Algebra I

Bernd Ammann, WS 2008/09

Inhaltsverzeichnis

Literaturverzeichnis

[1] M. Bosch, Algebra, Springer
[2] C. Karpfinger, K. Meyberg, Algebra, Spektrum
[3] S. Lang, Algebra, Addison-Wesley
[4] M. Artin, Algebra, Birkhäuser
[5] F. Lorenz, Einführung in die Algebra, Teil I, BI Wissenschaftsverlag
[6] F. Lorenz, Einführung in die Algebra, Teil II, BI Wissenschaftsverlag
[7] F. Lorenz, F. Lemmermeyer, Algebra 1, Spektrum

Wir werden uns vor allem an [**1**] orientieren, aber auch [**2**] ist recht nah an dem Inhalt der Vorlesung. Ein sehr gutes Nachschlagewerk ist [**3**]. Das Buch [**4**] hat manchmal einen etwas anderen, aber auch interessanten Blickwinkel. Es ist allerdings in der Stoffauswahl weiter von der Vorlesung entfernt.

Motivation

Das Wort „Algebra" stammt aus dem Arabischen (9. Jhdt nach Christus) und bedeutet „Rechnen mit Gleichungen".

Die Ursprünge der Algebra sind in der griechischen Antike zu finden. Man fragte sich damals zum Beispiel:

> Gegeben sei ein Würfel mit Volumen 1 (also Kantenlänge 1), kann man daraus mit Zirkel und Lineal einen Würfel mit Volumen 2 (also Kantenlänge $\sqrt[3]{2}$) mit Zirkel konstruieren?

Heute weiß man, dass dies nicht geht.

Um dies zu sehen, nutzt man sogenannte **Körpererweiterungen**. Man redet von einer Körpererweiterung, wenn ein kleinerer Körper in einem größeren enthalten ist, wie zum Beispiel $\mathbb{Q} \subset \mathbb{R}$ oder $\mathbb{R} \subset \mathbb{C}$. Dass man eine Zahl nicht mit Zirkel und Lineal konstruieren kann, erscheint uns heute nicht mehr problematisch. Wir haben uns an Zahlen wie $\sqrt[3]{2} = 1,25992...$, $\pi = 3,14159265..$ und $e = 2,71828...$ gewöhnt. Den Leuten in der Antike erschienen diese Zahlen unwirklich, so wie viele Nichtmathematiker heutzutage komplexe Zahlen als unwirklich ansehen.

Es gibt sehr viele Körper, die $\mathbb{Q}$ enthalten und die selber Teilkörper von $\mathbb{C}$ sind. Eine Unterklasse von solchen Körpern sind die algebraischen Erweiterungen von $\mathbb{Q}$. Um sie gut zu verstehen, muss man **Polynomringe** untersuchen, wir müssen also mehr über Ringe wissen. Wenn wir die Körpererweiterungen besser verstanden haben, sehen wir, dass man $\sqrt[3]{2}$ nicht mit Zirkel und Lineal konstruieren kann.

Ein anderes wichtiges Problem hat ebenfalls die Algebra geprägt, die Suche nach Nullstellen algebraischer Gleichungen, d.h. von Gleichungen der Form $P(x) = 0$, wobei P ein Polynom ist. Wir alle kennen die Formel für die Nullsteleln im Fall $\deg P = 2$: Die Nullstellen von $X^2 + pX + q$ sind

$$x_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Dies war bereits in der Antike bekannt, und es ist naheliegend nach der Auflösung im Fall $\deg P > 2$ zu fragen. In den Fällen $\deg P = 3$ und $\deg P = 4$ kennt man seit dem 16. Jhdt ähnliche Lösungsformeln. Man glaubte, dass man jede Gleichung der Form $P(x)$ durch Wurzelziehen lösen könne. Aus diesem Grund bezeichnet man auch heute noch die Nullstellen einer solchen Gleichung als die Wurzeln des Polynoms P. Jahrhundertelang versuchte man eine Formel für $\deg P \geq 5$ zu finden, die nur die Grundrechenarten und den Ausdruck $\sqrt[k]{\ }$ enthält.

