- $S_n := \{\sigma: \{1,\dots,n\} \to \{1,\dots,n\} \mid \sigma \text{ ist bijektiv}\}$ ist mit der Abbildungskomposition $\sigma \cdot \tau := \sigma \circ \tau$ als Verknüpfung eine Gruppe und heißt **Symmetrische Gruppe**. Ein Element $\sigma \in S_n$ heißt auch eine **Permutation**.
- Die **Ordnung einer Gruppe** ist die Anzahl der Elemente der Gruppe. Es gilt z.B. $|S_n| = n!$.
- Schreibweise $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ und Zykelschreibweise z.B. $(1\ 4\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \in S_4$.
- Disjunkte Zykel kommutieren, aber es gilt z.B. $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$.
- Jedes $\sigma \in S_n$ kann als **Produkt disjunkter Zykel** $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ geschrieben werden, eindeutig bis auf
  - Reihenfolge der einzelnen Zykel, z.B. $(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$ und
  - Zyklische Vertauschung innerhalb der Zykel, z.B. $(1\ 2) = (2\ 1)$.

  Dabei werden Zykel der Länge 1 meistens weggelassen, wenn klar ist, zu welcher Symmetrischen Gruppe S_n die Permutation σ gehört.

  Wir können durch Umnummerierung annehmen, dass $k_1 \geq k_2 \geq \ldots \geq k_r \geq 2$ für die zugehörigen Zykellängen gilt und es heißt $(k_1, k_2, \dots, k_r)$ der **Zykeltyp** von σ.
- Die **Ordnung** $\operatorname{ord}(\sigma) = \min\{k \geq 1 \mid \sigma^k = \mathrm{id}\}$ eines Zykels σ ist seine Länge, die Ordnung eines Produkts disjunkter Zykel ist das kgV dessen Längen, so ist z.B.

$$\operatorname{ord}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 4 & 7 & 6 \end{pmatrix} = \operatorname{ord}((1\ 2\ 3)(4\ 5)(6\ 7)) = \operatorname{kgV}(3,2,2) = 6.$$

  Aufgabe (H15T2A2). Es gibt genau $2688 = 2 \cdot 1344$ Elemente σ der Ordnung 15 in S_8, was man wie folgt sieht: Ist $(k_1, k_2, \dots, k_r)$ der Zykeltyp von σ, so gilt $k_1 + \ldots + k_r \leq 8$ und $15 = \operatorname{ord}(\sigma) = \operatorname{kgV}(k_1, \dots, k_r)$ und also ist der Zykeltyp $(5,3)$. Daher entsprechen die gesuchten Elemente σ genau den disjunkten Produkten eines 3- und eines 5-Zykels. Es gibt genau $\binom{8}{5}\frac{5!}{5} = 1344$ viele 5-Zykel in S_8 (Die 5 im Nenner kommt durch die Identifikation der zyklischen Permutationen wie z.B. $(1\ 2\ 3\ 4\ 5) = (2\ 3\ 4\ 5\ 1)$). Ist ein solcher 5-Zykel gewählt, liegten die Zahlen für einen 3-Zykel schon fest und es gibt genau $\frac{3!}{3} = 2$ viele 3-Zykel der gesuchten Form.
- Die Zykeltypen von σ und σ^{-1} sind gleich, da das Inverse eines Zykels wieder ein Zykel gleichen Typs ist, nämlich der mit „umgekehrter Reihenfolge“ der Zahlen.
- Für $\sigma, \tau \in S_n$ gilt $\left(\begin{array}{c}\sigma \text{ und } \tau \text{ sind } \textbf{konjugiert} \\ \text{d.h. } \exists g \in S_n : \sigma = g\tau g^{-1}\end{array}\right) \iff \left(\begin{array}{c}\sigma \text{ und } \tau \text{ haben den} \\ \text{gleichen Zykeltyp}\end{array}\right)$

  und so sind z.B. $(1\ 2\ 3)(4\ 5)(6\ 7)$ und $(7\ 2\ 1)(3\ 4)(5\ 6)$ in S_{100} konjugiert.
- Das **Signum** ist ein (für $n \geq 2$ surjektiver) Gruppenhomomorphismus

$$\begin{array}{rcll} \operatorname{sign}: S_n & \to & (\{\pm 1\}, \cdot) & \cong (\mathbb{Z}/2, +) \\ \sigma & \mapsto & \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j} & \end{array}$$

  und es gilt $\operatorname{sign}(\text{Zykel der Länge } k) = (-1)^{k-1}$. (Man kann alternativ das Signum einer Permutation auch als $(-1)^{(\text{Anzahl von Transpositionen (d.h. 2-Zykeln) in die } \sigma \text{ zerlegt werden kann})}$ schreiben. Obwohl diese Anzahl nicht eindeutig ist, ist überraschenderweise schon eindeutig, ob sie gerade oder ungerade ist.) Praktisch berechnet man das Signum einer Premutation durch die disjunkte Zykelzerlegung

$$\operatorname{sign}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} = \operatorname{sign}((1\ 3\ 4)(2\ 6)) = \operatorname{sign}(1\ 3\ 4) \cdot \operatorname{sign}(2\ 6) = (-1)^2 \cdot (-1)^1 = -1.$$

- Die **Alternierende Gruppe** $A_n := \ker(\operatorname{sign}) \subseteq S_n$ enthält also beispielsweise 3-Zykel, aber keine 2-Zykel.

- Durchschnitte, Bilder und Urbilder von Untergruppen unter Gruppenhomomorphismen sind wieder Untergruppen.
- Es gilt in jeder Gruppe $\operatorname{ord}(a^k) = \frac{\operatorname{ord}(a)}{\operatorname{ggT}(\operatorname{ord}(a),k)}$ und in einer abelschen Gruppe gilt $\operatorname{ord}(ab) | \operatorname{kgV}(\operatorname{ord}(a),\operatorname{ord}(b))$.

Beispiel 1. Es gilt $\operatorname{ord}(12) = \operatorname{ord}(13) = 2$ und $\operatorname{ord}((12)(13)) = \operatorname{ord}(132) = 3$ und in der nicht-abelschen Gruppe S_3.

- Für eine Teilmenge $X \subseteq G$ heißt

$$\langle X \rangle := \bigcap_{\substack{X \subseteq U \subseteq G \\ U \text{ Untergruppe}}} U = \{x_1 \cdot \ldots \cdot x_n \in G \mid x_1, \ldots, x_n \in X \cup X^{-1}\}$$

die **von X erzeugte Untergruppe** und es gilt offenbar $X \subseteq \langle X \rangle \subseteq G$. Ist X konkret gegeben, so werden die Mengenklammern bei dieser Schreibweise oft weggelassen.

- Eine Gruppe G heißt **zyklisch**, wenn sie von einem ihrer Elemente erzeugt wird, also wenn $G = \langle g \rangle$ gilt. Dieses ist also genau dann der Fall wenn jedes Element $a \in G$ als $a = g^k$ für ein $k \in \mathbb{Z}$ geschrieben werden kann. Es ist eine endliche Gruppe G zyklisch genau dann, wenn es ein Element gibt mit $\operatorname{ord}(g) = |G|$.

Beispiel 2. Es gilt $(2\mathbb{Z}, +) = \langle 2 \rangle \subseteq (\mathbb{Z}, +) = \langle 1 \rangle$. (Diese beiden zyklischen Gruppen sind isomorph, allerdings nicht durch die Inklusion.)

- Jede endliche zyklische Gruppe ist zu $(\mathbb{Z}/n, +)$ und jede unendliche zyklische Gruppe zu $(\mathbb{Z}, +)$ isomorph. Ein Isomorphismus ist durch $g^k \mapsto k$ gegeben. Insbesondere sind alle zyklischen Gruppen offenbar abelsch.
- Die **Struktur einer zyklischen Gruppe** $G = \langle g \rangle$ ist einfach: Es gibt zu jedem Teiler $d | n$ der Gruppenordnung n genau eine Untergruppe U der Ordnung d, nämlich $U = \langle g^{\frac{n}{d}} \rangle$.
- Für eine Untergruppe $U \subseteq G$ und $a \in G$ heißt die Menge $aU := \{au \in G \mid u \in U\}$ eine **Linksnebenklasse** von U. Sei G/U die Menge der Linksnebenklassen von U in G. Die Linksnebenklassen von U sind die Äquivalenzklassen bezüglich der Relation $a \sim b \Leftrightarrow a^{-1}b \in U$ und bilden daher eine Partition von G. Weil die Linksnebenklassen von U alle gleichmächtig sind, also $|aU| = |U|$ gilt, folgt der **Satz von Lagrange**

$$|G| = [G : U] \cdot |U|,$$

wobei $[G : U] = |G/U|$ die Anzahl der Linksnebenklassen von U bezeichnet, die auch der **Index** von U in G heißt. Insbesondere teilt die Ordnung einer Untergruppe also die Gruppenordnung.

Bemerkung 3. Die „Umkehrung“ zum Satz von Lagrange ist im Allgemeinen falsch: Es gibt nicht unbedingt zu jedem Teiler d der Gruppenordnung eine Untergruppe U mit dieser Ordnung. (So hat beispielsweise A_5 keine Untergruppe der Ordnung $(5!/2)/2 = 30$, da diese vom Index 2 und daher ein Normalteiler wäre, A_5 aber eine einfache Gruppe ist (s.u.).) Für abelsche Gruppen ist sie richtig, wie wir unten mit dem Klassifikationssatz sehen werden.

- Eine Untergruppe $N \subseteq G$ heißt **Normalteiler**, falls $aN = Na$ gilt für alle $a \in G$. In diesem Fall definiert $aN \cdot bN := abN$ eine Gruppenstruktur auf der Menge der Linksnebenklassen G/N und es ist

$$\begin{array}{rccc} \pi\colon & G & \twoheadrightarrow & G/N \\ & a & \mapsto & aN \end{array}$$

ein surjektiver Gruppenhomomorphismus mit Kern N. Dieser induziert eine Bijektion

$$\left\{ \begin{array}{c} \text{Untergruppen } U \subseteq G \\ \text{mit } N \subseteq U \end{array} \right\} \underset{\pi^{-1}(\tilde{U}) \hookleftarrow \tilde{U}}{\overset{U \mapsto U/N}{\rightleftarrows}} \left\{ \begin{array}{c} \text{Untergruppen } \tilde{U} \\ \text{von } G/N \end{array} \right\}$$

die auf normale Untergruppen einschränkt, wobei für diese der **Isomorphiesatz** $G/U \cong (G/N)/(U/N)$ gilt.

- Normalteiler $N \subseteq G$ sind genau die Kerne von Gruppenhomomorphismen $\varphi\colon G \to H$ und es gilt der **Homomorphiesatz** $G/\ker(\varphi) \cong \varphi(G)$.

- Jede Untergruppe einer abelschen Gruppe ist offenbar ein Normalteiler.
- Untergruppen und Quotienten abelscher Gruppen sind offenbar wieder abelsch.
- Eine Untergruppe $U \subseteq G$ vom **Index** 2 **ist ein Normalteiler** denn in diesem Fall gibt es nur die Linksnebenklassen U, aU und gäbe es mindestens drei Rechtsnebenklassen U, Ua, Ub mit $a, b \notin U$, so ist $aU = bU$, also $b^{-1}a \in U$, also $ba^{-1} \in U$ und daher $b \in Ua$, also $Ua = Ub$, und folglich $aU = Ua$ da sowohl U, aU als auch U, Ua die Menge G partitionieren.

- Sind G_α Gruppen, so ist die Menge $\prod_\alpha G_\alpha$ mit komponentenweiser Gruppenoperation eine Gruppe und heißt das (äußere) **direkte Produkt**. Die Projektionen $\prod_\alpha G_\alpha \twoheadrightarrow G_\alpha$ sind jeweils surjektive Gruppenhomomorphismen.
- Es ist $\prod G_\alpha$ eine abelsche Gruppe genau dann, wenn alle G_α abelsche Gruppen sind. Ist das Produkt endlich indiziert, so schreibt man in diesem Fall auch $\bigoplus_{i=1}^n G_i := \prod_{i=1}^n G_i$.
- In einem direkten Produkt $N \times H$ gilt offenbar immer $\operatorname{ord}((n,h)) = \operatorname{kgV}(\operatorname{ord}(n), \operatorname{ord}(h))$.
- Sind $U, V \subseteq G$ Untergruppen, so ist die Menge $UV := \{uv \in G \mid u \in U \text{ und } v \in V\}$ mit der eingeschränkten Multiplikation von G nicht unbedingt eine Untergruppe. Dieses ist aber der Fall, wenn $UV = VU$ gilt, also beispielsweise dann, wenn einer der beiden Untergruppen ein Normalteiler ist. (Sind U und V beide Normalteiler, so ist auch UV ein Normalteiler.)

  Beispiel 4. Es sind $U := \langle (1\,2) \rangle$ und $V := \langle (2\,3) \rangle$ Untergruppen von S_3, aber

  $$UV = \left\{ \mathrm{id},\ (1\,2),\ (2\,3),\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

  ist nach Lagrange keine Untergruppe von S_3. Daher ist weder U noch V ein Normalteiler von S_3.
- Sind N und H Normalteiler mit $N \cap H = \{e\}$ so ist kommutieren Elemente von N und H miteinander (das bedeutet nicht, dass N und H abelsche Gruppen sind), denn $n(hn^{-1}h^{-1}) \in N$ und $(nhn^{-1})h^{-1} \in H$, also $nh = hn$. Daher ist in diesem Fall die Abbildung

  $$\begin{array}{ccc} N \times H & \hookrightarrow & G \\ (n,h) & \mapsto & nh \end{array}$$

  ein injektiver Gruppenhomomorphismus dessen Bild die oben betrachtete Menge NH ist, die in diesem Fall auch (inneres) **direktes Produkt** genannt wird.

  Beispiel 5. Sind n und m teilerfremd, so ist $\mathbb{Z}/n \times \mathbb{Z}/m \cong \mathbb{Z}/nm = G$, was **Chinesischer Restsatz** genannt wird, und was wir später noch genauer betrachten werden. Die Untergruppen $N := \langle [m]_{nm} \rangle$ und $H := \langle [n]_{nm} \rangle$ sing beide zyklisch und von Ordnung n und Ordnung m, also gibt es Isomorphismen $\mathbb{Z}/n \cong N$ (durch $[a]_n \mapsto [am]_{nm}$) und $\mathbb{Z}/m \cong H$. Weil G abelsch ist, sind N und H Normalteiler und es gilt $N \cap H = \{0\}$ nach Lagrange. Der injektive Gruppenhomomorphismus $N \times H \hookrightarrow G$ ist nun auch surjektiv, da $nm = |N| \cdot |H| = |N \times H| \leq |G| = nm$.
- Eine Gruppe heißt endlich erzeugt, wenn sie von einer endlichen Menge erzeugt wird. Insbesondere sind natürlich alle endlichen Gruppen endlich erzeugt.
- Nach dem (beispielsweise mit dem Elementarteilersatz aus der linearen Algebra zu beweisende) **Hauptsatz für endlich erzeugte abelsche Gruppen** ist endlich erzeugte abelsche Gruppe G isomorph zu

  $$G \ \cong\ \mathbb{Z}^n \times \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_\ell^{k_\ell}$$

  wobei p_i (nicht unbedingt verschiedene) Primzahlen sind. Diese Darstellung ist bis auf Isomorphie und Permutation der Faktoren eindeutig.

  Beispiel 6. Es gibt (bis auf Isomorphie) genau zwei abelsche Gruppen der Ordnung $12 = 2^2 \cdot 3$, nämlich

  $$\begin{array}{lll} & \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 & (\cong \mathbb{Z}/2 \times \mathbb{Z}/6 \text{ nach dem Chinesischen Restsatz}) \\ \text{und} & \mathbb{Z}/4 \times \mathbb{Z}/3 & (\cong \mathbb{Z}/12 \text{ nach dem Chinesischen Restsatz}) \end{array}$$

  (es ist also übrigens überraschenderweise $\mathbb{Z}/4 \times \mathbb{Z}/3$ eine zyklische Gruppe).

- Eine **Operation** einer Gruppe G auf einer nichtleeren Menge X ist eine Abbildung $G \times X \to X$ mit Eigenschaften oder alternativ ein Gruppenhomomorphismus $G \to (\text{Bijektionen}(X), \circ)$.
- Für ein $x \in X$ heißt
  - die Menge $G \cdot x = \{ax \in X \mid a \in G\} \subseteq X$ die **Bahn von** x
  - und die Untergruppe $G_x = \{a \in G \mid ax = x\} \subseteq G$ der **Stabilisator von** x

  und es gilt die **Bahnenformel**
  $$|G| = |G \cdot x| \cdot |G_x|.$$

  Beispiel 7. Die Drehgruppe G des Würfels operiert auf seiner Eckenmenge X. Ist eine Ecke $x \in X$ fixiert, so ist deren Bahn $G \cdot x = X$, da jede andere Ecke durch eine Drehung erreicht werden kann. Es gilt also $|G \cdot x| = |X| = 8$. Für den Stabilisator der fixierten Ecke x gilt $|G_x| = 3$ und die Drehgruppe G hat also nach der Bahnenformel $|G| = 8 \cdot 3 = 24$ Elemente.
- Eine Operation heißt **transitiv**, wenn die (folglich einzige) Bahn alles ist, also ganz X.
- Die **Bahnen partitionieren** X, also $X = \bigsqcup_{x \in R \subseteq X} G \cdot x$ für ein Repräsentantensystem R, und damit $|X| = \sum_{x \in R} |G \cdot x|$ und es gilt die **Fixpunktformel**
  $$|X| = |\text{Fixpunkte}| + \sum_{\substack{x \in R \\ |G \cdot x| > 1}} |G \cdot x|,$$
  denn $x \in X$ ist Fixpunkt genau dann, wenn $G \cdot x = \{x\}$ genau dann, wenn $G_x = G$.

