1

Ring: Menge R, mit Abb.

$(+) : R \times R \longrightarrow R : (r,s) \longmapsto r+s$

$(\cdot) : R \times R \longrightarrow R : (r,s) \longmapsto r\cdot s$

derart, daß gelten:

(Ring 1) Für $r,s \in R$ ist $r+s = s+r$ $\quad$ } $(R,+)$ abelsche Gruppe

(Ring 2) Für $r,s,t \in R$ ist $(r+s)+t = r+(s+t) =: r+s+t$

(Ring 3) $\exists\, 0_R \in R$ mit $r + 0_R = r$ für $r \in R$.

(Ring 4) Für $r \in R$ gibt es ein $s \in R$ mit $r+s = 0_R$

(Ring 5) Für $r,s,t \in R$ ist

$$(r\cdot s)\cdot t = r\cdot(s\cdot t) =: r\cdot s\cdot t$$

(Ring 6) $\exists\, 1_R \in R$ mit $r\cdot 1_R = r = 1_R \cdot r$ für $r \in R$

(Ring 7) Für $r, r', s, s' \in R$ ist

$$(r+r')\cdot s = r\cdot s + r'\cdot s$$

und $r\cdot(s+s') = r\cdot s + r\cdot s'$

Ein Ring R heißt **kommutativ**, falls $r\cdot s = s\cdot r$ für $r,s \in R$ gilt.

Ein kommutativer Ring R heißt **Integritätsbereich**, falls $r,s \in R^\times \Longrightarrow r\cdot s \in R^\times$, wobei $R^\times = R\setminus\{0\}$.

Satz von Descartes:

Sei ein Polynom

$$f(X) = \underbrace{a_n}_{\neq 0} X^n + a_{n-1} X^{n-1} + \ldots + \underbrace{a_0}_{\neq 0} X^0 \in \mathbb{Z}[X]$$

gegeben, wobei $n \geq 1$.

Sei $\frac{u}{v} \in \mathbb{Q}$, mit $u, v \in \mathbb{Z}^\times$ teilerfremd, eine Nullstelle von $f(X)$: $f(\frac{u}{v}) = 0$.

Dann ist u ein Teiler von a_0,

und v ein Teiler von a_n.

R, S : Ringe

$\varphi : R \to S$ heißt Ringmorphismus,

falls $\varphi(1) = 1$, $\varphi(r + r') = \varphi(r) + \varphi(r')$

und $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$ ist, für $r, r' \in R$.

Falls zudem φ bijektiv: Ringisomorphismus.

$I \subseteq R$ heißt Ideal $(I \trianglelefteq R)$, falls

$r, r' \in R$, $x, x' \in I$

$$\Rightarrow \begin{cases} rx + r'x' \in I & (\text{Linksideal}) \\ \quad \text{und} & \\ xr + x'r' \in I & (\text{Rechtsideal}) \end{cases}$$

Sei $I \trianglelefteq R$. Für $r \in R$ sei

$$r + I := \{ r + x : x \in I \} \leftarrow \begin{array}{l} r + I = r' + I \\ \Leftrightarrow r - r' \in I \end{array}$$

die Restklasse von r mod(ulo) I.

Sei $R/I := \{ r + I : r \in R \}$ der Faktorring,

mit $(r + I) + (r' + I) := (r + r') + I$,

$(r + I) \cdot (r' + I) := (r \cdot r') + I$.

Beispiel:

$$\mathbb{Z}/3\mathbb{Z} = \{ 0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, \underbrace{2 + 3\mathbb{Z}}_{= -1 + 3\mathbb{Z}} \} \overset{\text{Konvention}}{=} \{ 0, 1, \underbrace{2}_{= -1} \}$$

R : kommutativer Ring

$I \triangleleft R$: Ideal in R

$r, r' \in R, \quad x, x' \in I \Rightarrow rx + r'x' \in I$

Es heißt $I \triangleleft R$ maximal, falls

$$I \subseteq J \triangleleft R \quad \Rightarrow \quad I = J,$$

falls also kein Ideal von R existiert, das echt zwischen I und R liegt.

