int(G)$
(c) G abelsch $\Leftrightarrow int(G) = \{id_G\}$
(d) $G/Z(G)$ zyklisch $\Leftrightarrow G$ abelsch.

Definition 18.0.8. G Gruppe, M Menge, G operiere auf M, $x \in M$.
$Gx := \{gx | g \in G\} \subseteq M$ heißt die Bahn von X (Orbit von X)
$G_x := \{g \in G | gx = x\} \subseteq G$ heißt der Stabilisator (Isotropiegruppe, Standgruppe) von X

Bemerkung 18.0.9. G Gruppe, M Menge, G operiere auf M. Dann gilt:
(a) Für alle $x \in M$ ist $G_x \subseteq G$ eine Untergruppe
(b) Durch $x \sim y \Leftrightarrow$ Es existiert ein $g \in G$ mit $gx = y$ ist eine Äquivalenzrelation auf A gegeben: Die Äquivalenzklasse von $x \in M$ ist die Bahn von x.
(c) M ist die disjunkte Vereinigung von Bahnen.
(d) Für $x \in M$ induziert $G \to M$, $g \mapsto gx$ eine Bijektion $G/G_x \xrightarrow{\sim} Gx$
Hierbei bezeichnet G/G_x die Menge der Linksnebenklassen von G_x in G.
(Beachte: G_x ist im Allgemeinen kein Normalteiler von G).

Satz 18.0.10. (Bahnengleichung)
G Gruppe, M endliche Menge, G operiere auf M. $x_1, \ldots, x_n$ Vertretersystem der Bahnen von M. Dann gilt:

$$\#M = \sum_{i=1}^{n} \#Gx_i = \sum_{i=1}^{n} (G : G_{x_i})$$

Definition 18.0.11. G Gruppe, $S \subset G$ Teilmenge
$Z_s := \{g \in G | gs = sg \text{ für alle } s \in S\}$ heißt der Zentralisator von S in G
$N_s := \{g \in G | gS = Sg\}$ heißt der Normalisator von S in G.

Bemerkung 18.0.12. G Gruppe, $S \subseteq G$ Teilmenge. Dann gilt:
(a) Z_s, N_s sind Untergruppen von G
(b) $Z_s \subseteq N_s$
(c) $S \subseteq G$ Untergruppe $\Rightarrow N_s$ ist die größte Untergruppe H in G, sodass $S \trianglelefteq H$.

Satz 18.0.13. G endlicher Gruppe, $x_1, \ldots, x_n$ Vertretersystem der Bahnen in $G \backslash Z(G)$ bzgl. der Konjugation (vgl. 18.2(b)). Dann gilt:

$$ord(G) = ord(Z(G)) + \sum_{i=1}^{n} (G : Z_{\{x_i\}})$$

19. Sylowgruppen

Definition 19.0.1. G endliche Gruppe, p Primzahl
G heißt p-Gruppe $\Leftrightarrow$ Es existiert ein $n \in \mathbb{N}_0$ mit $ord(G) = p^n$
$H \subseteq G$ Untergruppe heißt p-Sylowgruppe von $G \Leftrightarrow H$ ist eine p-Gruppe mit $p \nmid (G:H) \Leftrightarrow$ Es existiert ein $k \in \mathbb{N}_0$, $m \in \mathbb{N}$ mit $ord(G) = p^k m$, $ord(H) = p^k$ und $p \nmid m$

Anmerkung: $\{1\}$ ist eine p-Gruppe für alle Primzahlen p
Für alle Primzahlen p mit $p \nmid ord(G)$ ist $\{1\} \subseteq G$ eine p-Sylowgruppe.

Beispiel 19.0.2. $G = A_4 \Rightarrow ord(G) = 12 = 2^2 \cdot 3$
G besitzt genau eine 2-Sylowgruppe (mit 4 Elementen), nämlich $< (12)(34), (13)(24) >$.
und 4 3-Sylowgruppen (mit jeweils 3 Elementen), nämlich $< (123) >, < (124) >, < (134) >, < (234) >$.

Bemerkung 19.0.3. G endliche Gruppe p Primzahl. Dann gilt:
(a) G p-Gruppe, $g \in G \Rightarrow ord(g)$ ist eine p-Potenz
(b) $H \subseteq G$ p-Sylowgruppe, $H' \subseteq G$ p-Gruppe mit $H \subseteq H' \Rightarrow H = H'$

Satz 19.0.4. p Primzahl, G p-Gruppe, $ord(G) > 1$. Dann gilt:
(a) $p | ord(Z(G))$
(b) $Z(G) \neq \{1\}$

Folgerung 19.0.5. p Primzahl, G Gruppe der Ordnung p^2. Dann ist G abelsch.