  Beispiel 8. Die Gruppe G operiert auf $X := G$ durch **Konjugation**, also $(a, x) \mapsto axa^{-1}$. Die Bahn $G \cdot x = \{axa^{-1} \in G \mid a \in G\}$ heißt **Konjugationsklasse von** x. Es ist x ein Fixpunkt genau dann, wenn x im **Zentrum**
  $$Z(G) = \{x \in G \mid ax = xa \text{ für alle } a \in G\}$$
  liegt, welches ein Normalteiler von G ist. Das Zentrum besteht also genau aus den Elementen, die mit allen Elementen der Gruppe kommutieren und insbesondere ist G genau dann abelsch, wenn $Z(G) = G$ gilt. Der Stabilisator $Z_x = \{a \in G \mid ax = xa\}$ von x heißt auch **Zentralisator von** x und aus der Fixpunktformel zusammen mit der Bahnenformel folgt die **Klassengleichung**
  $$|G| \quad = \quad |Z(G)| + \sum_{i=1}^{r} \underbrace{|G \cdot x_i|}_{>1} \quad = \quad |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : Z_{x_i}]}_{>1},$$
  wobei G endlich ist und $K_1, \ldots K_r$ die verschiedenen Konjugationsklassen mit mindestens zwei Elementen $x_i \in K_i$ sind.
- Für eine Primzahl p heißt eine Gruppe p**-Gruppe**, falls $|G| = p^{k \geq 1}$.
- Ist G eine endliche Gruppe, so heißt eine p-Untergruppe größter Ordnung eine p**-Sylowgruppe** von G.
- Eine Gruppe $G \neq \{e\}$ heißt **einfach**, wenn sie nur triviale Normalteiler (also nur G und $\{e\}$) hat.

  Beispiel 9.
  - Eine endliche abelsche Gruppe ist nach dem Struktursatz einfach genau dann, wenn sie Primzahlordnung hat (also zyklisch ist). Dieses sind tatsächlich genau alle abelschen einfachen Gruppen. Insbesondere gibt es keine unendliche abelsche einfache Gruppe.
  - Eine p-Gruppe hat ein **nicht-triviales Zentrum**, da p nach der Klassengleichung $|Z(G)|$ teilen muss und damit Insbesondere $|Z(G)| > 1$ gilt. Eine p-Gruppe ist also nicht-einfach ($Z(G) \neq G$) oder abelsch ($Z(G) = G$).
  - $A_{\geq 5}$ ist einfach. Hierfür zeigt man dass zwei beliebige 3-Zykel in $A_{\geq 5}$ konjugiert sind. Weil aber die $A_{\geq 3}$ von den 3-Zykeln erzeugt wird, genügt es zu zeigen, dass jeder Normalteiler $\neq \{e\}$ von $A_{\geq 5}$ einen 3-Zykel enthält.
- Ist $G/Z(G)$ **zyklisch, so ist** G **abelsch**, denn in diesem Fall lassen sich $a, b \in G$ als $a = g^n z$ und $b = g^m z'$ schreiben und es gilt
  $$ab = g^n z g^m z' = g^n g^m z z' = g^m g^n z' z = g^m z' g^n z = ba.$$

  Beispiel 10. Jede **Gruppe der Ordnung** p^2 **ist abelsch**, da sie als p-Gruppe nicht-triviales Zentrum hat, also $G/Z(G)$ Ordnung p hat oder $G = Z(G)$ gilt (was schon bedeutet, dass G abelsch ist). Also ist $G/Z(G)$ zyklisch und G damit abelsch. Nach dem Struktursatz sind also $\mathbb{Z}/p^2$ und $\mathbb{Z}/p \times \mathbb{Z}/p$ die einzigen Gruppen der Ordnung p^2.

- Für eine endliche Gruppe mit $|G| = p^{k\geq 1} \cdot m$ für eine Primzahl p mit $p \nmid m$ gilt nach den **Sylowsätzen**:

  (1) G hat Untergruppen $U_1 \subseteq U_2 \subseteq \ldots \subseteq U_k$ mit $|U_i| = p^i$ und insbesondere eine p-Sylowgruppe U_k.

  (2) Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

  (3) Alle p-Sylowgruppen von G sind konjugiert.

  (4) Ist n_p die Anzahl der p-Sylogruppen von G so gilt:

$$n_p | m \qquad \text{und} \qquad n_p \equiv 1 \mod p$$

Beispiel 11. Ist G eine abelsche Gruppe und $|G| = p^{k\geq 1} \cdot m$ für eine Primzahl p mit $p \nmid m$, so gibt es wegen Sylow-(1) und Sylow-(3) genau eine p-Sylowgruppe. Diese ist genau das direkte Produkt $\prod_i \mathbb{Z}/p^{k_i}$ der Faktoren aus dem Hauptsatz für endlich erzeugte abelsche Gruppen, in denen die Primzahl p vorkommt (Primärzerlegung). Äquivalent besteht diese genau aus den Elementen von G, deren Ordnung eine Potenz von p ist. Im abelschen Fall ist also G ein direktes Produkt ihrer p-Sylowgruppen für Teiler p der Gruppenordnung. Beispielsweise hat die **Kleinsche Vierergruppe** $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ genau eine 2-Sylowgruppe G der Ordnung 4 und diese ist nicht zyklisch.

Beispiel 12. Besitzt eine endliche Gruppe G **genau eine p-Sylowgruppe U, so ist diese ein Normalteiler**. Achtung: Dieses folgt *nicht* aus Sylow-(3) sondern so: Ist $a \in G$, so ist auch aUa^{-1} eine Untergruppe von G mit gleicher Ordnung wie U. War also U eine p-Sylowgruppe (also eine Untergruppe größter p-Ordnung), so ist auch aUa^{-1} eine solche. Weil es nach Voraussetzung aber nur eine davon gibt, gilt $U = aUa^{-1}$, also $Ua = aU$ und U ist ein Normalteiler. Ist umgekehrt eine p-Sylowgruppe U ein Normalteiler von G, so gibt es nur eine p-Sylowgruppe, da alle diese nach Sylow-(3) konjugiert sind. Also gilt:

$$\text{Eine } p\text{-Sylowgruppe von } G \text{ ist ein Normalteiler} \quad \Leftrightarrow \quad n_p = 1$$

- Ist G eine endliche Gruppe, deren Ordnung von einer Primzahl p geteilt wird, so gibt es in G nach Sylow-(1) ein Element der Ordnung p, was auch **Satz von Cauchy** genannt wird.

Aufgabe (H15T1A3). Jede Gruppe der Ordnung $143 = 11 \cdot 13$ ist zyklisch, denn: Für die Anzahl n_{11} der 11-Sylowgruppen gilt nach den Sylowsätzen $n_{11} \in \{1, 13\}$ und mit der anderen Bedingung $n_{11} = 1$. Es gibt also einen Normalteiler N der Ordnung 11. Ebenso gibt es einen Normalteiler H der Ordnung 13 in G. Da $N \cap H = \{e\}$ nach Lagrange und $|N| \cdot |H| = |G|$, ist $G \cong N \times H \cong \mathbb{Z}/11 \times \mathbb{Z}/13 \cong \mathbb{Z}/143$.

- Ist jede Sylowgruppe von G ein Normalteiler, so ist G das direkte Produkt seiner Sylowgruppen.

Aufgabe (F17T2A1). In einer einfachen Gruppe G der Ordnung $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$ gibt es genau 120 Elemente der Ordnung 11, denn: Für die Anzahl n_{11} der 11-Sylowgruppen gilt nach den Sylowsätzen $n_{11} \mid 2^2 \cdot 3 \cdot 5 = 60$, also $n_{11} \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ und mit der anderen Bedingung $n_{11} \in \{1, 12\}$. Weil G einfach ist, gilt $n_{11} \neq 1$. Zwei verschiedene 11-Sylowgruppen schneiden sich nach Lagrange nur in $\{e\}$ und sind jeweils isomorph zu $\mathbb{Z}/11$. Daher gibt es $10 \cdot n_{11} = 120$ Elemente der Ordnung 11 in den 11-Sylowgruppen. Nach Sylow-(2) ist andererseits jedes Element der Ordnung 11 von G in einer der 11-Sylowgruppen enthalten.

Aufgabe (F15T1A3a). Eine Gruppe G der Ordnung $105 = 3 \cdot 5 \cdot 7$ hat (bis auf Isomorphie) $\mathbb{Z}/5$ oder $\mathbb{Z}/7$ als Normalteiler, denn: Nach den Sylowsätzen gilt $n_5 \in \{1, 21\}$ und $n_7 \in \{1, 15\}$. Wir wollen den Fall $n_5 = 21$ und $n_7 = 15$ zu einem Widerspruch führen, indem wir zeigen, dass in G dafür nicht „genug Platz“ ist. In diesem Fall gäbe es $4 \cdot n_5 = 84$ Elemente der Ordnung 5 und $6 \cdot n_7 = 90$ Elemente der Ordnung 7 in G, womit $|G| \geq 84 + 90 + 1 = 175$ gelten würde (die Eins kommt vom neutralen Element), was ein Widerspruch ist.

Aufgabe (H13T1A2). Jede Gruppe G der Ordnung $750 = 2 \cdot 3 \cdot 5^3$ ist nicht einfach, denn: Nach den Sylowsätzen gilt $n_5 \in \{1, 6\}$. Wir können $n_5 = 6$ annehmen, da sonst die einzige 5-Sylowgruppe ein Normalteiler von G und G somit nicht einfach wäre. Nun operiert G auf der Menge X der 5-Sylogruppen durch **Untergruppenkonjugation**

$$\begin{array}{rcl} G \times X & \to & X \\ (a, U) & \mapsto & aUa^{-1} \end{array}$$

(und Sylow-(3) sagt übrigens gerade, dass diese Operation transitiv ist). Alternativ können wir die Operation als einen Gruppenhomomorphismus $\varphi: G \to \text{Bijektionen}(X)$ auffassen und dessen Kern ist ein Normalteiler. Wäre der $\text{Kern}(\varphi) = \{e\}$, so wäre φ injektiv und G eine Untergruppe von $S_{|X|} = S_6$ was nach Lagrange nicht sein kann, da 750 nicht $6! = 720$ teilt. Wäre der Kern $\text{Kern}(\varphi) = G$, so wäre $aUa^{-1} = U$ für alle $a \in G$ und $U \in X$, womit es nur ein Element in X gäbe, was ein Widerspruch ist. Also ist $\text{Kern}(\varphi)$ nicht-trivial und G nicht einfach.

- Ist G eine Gruppe, so bezeichnet die Untergruppe $\mathrm{Aut}(G) = \{f: G \to G \mid f \text{ Gruppenhom und bijektiv}\} \subseteq S_{|G|}$ der symmetrischen Gruppe die **Automorphismengruppe** von G.

  Beispiel 13.

  - $\mathrm{Aut}(\mathbb{Z}) = \{\pm \mathrm{id}\} \cong \mathbb{Z}/2$.
  - Es gilt
    $$\begin{array}{ccccc} \mathrm{Aut}(\mathbb{Z}/n) & = & \{a \mapsto k \cdot a \mid \mathrm{ggT}(k,n) = 1\} & \cong & \mathbb{Z}/n^\times \\ & & k \cdot (-) & \mapsfrom & k \end{array} \qquad \text{(Einheiten, Gruppe bzgl „·“)}$$
    (da ein Automorphismus der zyklischen Gruppe $\mathbb{Z}/n$ den Erzeuger 1 auf einen Erzeuger schicken muss) und daher gilt insbesondere $|\mathrm{Aut}(\mathbb{Z}/n)| = \varphi(n)$, wobei $\varphi(n)$ die **Eulersche Phi-Funktion** bezeichnet. Ein (nicht unbedingt existenter) Erzeuger der Gruppe $(\mathbb{Z}/n^\times, \cdot)$ heißt eine **Primitivwurzel modulo** n oder eine **primitive Einheitswurzel modulo** n.

- Für endliche Gruppen G und H mit koprimer (d.h. ggT=1) Ordnung gilt $\mathrm{Aut}(G \times H) = \mathrm{Aut}(G) \times \mathrm{Aut}(H)$. Ist $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ die Primfaktorzerlegung von n, so gilt also nach dem Chinesischen Restsatz
  $$\mathbb{Z}/n \quad \cong \quad \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_m^{k_m}$$
  und daher
  $$\mathbb{Z}/n^\times \quad \cong \quad (\mathbb{Z}/p_1^{k_1})^\times \times \ldots \times (\mathbb{Z}/p_m^{k_m})^\times.$$
  Für eine Primzahl $p \neq 2$ kann man nun zeigen, dass $(\mathbb{Z}/p^k)^\times \cong \mathbb{Z}/(p-1)p^{k-1}$. Für die Primzahl $p = 2$ ist diese Gruppe komplizierter zu bestimmen. Es gilt beispielsweise zwar $\mathbb{Z}/2^\times = \{e\}$, $\mathbb{Z}/4^\times = \mathbb{Z}/2$, aber $\mathbb{Z}/8^\times = \mathbb{Z}/2 \times \mathbb{Z}/2$, was nicht zyklisch ist. Immerhin gilt für jede Primzahl die Formel $\varphi(p^k) = (p-1)p^{k-1}$.

  Aufgabe (F20T3A2). Möchte man die letzten beiden Ziffern der Zahl $a := 2018^{\left(2019^{2020}\right)}$ bestimmen, können wir die zugehörige Restklasse in $\mathbb{Z}/100$ bestimmen (Achtung: Es ist nicht erlaubt, dazu die Restklasse des Exponenten in $\mathbb{Z}/100$ zu bestimmen!). Mit dem Chinesischen Restsatz $\mathbb{Z}/100 \cong \mathbb{Z}/4 \times \mathbb{Z}/25$ genügt es, die Restklassen von a in $\mathbb{Z}/4$ und $\mathbb{Z}/25$ zu bestimmen. Wir werden diese als $[a]_4 = [0]_4$ und $[a]_{25} = [18]_{25}$ identifizieren und erhalten somit $[a]_{100} = [68]_{100}$, die letzten beiden Stellen von a sind also 68. In $\mathbb{Z}/4$ gilt
  $$[a]_4 = [2018^{\left(2019^{2020}\right)}]_4 = [2018]_4^{\left(2019^{2020}\right)} = [2]_4^{\left(2019^{2020}\right)} = [0]_4,$$
  da der Exponent offenbar größer als 2 ist und $[-]_4 : \mathbb{Z} \to \mathbb{Z}/4$ ein Ringhomomorphismus (s.u.). Nun zu $\mathbb{Z}/25$: Da $\mathrm{ggT}(2018, 25) = 1$, ist $[2018]_{25} \in \mathbb{Z}/25^\times$ eine Einheit und da $\mathbb{Z}/25^\times \cong \mathbb{Z}/20$, gilt für den Exponenten
  $$[2019^{2020}]_{20} = [2019]_{20}^{2020} = [19]_{20}^{2020} = [-1]_{20}^{2020} = [1]_{20}^{1010} = [1]_{20}$$
  und daher
  $$[a]_{25} = [2018^{\left(2019^{2020}\right)}]_{25} = [2018^1]_{25} = [18]_{25}.$$

- Interessiert man sich auch für nicht-bijektive Gruppenhomomorphismen $\mathbb{Z}/n \to \mathbb{Z}/m$, so hilft die Bijektion
  $$\begin{array}{ccc} \hom_{\mathrm{Grp}}(\mathbb{Z}/n, \mathbb{Z}/m) & \cong & \mathbb{Z}/\mathrm{ggT}(n,m) \\ \frac{km}{\mathrm{ggT}(n,m)} \cdot (-) & \mapsfrom & k. \end{array}$$

- Sind N und H Gruppen und $\varphi: H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus, so definiert
  $$(n,h) \cdot (n',h') := (n\varphi(h)(n'), hh')$$
  eine Gruppenstruktur auf der Menge $N \times H$, die mit $N \rtimes_\varphi H$ bezeichnet wird und **semidirektes Produkt** heißt. (Insbesondere ist mit dem trivialen φ das direkte Produkt ein spezielles semidirektes Produkt, wobei „trivial“ bedeutet, dass nur die Identität getroffen wird.)

- Es ist $* \to N \to N \rtimes_\varphi H \to H \to *$ eine (spaltende) kurze exakte Sequenz von Gruppen und insbesondere ist die Untergruppe N stets ein Normalteiler. Es gilt:
  $$H \text{ Normalteiler von } N \rtimes_\varphi H \quad \Leftrightarrow \quad N \rtimes_\varphi H \cong N \times H \quad \Leftarrow \quad \varphi \text{ ist trivial}$$
  Falls N und H abelsch sind, so gilt
  $$N \rtimes_\varphi H \text{ abelsch} \quad \Leftrightarrow \quad N \rtimes_\varphi H \cong N \times H \quad \Rightarrow \quad \varphi \text{ ist trivial}$$
  und insbesondere können wir mit einem nicht-trivialen φ aus zwei abelschen Gruppen N und H eine nicht-abelsche Gruppe konstruieren.

Aufgabe (F13T3A1). Eine nicht-abelsche Gruppe der Ordnung $2013 = 3 \cdot 11 \cdot 61$ ist beispielsweise $\mathbb{Z}/11 \times G$, wobei $G := \mathbb{Z}/61 \rtimes_\varphi \mathbb{Z}/3$ mit dem nicht-trivialen

$$\begin{array}{rccl} \varphi\colon & \mathbb{Z}/3 & \to & \mathrm{Aut}(\mathbb{Z}/61) \cong \mathbb{Z}/60 \\ & a & \mapsto & 20a. \end{array}$$

Beispiel 14. Jedes semidirekte Produkt $\mathbb{Z}/5 \rtimes_\varphi \mathbb{Z}/3$ ist isomorph zu $\mathbb{Z}/15$, denn jeder Gruppenhomomorphismus $\varphi\colon \mathbb{Z}/3 \to \mathrm{Aut}(\mathbb{Z}/5) \cong \mathbb{Z}/4$ ist trivial.

- (Für gegebene Gruppen N und H ist es üblicherweise nicht einfach zu sagen, wann $N \rtimes_\varphi H \cong N \rtimes_{\varphi'} H$ gilt. Nur die hinreichende Bedingung ist oft einfach: Ein solcher Isomorphismus existiert beispielsweise, wenn $\varphi' = \varphi \circ f$ für einen Automorphismus $f\colon H \xrightarrow{\cong} H$ gilt. Ebenso können wir N durch eine isomorphe Gruppe ersetzen.)

- Ist G eine Gruppe, N ein Normalteiler und H eine Untergruppe von G mit $N \cap H = \{e\}$, so ist die Abbildung

$$\begin{array}{rcl} N \rtimes_\varphi H & \hookrightarrow & G \\ (n,h) & \mapsto & nh \end{array}$$

wobei $\varphi\colon H \to \mathrm{Aut}(N)$ durch $h \mapsto \left(n \mapsto hnh^{-1}\right)$ definiert ist, ein injektiver Gruppenhomomorphismus dessen Bild die Untergruppe NH von G ist, die in diesem Fall auch (inneres) **semidirektes Produkt** genannt wird. (Der Unterschied zum (inneren) direkten Produkt ist also, dass H hier nur eine Untergruppe und kein Normalteiler zu sein braucht.)