<u>Lemma 23:</u> Sei $I \triangleleft R$. Dann:

$$I \triangleleft R \text{ maximal} \iff \underbrace{R/I}_{=\{r+I \,:\, r \in R\}} \text{ Körper}$$

Faktorring, bestehend aus Restklassen

<u>Beispiel 24</u>

$$p \in \mathbb{Z}_{\geq 2} \text{ prim} \Rightarrow p\mathbb{Z} \triangleleft \mathbb{Z} \text{ maximal}$$

$$\iff \underbrace{\mathbb{Z}/p\mathbb{Z}}_{=:\, \mathbb{F}_p} \text{ Körper}$$

<u>Bsp</u> $\mathbb{F}_3 = \{0, 1, 2\}$
$= \{0, 1, -1\}$

Chinesischer Restsatz:

R: Ring

$I_1, \dots, I_k \trianglelefteq R$ mit $I_i + I_j = R$
für $i, j \in [1, k]$ mit $i \neq j$

Dann haben wir den surjektiven Ringmorphismus

$$R \xrightarrow{\varphi} R/I_1 \times R/I_2 \times \dots \times R/I_k$$
$$r \longmapsto (r + I_1, \; r + I_2, \; \dots, \; r + I_k)$$

Es ist $\operatorname{Kern}(\varphi) = I_1 \cap I_2 \cap \dots \cap I_k =: I$

Also liefert der Homomorphiesatz den Ringisomorphismus

$$R/I \xrightarrow[\sim]{\bar{\varphi}} R/I_1 \times R/I_2 \times \dots \times R/I_k$$
$$r + I \longmapsto (r + I_1, \; r + I_2, \; \dots, \; r + I_k)$$

Bsp. $2\mathbb{Z} \cap 5\mathbb{Z} = 10\mathbb{Z}$, $2\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$

$3 \cdot 2 + (-1) \cdot 5 = 1$ gibt $\supseteq$

$$\rightarrow \quad \mathbb{Z}/10\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$z + 10\mathbb{Z} \longmapsto (z + 2\mathbb{Z}, \; z + 5\mathbb{Z})$$

R : kommutativer Ring

$x_1, \dots, x_k \in R$

Wir schreiben

$$(x_1, x_2, \dots, x_k)$$

$$:= \Big\{ \sum_{i \in [1,k]} r_i x_i \;:\; r_i \in R \text{ für } i \in [1,k] \Big\}$$

$$\trianglelefteq R$$

für das von $x_1, \dots, x_k$ in R

erzeugte Ideal.

Bsp

- $(7) = 7\mathbb{Z} \trianglelefteq \mathbb{Z}$,

  $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}/(7)$

  Hauptideal, da von einem Element erzeugt

- $(4,6) = (2)$ in $\mathbb{Z}$:

  $\subseteq$: $4 \in (2)$ und $6 \in (2)$

  $\supseteq$: $2 = (-1)\cdot 4 + 1 \cdot 6 \in (4,6)$

R heißt noethersch, falls

jedes Ideal in R von der Form

$(x_1, \dots, x_k)$ ist, für gewisse $k \geq 0$, $x_1, \dots, x_k \in R$.

R: Integritätsbereich

$d: R^\times \longrightarrow \mathbb{Z}_{\geq 0}$ **Gradfunktion**, falls:

für $x \in R$, $y \in R^\times$ gibt es $q, r \in R$ mit

$$x = yq + r$$ "Teilen durch y mit Rest r"

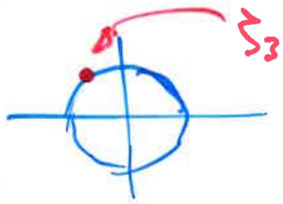
und ($r = 0$ oder $d(r) < d(y)$)

R, zusammen mit Gradfunktion d, heißt **euklidischer Ring**.