Satz 19.0.6. (Sylowsätze)
G endliche Gruppe, p Primzahl. Dann gilt:
(a) G besitzt eine p-Sylowgruppe
(b) Ist $H \subseteq G$ eine p-Untergruppe, dann existiert eine p-Sylowgruppe $S \subseteq G$ mit $H \subseteq S$.
(c) Ist $S \subseteq G$ eine p-Sylowgruppe, dann ist jede zu S konjugierte Untergruppe von G eine p-Sylowgruppe von G. Je zwei p-Sylowgruppen von G sind konjugiert zueinander.
(d) Für die Anzahl s_p der p-Sylowgruppen von G gilt: $s_p | ord(G)$, $s_p \equiv 1 (mod\, p)$

Folgerung 19.0.7. G endliche Gruppe, p Primzahl. Dann gilt:
(a) $p | ord(G) \Leftrightarrow$ Es existiert ein $g \in G$ mit $ord(g) = p$
(b) G p-Gruppe $\Leftrightarrow$ Für alle $g \in G$ existiert ein $r \in \mathbb{N}_0$ mit $ord(g) = p^r$

Folgerung 19.0.8. G endliche Gruppe, p Primzahl. Dann gilt:
Besitzt G genau eine p-Sylowgruppe S, dann ist $S \trianglelefteq G$

Beispiel 19.0.9. G Gruppe mit 30 Elementen $\Rightarrow G$ besitzt einen nichttrivialen Normalteiler, denn:
$ord(G) = 30 = 2 \cdot 3 \cdot 5 \Rightarrow$ Für $p \in \{2,3,5\}$ gilt $s_p | 30$ und $s_p \equiv 1 (mod\, p) \Rightarrow s_2 \in \{1,3,5,15\}, s_3 \in \{1,10\}, s_5 \in \{1,6\}$.
Annahme: $s_2, s_3, s_5 > 1 \Rightarrow s_3 = 10$, $s_5 = 6$
Sind H_1, H_2 verschiedene 5-Sylowgruppen von G, dann $H_1 \cap H_2 \subsetneq H_1$, $ord(H_1 \cap H_2) | ord(H_1) = 5$ und somit $H_1 \cap H_2 = \{1\}$
$\Rightarrow G$ enthält $s_5 \cdot (5-1) = 6 \cdot 4 = 24$ Elemente der Ordnung 5
Analog: G enthält $s_3 \cdot (3-1) = 10 \cdot 2 = 20$ Elemente der Ordnung 3
$\Rightarrow ord(G) > 44 \lightning$ zu $ord(G) = 30$

20. Auflösbare Gruppen

Definition 20.0.1. G Gruppe. $a,b \in G$, $H,H' \subseteq G$ Untergruppen
$[a,b] := aba^{-1}b^{-1}$ heißt der Kommutator von a und b
$[H,H'] :=< \{[h,h']|h \in H, h' \in H'\} >$
$[G,G]$ heißt der Kommutator von G

Bemerkung 20.0.2. G Gruppe. Dann gilt:
(a) $[G,G]$ besteht aus allen endlichen Produkten von Kommutatoren aus G.
(b) $[G,G] \trianglelefteq G$
(c) $G/[G,G]$ abelsch
(d) Ist $N \trianglelefteq G$, sodass G/N abelsch ist, dann ist $N \supseteq [G,G]$

Bemerkung 20.0.3. Es gilt:
(a) $[S_n,S_n] = A_n$ für $n \geq 2$
(b) $[A_n,A_n] = \begin{cases} \{()\} & \text{für } n = 2,3 \\ V_4 := \{(), (12)\circ(34), (13)\circ(24), (14)\circ(23)\} & \text{für } n = 4 \\ A_n & \text{für } n \geq 5 \end{cases}$

Definition 20.0.4. G Gruppe $D^\circ G := G, D^{i+1}G := [D^iG, D^iG]$ für alle $i \in \mathbb{N}_0$
D^iG heißt der i-te iterierte Kommutator.

Bemerkung 20.0.5. G Gruppe. Dann ist $G = D^\circ G \supseteq D^1G \supseteq D^2G \supseteq \ldots \supseteq D^iG \supseteq \ldots$ eine Kette von Untergruppen von G mit $D^{i+1}G \trianglelefteq D^iG$ und $D^iG/D^{i+1}G$ abelsch für alle $i \in \mathbb{N}_0$

Definition 20.0.6. G Gruppe. Eine Kette von Untergruppen $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}$ heißt eine Normalreihe von $G \Leftrightarrow G_{i+1} \trianglelefteq G_i$ für alle $i \in \{0,\ldots,n-1\}$
G_i/G_{i+1}, $i = 0,\ldots,n-1$ heißen die Faktoren der Normalreihe.
G heißt auflösbar $\Leftrightarrow$ G besitzt eine Normalreihe, deren sämtliche Faktoren abelsch sind.

Satz 20.0.7. G Gruppe. Dann sind äquivalent:
(i) G ist auflösbar
(ii) Es existiert ein $n \in \mathbb{N}_0$ mit $D^nG = \{1\}$

Beispiel 20.0.8. Jede abelsche Gruppe ist auflösbar: $D^1G = [G,G] = \{1\}$

Bemerkung 20.0.9. Die symmetrische Gruppe S_n ist auflösbar für $n \leq 4$, nicht auflösbar für $n \geq 5$

Satz 20.0.10. G endlich auflösbare Gruppe. Dann gilt:
Jede echt absteigende Normalreihe von G mit abelschen Faktoren lässt sich zu einer Normalreihe verfeinern, deren Faktoren zyklisch von Primzahl-Ordnung sind.

Bemerkung 20.0.11. G auflösbare Gruppe, $H \subseteq G$ Untergruppe. Dann ist H auflösbar.

Bemerkung 20.0.12. G Gruppe, $H \trianglelefteq G$. Dann sind äquivalent:
(i) G auflösbar
(ii) H und G/H auflösbar

Satz 20.0.13. p Primzahl, G p-Gruppe
Dann ist G auflösbar und es existiert eine Normalreihe

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\},$$

sodass G_i/G_{i+1} zyklisch der Ordnung p sind.