Beispiel 15. Es gibt (bis auf Isomorphie) nur zwei Gruppen G der Ordnung $55 = 5 \cdot 11$. Die Sylowsätze zeigen $n_{11} = 1$ und $n_5 \in \{1, 11\}$. Sei $N \cong \mathbb{Z}/11$ die normale 11-Sylowgruppe und $H \cong \mathbb{Z}/5$ eine 5-Sylowgruppe von G. Mit Lagrange gilt $N \cap H = \{e\}$ und $|NH| = |G|$. Wäre H die einzige 5-Sylowgruppe und damit normal, so wäre $G \cong N \times H \cong \mathbb{Z}/11 \times \mathbb{Z}/5 \cong \mathbb{Z}/55$ zyklisch. Andernfalls ist $G \cong N \rtimes_\varphi H$ für ein nicht-triviales $\varphi\colon \mathbb{Z}/5 \to \mathrm{Aut}(\mathbb{Z}/11) \cong \mathbb{Z}/10$ (und insbesondere ist G nicht abelsch). Es gibt vier nicht-triviale verschiedene solche Gruppenhomomorphismen $\mathbb{Z}/5 \to \mathbb{Z}/10$:

$$\begin{array}{rccl} \varphi_1'\colon & 1 & \mapsto & 2 \\ \varphi_2'\colon & 1 & \mapsto & 4 \\ \varphi_3'\colon & 1 & \mapsto & 6 \\ \varphi_4'\colon & 1 & \mapsto & 8 \end{array}$$

Um diese als Gruppenhomomorphismen $\mathbb{Z}/5 \to \mathrm{Aut}(\mathbb{Z}/11) \cong \mathbb{Z}/11^\times$ zu interpretieren, müssen wir den Isomorphismus $\mathbb{Z}/10 \xrightarrow{\cong} \mathbb{Z}/11^\times$ explizit machen. Dieser ist durch $j \mapsto g^j$ gegeben, wobei g eine (beliebige) primitive Einheitswurzel ist, also ein Element g, dessen Potenzen die gesamte Menge $\{1, 2, \ldots, 10\}$ sind. Für $g = 2$ ist dieses der Fall, da $g^1 = 2, g^2 = 4, g^3 = 8, g^4 = 5, g^5 = 10, g^6 = 9, g^7 = 7, g^8 = 3, g^9 = 6$ und $g^{10} = 1$. Wir bekommen also vier nicht-triviale verschiedene Gruppenhomomorphismen $\mathbb{Z}/5 \to \mathrm{Aut}(\mathbb{Z}/11)$:

$$\begin{array}{rccl} \varphi_1\colon & 1 & \mapsto & g^2 \cdot (-) = 4 \cdot (-) \\ \varphi_2\colon & 1 & \mapsto & g^4 \cdot (-) = 5 \cdot (-) \\ \varphi_3\colon & 1 & \mapsto & g^6 \cdot (-) = 9 \cdot (-) \\ \varphi_4\colon & 1 & \mapsto & g^8 \cdot (-) = 3 \cdot (-) \end{array}$$

So ist beispielsweise die Gruppenstruktur auf $\mathbb{Z}/11 \rtimes_{\varphi_1} \mathbb{Z}/5$ gegeben durch $(n,h) \cdot (n'h') = (n + \varphi(h)(n'), h + h') = (n + 4^h n', h + h')$. Tatsächlich sind (trotz verschiedener φ) alle vier zugehörigen semidirekten Produkte isomorph und es gibt insgesamt nur zwei Gruppen der Ordnung 55. (Beispielsweise ist ein Isomorphismus $\mathbb{Z}/11 \rtimes_{\varphi_1} \mathbb{Z}/5 \cong \mathbb{Z}/11 \rtimes_{\varphi_2} \mathbb{Z}/5$ durch $(n,h) \mapsto (3n, h)$ gegeben.)

- Für ein $n \geq 1$ ist die **Diedergruppe** D_n definiert als das semidirekte Produkt $\mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$, wobei der Gruppenhomomorphismus $\varphi\colon \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/n)$ durch $1 \mapsto (a \mapsto -a)$ gegeben ist. Folglich gilt $|D_n| = 2n$.

- Es gilt $D_1 \cong \mathbb{Z}/2$ und $D_2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, aber für $n \geq 3$ ist D_n die Symmetriegruppe eines regelmässigen n-Ecks in der Ebene und **nicht-abelsch**. Wir können sie (bis auf Isomorphie) als Untergruppe $D_n \subseteq S_n$ auffassen, wobei $\{1, \ldots n\}$ die Ecken eines regelmässigen n-Ecks in der Ebene bezeichnen und D_n als Untergruppe erzeugt ist von

$$d := (1\ 2\ \ldots\ n) \quad (\text{„Drehung“}) \qquad \text{und} \qquad s := (2\ n)(3\ (n-1))\cdots \quad (\text{„Spiegelung an der } y\text{-Achse“})$$

(es ist $s := (2\ n)$ für $n = 3$ gemeint), wobei man sich die Ecke „1“ oben auf der y-Achse vorstellen sollte. Offenbar gelten die Relationen

$$d^n = s^2 = sdsd = e.$$

und es gilt

$$D_n = \{1, d, \ldots, d^{n-1},\ s, sd, \ldots, sd^{n-1}\},$$

wobei die Elemente, die ein s enthalten, wegen $sd^k = d^{-k}s$ jeweils Ordnung 2 haben (also „Spiegelungen sind“).

Beispiel 16. Eine Übersicht aller „kleinen“ Gruppen bis auf Isomorphie, wobei Q_8 die nicht-abelsche Quaternionengruppe ist, ist:

1	2	3	4	5	6	7	8	9	10	⋯
$\{e\}$	$\mathbb{Z}/2$	$\mathbb{Z}/3$	$\mathbb{Z}/4$	$\mathbb{Z}/5$	$\mathbb{Z}/6$	$\mathbb{Z}/7$	$\mathbb{Z}/8$	$\mathbb{Z}/9$	$\mathbb{Z}/10$	
			$\mathbb{Z}/2\times\mathbb{Z}/2$		$S_3\cong D_3$		$\mathbb{Z}/4\times\mathbb{Z}/2$	$\mathbb{Z}/3\times\mathbb{Z}/3$	D_5	
							$\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/2$			
							D_4			
							Q_8			

- Es gibt jeweis nur eine (zyklische) Gruppe der Primzahlordnungen $2, 3, 5$ und 7.
- Gruppen der Primzahlquadratordnungen 4 und 9 sind abelsch und daher durch den Hauptsatz beschrieben.
- Eine Gruppe der Ordnung $6 = 2\cdot 3$ (und analog $10 = 2\cdot 5$) hat nach den Sylowsätzen einen zu $\mathbb{Z}/3$ isomorphen Normalteiler und (mindestens) eine zu $\mathbb{Z}/2$ isomorphe 2-Sylowgruppe. Daher ist sie ein semidirektes Produkt $\mathbb{Z}/3 \rtimes_\varphi \mathbb{Z}/2$ mit $\varphi\colon \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/3)$. Es ist also φ trivial oder definiert die Diedergruppe D_3.
- Die nicht-abelschen Gruppen der Ordnung 8 sind schwieriger zu klassifizieren.

- Die **Kommutatorgruppe** $K(G)$ einer Gruppe G ist die von allen **Kommutatoren** $[a,b] = aba^{-1}b^{-1}$ erzeugte Untergruppe von G. (Achtung: Ein Produkt zweier Kommutatoren ist nicht unbedingt wieder ein Kommutator.)
- Es ist $K(G) \subseteq G$ ein Normalteiler und $G^{\text{ab}} = G/K(G)$ ist eine abelsche Gruppe, die die **Abelianisierung** von G genannt wird. Es gilt:
$$K(G) = \{e\} \quad \Longleftrightarrow \quad G \text{ ist abelsch} \quad \Longleftrightarrow \quad G = G^{\text{ab}}$$
Gruppen mit $K(G) = G$ werden auch **perfekt** oder **vollkommen** genannt.

Beispiel 17.
- $K(S_n) = A_n$
- $K(A_1) = K(A_2) = K(A_3) = \{e\}$ und $K(A_4) = \mathbb{Z}/2 \times \mathbb{Z}/2$
- $K(A_{\geq 5}) = A_{\geq 5}$ weil $A_{\geq 5}$ einfach und nicht abelsch ist.

- Eine Gruppe G ist **auflösbar**, falls es eine Kette von Untergruppen
$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_m = G$$
gibt, sodass jede Untergruppe G_i der Kette ein Normalteiler ihres Vorgängers G_{i+1} ist (soetwas nennt man auch eine **Subnormalreihe**) und alle Quotienten G_{i+1}/G_i abelsch sind.
- Eine Gruppe G ist auflösbar genau dann, wenn die iterierte Bildung der Kommutatorgruppe nach endlich vielen Schritten trivial wird, also $K(K(\ldots K(G)\ldots)) = \{e\}$.
- Tatsächlich gibt es für eine endliche auflösbare Gruppe sogar eine Subnormalreihe, sodass für die zugehörigen Quotienten gilt $G_{i+1}/G_i \cong \mathbb{Z}/p_i$ für Primzahlen p_i.
- Untergruppen, direkte und semidireke Produkte auflösbarer Gruppen sind wieder auflösbar. Für einen Normalteiler $N \subseteq G$ gilt:
$$G \text{ auflösbar} \quad \Longleftrightarrow \quad N \text{ auflösbar} \ \wedge \ G/N \text{ auflösbar}$$

Beispiel 18.
- Jede abelsche Gruppe ist auflösbar.
- Jede p**-Gruppe ist auflösbar**, da sie ein nicht-triviales Zentrum $Z(G)$ hat und $G/Z(G)$ wieder eine p-Gruppe kleinerer Ordnung ist (dann Induktion). Insbesondere ist jede Sylow-Gruppe auflösbar.
- Nach dem pq**-Satz von Burnside** ist jede Gruppe der Ordnung $p^a q^b$ für Primzahlen p und q auflösbar.
- Nach dem **Satz von Feit-Thompson** ist jede Gruppe ungerader Ordnung auflösbar.
- Eine nicht-abelsche und auflösbare Gruppe kann nicht einfach sein. Nach dem Satz von Feit-Thompson muss also eine nicht-abelsche und einfache endliche Gruppe eine gerade Ordnung haben.
- $A_{\geq 5}$ **ist nicht auflösbar**, da $K(A_{\geq 5}) = A_{\geq 5}$. Tatsächlich sind alle Gruppen der Ordnung < 60 auflösbar und die A_5 mit $|A_5| = 60$ ist das kleinste Beispiel einer nicht-auflösbaren Gruppe.
- $S_{\geq 5}$ **ist nicht auflösbar**, da die Untergruppe $A_{\geq 5}$ nicht auflösbar ist.

Aufgabe (F15T1A3b). Jede Gruppe der Ordnung $105 = 3 \cdot 5 \cdot 7$ ist auflösbar: Wir haben oben gezeigt, dass jede solche Gruppe G einen zu $\mathbb{Z}/5$ oder einen zu $\mathbb{Z}/7$ isomorphen Normalteiler N hat. Dieser Normalteiler N ist eine auflösbare Gruppe. Es genügt also zu zeigen, dass G/N auflösbar ist. Wir zeigen allgemeiner: **Jede Gruppe** G **der Ordnung** $p \cdot q$ **ist auflösbar** für Primzahlen p und q. Da jede p-Gruppe auflösbar ist, können wir $p < q$ annehmen. Mit den Sylowsätzen gilt dann $n_q \mid p$, also $n_q \in \{1, p\}$, und $n_q \equiv 1 \mod q$, also $n_q = 1$. Die einzige q-Sylowgruppe in G ist also ein auflösbarer Normalteiler N und es genügt zu zeigen, dass G/N auflösbar ist. Diese Gruppe hat aber Ordnung p und ist dann ebenfalls auflösbar.

Sei K ein Körper und V und W endlichdimensionale K-Vektorräume.

- Für eine lineare Abbildung $f: V \to W$ gilt die **Dimensionsformel**

$$\dim V \;=\; \dim \mathrm{Bild}(f) \;+\; \dim \mathrm{Kern}(f)$$

und insbesondere damit für $f: V \to V$:

$$\text{injektiv (d.h. } \mathrm{Kern}(f) = 0) \iff \text{surjektiv (d.h. } \mathrm{Bild}(f) = V) \iff \text{bijektiv}$$

- Ist $\mathcal{A} = (v_1, \ldots, v_n)$ eine Basis von V und $\mathcal{B} = (w_1, \ldots, w_m)$ eine Basis von W und sind

$$\begin{array}{rccc} \Phi_{\mathcal{A}}\colon & K^n & \xrightarrow{\cong} & V \\ & e_j & \mapsto & v_j \end{array} \qquad \text{und} \qquad \begin{array}{rccc} \Phi_{\mathcal{B}}\colon & K^m & \xrightarrow{\cong} & W \\ & e_i & \mapsto & w_i, \end{array}$$

Koordinatensysteme, so gibt es Bijektionen

$$\begin{array}{rccc} M_{\mathcal{B}}^{\mathcal{A}}\colon & \mathrm{LAbb}(V,W) & \xrightarrow[\Phi_{\mathcal{B}}^{-1} \circ (-) \circ \Phi_{\mathcal{A}}]{\cong} & \mathrm{LAbb}(K^n, K^m) \xrightarrow{\cong} \mathrm{Mat}(m \times n; K) \\ & f & \longmapsto & \begin{pmatrix} \vdots & & \vdots \\ f(e_1) & \cdots & f(e_n) \\ \vdots & & \vdots \end{pmatrix} =: A_f \\ & f_A := (v \mapsto A \cdot v) & \longmapsfrom & A \end{array}$$

verträglich mit Abbildungskomposition und Matrizenmultiplikation. Die Matrix $M_{\mathcal{B}}^{\mathcal{A}}(f)$ heißt **Darstellungsmatrix** oder darstellende Matrix von f (bezüglich $\mathcal{A}$ und $\mathcal{B}$).

Beispiel 19. Sei $\mathcal{A} := \left(v_1 := \begin{pmatrix} 0 \\ -1 \end{pmatrix}, v_2 := \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$ eine Basis von $V = K^2$, $\mathcal{B} := \left(w_1 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}, w_2 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)$ eine Basis von $W = K^2$ und $g: V \to W$ mit $v_1 \mapsto w_2 - w_1$ und $v_2 \mapsto w_2 - w_1$ eine lineare Abbildung. Es gilt also $M_{\mathcal{B}}^{\mathcal{A}}(g) = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$ („die Spalten sind die Bilder der Basisvektoren“).
Sei nun $\mathcal{A}' := \left(v_1' := \begin{pmatrix} 1 \\ 2 \end{pmatrix}, v_2' := \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ eine weitere Basis von V und $\mathcal{B}' := \left(w_1' := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, w_2' := \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right)$ eine weitere Basis von W. Wir möchten $M_{\mathcal{B}'}^{\mathcal{A}'}(g)$ bestimmen. durch Umstellen von $M_{\mathcal{B}}^{\mathcal{A}}(g) = A_{\Phi_{\mathcal{B}}^{-1} \circ g \circ \Phi_{\mathcal{A}}} = A_{\Phi_{\mathcal{B}}^{-1}} \cdot A_g \cdot A_{\Phi_{\mathcal{A}}} = A_{\Phi_{\mathcal{B}}}^{-1} \cdot A_g \cdot A_{\Phi_{\mathcal{A}}}$ bekommen wir

$$A_g = A_{\Phi_{\mathcal{B}}} \cdot M_{\mathcal{B}}^{\mathcal{A}}(g) \cdot A_{\Phi_{\mathcal{A}}}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix} \quad \text{und damit}$$

$$M_{\mathcal{B}'}^{\mathcal{A}'}(g) = A_{\Phi_{\mathcal{B}'}^{-1} \circ g \circ \Phi_{\mathcal{A}'}} = A_{\Phi_{\mathcal{B}'}}^{-1} \cdot A_g \cdot A_{\Phi_{\mathcal{A}'}} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}.$$

(Wenn wir in der unteren Gleichung direkt die obere Gleichung mit A_g einsetzen, erhalten wir die Matrix $A_{\Phi_{\mathcal{B}'}}^{-1} A_{\Phi_{\mathcal{B}}}$ die man Transformationsmatrix von $\mathcal{B}$ zu $\mathcal{B}'$ nennt.)

- Für eine Matrix $A \in M(n \times n; K)$ entsprechen **Zeilentransformationen** der Multiplikation mit Elementarmatrizen **von Links**, also einer **Basisänderung im Ziel** K^m. Hierdurch verändert sich also der Kern von f_A nicht. (Analog entsprechen Spaltentransformationen der Multiplikation mit Elementarmatrizen von rechts, also Basisänderung in der Quelle K^n und das Bild von f_A verändert sich nicht.)

- Die Abbildung

$$\begin{array}{rccc} \det\colon & M(n \times n; K) & \to & K \\ & A & \mapsto & \displaystyle\sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \end{array}$$

heißt **Determinante** und es gilt $\det(A \cdot B) = \det(A) \det(B)$.

- Eine Matrix $A \in M(n \times n; K)$ ist **invertierbar**
  $\Leftrightarrow$ $\exists B \in M(n \times n; K) : BA = E$
  $\Leftrightarrow$ $\exists B \in M(n \times n; K) : AB = E$
  $\Leftrightarrow$ $\det(A) \neq 0$
  $\Leftrightarrow$ A ist Produkt von Elementarmatrizen
  $\Leftrightarrow$ Die Spalten (oder Zeilen) von A bilden eine Basis von K^n
  $\Leftrightarrow$ f_A ist bijektiv ($\Leftrightarrow$ f_A ist injektiv $\Leftrightarrow$ f_A ist surjektiv)

Sei eine Matrix $A \in M(n \times n; K)$ mit zugehöriger linearer Abbildung $f := f_A : K^n \to K^n$ fixiert. (Umgekehrt kann man auch ein lineares $f : V \to V$ mit zugehöriger (beliebiger) darstellender Matrix $A := M_{\mathcal{B}}^{\mathcal{A}}(f)$ fixieren). Bei der Definition und Benutzung der folgenden Begriffe kann man f jeweils durch A ersetzen.