Bsp

- $\mathbb{Z}$ ist euklidisch mit $d(z) = |z|$
- Für jeden Körper Q ist $Q[X]$ euklidisch, mit $d(f(x)) = \deg(f(x))$
- $\mathbb{Z}[i]$ ist euklidisch, mit $d(z) = |z|^2$
- Ü: $\mathbb{Z}[\zeta_3]$ ist euklidisch, mit $d(z) = |z|^2$

$$\begin{cases} \zeta_3 = \exp\left(\frac{2\pi i}{3}\right) \\ \quad = -\frac{1}{2} + \frac{i}{2}\sqrt{3} \\ \zeta_3^2 + \zeta_3 + 1 = 0 \end{cases}$$



R : Integritätsbereich

$a \in R^{\times} \setminus U(R)$

Es heißt a irreduzibel, falls stets

$$(a) = (x \cdot y) \implies (a) = (x) \;\vee\; (a) = (y)$$

Es heißt a prim, falls stets

$$\underbrace{(a) \supseteq (x \cdot y)}_{a \text{ teilt } x \cdot y} \implies \underbrace{(a) \supseteq (x)}_{a \text{ teilt } x} \;\vee\; \underbrace{(a) \supseteq (y)}_{a \text{ teilt } y}$$

Elementar:

- a irreduzibel, falls alle Teiler von a von der Form u oder $a \cdot u$ sind, mit $u \in U(R)$.

- a prim, falls stets:

$$a \text{ teilt } x \cdot y \implies a \text{ teilt } x \;\vee\; a \text{ teilt } y$$

Bsp

- In $\mathbb{Z}$ gilt:

$$a \text{ prim} \iff a \text{ irreduzibel}$$

- In $\mathbb{Z}[i\sqrt{5}]$ gilt

$$a \text{ prim} \implies a \text{ irreduzibel}$$

$\not\Longleftarrow$ ← $2 \in \mathbb{Z}[i\sqrt{5}]$ irreduzibel, aber nicht prim

R : faktorieller Integritätsbereich

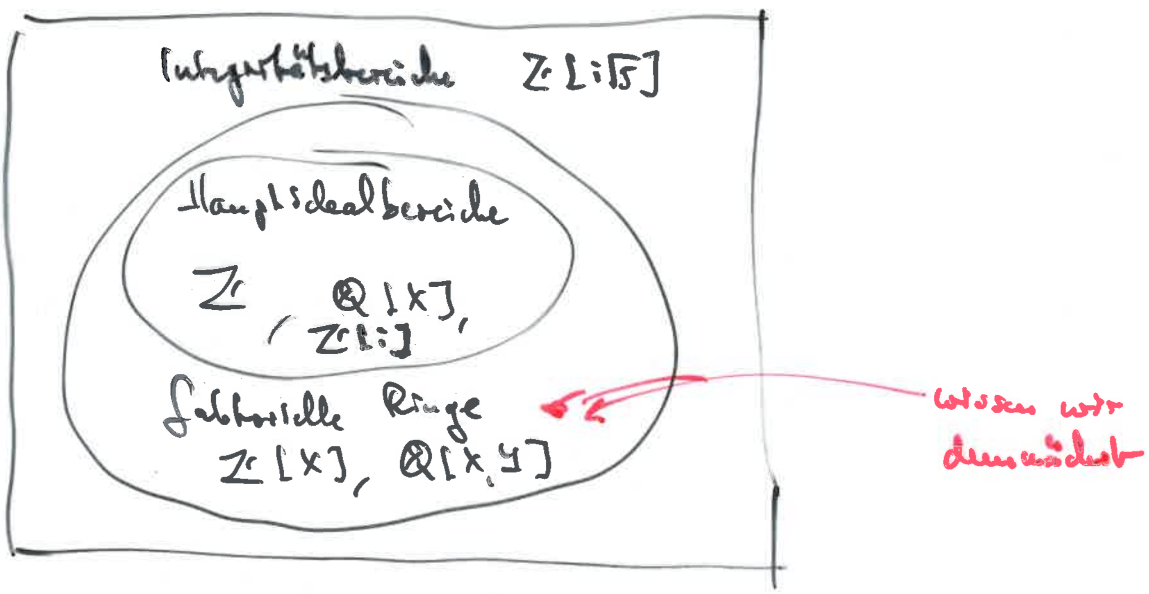
$\Leftrightarrow$ R noethersch und (irreduzibel $\Leftrightarrow$ prim)

$P \subseteq R$: bestehe aus Primelementen derart, dass jedes Primelement von R zu genau einem Element von P assoziiert ist

$$\mathrm{ggT}(x_1, \ldots, x_k) = \prod_{p \in P} p^{\overbrace{\min\{ v_p(x_i) \,:\, i \in [1,k] \}}^{\text{Bewertung von } x_i \text{ bei } p}}$$