Ab der zweiten Hälfte des 18. Jhdts untersucht man diese Gleichungen systematischer, das heißt mit Hilfsmitteln, die dem, was wir in der Algebra behandlen, näher kommen. Der Fundamentalsatz der Algebra, ($\mathbb{C}$ ist algebraisch abgeschlossen) wurde (mit zunehmend überzeugenden Beweisen) von d'Alembert (1746), Euler (1749), Lagrange (1772) und Gauß (1799) gegeben.

Zu einem wirklichen Durchbruch gelangte der Mathematiker Evariste Galois (1811–1832). Galois erkannte, dass man das Konzept der **Gruppen** nutzen kann, um Körpererweiterungen besser zu verstehen. Dies markiert den Anfang der Gruppentheorie.

Galois war ein begabter junger Mathematiker, der außerdem politisch sehr aktiv war. Er wurde in der bewegten Revolutionszeit mehrfach verhaftet. Er starb mit 20 Jahren an einem Bauchschuss in einem Duell. Wahrscheinlich ging es in diesem Duell um eine Frau, um Stéphanie-Félicie Poterine du Motel, eine unglückliche Liebe von Galois.

In der Nacht vor seinem Duell schrieb er einen langen Brief, dessen Bedeutung erst 1843 von Liouville erkannt wurde.

Aus der Galois-Theorie folgt, dass man die Lösungen von $P(x) = 0$ für $\deg P \geq 5$ nicht mit einer wie oben gewünschten Formel berechnen kann.

Mehr Informationen hierzu finden Sie zum Beispiel auf wikipedia.

Die Themen der Vorlesung sind somit: Gruppen, Ringe, Körper, Galoistheorie.

KAPITEL 1

Gruppen, Teil I

1. Grundlagen

Sei $(M, \cdot)$ eine Menge mit Verknüpfung, $\cdot : M \times M \to M$. Man nennt $(M, \cdot)$ ein *Monoid*, falls gilt:

(Ma) **assoziativ**
Für alle $x, y, z \in M$ gilt
$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$
(Mn) **neutrales Element**
Es gibt ein Element $e \in M$, so dass für alle $x \in M$ gilt
$$x \cdot e = e \cdot x = x.$$

Falls zusätzlich

(Mk) **kommutativ**
Für alle $x, y \in X$ gilt
$$x \cdot y = y \cdot x.$$

gilt, so nennt, man $(M, \cdot)$ ein kommutatives Monoid.

Lemma 1.1. *In einem Monoid gibt es nur ein neutrales Element.*

$$e_1 = e_1 \cdot e_2 = e_2$$

□

Wenn in einem (kommutativen) Monoid zusätzlich die Eigenschaft

(Mi) **inverse Elemente**
Zu jedem $x \in X$ gibt es ein $y \in X$, so dass
$$x \cdot y = y \cdot x = e.$$

gilt, nennt man es eine (kommutative) Gruppe. Es gibt dann zu jedem x genau ein Inverses y, und wir schreiben x^{-1} für dieses y.

PROPOSITION 1.2. *Sei $\cdot$ eine assoziative Verknüpfung auf einer Menge M, so dass*

(Ml-n) ***links-neutrales Element***
Es gibt ein Element $e \in M$, so dass für alle $x \in M$ gilt

$$e \cdot x = x.$$

(Ml-i) ***links-inverse Elemente***
Zu jedem $x \in X$ gibt es ein $y \in X$, so dass

$$y \cdot x = e.$$

Dann ist $(M, \cdot)$ eine Gruppe.

Beweis. Es gelte $yx = e$, d.h. y ist Linksinverses von x. Da e linksneutral ist, folgt

$$yxy = ey = y. \tag{1.3}$$

Sei z ein Linksinverses von y, d.h. $zy = e$. Wir multiplizieren (1.3) von links mit z und erhalten

$$zyxy = zy.$$

Die rechte Seite ist wieder e. Die linke ergibt $((zy)x)y = (ex)y = xy$. Also haben wir $xy = e$ gezeigt, somit ist y Rechtsinverses von x. Wir erhalten (Mi).