- Für ein $\lambda \in K$ heißt der Untervektorraum $\mathrm{Eig}(\lambda) := \mathrm{Kern}(f - \lambda \mathrm{id}) \subseteq V$ der **Eigenraum zu** λ und dessen Elemente $v \neq 0$ **Eigenvektoren zum Eigenwert** λ. (Ein λ heißt **Eigenwert**, falls es einen Eigenvektor dazu gibt, also ein $v \neq 0$ mit $f(v) = \lambda v$.)
- Es heißt $\mathrm{geo}(\lambda) := \dim(\mathrm{Eig}(\lambda))$ die **geometrische Vierlfachheit von** λ.
- Das Polynom $\chi_f(x) = \det(xE - A) \quad \in K[x]$
  heißt das **charakteristische Polynom** von f und es gilt:
  $$\chi_f(\lambda) = 0 \iff \mathrm{Eig}(\lambda) \neq \{0\} \iff f \text{ hat Eigenwert } \lambda$$
- Das **Minimalpolynom** $\mu_f(x) \in K[x]$ von f ist das normierte Polynom kleinsten Grades mit $\mu_f(A) = 0$ (Dieses existiert, da nach dem Satz von Cayley-Hamilton $\chi_f(A) = 0$ gilt). Es gilt $\mu_f \mid \chi_f$ und beide haben die gleichen irreduziblen Faktoren (also insbesondere Linearfaktoren und daher genau die gleichen Nullstellen).

  Beispiel 20. Für die Matrix $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ ist $\chi_A(x) = (x-1)^3$, aber $\mu_A(x) = (x-1)^2$, da $A - E \neq 0$ und $(A-E)^2 = 0$.
- Die **algebraische Vielfachheit von** λ ist der Exponent $\mathrm{alg}(\lambda)$ des Linearfaktors $(x - \lambda)$ in $\chi_f(x)$ und es gilt
  $$\mathrm{geo}(\lambda) \leq \mathrm{alg}(\lambda) \leq n$$
- Eine Matrix $A \in M(n \times n; K)$ ist **diagonalisierbar** $\Leftrightarrow$ $A = SDS^{-1}$, wobei D eine Diagonalmatrix ist
  (Es folgt, dass $S = A_{\Phi_{\mathcal{B}}}$, wobei $\mathcal{B} := (b_1, \ldots, b_n)$ eine Basis aus Eigenvektoren ist.)
  $\Leftrightarrow$ Es gibt eine Basis aus Eigenvektoren
  $\Leftrightarrow$ $\sum_\lambda \mathrm{geo}(\lambda) = n$
  $\Leftrightarrow$ χ_A zerfällt in Linearfaktoren und $\mathrm{geo}(\lambda) = \mathrm{alg}(\lambda)$ für alle λ
  $\Leftrightarrow$ μ_A zerfällt in verschiedene Linearfaktoren

  Beispiel 21.
  - $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ist diagonalisierbar aber nicht invertierbar und $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ist invertierbar aber nicht diagonalisierbar, da $\chi_A = \mu_A = (x-1)^2$ und das Minimalpolynom somit nicht in verschiedene Linearfaktoren zerfällt. Invertierbarkeit und Diagonalisierbarkeit haben also nichts miteinander zutun.
  - Reelle symmetrische Matrizen sind immer diagonalisierbar, sogar mit $S^{-1} = S^T$, also einer orthogonalen Matrix S.
  - $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ hat das Minimalpolynom $\chi_A = x^2 - x - 1$, was über $\mathbb{R}$ in $(x - \frac{1 \pm \sqrt{5}}{2})$ zerfällt und $\chi_A = \mu_A$, da beide die gleichen Linearfaktoren haben. Daher ist A über $\mathbb{R}$ diagonalisierbar, aber nicht über $\mathbb{Q}$.
  - Es ist $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ mit $\chi_A = x^2 + 1$ nicht über $\mathbb{R}$ diagonalisierbar, aber über $\mathbb{F}_5$, da hier $\chi_A = (x-2)(x-3)$.
- Für $\lambda \in K$ heißt die Matrix $J(n, \lambda) := \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} \in M(n \times n; K)$ ein **Jordankästchen**. Eine Matrix $J \in M(n \times n; K)$ ist eine **Jordanmatrix** (oder in **Jordanform**), wenn
  $$J = \begin{pmatrix} \underbrace{\boxed{\begin{matrix} J(n_{11}, \lambda_1) & & \\ & \ddots & \\ & & J(n_{1k_1}, \lambda_1) \end{matrix}}}_{\textbf{Jordanblock zum EW } \lambda_1} & & \\ & \boxed{\ddots} & \\ & & \boxed{\ddots} \end{pmatrix}.$$
- Für eine Matrix $A \in M(n \times n; K)$ zerfällt χ_A in Linearfaktoren (z.B. falls $K = \mathbb{C}$) $\Leftrightarrow$ $A = SJS^{-1}$, wobei J eine (bis auf Permutation der Jordankästchen eindeutige) Jordanmatrix ist.
- Es gilt:
  $$\begin{aligned} \mathrm{alg}(\lambda) &= \text{Länge des Jordanblocks zu } \lambda \\ \mathrm{geo}(\lambda) &= \text{Anzahl der Jordankästchen zu } \lambda \\ \text{Exponent des Linearfaktors } (x-\lambda) \text{ im Mipo } \mu &= \text{Größe des größten Jordankästchens zu } \lambda \end{aligned}$$

- Ein **Ring** $R = (R, +, \cdot)$ hat (soweit nichts anderes gesagt ist) eine Eins 1 und ist kommutativ.
  Es ist der **Nullring** $(0) := \{0\}$ der einzige Ring mit $1 = 0$.

- Ein **Ringhomomorphismus** respektiert $+$ und $\cdot$ und bildet die 1 auf die 1 ab. Für jeden Ring R gibt es zwei eindeutige Ringhomomorphismen $\mathbb{Z} \to R \to (0)$.

- Ein **Ideal (von** R**)** $I \subseteq R$ ist eine additive Untergruppe, die unter Multiplikation mit beliebigen Ringelementen abgeschlossen ist. (Ein Ideal ist nicht im Allgemeinen ein Ring, da es oft keine Eins hat.) Es gilt:

$$1 \in I \quad \Longleftrightarrow \quad I = R.$$

- Ideale $I \subseteq R$ sind genau die R-Untermoduln von R.

- Ideale $I \subseteq R$ sind genau die Kerne von Ringhomomorphismen $\varphi: R \to S$ und es gilt der **Homomorphiesatz** $R/\ker(\varphi) \cong \varphi(R)$.

- Durchschnitte und Urbilder von Idealen unter Ringhomomorphismen sind wieder Ideale.

- Für eine Teilmenge $X \subseteq R$ heißt

$$(X) := \bigcap_{\substack{X \subseteq I \subseteq R \\ I \text{ Ideal}}} I \;=\; \{\lambda_1 x_1 + \ldots + \lambda_n x_n \in R \mid \lambda_i \in R \text{ und } x_i \in X\}$$

  das **von** X **erzeugte Ideal** und es gilt offenbar $X \subseteq (X) \subseteq R$. Ist X konkret gegeben, so werden die Mengenklammern bei dieser Schreibweise oft weggelassen. Ein von einem Element $a \in R$ erzeugtes Ideal $(a) \subseteq R$ heißt **Hauptideal**.

- In einem Ring **teilt** ein Element a ein Element b genau dann, wenn $ak = b$ gilt für ein $k \in R$, wofür man $a \mid b$ schreibt. Offenbar gilt

$$a \mid b \qquad \Longleftrightarrow \qquad (b) \subseteq (a).$$

Beispiel 22. Die 0 teilt nur die 0. Jedes Element teilt die 0. Die 1 teilt jedes Element.

- Ein Element $a \in R$ ist eine **Einheit** oder **invertierbar**
$$\begin{aligned} &\Leftrightarrow \quad \exists b \in R : \; ab = 1 \\ &\Leftrightarrow \quad a \text{ teilt die Eins} \quad (\text{d.h. } a \mid 1) \\ &\Leftrightarrow \quad (a) = R. \end{aligned}$$
  Die Menge der Einheiten $R^\times \subseteq R$ ist mit der Multiplikation von R eine Gruppe und heißt die **Einheitengruppe** $(R^\times, \cdot)$ von R. Ein Ringhomomorphismus $R \to S$ induziert einen Gruppenhomomorphismus $R^\times \to S^\times$.

- Ein Ring R ist ein **Körper**
$$\begin{aligned} &\Leftrightarrow \quad R \neq (0) \text{ und jedes Element } a \neq 0 \text{ ist eine Einheit} \\ &\Leftrightarrow \quad R^\times = R \setminus \{0\} \\ &\Leftrightarrow \quad R \text{ hat genau die Ideale } (0) \text{ und } R. \end{aligned}$$
  Jeder Ringhomomorphismus $K \to R$ von einem Körper K in einen Ring $R \neq 0$ ist injektiv. Insbesondere ist jeder Ringhomomorphismus zwischen Körpern injektiv (und wird manchmal auch Körperhomomorphismus genannt).

Beispiel 23. In einem Körper teilt jedes $a \neq 0$ jedes andere Element. Daher ist der Begriff der Teilbarkeit in Körpern uninteressant.

- Ein Element $a \in R$ ist ein **Nullteiler** $\Leftrightarrow \exists b \in R : \; b \neq 0 \;\wedge\; ab = 0$.
  Ein Ring R heißt **Integritätsbereich**, falls $R \neq 0$ und R keine nicht-trivialen (d.h. $\neq 0$) Nullteiler hat.

  Beispiel 24.
  - Da in einem Ring $R \neq 0$ Einheiten nie Nullteiler sind, ist jeder Körper ein Integritätsbereich.
  - Jeder **endliche Integritätsbereich ist ein Körper**, denn ist $a \neq 0$ ein Element, so ist die Abbildung $a\cdot : R \to R$ injektiv, denn mit $ab = ab' \Leftrightarrow a(b - b') = 0$, folgt im Integritätsbereich R, dass $b - b' = 0 \Leftrightarrow b = b'$. Die injektive Abbildung $a\cdot$ zwischen gleichen endlichen Mengen ist auch surjektiv. Also wird die Eins im Ziel getroffen und es gibt ein $b \in R$ mit $ab = 1$.

- In einem Ring heißen Elemente a und b **assoziiert**, falls $a \mid b$ und $b \mid a$. In einem Integritätsbereich bedeutet dieses genau, dass sich $a$und b durch eine Einheit unterscheiden, es also ein $k \in R^\times$ gibt mit $ak = b$.

- Für ein Ideal $I \subseteq R$ gilt:

$$\left\{\begin{array}{rl} I \text{ ist } \textbf{Maximalideal} & \Leftrightarrow\ I \neq R \text{ und kein Ideal} \\ & \quad \text{liegt echt zwischen } I \text{ und } R \\ & \Leftrightarrow\ R/I \text{ ist Körper} \end{array}\right\} \Longrightarrow \left\{\begin{array}{rl} I \text{ ist } \textbf{Primideal} & \Leftrightarrow\ I \neq R \text{ und} \\ & \quad ab \in I \ \Rightarrow\ a \in I \vee b \in I \\ & \Leftrightarrow\ R/I \text{ ist Integritätsb.} \end{array}\right\}$$

Beispiel 25.

- $6\mathbb{Z} \subsetneq \mathbb{Z}$ ist kein Primideal, da $\mathbb{Z}/6\mathbb{Z}$ kein Integritätsbereich ist, da $[2]\cdot[3] = [6] = [0]$.
- $(0) \subsetneq \mathbb{Z}$ ist ein Primideal, aber nicht maximal, da $\mathbb{Z}/(0) = \mathbb{Z}$ kein Körper ist.
- Urbilder von Primidealen unter Ringhomomorphismen sind wieder Primideale, aber nicht Urbilder maximaler Ideale maximal, wie das Beispiel $\mathbb{Z} \hookrightarrow \mathbb{Q} \supseteq (0)$ zeigt.

- Für ein Element $p \in R$ gilt:

$$\left\{\begin{array}{rl} p \text{ ist } \textbf{Primelement} & \Leftrightarrow\ p \neq 0 \wedge p \text{ ist keine Einheit} \wedge \\ & \quad p \mid ab \ \Rightarrow\ p \mid a \vee p \mid b \\ & \Leftrightarrow\ p \neq 0 \wedge (p) \text{ ist Primideal} \end{array}\right\} \begin{array}{c} \xRightarrow{R \text{ IB}} \\ \xLeftarrow{R \text{ fakt.}} \end{array} \left\{\begin{array}{rl} p \text{ ist } \textbf{irreduzibel} & \Leftrightarrow\ p \neq 0 \wedge p \text{ ist keine Einheit} \wedge \\ & \quad p = ab \ \Rightarrow\ a \in R^\times \vee b \in R^\times \\ & \overset{IB}{\Leftrightarrow}\ p \neq 0 \wedge (p) \text{ ist maximales} \\ & \quad \text{Hauptideal} \neq R \end{array}\right\}$$

- Die Eigenschaften ein Primelement oder irreduzibel zu sein sind invariant unter Assoziiertheit.
- In einem Integritätsbereich ist die Zerlegung eines Elements $a = p_1 \cdot \ldots \cdot p_n$ in Primelemente (falls sie existiert) eindeutig bis auf Umordnung und Einheiten.
- Es gibt die folgenden speziellen Bezeichnungen für Ringe:

IBereiche	$\supseteq$	Faktorielle Ringe	$\supseteq$	Hauptidealringe	$\supseteq$	Euklidische Ringe	$\supseteq$	Körper
		IB und jedes Element $a \neq 0$ und keine Einheit besitzt eine Zerlegung $a = p_1 \cdot \ldots \cdot p_n$ in Primelemente. **Bsp:** $\mathbb{Q}[x,y]$, kein Hauptidealring		IB und jedes Ideal ist Hauptideal. **Bsp:** $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, nicht euklidisch (hier gibt es nur komplizierte Bsp, die nicht euklidisch sind.)		IB und es gibt **Division mit Rest** bzgl. einer Abbildung $\delta: R \setminus \{0\} \to \mathbb{N}$, d.h. $\forall a, b \neq 0 \exists q, r:$ $a = q \cdot b + r \ \wedge\ (r = 0 \vee \delta(r) < \delta(b))$ **Bsp:** $\mathbb{Z}, \mathbb{Z}[i]$, keine Körper		

Beispiel 26. Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell: Dafür zeigen wir, dass es darin ein irreduzibles Element gibt, das nicht prim ist. Die Normabbildung $N: R \to \mathbb{N}$ mit $x + y\sqrt{-5} \mapsto x^2 + 5y^2$ ist multiplikativ, woraus $a \mid b \Rightarrow N(a) \mid N(b)$ und $a \in R^\times \Leftrightarrow N(a) = 1$ folgt. Das Element 2 ist nicht prim, da $2 \mid 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, aber 2 keinen der beiden Faktoren teilt, da $N(2) = 4$ nicht $N(1 \pm \sqrt{-5}) = 6$ teilt. Andererseits ist 2 irreduzibel: Es gilt $2 \neq 0$ und wegen $N(2) = 4 \neq 1$ ist 2 keine Einheit. Gilt $2 = ab$ so folgt $4 = N(2) = N(a)N(b)$ und sind a und b Nichteinheiten, folgt $2 = N(a) = x^2 + 5y^2$, was für $x, y \in \mathbb{Z}$ nicht lösbar ist.

- Ist R ein faktorieller Ring und P ein Repräsentatensystem der Primelemente bzgl. der Äquivalenzrelation der Assoziiertheit (also z.B. die Primzahlen in $\mathbb{Z}$), so hat jedes $a \neq 0$ eine **eindeutige Darstellung**

$$a = u_a \cdot \prod_{p \in P} p^{v_p(a)}$$

für eine Einheit u_a. Für Elemente $a_1, \ldots, a_n \neq 0$ definiert man

$$\text{ggT}(a_1, \ldots, a_n) := \textstyle\prod_{p \in P} p^{\min\{v_p(a_1), \ldots, v_p(a_n)\}} \qquad \text{und} \qquad \text{kgV}(a_1, \ldots, a_n) := \textstyle\prod_{p \in P} p^{\max\{v_p(a_1), \ldots, v_p(a_n)\}}$$

als deren **größten gemeinsamen Teiler** und deren **größtes gemeinsames Vielfaches**. Diese Elemente erfüllen auch die offensichtliche allgemeine Definition eines größten gemeinsamen Teilers bzw. eines kleinsten gemeinsamen Vielfachen. Es gilt offenbar $\text{ggT}(a,b) \cdot \text{kgV}(a,b) = ab$ und in einem Hauptidealring gilt

$$(\text{ggT}(a_1, \ldots, a_n)) = (a_1, \ldots, a_n) \qquad \text{und} \qquad (\text{kgV}(a_1, \ldots, a_n)) = (a_1) \cap \ldots \cap (a_n).$$

Für den Fall $n = 2$ gibt es also $\lambda, \mu \in R$ mit $\text{ggT}(a,b) = \lambda a + \mu b$, was auch der **Satz von Bézout** genannt wird.

Beispiel 27. Für $n = 3$ setzt man die obige Darstellung für $n = 2$ in $\text{ggT}(a,b,c) = \text{ggT}(\text{ggT}(a,b),c) = \alpha\,\text{ggT}(a,b) + \beta c = \alpha\lambda a + \alpha\mu b + \beta c$ ein.

- In einem euklidischen Ring kann man $\text{ggT}(a,b) \in R$ (bis auf Assoziiertheit) und die Elemente $\lambda, \mu \in R$ in dem obigen Satz von Bézout systematisch mit dem **Euklidischen Algorithmus** bestimmen: Setzt man $a_1 := a$ und $a_2 := b$ bekommt man durch wiederholtes Anwenden der Division mit Rest (hier im Beispiel mit 3 Schritten)

$$\begin{array}{rcl} a_1 & = & q_1\, a_2 + a_3 \\ a_2 & = & q_2\, a_3 + \boxed{a_4} \\ a_3 & = & q_3\, a_4 + 0 \end{array}$$

und es ist $\boxed{a_4}$ der ggT von a und b (bis auf Assoziiertheit).