Falls R Hauptidealbereich (insbes. faktoriell):

$$\underbrace{(\mathrm{ggT}(x_1, \ldots, x_k))}_{\text{Idealerzeugnis}} = \underbrace{(x_1, \ldots, x_k)}_{\text{Idealerzeugnis}} \trianglelefteq R$$



Satz (Gauß)

R : Integritätsbereich

R faktoriell $\Longrightarrow$ $R[X]$ faktoriell

Korollar Q Körper, $k \geq 1$

Es ist $Q[X_1, \dots, X_k]$ faktoriell.

Bsp • In $\mathbb{Q}[X, Y]$ haben wir eine (bis auf Einheiten und Reihenfolge) eindeutige Primfaktorzerlegung

• Sei $p(X,Y) \in \mathbb{Q}[X,Y]$ irreduzibel,

also z.B. $p(X,Y) = X^2 - Y$.

Sei $p(X,Y)$ ein Teiler von $g(X,Y)\,h(X,Y)$.

Da $p(X,Y)$ prim ist, teilt $p(X,Y)$ neun $g(X,Y)$ oder $h(X,Y)$

• Vorsicht, $\mathbb{Q}[X,Y]$ ist kein Hauptidealbereich

z.B.: $(X,Y) \subsetneq (\mathrm{ggT}(X,Y)) = (1)$

[bildbar in $\mathbb{Q}[X,Y]$

Symmetrische Gruppe:

$$S_n = \{ [1,n] \xrightarrow{f} [1,n] : f \text{ ist bijektiv} \}$$

"nach"

Multiplikation := Komposition $(\circ)$

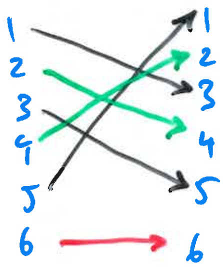
Zykeldarstellung

$$(k_{1,1}, k_{1,2}, \dots, k_{1,\ell_1})(k_{2,1}, k_{2,2}, \dots, k_{2,\ell_2}) \dots (k_{m,1}, k_{m,2}, \dots, k_{m,\ell_m})$$

Zykel der Länge 1 dürfen weggelassen werden.

Bsp

$$S_6 \ni \underbrace{(1,3,5)}\underbrace{(2,4)} = \underbrace{(1,3,5)}\underbrace{(2,4)}\underbrace{(6)} =: f$$



Bsp in S_6:

$$(1,3,5)(2,4) \circ (1,4,2,3)$$

$$= (1,2,5)(3)(4)(6) = (1,2,5)$$

G: Gruppe

$U \subseteq G$ heißt **Untergruppe**, falls:

- $1_G \in U$
- für $x, y \in U$ ist $xy^{-1} \in U$

Geschrieben: $U \leq G$.

Sei G endlich. Seien $x_1, \dots, x_n \in G$.

Dann heißt

falls G nicht endlich, müssen auch Exponenten ± 1 zugelassen werden

$$\langle x_1, \dots, x_n \rangle := \{ x_{k_1} \cdot x_{k_2} \cdot \dots \cdot x_{k_m} : m \geq 0,\ k_i \in [1, n] \text{ für } i \in [1, m] \} \leq G$$

das **Untergruppenerzeugnis** von $x_1, \dots, x_n$.

Ist $\{x_1, \dots, x_n\} \subseteq V \leq G$, dann ist

$$\langle x_1, \dots, x_n \rangle \leq V \leq G.$$

Es ist $\langle x_1, \dots, x_n \rangle$ die "kleinste Untergruppe von G, die $x_1, \dots, x_n$ enthält"

Für $x \in G$ heißt $|\langle x \rangle|$ die **Ordnung** von x.

Ist $G = \langle x \rangle$ für ein $x \in G$, dann heißt G **zyklisch**.

G : Gruppe

$U \leq G$

$G/U = \{ gU : g \in G \}$: Menge der Linksnebenklassen

$U \backslash G = \{ Ug : g \in G \}$: Menge der Rechtsnebenklassen

---

$N \leq G$ heißt Normalteiler, falls $gN = Ng$ für $g \in G$.