Um zu zeigen, dass e ein Rechtsinverses ist, rechnen wir für ein beliebiges x und sein Inverses y:

$$xe = x(yx) = (xy)x = ex = x.$$

Es folgt (Mn). □

BEMERKUNG 1.4. Ist $(M, \cdot)$ ein endliches Monoid, auf dem die Rechtskürzungsregel gilt, dann ist $(M, \cdot)$ eine Gruppe. (Beweis LA1, Prop. II 1.5).

Beispiele: (1) $\mathbb{N}_0$ ist ein abelsches Monoid.
(2) $\mathbb{Z}$ ist eine kommutative Gruppe.
(3) Die Symmetriegruppe eines gleichseitigen Dreiecks in der Ebene hat 3 Elemente, die Verknüpfung ist die Verkettung. Sie ist nicht kommutativ.
(4) Die symmetrische Gruppe $\mathcal{S}_n$ mit der Verkettung ist eine Gruppe

Ist jedes Monoid Teilmenge einer Gruppe? Nein. Es gibt Monoide, in denen die Kürzungsregeln nicht gelten, z.B.

(5) $\{0, 1\}$ mit der Verknüpfung

$\cdot$	0	1
0	0	1
1	1	1

ist ein abelsches Monoid.

(6) Sei X eine Menge, dann ist $\mathrm{Abb}(X, X)$ mit der Verknüpfung ein Monoid.

2. Homomorphismen

Eine Abbildung $f : M_1 \to M_2$ zwischen Monoiden heißt *Homomorphismus von Monoiden*, falls für alle $a, b \in M_1$ gilt

$$f(ab) = f(a)f(b) \qquad \text{und} \qquad f(e_1) = e_2.$$

Falls M_1 und M_2 Gruppen sind, so nennt man f auch *Homomorphismus von Gruppen*.

Die Begriffe Epi-, Mono-, Iso-, Endo- und Automorphismus benutzt man wie in der Vektorraumtheorie. Die Menge aller Homomorphismen schreiben wir auch als $\mathrm{Hom}(M_1, M_2)$, ebenso $\mathrm{End}(M_1)$, $\mathrm{Aut}(M_1)$, ...

Proposition 2.1. *Sei G_1 und G_2 Gruppen, so dass sei $f : G_1 \to G_2$ eine Abbildung für alle $a, b \in G_1$ gilt $f(ab) = f(a)f(b)$. Dann gilt auch $f(e_1) = e_2$ und für alle $x \in G_1$ gilt $f(x^{-1}) = f(x)^{-1}$.*

Insbesondere ist als f ein Homomorphismus von Gruppen.

Beweis. Es gilt

$$f(e_1)e_2 = f(e_1) = f(e_1e_1) = f(e_1)f(e_1).$$

Kürzen von links ergibt $e_2 = f(e)^{-1}$.

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2.$$

□

Übungen: Sei M ein Monoid. Dann ist auch $(\mathrm{End}(M), \circ)$ ist ein Monoid. Und $(\mathrm{Aut}(M), \circ)$ ist eine Gruppe.

Analog (Vektorraum-Theorie):
Sei V ein Vektorraum. Dann ist die Menge aller Vektorraum-Endomorphismen ein Monoid mit Verknüpfung $\circ$. Die Menge aller Vektorraum-Automorphismen ist eine Gruppe mit Verknüpfung $\circ$.

3. Untergruppen und Normalteiler

Sei $(G, \cdot)$ eine Gruppe. Ein Teilmenge H von G heißt *Untergruppe*, wenn die Restriktion H unter $\cdot$ abgeschlossen ist ($\forall a, b \in H$ gilt $a \cdot b \in H$), und wenn $(H, \cdot)$ eine Gruppe ist. Wir schreiben dann $H \leq G$.

Lemma 3.1. *Ist $f : K \to G$ ein Homomorphismus von Gruppen, dann ist $f(K)$ eine Untergruppe von G.*

□

Umgekehrt gibt es zu jeder Untergruppe H von G einen Homomorphismus, so dass H dessen Bild ist: Man nehme $K := H$ und die Inklusion $K = H \to G$. Untergruppen sind also genau die genau die Bilder von Homomorphismen.