Formt man die obigen Gleichungen „nach a_4“ um, so erhält man (was manchmal auch „erweiterter Euklidischer Algorithmus“ genannt wird)

$$\boxed{a_4} = a_2 - q_2 a_3 = a_2 - q_2(a_1 - q_1 a_2) = (-q_2)a_1 + (1 + q_1 q_2)a_2,$$

also eine Darstellung aus dem Satz von Bézout.

Beispiel 28. Ein Inverses zu $[a]_n \in \mathbb{Z}/n$ kann man genau dann finden, wenn $\mathrm{ggT}(n,a) = 1$ explizit ist dieses dann durch eine Darstellung aus dem Satz von Bézout gegeben als $[1]_n = [\lambda n + \mu a]_n = [\lambda n]_n + [\mu a]_n = [\mu]_n [a]_n$.

- Nach dem **Chinesischen Restsatz** gibt es für teilerfremde n und m einen Ringisomorphismus

$$\begin{array}{rcl} \mathbb{Z}/n \times \mathbb{Z}/m & \to & \mathbb{Z}/nm \\ ([a]_n, [b]_m) & \mapsto & [a\mu m + b\lambda n]_{nm} \\ ([c]_n, [c]_m) & \leftarrow\!\shortmid & [c]_{nm} \end{array}$$

wobei $1 = \lambda n + \mu m$ eine (beliebige) Darstellung aus dem Satz von Bézout ist.

Aufgabe (F11T2A1). Um die Lösungen $x \in \mathbb{Z}$ des Systems

$$\begin{array}{ll} x \cong 1 & \mod 2 \\ x \cong 2 & \mod 3 \\ x \cong 3 & \mod 5 \end{array}$$

zu bestimmen benutzen wir (zweimal) den Chinesischen Restsatz $(\mathbb{Z}/2 \times \mathbb{Z}/3) \times \mathbb{Z}/5 \cong \mathbb{Z}/6 \times \mathbb{Z}/5 \cong \mathbb{Z}/30$. Die Darstellungen $1 = (-1)\cdot 2 + 1\cdot 3$ und $1 = 1\cdot 6 + (-1)\cdot 5$ bekommen wir durch Raten oder durch den Euklidischen Algorithmus wie oben. Damit ist

$$(([a]_2, [b]_3), [c]_5) \mapsto (([a\cdot 1\cdot 3 + b\cdot(-1)\cdot 2]_6, [c]_5) \mapsto [(3a - 2b)\cdot(-1)\cdot 5 + c\cdot 1\cdot 6]_{30} = [10b - 15a + 6c]_{30} = [20 - 15 + 18]_{30} = [23]_{30}$$

Also sind $x \in 23 + 30\mathbb{Z}$ die gesuchten Lösungen.

- Die (eindeutig bestimmte) natürliche Zahl n mit $(n) = \ker(\mathbb{Z} \to R)$ heißt **Charakteristik** $\mathrm{char}(R)$ des Rings R. (Diese ist also Null genau dann, wenn eine Summe $1 + \ldots + 1$ von Einsen niemals Null wird und sonst die kleinste Anzahl socher Summanden.)

Beispiel 29.

- $\mathrm{char}(\mathbb{Z}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = 0$ und $\mathrm{char}(\mathbb{Z}/n) = n$.
- Es ist $R = (0)$ der einzige Ring mit $\mathrm{char}(R) = 1$.
- Ein Integritätsbereich (also z.B. ein Körper) der Charakteristik > 0 hat eine prime Charakteristik, denn aus $n \cdot 1 = (a \cdot b) \cdot 1 = (a \cdot 1) \cdot (b \cdot 1)$ folgte $a = 0$ oder $b = 0$, was ein Widerspruch zur Minimalität von n wäre.

- Ist $\mathrm{char}(R) = p$ eine Primzahl, so ist die Mengenabbildung $\begin{array}{rcl} R & \to & R \\ a & \mapsto & a^p \end{array}$ ein Ringhomomorphismus und heißt der **Frobenius**. (Nach dem kleinen Satz von Fermat ist der Frobenius auf $\mathbb{Z}/p$ sogar die Identität.) Ist R ein Integritätsbereich, so ist der Frobenius injektiv. Ist dieser auch surjektiv, so heißt R **perfekt**.

- Für einen Integritätsbereich R kann man die Konstruktion $R = \mathbb{Z} \subseteq \mathbb{Q}$ generalisieren und definiert den **Quotientenkörper** $\mathrm{Quot}(R)$ als die Menge $(R \times R \setminus \{0\})/\sim$ mit $(a,b) \sim (c,d) \Leftrightarrow ad = cb$ und der zu der von $\mathbb{Q}$ analogen Addition und Multiplikation. Man schreibt $\frac{a}{b} := [(a,b)]$ und es gibt einen injektiven Ringhomomorphismus

$$\begin{array}{rcl} R & \hookrightarrow & \mathrm{Quot}(R) \\ a & \mapsto & \frac{a}{1} \end{array}$$

und jeder injektive Ringhomomorphismus $R \hookrightarrow K$ in einen anderen Körper K faktorisiert automatisch darüber.

- Für einen Ring R ist der **Polynomring** $R[x]$ die Menge $\{a_\bullet : \mathbb{N} \to R \mid \text{fast alle } a_k \text{ sind Null}\}$ von Folgen mit Addition $(a_\bullet + b_\bullet)_k := a_k + b_k$, Multiplikation $(a_\bullet \cdot b_\bullet)_k := \sum_{i+j=k} a_i b_j$, Null $0 := (0,0,\ldots)$, Eins $1 := (1,0,\ldots)$ und injektivem Ringhomomorphismus
$$\begin{aligned} R &\hookrightarrow R[x] \\ a &\mapsto (a,0,\ldots), \end{aligned}$$
dessen Elemente $a_\bullet$ **Polynome** genannt werden. Man setzt $x := (0,1,0,\ldots)$ und schreibt $a_\bullet = \sum_k a_k x^k$. Die mit dieser Definition triviale Tatsache, dass zwei Polynome gleich sind genau dann, wenn alle ihre Koeffizienten a_k jeweils gleich sind, wird manchmal **Koeffizientenvergleich** genannt.

- Man definiert $R[x,y] := (R[x])[y]$ ($\cong (R[y])[x]$), etc. für mehrere Variablen. Ein Element $f \in R[x_1,\ldots,x_n]$ kann eindeutig als
$$f = \sum_{(k_1,\ldots,k_n)=k} a_k x_1^{k_1} \cdots x_n^{k_n}$$
geschrieben werden.

- Der **Grad** ist
$$\begin{aligned} \deg\colon R[x] &\to \mathbb{N} \cup \{-\infty\} \\ f &\mapsto \begin{cases} -\infty \text{ falls } f = 0, \text{ sonst} \\ \text{größtes } k \text{ mit } a_k \neq 0 \end{cases} \end{aligned}$$
und es gilt
  - $\deg(f) = 0 \Leftrightarrow f$ ist konstant und $\neq 0$,
  - $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$,
  - $\deg(fg) \leq \deg(f) + \deg(g)$ mit Gleichheit, falls R ein Integritätsbereich ist oder f oder g normiert,

  wobei ein Polynom $f = \sum a_k x^k \neq 0$ **normiert** heißt, falls $a_{\deg(f)} = 1$ gilt. (Insbesondere ist dann $f \neq 0$.)

- $R[x]$ ist Integritätsbereich $\Leftrightarrow$ R ist Integritätsbereich. In diesem Fall gilt für die Einheiten $R[x]^\times = R^\times$.

- $R[x]$ ist Hauptidealring $\Leftrightarrow$ R ist Körper $\Leftrightarrow$ $R[x]$ ist euklidisch (mit $\delta = \deg$).

Beispiel 30. $\mathbb{Z}[x]$ ist kein Hauptidealring, da $\mathbb{Z}$ kein Körper ist.

- R ist faktoriell $\Leftrightarrow$ $R[x]$ ist faktoriell (Lemma von Gauß).

- Obwohl $R[x]$ nicht immer ein euklidischer Ring ist, kann man **durch ein normiertes Polynom dividieren**: Sind $f, g \in R[x]$ und g normiert, so gibt es $q, r \in R[x]$ mit $f = q \cdot g + r$ und $(r = 0 \vee \deg(r) < \deg(g))$.

- Ein $a \in R$ ist eine **Nullstelle** (oder **Wurzel**) von f
$$\begin{aligned} &\Leftrightarrow f(a) = 0 \\ &\Leftrightarrow f \in (x-a) \\ &\Leftrightarrow f = (x-a) \cdot h \quad \text{für ein } h \in R[x] \text{ mit } \deg(h) < \deg(f) \end{aligned}$$

- In einem Integritätsbereich hat f höchstens $\deg(f)$-viele Nullstellen.

Beispiel 31.

- Es kann (in einem Nicht-Integritätsbereich) sein, dass es mehr als $\deg(f)$-viele Nullstellen gibt. Beispielsweise gilt in $R = \mathbb{Z}/8$, dass $(x-3)(x-5) = x^2 - 1 = (x-1)(x-7)$.
- In $R = \mathbb{R}$ hat $x^2 + 1$ keine Nullstellen.

Sei R ein Integritätsbereich. (Zur Erinnerung: Ein Polynom f aus $R[x]$ mit $\deg(f) \geq 1$ ist keine Einheit.)

- **Linearfaktoren** $(x-a)$, also normierte Polynome vom Grad 1, **sind irreduzibel** in $R[x]$.
- Wollen wir die Irreduzibilität eines Polynoms $f \neq 0$ in $K[x]$ für einen Körper K untersuchen, können wir immer annehmen, dass das Polynom normiert ist, da Irreduzibilität unter Assoziiertheit invariant ist und wir durch den Leitkoeffizienten $a_{\deg(f)}$ teilen können. Auch die Eigenschaft, eine Nullstelle zu haben, ändert sich unter diesem Normierungsprozess nicht.
- Für $f \in R[x]$ normiert gilt: $\underset{\text{(und folglich } \deg(f)\geq 1)}{f \text{ hat Nullstelle}} \implies \underset{\text{(da } f=(x-a)\cdot h \text{ mit } \deg(h)\geq 1)}{f \text{ ist nicht-irreduzibel}} \vee f \text{ ist Linearfaktor}$
- Sei R faktoriell mit Quotientenkörper K und $f \in R[x]$ nicht-konstant. Dann gilt das **Lemma von Gauß**

$$f \text{ irreduzibel in } R[x] \iff f \text{ irreduzibel in } K[x] \wedge \underset{\substack{\text{d.h. der ggT der Koeffizienten ist = 1}\\ \text{(also z.B. bei normiertem } f)}}{f \text{ ist \textbf{primitiv}}}$$

(wobei „⇒“ die nicht-triviale Richtung ist).

Wir wollen im Folgenden die Irreduzibilität eines Polynoms $f = \underbrace{a_n}_{\neq 0} x^n + \ldots + a_0$ mit R-Koeffizienten in $R[x]$ und in $K[x]$ untersuchen, wobei $K := \mathrm{Quot}(R)$.

- Nullstellentest R faktoriell und $\frac{a}{s} \in K$ gekürzte Nullstelle von $f \implies a \mid a_0$ und $s \mid a_n$ in R

Beispiel 32. Das Polynom $f = x^3 + x + 1 \in \mathbb{Q}[x]$ hat keine Nullstellen, da nach dem Nullstellentest nur $a = \pm 1$ dafür in Frage kämen, aber $f(\pm a) \neq 0$ gilt. Also „enthält“ das Polynom keinen Linearfaktor, lässt sich also nicht als $f = (x-a)\cdot h$ mit schreiben. Damit folgt schon, dass f irreduzibel ist, denn wäre $f = gh$ für nicht-Einheiten g und h, folgt $\deg(g) \geq 1$ und $\deg(h) \geq 1$, was sich aber nur dann zu $\deg(f) = 3$ addieren könnte, wenn $\deg(g) = 1$ oder $\deg(h) = 1$ wäre.

- Eisenstein Sei R faktoriell, $n \geq 2$, f primitiv und $p \in R$ Primelement. Dann ist $f \in R[x]$ irreduzibel, falls gilt:

$$p \text{ teilt } a_{n-1}, \ldots, a_0 \quad \wedge \quad p^2 \text{ teilt nicht } a_0 \quad \wedge \quad p \text{ teilt nicht } a_n \quad \text{(z.B. } f \text{ normiert)}$$

Beispiel 33. Das Polynom $f = x^n - p$ in $\mathbb{Z}[x]$ mit $n \geq 2$ und einer Primzahl p ist irreduzibel in $\mathbb{Z}[x]$ nach Einsenstein zur Primzahl p und nach dem Lemma von Gauß auch in $\mathbb{Q}[x]$. Daher hat $x^n - p$ keine Nullstelle in $\mathbb{Q}$ und wir haben auf diese Weise gezeigt, dass $\sqrt[n]{p} \notin \mathbb{Q}$.

- Verschiebekriterium Für $c \in R$ gilt: $f \in R[x]$ irreduzibel $\iff f((-)-c) \in R[x]$ irreduzibel

Beispiel 34. Das Polynom $f = x^{p-1} + \ldots + x + 1$ in $\mathbb{Z}[x]$ mit einer Primzahl p ist irreduzibel in $\mathbb{Z}[x]$ (und nach dem Lemma von Gauß auch in $\mathbb{Q}[x]$), denn wegen

$$f(x) = \frac{x^p - 1}{(x-1)} \quad \text{ist} \quad f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-1},$$

was nach Eisenstein zur Primzahl p irreduzibel ist. Also ist nach dem Verschiebekriterium auch f irreduzibel.

- Reduktionskriterium Ist $\varphi: R \to S$ ein Ringhomomorphismus in einen Integritätsbereich S mit $\varphi(a_n) \in S^\times$ (z.B. f normiert), so gilt

$$f \in R[x] \text{ irreduzibel} \impliedby f^\varphi \in S[x] \text{ ist irreduzibel}$$

wobei f^φ das Bild von f unter dem induzierten Ringhomomorphismus $R[x] \to S[x]$ bezeichnet, also das Polynom $f^\varphi := \varphi(a_n)x^n + \ldots + \varphi(a_0)$, also φ angewandt auf die Koeffizienten.

Beispiel 35. Es ist $f = x^5 - x - 1$ in $\mathbb{Z}[x]$ (und nach Gauß auch in $\mathbb{Q}[x]$) irreduzibel nach dem Reduktionskriterium, da das „reduzierte Polynom“ $f^\varphi \in \mathbb{Z}/5[x]$ keine Nullstellen in $\mathbb{Z}/5$ hat (was man leicht durch Einsetzen der endlich vielen Elemente $0, 1, 2, 3, 4$ sieht) und auch keine quadratischen Faktoren: Die einzigen quadratischen Polynome in $\mathbb{Z}/5[x]$ ohne Nullstellen (Nullstellen von Faktoren von f wären auch Nullstellen von f, aber f hat keine Nullstellen) sind x^2+1, x^2+x+1 und x^2-x-1 und f ist kein Produkt aus diesen.
Es kann allerdigs sein, dass f^φ in einem anderen $\mathbb{Z}/n[x]$ reduzibel wird. So gilt in $\mathbb{Z}/2[x]$ beispielsweise: $x^5 - x - 1 = (x^2+x+1)(x^3+x^2+1)$.

Sei K ein Körper.

- Jeder Ringhomomorphismus $K \to R \neq 0$ in einen nicht-trivialen Ring ist injektiv und damit insbesondere jeder Körperhomomorphismus $\varphi: K \hookrightarrow L$ (dieses ist ein Ringhomomorphismus zwischen Körpern K und L). Es ist $\varphi(K)$ ein Körper und man nennt $\varphi(K) \subseteq L$ eine Körpererweiterung. Manchmal identifiziert man K mit seinem isomorphen Bild $\varphi(K)$ und schreibt $K \subseteq L$.

- Die Charakteristik eines Körpers K ist Null oder eine Primzahl. Im ersten Fall gilt $\mathbb{Q} \subseteq K$ und im zweiten $\mathbb{Z}/p \subseteq K$ und den jeweils kleinen Körper nennt man den **Primkörper** von K.

- Ist $K \subseteq L$ eine Körpererweiterung, so ist L mit der eingeschränkten Multiplikation ein K-Vektorraum und es heißt $[L:K] := \dim_K(L)$ der **Grad der Körpererweiterung**. Für Körpererweiterungen $K \subseteq M \subseteq L$ gilt die die **Gradformel**
$$[L:K] = [L:M] \cdot [M:K].$$

Sei nun $K \subseteq L$ eine vorgegebene Körpererweiterung.

- Sind $\alpha_1, \ldots, \alpha_n \in L$ Elemente, so definiert man
$$\begin{aligned} K[\alpha_1,\ldots,\alpha_n] &:= \text{Kleinster } \textbf{Unterring} \text{ von } L, \text{ der } K \text{ und } \alpha_1,\ldots,\alpha_n \text{ enthält} \\ &= \{\, f(\alpha_1,\ldots,\alpha_n) \in L \mid f \in K[x_1,\ldots,x_n] \,\} \\ K(\alpha_1,\ldots,\alpha_n) &:= \text{Kleinster } \textbf{Unterkörper} \text{ von } L, \text{ der } K \text{ und } \alpha_1,\ldots,\alpha_n \text{ enthält} \\ &= \operatorname{Quot}(K[\alpha_1,\ldots,\alpha_n]) \end{aligned}$$
und es gilt offenbar $K \subseteq K[\alpha_1,\ldots,\alpha_n] \subseteq K(\alpha_1,\ldots,\alpha_n) \subseteq L$.