Äquivalent : • $gNg^{-1} = N$ für $g \in G$
• $g^{-1}Ng = N$ für $g \in G$

Geschrieben : $N \trianglelefteq G$

$N \trianglelefteq G \Rightarrow$ Faktorgruppe G/N, mit

$$gN \cdot hN := (g \cdot h)N$$

für $g, h \in G$.

G endlich, $U \leq G$

$\Rightarrow |G| = |G/U| \cdot |U| = |U \backslash G| \cdot |U|$

Insbesondere ist $|U|$ ein Teiler von $|G|$

Es heißt $[G:U] := |G/U| = |U \backslash G|$ der Index von U in G.

G, H : Gruppen

$\varphi : G \to H$ heißt **Gruppenmorphismus**,

falls $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ für $x, y \in G$.

Haben: $\operatorname{Kern}(\varphi) := \{ g \in G : \varphi(g) = 1 \} \trianglelefteq G$

$\operatorname{Kern}(\varphi) = 1 \iff \varphi$ injektiv

Bem. 112 G : Grp.

$x \in G$

Die **Konjugation** mit x, also

$$\varphi : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & \underbrace{{}^{x}g}_{\text{"g links hoch x"}} := x \cdot g \cdot x^{-1} \end{array},$$

ist ein **Gruppenautomorphismus** auf G,

d.h. ein bijektiver Gruppenmorphismus

von G nach G.

G, H : Gruppen

$\varphi : G \to H$ Gruppenhomomorphismus : $\varphi(g \cdot \tilde{g}) = \varphi(g) \cdot \varphi(\tilde{g})$ stets

Normalteiler

$\mathrm{Kern}(\varphi) = \{ g \in G : \varphi(g) = 1 \} \trianglelefteq G$

φ injektiv $\Longleftrightarrow$ $\mathrm{Kern}(\varphi) = 1$

Situation:

$$\begin{tikzcd}
\mathrm{Kern}(\varphi) \arrow[dr, hook] & & & \\
& G \arrow[rrr, "\varphi"] \arrow[dr, "\rho"'] & & & H \\
& & G/\mathrm{Kern}(\varphi) \arrow[r, "\bar{\varphi}", "\sim"'] & \varphi(G) \arrow[ur, hook] &
\end{tikzcd}$$

Homomorphismus

$$g \cdot \mathrm{Kern}(\varphi) \longmapsto \bar{\varphi}(g \cdot \mathrm{Kern}(\varphi)) := \varphi(g)$$

X : Menge

$S_X = \{ X \xrightarrow{f} X : f$ bijektive Abbildung $\}$

symmetrische Gruppe auf X,

Multiplikation auf S_X ist Komposition $(\circ)$

$\boxed{f \circ g : \text{"}f \text{ nach } g\text{"}}$

G: Gruppe

X: Menge

- Es heißt X, zusammen mit einem **Operationsmorphismus** $\varphi : G \longrightarrow \underbrace{S_X}_{\text{symm. Gr. auf } X}$, eine **$G$-Menge**.

- Sei $g \cdot x := (\varphi(g))(x)$ für $g \in G$, $x \in X$.

  Dann:

  (1) $1 \cdot x = x$ für $x \in X$

  (2) $g \cdot (\tilde{g} \cdot x) = (g \cdot \tilde{g}) \cdot x$ für $g, \tilde{g} \in G$, $x \in X$.

  $\uparrow$ Multiplikation in G

- Sei umgekehrt $(\cdot) : G \times X \longrightarrow X : (g, x) \longmapsto g \cdot x$ derart gegeben, daß (1, 2) gelten. Dann ist

$$\varphi : G \longrightarrow S_X : g \longmapsto \left(\begin{array}{l} \varphi(g) : X \to X \\ \qquad x \mapsto g \cdot x \end{array} \right)$$

  ein Operationsmorphismus, der auf X die Struktur einer G-Menge definiert.