Eine Untergruppe H von G heißt *Normalteiler von G*, falls zusätzlich gilt:

$$\forall h \in H \forall g \in G : \qquad ghg^{-1} \in H.$$

Wir schreiben dann $H \trianglelefteq G$.

Lemma 3.2. *Ist $f : K \to G$ ein Homomorphismus von Gruppen, dann ist* Kern f *ein Normalteiler von K.*

Beweis. Kern f ist eine Untergruppe von K: trivial.

Sei $g \in K$, $h \in$ Kern f. Dann gilt

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)ef(g)^{-1} = e.$$

□

4. Erzeugendensysteme und zyklische Gruppen

Lemma 4.1. *Sei G eine Gruppe und $(H_i|i \in I)$ eine Familie von Untergruppen. Dann ist*

$$\bigcap_{i \in I} H_i = \{x \in G \,|\, x \in H_i \quad \forall i \in I\}$$

eine Untergruppe. Falls alle H_i Normalteiler sind, dann ist auch $\bigcap_{i \in I} H_i$ ein Normalteiler.

Beweis. $M \subset G$ ist eine Untergruppe gdw

- $e_G \in M$ und
- $\forall x, y \in M : \quad xy^{-1} \in M$

Offensichtlich gilt $e_G \in \bigcap_{i \in I} H_i$.

Seien $x, y \in \bigcap_{i \in I} H_i$. Dann gilt also $xy^{-1} \in H_i$ für alle $i \in I$. Somit auch $xy^{-1} \in \bigcap_{i \in I} H_i$. Somit ist $\bigcap_{i \in I} H_i$ eine Untergruppe.

Sei nun $H_i \trianglelefteq G$. Zu zeigen: $\bigcap_{i \in I} H_i \trianglelefteq G$. Sei $h \in \bigcap_{i \in I} H_i$, $g \in G$. Dann ist für alle $i \in I$: $h \in H_i$ und somit $ghg^{-1} \in H_i$. Also $ghg^{-1} \in \bigcap_{i \in I} H_i$. Somit $\bigcap_{i \in I} H_i \trianglelefteq G$. □

Definition 4.2. Sei G eine multiplikative Gruppe, M eine Teilmenge von G. Dann heißt

$$\langle M \rangle := \bigcap \{H | H \text{ ist Untergruppe von } G \text{ und } M \subset H\}$$

die *von M erzeugte Untergruppe*, und

$$\langle M \rangle_{\trianglelefteq G} := \bigcap \{H | H \text{ ist Normalteiler von } G \text{ und } M \subset H\}$$

heißt der *von M erzeugte Normalteiler in G*. Eine Erzeugendensystem von G ist eine Menge $M \subset G$, so dass $\langle M \rangle = G$. Eine Gruppe G heißt *endlich erzeugt*, wenn es eine endliche Menge $M \subset G$ gibt, so dass $\langle M \rangle = G$. Eine Gruppe G heißt *zyklisch]*, falls G von einem Element erzeugt wird.

Ordnung einer Gruppe $\mathrm{ord}(G) := \#G$. Ordnung von $x \in G$: $\mathrm{ord}(x) := \mathrm{ord}(\langle x \rangle)$. Wir definieren für $x \in G$, $n \in M$:

$$x^n := \underbrace{x \cdot \ldots \cdot x}_{n\text{-mal}}$$
$$x^n := \underbrace{x^{-1} \cdot \ldots \cdot x^{-1}}_{n\text{-mal}}$$
$$X^0 := e$$

Dann ist $\phi_x : \mathbb{Z} \to G$ ein Gruppenhomomorphismus. Das Bild von ϕ_x ist eine Untergruppe von G, die x enthält. Also $\langle x \rangle \subset \mathrm{Bild}\phi_x$. Andererseits zeigt man leicht durch vollständige Induktion $x^n \in \langle x \rangle$ für alle $n \in \mathbb{Z}$. Somit $\langle x \rangle = \mathrm{Bild}\phi_x$.