- Ist $\alpha \in L$ und $\varphi_\alpha: K[x] \to L$ mit $x \mapsto \alpha$ der Einsetzhomomorphismus so gilt entweder
$$\begin{aligned} \varphi_\alpha \text{ ist injektiv} &\iff \alpha \text{ ist } \textbf{transzendent} \text{ über } K \\ &\iff K[x] \cong K[\alpha] \\ &\quad (\text{und } [K(\alpha):K] = \infty \text{ mit Basis } \alpha^{\mathbb{Z}}) \end{aligned}$$
oder
$$\begin{aligned} \varphi_\alpha \text{ ist nicht injektiv} &\iff \alpha \text{ ist } \textbf{algebraisch} \text{ über } K \\ &\iff \alpha \text{ ist Nullstelle eines Polynoms } f \neq 0 \text{ in } K[x] \\ &\iff \operatorname{Kern}(\varphi_\alpha) = (m_\alpha) \text{ für ein (folglich eindeutiges) normiertes Polynom } m_\alpha \in K[x], \\ &\quad \text{das } \textbf{Minimalpolynom (Mipo)} \text{ von } \alpha \text{ über } K, \text{ und es gilt:} \\ &\quad - \ m_\alpha \text{ ist irreduzibel} \\ &\quad - \ K[x]/(m_\alpha) \cong K[\alpha] = K(\alpha) \\ &\quad - \ [K(\alpha):K] = \deg(m_\alpha) < \infty \text{ mit Basis } 1, \alpha, \ldots, \alpha^{\deg(m_\alpha)-1} \end{aligned}$$
und für ein Polynom $f \in K[x]$ gilt
$$\begin{aligned} f \text{ ist Mipo von } \alpha \text{ über } K &\iff f(\alpha) = 0 \ \wedge \ f \text{ normiert} \ \wedge \ f \text{ irreduzibel} \\ &\iff f(\alpha) = 0 \ \wedge \ f \text{ normiert} \ \wedge \ [K(\alpha):K] = \deg(f) \end{aligned}$$

- Sind $K \subseteq M \subseteq L$ Körpererweiterungen, $\alpha \in L$, $m_\alpha^K \in K[x]$ das Mipo von α über K und $m_\alpha^M \in M[x]$ das Mipo von α über M, so gilt $m_\alpha^M \mid m_\alpha^K$ und insbesondere $[M(\alpha):M] \leq [K(\alpha:K)]$.

- Eine Körpererweiterung $K \subseteq L$ ist **algebraisch** $\iff$ Jedes Element $\alpha \in L$ ist algebraisch über K
$\impliedby$ $[L:K] \leq \infty$, d.h. $K \subseteq L$ ist eine **endliche** Körpererweiterung
$\iff$ Es gibt $\alpha_1,\ldots,\alpha_n \in L$, algebraisch über K, mit $L = K(\alpha_1,\ldots,\alpha_n)$

- Sind $K \subseteq M \subseteq L$ Körpererweiterungen, $K \subseteq M$ algebraisch und $\alpha \in L$ algebraisch über M, so ist α auch algebraisch über K. Insbesondere ist die Relation „$\subseteq$ algebraische Körpererweiterung“ transitiv.

Beispiel 36.

- $\mathbb{Q} \subseteq \mathbb{Q}(\pi)$ ist nicht algebraisch und also insbesondere keine endliche Körpererweiterung.
- Für $k \geq 2$ ist das normierte Polynom $x^k - 2 \in \mathbb{Q}[x]$ nach Eisenstein irreduzibel und hat Nullstelle $\sqrt[k]{2} \in \mathbb{R}$, also gilt $[\mathbb{Q}(\sqrt[k]{2}) : \mathbb{Q}] = k$ und nach dem Gradsatz $[\mathbb{R} : \mathbb{Q}] \geq \infty$.

- Ein Körper K ist **algebraisch abgeschlossen** $\iff$ Jedes nichtkonstante $f \in K[x]$ hat eine Nullstelle in K
  $\iff$ $f \in K[x]$ irreduzibel $\Leftrightarrow$ $\deg(f) = 1$
  $\iff$ Ist $K \subseteq L$ algebraische Körpererweiterung $\Rightarrow$ $K = L$

  Ein Körper $\overline{K}$ heißt **algebraischer Abschluss** von K, falls $K \subseteq \overline{K}$ eine algebraische Körpererweiterung ist und $\overline{K}$ algebraisch abgeschlossen. Ein Körper K hat einen (bis auf Isomorphie über K) eindeutigen algebraischen Abschluss, was aus dem Lemma von Zorn und den nächsten beiden Sätzen folgt.

Beispiel 37.

- Es ist $\mathbb{C}$ algebraisch abgeschlossen nach dem **Fundamentalsatz der Algebra** und der algebraische Abschluss von $\mathbb{R}$, da $\mathbb{R} \subseteq \mathbb{C}$ eine algebraische Körpererweiterung ist.
- Es ist $\mathbb{Q}$ nicht algebraisch abgeschlossen, da das Polynom $x^2 + 1 \in \mathbb{Q}[x]$ keine Nullstelle in $\mathbb{Q}$ hat.

- Kronecker Trick Ist K ein Körper und $f \in K[x]$ ein irreduzibles Polynom, so liefert die Komposition φ von Ringhomomorphismen

$$K \hookrightarrow K[x] \xrightarrow{p} K[x]/(f) =: L \quad (\varphi)$$

eine Körpererweiterung vom Grad $[L : K] = \deg(f)$ und das Polynom $f^\varphi \in L[x]$ hat die Nullstelle $[x] := p(x)$.

Beispiel 38. Das irreduzible Polynom $f := x^2 + 1$ aus $\mathbb{R}[x]$ hat mit Koeffizienten in $L := \mathbb{R}[x]/(f)$ die Form $f^\varphi = [1] \cdot x^2 + [1]$ und es gilt $f^\varphi([x]) = [1] \cdot [x]^2 + [1] = [1 \cdot x^2 + 1] = [f] = 0$. Achtung: $x \in L[x]$ und $[x] \in L$ sind verschiedene Elemente. Man könnte $i := [x]$ setzen und erhielte in $L[x]$, dass $f^\varphi = (x + i)(x - i)$.

- Fortsetzungssatz Sind $K \subseteq L$ und $K' \subseteq L'$ Körpererweiterungen (oft ist $K = K'$ und $L = L' = \overline{K}$) und $\sigma : K \xrightarrow{\cong} K'$ ein Isomorphismus, und $\alpha \in L$ algebraisch über K mit Mipo m_α, so gibt es eine Bijektion

$$\left\{ \begin{array}{c} \text{Vervollständigungen des Diagramms} \\ \begin{array}{ccc} L & & L' \\ \cup\!| & \overset{\varphi}{\nearrow} & \cup\!| \\ K(\alpha) & & K'(\varphi(\alpha)) \\ \cup\!| & & \cup\!| \\ K & \xrightarrow[\sigma]{\cong} & K' \end{array} \\ \text{durch Homomomorphismen } \varphi \\ \text{(diese faktorisieren dann eindeutig über Isos} \\ K(\alpha) \xrightarrow{\cong} K'(\varphi(\alpha)) \\ \text{auf ihr Bild } K'(\varphi(\alpha)) \text{ wie ins Diagramm eintragbar)} \end{array} \right\} \underset{\left(\sum_{i=0}^{n-1} \lambda_i \alpha^i \mapsto \sum_{i=0}^{n-1} \sigma(\lambda_i) \beta^i\right) \mapsfrom \beta}{\overset{\varphi \mapsto \varphi(\alpha) =: \beta}{\longrightarrow}} \left\{ \begin{array}{c} \text{Nullstellen } \beta \in L' \text{ von } m_\alpha^\sigma \\ (m_\alpha^\sigma \text{ ist automatisch das} \\ \text{Mipo von } \beta \text{ über } K') \end{array} \right\}$$

Beispiel 39.

- Es gibt keinen Isomorphismus $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$ über $\mathbb{Q}$, der $\sqrt{2}$ auf $\sqrt{3}$ abbildet, denn $\beta := \sqrt{3}$ ist keine Nullstelle von $m_\alpha = x^2 - 2$, wobei $\alpha := \sqrt{2}$. Es ist richtig (aber nicht unmittelbar klar), dass es überhaupt keinen Isomorphismus $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$ über $\mathbb{Q}$ gibt.
- Achtung: Es gilt $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2} + 1)$ (und es gibt daher trivialerweise einen Isomorphismus über $\mathbb{Q}$, die Identität), das Mipo von $\alpha := \sqrt{2}$ über $\mathbb{Q}$ ist $m_\alpha = x^2 - 2$ und das von $\beta := \sqrt{2} + 1$ ist $m_\beta = x^2 - 2x - 1$. Es ist β keine Nullstelle von m_α und nach dem Fortsetzungssatz gibt es also keinen Isomorphismus über $\mathbb{Q}$, der α auf β abbildet.
- Es gibt genau zwei Isomorphismen $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$ (hier ist $L = L' = \mathbb{C}$), denn es gibt genau die zwei Nullstellen $\pm\sqrt{2} \in \mathbb{C}$ von $m_\alpha = x^2 - 2$ und nach dem Fortsetzungssatz genau also zwei Homomomorphismen $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ über $\mathbb{Q}$. Diese induzieren zwei verschiedene Isomorphismen $\mathbb{Q}(\sqrt{2}) \xrightarrow{\cong} \mathbb{Q}(\sqrt{2})$ (die Identität) und $\mathbb{Q}(\sqrt{2}) \xrightarrow{\cong} \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2})$. (Es kann nicht mehr Homomomorphismen $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ geben, denn diese lieferten durch Komposition mit der Inklusion weitere Homomorphismen $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$.)
- Ist L' algebraisch abgeschlossen und $m_\alpha \in K[x]$ Minimalpolynom eines $\alpha \in L$, dann gibt es genau $\deg(m_\alpha)$-viele Homomorphismen $\varphi : K(\alpha) \to L'$ über σ.

Sei K ein Körper. (Mit einem „Homomorphismus“ zwischen Körpern ist immer ein Ringhomomorphismus gemeint.)

- Ist $f \in K[x]$ ein Polynom, das in einer Körpererweiterung L von K in Linearfaktoren zerfällt und die Nullstellen $\alpha_1, \ldots, \alpha_n \in L$ hat, so heißt
$$ZFK_K^L(f) := K(\alpha_1, \ldots, \alpha_n)$$
der **Zerfällungskörper** von f (über K in L). Es ist $K \subseteq K(\alpha_1, \ldots, \alpha_n)$ eine endliche (und folglich algebraische) Erweiterung vom Grad $\leq \deg(f)$!.
(Mit dem Fortsetzungssatz sieht man, dass zwei Zerfällungskörper für verschiedene L über K isomorph sind. Daher schreibt man auch $ZFK_K(f) := ZFK_K^L(f)$ und spricht weiterhin von *dem* Zerfällungskörper.)

- Analog definiert man den Zerfällungskörper für eine Menge $M \subseteq K[x]$ von Polynomen. Ist $M = \{f_1, \ldots, f_m\}$ eine endliche Menge, so ist der Zerfällungskörper $ZFK_K^L(M)$ dieser Menge genau $ZFK_K^L(f_1 \cdot \ldots \cdot f_m)$.

- Der Zerfällungskörper von f ist (per Definition) der kleinste Körper über K, in dem f in Linearfaktoren zerfällt.

Beispiel 40.

- Es ist $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i) = ZFK_{\mathbb{R}}^{\mathbb{C}}(x^2 + 1)$.
- Es ist $ZFK_{\mathbb{Q}}^{\mathbb{C}}(x^2 - 1) = \mathbb{Q}(\sqrt{2}) \neq \mathbb{R} = ZFK_{\mathbb{R}}^{\mathbb{C}}(x^2 - 1)$, der Zerfällungskörper eines Polynoms hängt also von K ab.

- Eine Körpererweiterung $K \subseteq L$ heißt **normal** $\Leftrightarrow$ $L \cong_K ZFK_K(M)$ für eine Menge $M \subseteq K[x]$
  $\Leftrightarrow$ Die Mipos aller $\alpha \in L$ (über K) zerfallen in Linearfaktoren und $K \subseteq L$ ist algebraisch
  $\Leftrightarrow$ Jedes irreduzible Polynom $f \in K[x]$ mit einer Nullstelle in L zerfällt in L in Linearfaktoren und $K \subseteq L$ ist algebraisch

Beispiel 41.

- Es ist $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ nicht normal, da $x^3 - 2$ nur eine Nullstelle in $\mathbb{Q}(\sqrt[3]{2})$ hat.
- Jede Körpererweiterung vom Grad = 2 ist normal.

- Die Relation „$\subseteq$ ist normale Körpererweiterung“ ist nicht transitiv, aber es gilt, dass für eine Kette algebraischer Körpererweiterungen $K \subseteq M \subseteq L$ mit $K \subseteq L$ normal auch $M \subseteq L$ normal ist.

Beispiel 42.

- Es ist $ZFK_{\mathbb{Q}}(f := x^4 - 5x^2 + 6) \cong \mathbb{Q}(\sqrt{2} + \sqrt{3})$, denn:
  - $f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ hat die Nullstellen $N := \{\pm\sqrt{2}, \pm\sqrt{3}\} \subseteq \mathbb{C}$ und per Definition ist $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong ZFK_{\mathbb{Q}}(f)$.
  - Es gilt $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, wobei „$\subseteq$“ klar ist und wir für „$\supseteq$“ zeigen müssen, dass $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Mit der dritten binomischen Formel gilt aber $(\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3}) = 2 - 3 \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ und, da man in einem Körper „teilen kann“ gilt folglich $(\sqrt{2} - \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Damit ist auch $(\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, also auch $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ und schließlich $(\sqrt{2} + \sqrt{3}) - \sqrt{2} = \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

  Um übrigens das Mipo von $\alpha := \sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$ zu finden, finden wir zunächst (durch Quadrieren, $\alpha^2 = \ldots$, etc.) ein normiertes Polynom $g := x^4 - 10x^2 + 1$ in $\mathbb{Q}[x]$ mit α als Nullstelle. Anstatt nun direkt zu zeigen, dass g irreduzibel ist (und damit das Mipo von α), können wir auch $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ mit dem Gradsatz
$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]}_{> 1 \text{ da } \sqrt{3} \notin \mathbb{Q}(\sqrt{2})} \cdot \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{=2} \quad \geq \quad 4$$
benutzen und sehen, dass das Mipo, welches g teilen muss, Grad ≥ 4 hat und damit schon g selber ist.

Sei K ein Körper, $K \subseteq L$ eine Körpererweiterung und bezeichne $f' \in K[x]$ die formale Ableitung eines $f \in K[x]$.

- Ein $\alpha \in L$ ist **mehrfache Nullstelle** von $f \in K[x] \iff f(\alpha) = 0 \ \wedge \ f'(\alpha) = 0$
- Ein Polynom $f \in K[x]$ heißt **separabel** $\Leftrightarrow$ Alle Nullstellen $\alpha_1, \dots, \alpha_n \in \overline{K}$ sind verschieden
  $\Leftrightarrow$ Alle Nullstellen $\alpha_1, \dots, \alpha_n \in L$ sind verschieden in einer beliebigen Körpererweiterung $K \subseteq L$, in der f in Linearfaktoren zerfällt

  (Und folglich gilt in den äquivalenten Fällen $n = \deg(f)$).

  Bemerkung 43. Es gibt eine veraltete Definition, mit der ein Polynom separabel heißt, wenn alle seine irreduziblen Faktoren separabel sind im obigen Sinn. Diese beiden Definitionen sind natürlich äquivalent, wenn f ein irreduzibles Polynom ist.

- Ein irreduzibles Polynom $f \in K[x]$ ist separabel $\iff f' \neq 0$

  Da in einem Körper der Charakteristik $\mathrm{char}(K) = 0$ gilt, dass $f' \neq 0$ für jedes nicht-konstante Polynom $f \in K[x]$, ist hier **jedes irreduzible Polynom separabel**.

  Beispiel 44.
  - Das Polynom $x^3 - 3x + 2 = (x-1)^2(x+2)$ in $\mathbb{Q}[x]$ ist nicht separabel, da 1 eine doppelte Nullstelle ist.
  - Das Polynom $x^3 - 2$ in $\mathbb{Q}[x]$ ist separabel (und irreduzibel).
  - Das Polynom $x^3 - 2$ in $\mathbb{F}_3[x]$ ist nicht separabel, da hier $x^3 - 2 = (x+1)^3$ gilt.
  - Das Polynom $x^p - t = f$ in $\mathbb{F}_p(t) := \mathrm{Quot}(\mathbb{F}_p[t])$ ist irreduzibel (nach Eisenstein mit dem Primelement t) aber nicht separabel, da $f' = px^{p-1} = 0$ gilt. (Es ist der unendliche Körper $\mathbb{F}_p(t)$ der Charakteristik p ein Beispiel eines nicht-perfekten Körpers, s.u.)

- Eine Körpererweiterung $K \subseteq L$ heißt **separabel** $\Leftrightarrow$ Das Mipo jedes $\alpha \in L$ über K ist separabel
  (Falls $L = K(\alpha_1, \dots, \alpha_n)$ für algebraische α_i gilt: $\Leftrightarrow$ Das Mipo jedes α_i über K ist separabel)

- Ein Körper K heißt **perfekt** $\Leftrightarrow$ Jedes irreduzible $f \in K[x]$ ist separabel
  $\Leftrightarrow$ Jede algebraische Erweiterung von K ist separabel.
  $\Leftrightarrow$ $\mathrm{char}(K) = 0$ oder
  $\mathrm{char}(K) = p$ und der Frobenius $\begin{array}{ccc} K & \to & K \\ a & \mapsto & a^p \end{array}$ ist surjektiv (folglich bijektiv).

  Insbesondere ist also **jeder Körper der Charakteristik Null und jeder endliche Körper perfekt**.

Sei K ein Körper.

- Ist $K \subseteq L$ eine Körpererweiterung, so nennt man die Gruppe (bzgl. $\circ$)

$$\mathrm{Gal}(L:K) := \{\ \varphi: L \xrightarrow{\cong} L \ \text{ Körperiso } \mid \varphi(\lambda) = \lambda \text{ für alle } \lambda \in K\ \}$$

die **Galoisgruppe** der Körpererweiterung. (Diese wird auch mit $\mathrm{Aut}_K(L)$ bezeichnet.)

Beispiel 45.

- Es gilt immer $\mathrm{Gal}(K:K) = \{\mathrm{id}\}$.
- Es gilt $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) = \{\mathrm{id}, \varphi\} \cong \mathbb{Z}/2$ wie in Beispiel 39 mit dem Fortsetzungssatz gezeigt wurde.
- Es gilt $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}) = \{\mathrm{id}\}$, denn nach dem Fortsetzungssatz entsprechen die Isomorphismen $\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\cong} \mathbb{Q}(\sqrt[3]{2})$ genau der Anzahl der Nullstellen des Minimalpolynoms $m_\alpha = x^3 - 2 \in \mathbb{Q}[x]$ in $\mathbb{C}$, welche tatsächlich in $\mathbb{Q}(\sqrt[3]{2})$ liegen. Dieses ist aber wegen $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ und der bekannten Struktur von $\mathbb{C}$ nur eine, nämlich $\sqrt[3]{2}$.