Bsp 127.(5): Sei $n \geqslant 1$. Es ist $[1, n]$ eine S_n-Menge, wobei

$$f \cdot k := f(k) \quad \text{für } f \in S_n,\ k \in [1, n]$$

(Multiplikation durch Anwendung)

G: Gruppe

X, Y : G-Mengen

X ist G-Menge: haben $g \cdot x$, mit üblichen Regeln

$x \in X$

$$\mathrm{Stab}_G(x) := \{ g \in G : g \cdot x = x \} \leq G$$

ist der Stabilisator von x in G

Bsp: $\{1, 2, 3\}$ ist S_3-Menge mittels $f \cdot k := f(k)$

Dann ist

$$\mathrm{Stab}_{S_3}(2) = \{ \mathrm{id}, (1,3) \} = \langle (1,3) \rangle \leq S_3$$

G : endliche Gruppe

p : Primzahl

$|G| = \underbrace{p^a}_{\text{p-Anteil von } |G|} \cdot m$ mit $m \not\equiv_p 0$

$P \leq G$ heißt p-Sylow(unter)gruppe, falls $|P| = p^a$

$$\begin{aligned} \mathrm{Syl}_p(G) &:= \{ P : P \leq G \text{ ist p-Sylowgruppe} \} \\ &= \{ P : P \leq G \text{ und } |P| = p^a \} \\ &= \mathfrak{U}_{p^a}(G) \end{aligned}$$

<u>Bem. 147</u> $H, K \leq G$, $\underbrace{H \leq \overbrace{N_G(K)}^{\text{Normalisator}}}_{\text{d.h. } {}^hK = K \text{ für } h \in H}$

Dann:

(1) $HK = \{ hk : h \in H, k \in K \} \leq G$

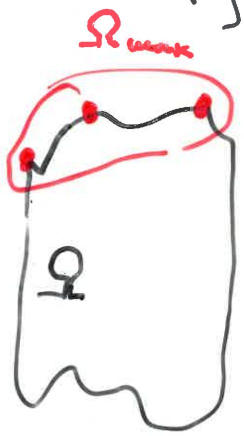
(2) $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$

G : endl. Grp.

p : Primzahl

$|G| = p^a \cdot m$ mit $m \not\equiv_p 0$

$$\Omega := \bigsqcup_{b \in [0,a]} \mathcal{U}_{p^b}(G) = \{ U \leq G : |U| \text{ ist Potenz von } p \}$$



$\Omega_{max} \subseteq \Omega$: Teilmenge der bzgl. Inklusion maximalen Elemente von Ω

$\mathrm{Syl}_p(G) := \mathcal{U}_{p^a}(G)$: Menge der p-Sylowgruppen von G

(Redundanzen)

<u>Satz 159</u> (Sylow)

(1) $\mathrm{Syl}_p(G) \neq \emptyset$

(2) $\mathrm{Syl}_p(G)$ ist eine transitive G-Menge unter der Konjugationsoperation

(3) Es ist $|\mathrm{Syl}_p(G)| \equiv_p 1$.

Für $P \in \mathrm{Syl}_p(G)$ ist $|\mathrm{Syl}_p(G)| = \dfrac{|G|}{|N_G(P)|}$.

Insbesondere ist $|\mathrm{Syl}_p(G)|$ ein Teiler von m.

(4) Sei $U \leq G$ eine p-Untergruppe. Dann gibt es ein $P \in \mathrm{Syl}_p(G)$ mit $U \leq P$.

<u>Beweis</u>: Noch zz.

$$\mathrm{Syl}_p(G) \overset{!}{=} \Omega_{max} .$$

Dabei $\subseteq$ bekannt, zz. ist $\overset{!}{\supseteq}$.

Bem. 158 $\quad G$ endl. Grp.

$$M \trianglelefteq G, \quad N \trianglelefteq G, \quad M \cap N = 1, \quad |M| \cdot |N| = |G|$$

$$\Longrightarrow \quad M \times N \xrightarrow{\sim} G \; : (m, n) \longmapsto m \cdot n$$