Sei nun G zyklisch. Also ist ϕ_x surjektiv. Der Kern von ϕ_x ist eine Untergruppe von $\mathbb{Z}$, also von der Form $n\mathbb{Z} := \{kn \mid k \in \mathbb{Z}\}$. Somit

$$\phi_x(a) = \phi_x(b) \quad \Leftrightarrow \quad x - y \in n\mathbb{Z} \quad \Leftrightarrow \quad n | x - y \quad \Leftrightarrow \quad x \equiv y \mod n$$

Es gibt also eine eindeutige Abbildung $\psi : \mathbb{Z}/n\mathbb{Z} \to G$, so dass das Diagramm

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\phi"] \arrow[d, "\pi"'] & G \\
\mathbb{Z}/n\mathbb{Z} \arrow[ur, "\psi"'] &
\end{tikzcd}$$

kommutiert. Hierbei ist $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ die Abbildung $x \mapsto x \mod n = \bar{x} = x + n\mathbb{Z}$. Man sieht leicht, dass ψ ein Isomorphismus von Gruppen ist (siehe auch den Homomorphiesatz, Satz **??**).

Notation $H \cong G \Leftrightarrow H$ ist isomorph zu G. Also $G \cong \mathbb{Z}/n\mathbb{Z}$.

KOROLLAR 4.3. *Sei G eine zyklische Gruppe. Falls* $\operatorname{ord}(G) = \infty$*, dann ist $G \cong \mathbb{Z}$. Falls* $\operatorname{ord}(G) < \infty$*, dann ist $G \cong \mathbb{Z}/n\mathbb{Z}$ mit $n := \operatorname{ord}(G)$.*

□

Eine Gruppe G ist genau dann zyklisch, wenn es einen surjektiven Gruppenhomorphismus $\mathbb{Z} \to G$ gibt.

5. Direkte Produkte und direkte Summen von Gruppen

Seien G_1 und G_2 Gruppen. Wir versehen $G := G_1 \times G_2$ mit der folgenden (komponentenweisen) Verknüpfung

$$\begin{array}{rcl} (G_1 \times G_2) \times (G_1 \times G_2) & \to & (G_1 \times G_2) \\ ((g_1, g_2), (h_1, h_2)) \to (g_1, g_2) \cdot (h_1, h_2) := (g_1 h_1, g_2 g h_2) & & \end{array}$$

Offensichtlich ist $G_1 \times G_2$ wieder eine Gruppe, das *direkte Produkt von G_1 und G_2*.

Die Gruppen $(G_1 \times G_2) \times G_3$ und $G_1 \times (G_2 \times G_3)$ sind im wesentlichen das gleiche und wir schreiben dann einfach $G_1 \times G - 2 \times G_3$. Das kann man so fortführen, um $G_1 \times \cdot \times G_n$ zu definieren.

Um unendliche Produkte zu definieren, muss man anders vorgehen. Sei $(G_i | i \in I)$ eine Familie von Gruppen. Dann definiert man das *direkte Produkt* als

$$\prod_{i \in I} G_i := \prod \left(G_i \,\middle|\, i \in I \right) := \left\{ (g_i | i \in I) \,\middle|\, \forall i \in I : \; g_i \in G_i \right\}.$$

Elemente in $\prod_{i \in I} G_i$ verknüpfen wir so:

$$(g_i | i \in I) \cdot (h_i | i \in I) := (g_i h_i | i \in I).$$

Bemerkung: Man schreibt oft auch $X_{i \in I} G_i$ an Stelle von $\prod_{i \in I} G_i$. Man nennt es oft auch das kartesische Produkt.

Die direkte Summe definiert man als

$$\sum_{i \in I} G_i := \{(g_i | i \in I) \,|\, \text{nur für endlich viele } i \in I \text{ gilt: } g_i \neq e_{G_i}\}.$$

Auch dies ist eine Gruppe. Offensichtlich gilt $\prod_{i \in I} G_i = \sum_{i \in I} G_i$, falls I endlich.

6. Gruppenwirkungen

Notation: Die Gruppe der Permutationen von M, also der bijektiven Abbildungen $M \to M$ bezeichnen wir im folgenden als $\mathrm{Perm}(M)$. Die Verknüpfung in $\mathrm{Perm}(M)$ ist die Verkettung von Abbildungen. (In LA1 notierten wir $\mathrm{Bij}(M)$ an stelle von $\mathrm{Perm}(M)$.)