- **Nullstellenpermutationslemma** Ist $f \in K[x]$ ein Polynom und $K \subseteq L$ eine Körpererweiterung, so gibt es einen Gruppenhomomorphismus

$$\begin{aligned} \mathrm{Gal}(L:K) &\xrightarrow{\quad per \quad} S_{\{\text{Nullstellen von } f \text{ in } L\}} \\ \varphi &\longmapsto (\ \alpha \mapsto \varphi(\alpha)\ ) \end{aligned}$$

(d.h. insbesondere permutiert ein Element der Galoisgruppe die Nullstellen von f in L).
Falls $L = K(\alpha_1, \ldots, \alpha_n)$ der Zerfällungskörper von f ist mit $\{\text{Nullstellen von } f \text{ in } L\} = \{\alpha_1, \ldots, \alpha_n\}$ (Achtung: Dieses ist eine *Menge* und doppelte Nullstellen von f werden daher nur einmal aufgelistet), so ist diese Abbildung **injektiv** und es gilt

$$\mathrm{Bild}(per) = \left\{ \varphi \in S_{\{\alpha_1,\ldots,\alpha_n\}} \;\middle|\; \begin{array}{l}\text{Für alle Polynome } g \in K[x_1,\ldots,x_n] \text{ mit } g(\alpha_1,\ldots,\alpha_n) = 0 \\ \text{folgt auch } g(\varphi(\alpha_1),\ldots,\varphi(\alpha_n)) = 0.\end{array} \right\}. \qquad (*)$$

Bemerkung 46. Die Beweisidee für das Nullstellenpermutationslemma (dieses ist kein offizieller Name) ist wie folgt: Es ist einfach zu sehen, dass ein φ Nullstellen in Nullstellen überführt. Weil φ ein Isomorphismus ist, induziert es also eine Permutation der Nullstellen. Ist nun $L = K(\alpha_1, \ldots, \alpha_n)$ der Zerfällungskörper, so ist die Injektivität einfach zu sehen, denn ein Isomorphismus $K(\alpha_1, \ldots, \alpha_n) \to K(\alpha_1, \ldots, \alpha_n)$ über K ist schon durch $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ eindeutig festgelegt (siehe Definition von $K(\alpha_1, \ldots, \alpha_n)$). Für die Aussage über das Bild sei $\varphi: L \to L$ aus $\mathrm{Gal}(L:K)$ gegeben und betrachte das (solide) Diagramm

$$\begin{array}{ccc} K[x_1,\ldots,x_n] & \xrightarrow{\ \epsilon\ } & K(\alpha_1,\ldots,\alpha_n) \\ & \searrow^{\epsilon'} & \downarrow \\ & & K(\varphi(\alpha_1),\ldots,\varphi(\alpha_n)) \end{array}$$

mit Einsetzhomomorphismen ϵ: $x_i \mapsto \alpha_i$ und ϵ': $x_i \mapsto \varphi(\alpha_i)$. Die Bedingung in der rechten Menge von $(*)$ ist genau die Bedingung $\mathrm{Kern}(\epsilon) \subseteq \mathrm{Kern}(\epsilon')$, was nach dem Homomorphiesatz äquivalent zu der Existenz der gestrichelten Abbildung ist (die dann automatisch ein Isomorphismus ist). Diese Abbildung existiert aber als Einschränkung von φ und die andere Inklusion folgt genauso.

Bemerkung 47. Man braucht für das Nullstellenpermutationslemma in der obigen Form (vielleicht überraschenderweise) keine Separabilität von f. Diese würde aber implizieren, dass alle Nullstellen $\alpha_1, \ldots, \alpha_n$ verschieden sind. Das subtile Problem bei nicht-separablen Polynomen wie $(x^2-2)^2$ aus $\mathbb{Q}[x]$ mit Nullstellen $\alpha_1, \alpha_2 := \sqrt{2}$, $\alpha_3, \alpha_4 := -\sqrt{2}$ in $\mathbb{C}$ ist, dass $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_3)$ und Körperisomorphismen φ: $L \xrightarrow{\cong} L$ somit keinen Unterschied zwischen α_1 und α_2 (bzw. α_3 und α_4) machen können.

- Ist $f \in K[x]$ ein Polynom, so nennt man $\mathrm{Gal}(f) := \mathrm{Gal}(ZFK_K(f):K)$ die **Galoisgruppe des Polynoms**.

Beispiel 48. Ist f ein separables Polynoms vom Grad n, so können wir nach dem Nullstellenpermutationslemma, die Galoisgruppe $\mathrm{Gal}(f)$ als genau die Untergruppe der S_n auffassen (und insbesondere gilt $|\mathrm{Gal}(f)| \leq n!$), die der Bedingung der rechten Site von $(*)$ genügt. Dieses ist die **klassische Sichtweise auf die Galoistheorie**: Das Polynom $f = x^2 - 2x - 1$ aus $\mathbb{Q}[x]$ hat die Nullstellen $\alpha_1 = 1 + \sqrt{2}$ und $\alpha_2 = 1 - \sqrt{2}$ in $\mathbb{C}$ und die Galoisgruppe ist eine Untergruppe von S_2. (In diesem Fall enthält sie also maximal zwei Permutationen: id und φ (welche α_1 und α_2 vertauscht).) Wie kann man nun sagen, dass eine Permutation $\varphi \in S_2$ *nicht* zur Galoisgruppe gehört? Zwischen den Nullstellen gibt es Relationen über $\mathbb{Q}$, wie beispielsweise

$$\alpha_1\alpha_2 + 1 = 0 \qquad (\text{aber auch } \alpha_1 + \alpha_2 - 2 = 0, \text{ etc.})$$

oder genauer gesagt $g(\alpha_1, \alpha_2) = 0$ für das Polynom $g := x_1x_2 + 1 = 0$ aus $\mathbb{Q}[x_1, x_2]$. Die Bedingung $(*)$ sagt nun, dass nach Anwenden einer Permutation φ aus der Galoisgruppe auf die Nullstellen, diese Relationen immer noch gelten müssen, was in in diesem Fall bedeutet, dass $g(\varphi(\alpha_1), \varphi(\alpha_2)) = g(\alpha_2, \alpha_1) = 0$. In diesem Beispiel gibt es tatsächlich keine Einschränkung an die Permutationen und es gilt $\mathrm{Gal}(f) = S_2$.

Beispiel 49. Wir zeigen, dass die Galoisgruppe des Polynoms $f = x^4 - 2$ aus $\mathbb{Q}[x]$ die Diedergruppe D_4 ist. Das Polynom f ist irreduzibel nach Eisenstein und hat die Nullstellen

$$\alpha_1 := \sqrt[4]{2}, \qquad \alpha_2 := -\sqrt[4]{2}, \qquad \alpha_3 := i\sqrt[4]{2}, \qquad \alpha_4 := -i\sqrt[4]{2}$$

in $\mathbb{C}$ und es ist $L := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ der Zerfällungskörper von f. (Man kann die Nullstellen nicht immer bestimmen und kann oft trotzdem die Galoisgruppe angeben. Wir haben in diesem Beispiel also viel Information.) Wir wollen alle Elemente $\varphi\colon L \xrightarrow{\cong} L$ der Galoisgruppe mit dem Fortsetzungssatz konstruieren:

- Da f Mipo eines jeden α_i ist, gibt es für jedes $i \in \{1,2,3,4\}$ nach dem Fortsetzungssatz genau einen Isomorphismus

$$\begin{array}{ccc} \mathbb{Q}(\alpha_1) & \xrightarrow[\cong]{\varphi_i} & \mathbb{Q}(\alpha_i) \\ \cup\!| & & \cup\!| \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$

- Sei nun ein $\varphi_i\colon \mathbb{Q}(\alpha_1) \xrightarrow{\cong} \mathbb{Q}(\alpha_i)$ gegeben. Da $\alpha_2 = -\alpha_1$ gilt, gibt es keine Wahl für eine Fortsetzung $\varphi_{ij}\colon \mathbb{Q}(\alpha_1, \alpha_2) \xrightarrow{\cong} \mathbb{Q}(\alpha_i, \alpha_j)$ von φ_i, denn $\varphi_{ij}(\alpha_2) = \varphi_{ij}(-\alpha_1) = -\varphi_{ij}(\alpha_1) = -\varphi_i(\alpha_1) = -\alpha_i =: \alpha_j$.

- Um eine Fortsetzung $\varphi_{ijk}\colon \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \xrightarrow{\cong} \mathbb{Q}(\alpha_i, \alpha_j, \alpha_k)$ von φ_{ij} zu konsruieren, betrachten wir das Polynom f in $\mathbb{Q}(\alpha_1, \alpha_2)[x]$. Dort zerfällt es als

  $$f = (x - \alpha_1)(x - \alpha_2)(x^2 + \sqrt{2}),$$

  wie man durch Polynomdivision durch $(x - \alpha_1)$ und anschliessend durch $(x - \alpha_2)$ oder durch Raten sieht. Der Faktor $f_3 := (x^2 + \sqrt{2})$ ist tatsächlich irreduzibel, da er sonst eine Nullstelle in $\mathbb{Q}(\alpha_1, \alpha_2) \subseteq \mathbb{R}$ hätte, die Nullstellen aber α_3 und α_4 sind, welche in $\mathbb{C} \setminus \mathbb{R}$ liegen. Es ist f_3 also das Mipo von α_3 in über $\mathbb{Q}(\alpha_1, \alpha_2)$, wir können den Fortsetzungssatz erneut anwenden und es gibt genau einen Isomorphismus

  $$\begin{array}{ccc} \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) & \xrightarrow[\cong]{\varphi_{ijk}} & \mathbb{Q}(\alpha_i, \alpha_j, \alpha_4) \\ \cup\!| & & \cup\!| \\ \mathbb{Q}(\alpha_1, \alpha_2) & \xrightarrow[\cong]{\varphi_{ij}} & \mathbb{Q}(\alpha_i, \alpha_j) \end{array}$$

  für jede Nullstelle α_k von $f_3^{\varphi_{ij}}$. Wir bemerken, dass $f_3 = x^2 + \sqrt{2} = x^2 - \alpha_1\alpha_2$. Das Polynom $f_3^{\varphi_{ij}} \in \mathbb{Q}(\alpha_i, \alpha_j)[x]$ ist also gegeben durch $f_3^{\varphi_{ij}} = x^2 - \varphi_{ij}(\alpha_1\alpha_2) = x^2 - \alpha_i\alpha_j = x^2 + \alpha_i\alpha_i$.

  - War $i = 1$ oder $i = 2$, so ist $f_3^{\varphi_{ij}} = x^2 + \alpha_i\alpha_i = x^2 + \sqrt{2}$ und wir können als α_k eine beliebige von dessen Nullstellen α_3 oder α_4 wählen.
  - War $i = 3$ oder $i = 4$, so ist $f_3^{\varphi_{ij}} = x^2 + \alpha_i\alpha_i = x^2 - \sqrt{2}$ und wir können als α_k eine beliebige von dessen Nullstellen α_1 oder α_2 wählen.

- Wir sind nun schon fertig, da $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ und schreiben $\varphi_{ijkl} := \varphi_{ijk}$, wobei l das fehlende (eideutige) Element aus $\{1,2,3,4\}$ ist.

Benutzen wir die Notation aus dem Nullstellenpermutationslemma, so besteht $\mathrm{Gal}(f)$ also genau aus den Elementen

$$per(\varphi_{1234}) = \mathrm{id} \qquad per(\varphi_{1243}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad per(\varphi_{2134}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad per(\varphi_{2143}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$per(\varphi_{3412}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad per(\varphi_{3421}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad per(\varphi_{4312}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad per(\varphi_{4321}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

von S_4, was eine zu D_4 isomorphe Untergruppe ist.
(Man hätte übrigens analog (und vielleicht einfacher) mit dem Körperturm für $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ argumentieren können.)

Sei K ein Körper.

- Ist $K \subseteq L$ eine Körpererweiterung und $H \subseteq \mathrm{Gal}(L:K)$ eine Untergruppe, so ist die Menge

$$\mathrm{Fix}_L(H) := \{\ a \in L \mid \varphi(a) = a \text{ für alle } \varphi \in H\ \}$$

ein Körper mit $K \subseteq \mathrm{Fix}(H) \subseteq L$ und heißt **Fixkörper von** H (in L). Man schreibt dafür manchmal nur $\mathrm{Fix}(H)$.

- Eine Körpererweiterung $K \subseteq L$ ist **galois** $\iff$ $K \subseteq L$ ist algebraisch, normal und separabel
$\iff$ $K \subseteq L$ ist algebraisch $\wedge$ $\mathrm{Fix}(\mathrm{Gal}(L:K)) = K$

Beispiel 50. Die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ ist nicht galois, da $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}) = \{\mathrm{id}\}$ und damit $\mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.

- Hauptsatz der (endlichen) Galoistheorie Sei $K \subseteq L$ eine **endliche** Körpererweiterung die **galois** ist. Bezeichne $G := \mathrm{Gal}(L:K)$ die Galoisgruppe. Dann gibt es eine inklusionsumkehrende Bijektion

$$\left\{ \begin{array}{c} \text{Zwischenkörper } M \\ K \subseteq M \subseteq L \end{array} \right\} \underset{\mathrm{Fix}_L(-)}{\overset{\mathrm{Gal}(-:K)}{\rightleftarrows}} \left\{ \begin{array}{c} \text{Untergruppen } H \\ G \supseteq H \supseteq \{e\} \end{array} \right\}$$

die auf galoissche Körpererweiterungen $K \subseteq M$ links und auf Normalteiler $G \supseteq H$ rechts einschränkt. Außerdem entsprechen sich $[M:K] = [G:H]$ (der Index von H in G) und $[L:M] = |H|$.

$$\begin{array}{ccc} L & & \{e\} \\ [L:M] \big(\ \cup & \overset{\mathrm{Gal}(L:M)}{\rightleftarrows} & \cap \ \big) |H| \\ M & & H \\ [M:K] \big(\ \cup \ \big) \text{galois} & & \text{normal} \big(\ \cap \ \big) \text{Index} \\ K & & G \end{array}$$

Aufgabe (H15T1A4). Sei $f := x^3 - x + 2$ in $\mathbb{Q}[x]$ und wir wollen zeigen, dass $\mathrm{Gal}(f) = S_3$ gilt. Das Polynom f ist irreduzibel mit dem Reduktionskriterium zu $\mathbb{Z}/3$ und dem Lemma von Gauß. Weil **die nicht-reellen Nullstellen eines Polynoms mit reellen Koeffizienten in komplex-konjugierten Paaren auftreten**, hat f entweder eine oder drei Nullstellen. Eine schnelle Kurvendiskussion zeigt, dass f genau eine reelle Nullstelle α_1 hat. Sind α_2, α_3 die übrigen komplexen Nullstellen, so gilt per Definition $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3):\mathbb{Q})$. Die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ ist algebraisch, normal (da Zerfällungskörper) und separabel (da $\mathbb{Q}$ perfekt), also galois. Wir können nach dem Nullstellenpermutationslemma $\mathrm{Gal}(f)$ als Untergruppe von S_3 auffassen. Es genügt ein Element $\varphi \in \mathrm{Gal}(f)$ der Ordnung 3 und ein Element $\tau \in \mathrm{Gal}(f)$ der Ordnung 2 zu finden, da wegen der Teilerfremdheit dann $|\mathrm{Gal}(f)| \geq 2 \cdot 3 = |S_3|$ gilt, womit $\mathrm{Gal}(f) = S_3$ folgt. Die **komplexe Konjugation** $\mathbb{C} \to \mathbb{C}$ ist ein Körperisomorphismus von Ordnung 2 und wir können die Einschränkung $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) \to \mathbb{C}$ betrachten. Diese überführt (als Ringhomomorphismus über $\mathbb{Q}$) Nullstellen von f in Nullstellen von f und weil $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ Zerfällungskörper ist, faktorisiert sie als Körperisomorphismus $\tau: \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) \to \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$. Dieser ist nicht die Identität, da $\tau(\alpha_2) = \overline{\alpha}_2 \neq \alpha_2$ (dieses ist gleich α_3) und ist also ein Element $\tau \in \mathrm{Gal}(f)$ von Ordnung 2. Eine Untergruppe $\mathrm{Gal}(f) \hookrightarrow S_3 := (\text{Bijektionen}(\{1,2,3\}), \circ)$ ist (als Gruppenhomomorphismus) eine Gruppenoperation auf der Menge $\{1,2,3\}$. Weil f irreduzibel ist, kann man (wie in Beispiel 49) einen Iso $\varphi_{j,i}: \mathbb{Q}(\alpha_j) \to \mathbb{Q}(\alpha_i)$ für alle $j,i \in \{1,2,3\}$ konstruieren und zu einem Element $\tilde{\varphi}_{j,i} \in \mathrm{Gal}(f)$ fortsetzen. Dieses bedeutet, dass die Gruppenoperation auf der Menge $X := \{1,2,3\}$ **transitiv** ist (die Bahn ist also ganz X), was nach der Bahnenformel impliziert, dass $|X| = 3$ die Ordnung $|\mathrm{Gal}(f)|$ teilt. Allgemeiner (und genauso begründet) gilt: **Der Grad eines irreduziblen Polynoms teilt die Ordnung der Galoisgruppe.** Dieses liefert (beispielsweise nach den Sylowsätzen) ein Element von Ordnung 3.