Def 159 $\quad n \geq 3$

$$a := (1, 2, \ldots, n)$$

$$b := \begin{cases} (2, 2k)(3, 2k-1) \ldots (k, k+2) & \text{falls } n = 2k \\ (2, 2k+1)(3, 2k) \ldots (k+1, k+2) & \text{falls } n = 2k+1 \end{cases}$$

$$D_{2n} := \langle a, b \rangle \leq S_n$$

Diedergruppe

$$D_{2n} = \{ \underbrace{a^i \circ b^j}_{\text{paarw. verschieden}} : i \in [0, n-1], \; j \in [0, 1] \}$$

$$^{b}a = a^{-1}$$

$$\Longrightarrow \quad a^i \circ b^j \circ a^{i'} \circ b^{j'}$$

$$= a^{i + (-1)^j \cdot i'} \circ b^{j + j'}$$

Bem 162 $\quad p \geq 3$ prim

G Grp. mit $|G| = 2p$

$$\Longrightarrow \quad G \simeq C_p \times C_2 \quad \text{oder} \quad G \simeq D_{2p}$$

Bew. Wählen $N \in \mathrm{Syl}_p(G)$, $U \in \mathrm{Syl}_2(G)$. Dann $N \trianglelefteq G$.

Fall $U \trianglelefteq G \Rightarrow G \simeq C_p \times C_2$

Fall $U \leq G$, aber $U \ntrianglelefteq G$: zu tun!

Elementarteilersatz

R : euklidischer Ring mit Gradfkt. d

↑ z.B. $R = \mathbb{Z}$, $d(z) = |z|$

$A \in R^{m \times n}$

Dann gibt es $S \in GL_m(R)$, $T \in GL_n(R)$ mit

$$SAT = D = \sum_{i \in [1,k]} x_i e_{i,i},$$

x_i : Elementarteiler

wobei $k \in [0, \min\{m,n\}]$

$$\underbrace{\text{und } x_i \in R^{\times} \text{ mit } x_1 \mid x_2 \mid \ldots \mid x_k}_{D \text{ in Elementarteilerform}}$$

$$\underbrace{S}_{\in GL_m(R)} \; A \; \underbrace{T}_{\in GL_n(R)} = \underbrace{\begin{pmatrix} x_1 & & & \\ & \ddots & & \\ & & x_k & \end{pmatrix}}_{D}$$

A : abelsche Gruppe

A heißt endlich erzeugt, falls $A = {}_{\mathbb{Z}}\underbrace{\langle a_1, \ldots, a_k \rangle}_{\exists}$

Bem. 168:

$$\underbrace{B}_{\text{e.e.}} \hookrightarrow A \longrightarrow \underbrace{A/B}_{\text{e.e.}}$$

e.e. $\Longrightarrow$ e.e. $\Longleftarrow$ e.e.

G : Gruppe

$U \leq G$

G-Menge G/U : $x \cdot gU = (xg)U$

$\Rightarrow$ dann auch U-Menge G/U,

durch Einschränkung

Sei $X \subseteq G/U$ eine Bahn unter U.

Dann: $|X|$ teilt $|U|$; cf Kor. 141.

L : Körper

$K \subseteq L$: Teilkörper

$\Big\}$ $L|K$ Körpererweiterung

$L \mid Z \mid K$

Z Zwischenkörper von $L|K$

Bsp: $\mathbb{C} \mid \mathbb{R} \mid \mathbb{Q}$

$L|K \Rightarrow [L:K] := \dim_K L$: Grad von $L|K$

Bsp: $[\mathbb{C}:\mathbb{R}] = 2$

$L|K$, $b \in L$

$$\Rightarrow \quad K[b] := \{ f(b) : f(X) \in K[X] \}$$

$$K(b) := \left\{ \frac{f(b)}{g(b)} : f(X), g(X) \in K[X], g(b) \neq 0 \right\}$$

b heißt algebraisch über K, falls $u(b) = 0$ für ein $u(X) \in K[X]^\times$.

b alg $/K \Rightarrow K[b] = K(b)$

b alg $/K \Longleftrightarrow [K[b]:K]$ endlich

b alg $/K$, $u(b) = 0$ mit $\deg(u(X)) =: n$

$$\Rightarrow K[b] = K(b) = {}_K\langle b^0, b^1, \dots, b^{n-1} \rangle$$

Bsp: i alg $/\mathbb{Q}$, da $i^2+1 = 0$, d.h. $u(i) = 0$ mit $u(X) = X^2+1$

$$\Rightarrow \mathbb{Q}(i) = {}_{\mathbb{Q}}\langle i^0, i^1 \rangle = \{ a+bi : a, b \in \mathbb{Q} \}$$

Lemma 194 $L|K$: Körpererweiterung

$b \in L$: alg. über K

Es gibt ein eindeutig bestimmtes normiertes Polynom $\mu_{b,K}(X) \in K[X]$ mit $\mu_{b,K}(b) = 0$, welches jedes $f(X) \in K[X]$ mit $f(b) = 0$ teilt.

Es heißt $\mu_{b,K}(X)$ das Minimalpolynom von b über K.

Es ist $\mu_{b,K}(X) \in K[X]$ irreduzibel.

Ist $n := \deg \mu_{b,K}(X)$, dann ist

$$(b^0, b^1, \ldots, b^{n-1})$$

eine K-lineare Basis von $K(b) = K[b]$.

Insbesondere : $[K(b) : K] = n = \deg \mu_{b,K}(X)$.

Konstruktion:

K : Körper

$m(X) \in K[X]$: $\underbrace{\text{irreduzibel}}_{\Downarrow}$ und normiert

$$L := K[X] / \underbrace{(m(X))}_{\text{max. Ideal}}$$

$\Rightarrow$ $L \mid K$ Körpererweiterung

$$b := X + (m(X)) \in L$$

$$\mu_{b,K}(X) = m(X) \in K[X]$$

Bsp $K = \mathbb{F}_2$

$$m(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$$

$$\mathbb{F}_4 := \mathbb{F}_2[X] / (X^2+X+1) \quad , \quad \mathbb{F}_4 \mid \mathbb{F}_2$$

$$\alpha := X + (X^2+X+1)$$

$\Rightarrow$ $\boxed{2 = 0}$ und $\boxed{\alpha^2 = \alpha + 1}$

da $\mathbb{F}_4$ Vektorraum über $\mathbb{F}_2$

da $0 = \mu_{\alpha,\mathbb{F}_2}(\alpha) = \alpha^2 + \alpha + 1$

$$\mathbb{F}_4 = \{ a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_2 \}$$

$$= \{ 0, 1, \alpha, 1+\alpha \}$$

Seien $M \mid L \mid K$ endliche Körpererweiterungen,

d.h. seien $[M:L] = \dim_L M$ und $[L:K] = \dim_K L$

endlich.

Dann ist

$$[M:K] = [M:L] \cdot [L:K].$$

Genauer: Ist $(b_1, \dots, b_\ell)$ eine K-lineare Basis von L,

und ist $(c_1, \dots, c_m)$ eine L-lineare Basis von M,

dann ist $\left(b_i \cdot c_j \;:\; i \in [1,\ell],\ j \in [1,m] \right)$

eine K-lineare Basis von M.

Bsp $\underbrace{\mathbb{Q}(\sqrt[3]{2}, \zeta_3)}_{M} \mid \underbrace{\mathbb{Q}(\sqrt[3]{2})}_{L} \mid \underbrace{\mathbb{Q}}_{K}$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, da $\mu_{\sqrt[3]{2}, \mathbb{Q}}(X) = X^3 - 2$

$[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})] = 2$, da $\mu_{\zeta_3, \mathbb{Q}(\sqrt[3]{2})}(X) = X^2 + X + 1$

Also $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$

$= 2 \cdot 3$

$= 6$

K: Körper

$U(K) = K^\times$: Einheitengruppe

$G \leq U(K)$: endliche Untergruppe

Dann ist G zyklisch, d.h. $\exists\, x \in G$ mit $G = \langle x \rangle$.

Bsp

- $\mathbb{F}_{11}$ endlich $\Longrightarrow$ $U(\mathbb{F}_{11})$ endlich

  $\Longrightarrow$ $U(\mathbb{F}_{11})$ zyklisch

Tatsächlich:

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
1	2	4	-3	5	-1	-2	-4	3	-5	1

$U(\mathbb{F}_{11}) = \langle 2 \rangle$

- $U(\mathbb{F}_4)$ zykl. : in $\mathbb{F}_4$ ist $2 = 0$, $\alpha^2 = \alpha + 1$

α^0	α^1	α^2	α^3
1	α	$\alpha+1$	$\alpha^2+\alpha = 1$

$U(\mathbb{F}_4) = \langle \alpha \rangle$