Aufgabe (F17T1A2). Sei $f := x^4 - 4x^2 + 1$ in $\mathbb{Q}[x]$ und wir wollen zeigen, dass $\mathrm{Gal}(f) = \mathbb{Z}/2 \times \mathbb{Z}/2$ gilt. Die vier komplexen Nullstellen $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ von f sind (leichte Rechnung, α_1 ist sogar angegeben) durch $\pm\sqrt{2 \pm \sqrt{3}}$ gegeben. Da $\mathbb{Q}$ perfekt (und damit f separabel) ist, können wir $\mathrm{Gal}(f)$ nach dem Nullstellenpermutationslemma als Untergruppe von S_4 auffassen. Man sieht $\alpha_1 - \alpha_3 = \sqrt{2+\sqrt{3}} - \sqrt{2-\sqrt{3}} = \sqrt{2}$ und zeigt damit $L := \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = \mathbb{Q}(\sqrt{2},\alpha_1)$. Mit dem Gradsatz gilt dann

$$|\mathrm{Gal}(f)| = [L:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\alpha_1):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\alpha_1):\mathbb{Q}(\sqrt{2})] \cdot \underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{=2}$$

und für den übrigens Faktor wollen wir das Minimalpolynom von $\alpha_1 = \sqrt{2+\sqrt{3}}$ über $\mathbb{Q}(\sqrt{2})$ bestimmen. Dieses muss über $\mathbb{C}$ den Linearfaktor $(x - \alpha_1)$ enthalten, da α_1 ja dort eine Nullstelle sein soll, und eine kurze Rechnung zeigt $(x-\alpha_1)(x-\alpha_4) = x^2 - \sqrt{2}x - 1$, welches in $\mathbb{Q}(\sqrt{2})[x]$ liegt. Dieses ist nun tatsächlich das gesuchte Minimalpolynom, da mit dem Gradsatz

$$[\mathbb{Q}(\sqrt{2},\alpha_1):\mathbb{Q}(\sqrt{2})] \cdot 2 = [\mathbb{Q}(\sqrt{2},\alpha_1):\mathbb{Q}] \ \geq\ [\mathbb{Q}(\alpha_1):\mathbb{Q}] = 4$$

gilt, weil f irreduzibel (was man z.B. mit dem Verschiebekriterium und Einsenstein sieht) und somit das Minimalpolynom von α_1 über $\mathbb{Q}$ ist. Also ist $|\mathrm{Gal}(f)| = 4$, womit $\mathrm{Gal}(f)$ entweder $\mathbb{Z}/4$ oder $\mathbb{Z}/2 \times \mathbb{Z}/2$ ist. Wir wollen $\mathrm{Gal}(f) \neq \mathbb{Z}/4$ mit dem Hauptsatz zeigen. Man sieht leicht, dass $\sqrt{3} \in L$. Somit hat man die beiden verschiedenen Zwischenkörper $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ von $\mathbb{Q} \subseteq L$, aber die zyklische Gruppe $\mathbb{Z}/4$ hat genau eine Untergruppe vom Index 2. Also gilt $\mathrm{Gal}(f) = \mathbb{Z}/2 \times \mathbb{Z}/2$.

Beispiel 51. Die Galoisgruppe von $f := x^5 - 5x + 1$ aus $\mathbb{Q}[x]$ ist S_5, denn allgemeiner gilt: Für eine Primzahl p ist **die Galoisgruppe eines irreduziblen Polynom $f \in \mathbb{Q}[x]$ vom Grad p mit genau zwei nicht-reellen Nullstellen die ganze S_p**, denn wie oben sieht man durch die Transitivität, dass $p \mid |\mathrm{Gal}(f)|$. Damit enthält $\mathrm{Gal}(f) \subseteq S_p$ einen p-Zykel, da diese (nach dem üblichen Argument) die einzigen Elemente von Ordnung p in S_p sind. Die komplexe Konjugation liefert wie oben ein Element der Ordnung 2 in $\mathrm{Gal}(f)$. Dieses ist nun aber genau eine Transposition (i,j) (und keine Doppeltransposition, etc.), weil es nur genau zwei nicht-reelle Nullstellen von f in $\mathbb{C}$ gibt. Nun kann man benutzen (dieses ist nicht hart, aber auch nicht trivial), dass S_p von einem p-Zykel und einer Transposition erzeugt wird.

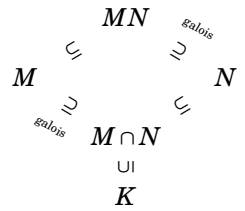
- Reduktionssatz Sei $f \in \mathbb{Q}[x]$ ein irreduzibles, normiertes Polynom mit ganzzahligen Koeffizienten und p eine Primzahl. Dann ist
$$\mathrm{Gal}(f^\varphi) \subseteq \mathrm{Gal}(f)$$
eine Untergruppe, wobei $\varphi: \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p$ die Projektion bezeichne.

Beispiel 52. Sei $f := x^5 - x - 1$ in $\mathbb{Q}[x]$ und wir wollen zeigen, dass $\mathrm{Gal}(f) = S_5$ gilt. Nach dem Reduktionskriterium zu $\mathbb{Z}/5$ und dem Lemma von Gauß sieht man die Irreduzibilität von f: Das reduzierte Polynom $\bar{f} := x^5 - x - 1$ hat keine Nullstellen in $\mathbb{Z}/5$ und wir müssen die Existenz eines quadratischen Faktors q ausschließen. Dieses rechnet man entweder nach oder benutzt in $\mathbb{Z}/5[x]/(q) \cong \mathbb{F}_{25}$, dass für $\alpha := [x]$ gilt
$$\alpha = \alpha^{25} = (\alpha^5)^5 = (\alpha+1)^5 = \alpha^5 + 1^5 = (\alpha+1) + 1 = \alpha + 2$$
also $0 = 2$, was ein Widerspruch wäre. Wie oben sieht man nun, dass $5 \mid |\mathrm{Gal}(f)|$ und das übliche Argument zeigt, dass Elemente von Ordnung 5 in S_5 genau die 5-Zykel sind. Also enthält $\mathrm{Gal}(f)$ einen 5 Zykel. Es genügt daher, eine Transposition in $\mathrm{Gal}(f)$ zu finden. Ist $\varphi: \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$ die Projektion, so ist $f^\varphi = (x^3 + x^2 + 1)(x^2 + x + 1)$ eine Zerlegung in irreduzible Faktoren in $\mathbb{Z}/2[x]$. Tatsächlich ist nach dem Translationssatz unten $\mathrm{Gal}((x^3+x^2+1)(x^2+x+1)) = \mathrm{Gal}(x^3+x^2+1) \times \mathrm{Gal}(x^2+x+1) = \mathrm{Gal}(x^3+x^2+1) \times \mathbb{Z}/2$ (und wir haben die Transposition gefunden), da $M = ZFK_{\mathbb{Z}/2}(x^3+x^2+1) = \mathbb{F}_8 = \mathbb{F}_{2^3}$ und $N = ZFK_{\mathbb{Z}/2}(x^2+x+1) = \mathbb{F}_4 = \mathbb{F}_{2^2}$ und daher $M \cap N = \mathbb{F}_2$, da $\mathrm{ggT}(3,2) = 1$.

Bemerkung 53. Es ist nicht im Allgemeinen einfach, die Galoisgruppe $\mathrm{Gal}(gh)$ eines Produkts zweier irreduzibler Polynome aus $\mathrm{Gal}(g)$ und $\mathrm{Gal}(h)$ zu berechnen. Der folgende Satz hilft dabei.

- Ist $K \subseteq L$ eine Körpererweiterung und M, N Zwischenkörper, so heißt der kleinste Unterkörper von L, der M und N enthält das **Kompositum** MN von N und M. Dieses ist offenbar ein Zwischenkörper $K \subseteq M \subseteq MN \subseteq L$ und $K \subseteq N \subseteq MN \subseteq L$ und ist $N = K(\alpha_1, \ldots, \alpha_n)$, so ist $MN = M(\alpha_1, \ldots, \alpha_n)$.

- Translationssatz Sei $K \subseteq L$ eine Körpererweiterung und M, N Zwischenkörper mit $K \subseteq M$ endlich und galois.



Dann sind auch $M \cap N \subseteq M$ und $N \subseteq MN$ endlich und galois und die Galoisgruppen sind gleich, also
$$\mathrm{Gal}(M : M \cap N) = \mathrm{Gal}(MN : N).$$
Außerdem ist
$$\mathrm{Gal}(MN : K) \hookrightarrow \mathrm{Gal}(M : K) \times \mathrm{Gal}(N : K)$$
injektiv, das Bild besteht genau aus den Paaren, die auf $\mathrm{Gal}(M \cap N : K)$ übereinstimmen und die beiden Kompositionen $\mathrm{Gal}(MN : K) \twoheadrightarrow \mathrm{Gal}(M : K)$ und $\mathrm{Gal}(MN : K) \twoheadrightarrow \mathrm{Gal}(N : K)$ sind surjektive Gruppenhomomorphismen.

Bemerkung 54. Die letzte Aussage im Translationssatz über die Injektivität impliziert insbesondere, dass $\mathrm{Gal}(MN : K)$ abelsch ist, falls $\mathrm{Gal}(M : K)$ und $\mathrm{Gal}(N : K)$ abelsch sind. In dem Fall ist (sogar rechts)
$$0 \to \mathrm{Gal}(MN : K) \to \mathrm{Gal}(M : K) \times \mathrm{Gal}(N : K) \to \mathrm{Gal}(M \cap N : K) \to 0$$
eine exakte Folge abelscher Gruppen.

Beispiel 55. Ist $f := (x^2 - 2)(x^2 - 3)$ aus $\mathbb{Q}[x]$ das **nicht irreduzible Polynom** mit Nullstellen $\alpha_{1,2} = \pm\sqrt{2}$ und $\alpha_{3,4} = \pm\sqrt{3}$, so ist
$$\mathrm{Gal}(f) = \mathrm{Gal}(\underbrace{\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}_{=MN} : \mathbb{Q}) = \mathrm{Gal}(\underbrace{\mathbb{Q}(\alpha_1,\alpha_2)}_{=M} : \mathbb{Q}) \times \mathrm{Gal}(\underbrace{\mathbb{Q}(\alpha_2,\alpha_3)}_{=N} : \mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3}) : \mathbb{Q}) = \mathbb{Z}/2 \times \mathbb{Z}/2,$$
da $M \cap N = \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. (Die Tatsache, dass $\mathrm{Gal}(f)$ eine Untergruppe des Produkts ist bedeutet übrigens, dass die **Nullstellen von den beiden irreduziblen Faktoren nicht „gemischt" werden**.)

- Es gibt für jede Primzahl p (bis auf Isomorphismus über $\mathbb{F}_p := \mathbb{Z}/p$) für jedes $n \geq 1$ **genau einen endlichen Körper** $\mathbb{F}_{p^n}$ mit p^n-vielen Elementen
$$\mathbb{F}_{p^n} := ZFK_{\mathbb{F}^p}\left(x^{(p^n)} - x\right),$$
und alle endlichen Körper sind von dieser Form. Ist ein algebraischer Abschluss $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ gewählt, so gilt
$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n|m.$$

Bemerkung 56. Die Beweisidee für die vorherigen Behauptungen ist wie folgt:

- Zuächst zur Eindeutigkeit: Ein endlicher Körper L hat prime Charakteristik p und daher $\mathbb{F}_p \subseteq L$.
- Da L ein endlichdimensionaler $\mathbb{F}_p$-Vektorraum ist, hat L genau $|\mathbb{F}_p \oplus \ldots \oplus \mathbb{F}_p| = p^n$-viele Elemente.
- Da die Einheiten $L^\times = L \setminus \{0\}$ eine Gruppe mit (p^n-1)-vielen Elementen ist, gilt für alle $a \in L$, dass $a^{p^n} = a$.
- Das Polynom $f := x^{p^n} - x$ aus $\mathbb{F}_p[x]$ zerfällt also in L in Linearfaktoren und daher $ZFK^L_{\mathbb{F}_p}(f) \subseteq L$. Außerdem haben wir gesehen, dass $L \subseteq ZFK^L_{\mathbb{F}_p}(f)$, also $L = ZFK^L_{\mathbb{F}_p}(f) \cong ZFK_{\mathbb{F}_p}(f)$.
- Für die Existenz ist noch zu zeigen, dass $|ZFK_{\mathbb{F}_p}(f)| = p^n$. Da $f' = p^n x^{p^n-1} - 1 = -1 \neq 0$ ist f separabel und $|ZFK_{\mathbb{F}^p}(f)| \geq p^n$.
- Sei $\overline{\mathbb{F}}^p$ ein algebraischer Abschluss und $\mathrm{NST} \subseteq \overline{\mathbb{F}}_p$ die Menge der Nullstellen von f. Per Definition gilt $\mathrm{NST} \subseteq \mathbb{F}_p(\mathrm{NST}) = ZFK_{\mathbb{F}_p}(f)$. Tatsächlich ist NST aber selbst ein Körper und daher $\mathrm{NST} = ZFK_{\mathbb{F}_p}(f)$. Da f ein Polynom über einem Integritätsbereich ist, gilt also $|ZFK_{\mathbb{F}_p}(f)| = |\mathrm{NST}| \leq p^n$.

Aufgabe (H18T1A5). Um die Multiplikation von $\mathbb{F}_{p^n}$ genauer zu beschrieben (es ist klar, was die Addition ist, da mit dieser als Gruppenoperation $\mathbb{F}_{p^n} \cong \mathbb{F}_p \oplus \ldots \oplus \mathbb{F}_p$ gilt), kann man ein **beliebiges** irreduziertes normiertes Polynom $f \in \mathbb{F}_p[x]$ vom Grad n wählen. Dann gilt $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(f)$ nach dem Hauptsatz über endliche Körper (Eindeutigkeit), da die rechte Seite ein Körper mit p^n Elementen ist. Beispielsweise ist für $p = 2$ und $n = 2$ das Polynom $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ irreduzibel und vom Grad 2. Setzen wir nun $\alpha := [x] \in \mathbb{F}_2[x]/(f)$ (siehe Kronecker Trick) so können wir die folgenden Additions- und Multiplikationstabellen von $\mathbb{F}_4$ aufstellen:

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

·	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

So ist beispielsweise $\alpha \cdot \alpha = [x] \cdot [x] = [x^2] = [-x-1] = [x+1] = [x] + 1 = \alpha + 1$.
Das Polynom $f = x^4 + x + 1 \in \mathbb{F}_4[x]$ ist nicht irreduzibel. Hierfür kann man entweder eine explizite Zerlegung $f = (x^2 + x + \alpha)(x^2 + x + (\alpha+1))$ angeben, oder anders vorgehen: Angenommen $f \in \mathbb{F}_4[x]$ ist irreduzibel, dann ist auch $f \in \mathbb{F}_2[x]$ irreduzibel. Wir wählen einen algebraischen Abschluss $\mathbb{F}_2 \subseteq \mathbb{F}_4 \subseteq \overline{\mathbb{F}}_2$ und eine Nullstelle $\beta \in \overline{\mathbb{F}}_2$ von f. Es ist $\mathbb{F}_2 \subseteq \mathbb{F}_2(\beta)$ eine Körpererweiterung vom Grad $\deg(f) = 4$, also $|\mathbb{F}_2(\beta)| = 2^4$ und mit dem Hauptsatz über endliche Körper $\mathbb{F}_2 \subseteq \mathbb{F}_4 \subseteq \mathbb{F}_2(\beta) \subseteq \overline{\mathbb{F}}_2$. Es ist $\mathbb{F}_2(\beta) \subseteq \mathbb{F}_4(\beta)$ eine Gleichheit, da $\mathbb{F}_4(\beta)$ per Definition der kleinste Unterkörper von $\overline{\mathbb{F}}_2$ ist, der $\mathbb{F}_4$ und β enthält. Mit der Gradformel gilt dann
$$4 = [\mathbb{F}_2(\beta) : \mathbb{F}_2] = [\mathbb{F}_4(\beta) : \mathbb{F}_4] \cdot \underbrace{[\mathbb{F}_4 : \mathbb{F}_2]}_{=2}$$
also $[\mathbb{F}_4(\beta) : \mathbb{F}_4] \neq 4$ womit $f \in \mathbb{F}_4[x]$ nicht irreduzibel sein kann.
Außerdem gilt $[ZFK_{\mathbb{F}_4}(f) : \mathbb{F}_4] = 2$ was man wie folgt sieht: Da f keine Nullstellen in $\mathbb{F}_4$ hat (Einsetzen!) und reduzibel ist, zerfällt es in zwei irreduzible Faktoren $f = gh$ in $\mathbb{F}_4[x]$, die jeweils den Grad 2 haben. Ist $\beta \in \overline{\mathbb{F}}_2$ eine Nullstelle von g und $\gamma \in \overline{\mathbb{F}}_2$ eine Nullstelle von h ist $ZFK_{\mathbb{F}_4}(f) = \mathbb{F}_4(\beta, \gamma)$. Nun sind aber $\mathbb{F}_4 \subseteq \mathbb{F}_4(\beta)$ und $\mathbb{F}_4 \subseteq \mathbb{F}_4(\gamma)$ beides Erweiterungen vom Grad = 2 und nach dem Hauptsatz über endliche Körper also $\mathbb{F}_4(\beta) = \mathbb{F}_4(\gamma) = \mathbb{F}_4(\beta, \gamma)$.

- Die Körpererweiterung $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ ist endlich und galois mit Galoisgruppe $\mathbb{Z}/(\frac{m}{n})$. Ein Erzeuger dieser zyklischen Gruppe ist der Frobenius
$$\begin{array}{ccc} R & \to & R \\ a & \mapsto & a^p. \end{array}$$

- Die **Einheitengruppe** $K^\times$ **eines endlichen Körpers** K **ist zyklisch**. (Tatsächlich ist sogar jede endliche Untergruppe der Einheitengruppe eines beliebigen Körpers zyklisch.) Dieses sieht man wie folgt: Nach dem Hauptsatz für endlich erzeugte abelsche Gruppen gilt
$$K^\times \cong \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_\ell^{k_\ell}$$
Sei $m = \mathrm{kgV}(p_1^{k_1}, \ldots, p_\ell^{k_\ell})$. Dann gilt natürlich $m \leq p_1^{k_1} \cdots p_\ell^{k_\ell}$ und wenn wir Gleichheit zeigen sind wir fertig, da dann alle Primzahlen $p_1, \ldots, p_\ell$ verschieden sind und somit $K^\times \cong \mathbb{Z}/p_1^{k_1} \cdots p_\ell^{k_\ell}$ nach dem Chinesischen Restsatz. Für jedes Element $a \in K^\times$ gilt $a^m = 1$, da für das entsprechende Element auf der rechten Seite der Isomorphie oben $m \cdot (a_1, \ldots, a_\ell) = (ma_1, \ldots, ma_\ell) = (0, \ldots, 0) = 0$ gilt. Jedes der $|K^\times| = (p_1^{k_1} \cdots p_\ell^{k_\ell})$-vielen Elemente $a \in K^\times$ ist also Nullstelle des Polynoms $x^m - 1 \in K[x]$. Dieses hat aber maximal m-viele Nullstellen. Also gilt Gleichheit.