Ist $b : X \to Y$ eine Bijektion, so definiert

$$\mathrm{Perm}(X) \to \mathrm{Perm}(Y), \qquad \sigma \mapsto b \circ \sigma \circ b^{-1}$$

einen Isomorphismus von Gruppen.

In der Literatur finden sich vor allem zwei Möglichkeiten Gruppenwirkungen zu definieren. Am besten ist, wenn Sie beide kennen und zeigen können, dass beide Sichtweise äquivalent sind. Wir nennen eine davon „eine Gruppenwirkung“ und die andere „eine gruppenwirkende Abbildung“.

Definition 6.1. Eine *Gruppenwirkung (oder Operation)* von einer Gruppe G auf einem Raum X ist ein Gruppenhomomorphismus

$$W : G \to \mathrm{Perm}(X).$$

Definition 6.2. Eine *gruppenwirkende Abbildung* ist eine Abbildung $w : G \times X \to X$ mit den folgenden Eigenschaften:

(Id) *Wirkung der Identität* $\forall x \in X : \; w(e, x) = x$,
(assoz) *Assoziativität* $\forall x \in X \forall g, h \in G : \; w(g, (w(h, x)) = w(gh, e)$.

Proposition 6.3.

(1) Ist W eine Gruppenwirkung, so definiert $w(g, x) := W(g)(x)$ eine gruppenwirkende Abbildung.
(2) Ist $w : G \times X \to X$ eine gruppenwirkende Abbildung, dann definiert $W(g)(x) := w(g, x)$ eine Gruppenwirkung.

Beweis.

(1) Angenommen W ist ein Homomorphismus von Gruppen. Die Eigenschaft $W(e) = \mathrm{Id}_X$ impliziert (id), die Eigenschaft $W(gh) = W(g)W(h)$ die Assoziativität von w.
(2) Wenn $w(g, x)$ eine gruppenwirkende Abbildung ist, definiert $W(g)(x) := w(g, x)$ eine Abbildung $W \to \mathrm{Abb}(X, X)$. Aus (id) folgt $W(e) = \mathrm{Id}_X$ und aus (assoz) folgt $W(gh) = W(g)W(h)$. Zu zeigen ist noch für alle $g \in G$: $W(g) \in \mathrm{Perm}(X)$, d.h. $W(g) : X \to X$ ist bijektiv. Wegen $W(g)W(g^{-1}) = \mathrm{Id}_X$ ist $W(g)$ surjektiv, und wegen $W(g^{-1})W(g) = \mathrm{Id}_X$ ist $W(g)$ injektiv.

$\square$

Bemerkung: Beachten Sie in diesem Beweis, an welcher Stelle die Eigenschaft (id) eingeht. Da jede Abbildung zwischen Gruppen mit $W(gh) = W(g)W(h)$ bereits das neutrale Element auf das neutrale Element abbildet, könnte man meinen, die eigenschaft (id) sei gar nicht nötig. Dies ist falsch. Konstruieren Sie eine Abbildung w, die (assoz), aber nicht (id) erfüllt. Sie werden sehen, dass dann die Bilder von W nicht bijektiv sind, also keine Elemente von $\mathrm{Perm}(X)$.

[1]

Ab sofort identifizieren wir Gruppenwirkungen mit den zugehörigen gruppenwirkenden Abbildungen.

Beispiele

(0) Sei G eine Gruppe und X eine Menge, dann ist $W(g)(x) = x$ eine Gruppenwirkung, die *triviale Gruppenwirkung von G auf X*.
(1) Sei $X = \mathbb{R}^n$, $G := \mathrm{GL}(n, \mathbb{R})$, $W(A) = \mathcal{L}_A \in \mathrm{Aut}(\mathbb{R}^n) \subset \mathrm{Perm}(\mathbb{R}^n)$, $w(A, v) = Av$,
(2) Sei $X = \{1, 2, \dots, n\}$, $G := \mathcal{S}_n = \mathrm{Perm}(X)$, $W = \mathrm{Id}_G$, $w(\sigma, k) = \sigma(k)$,
(3) Sei G eine Gruppe, $X := G$, $W(g)(x) = w(g, x) := gx$. *G operiert durch Linksmultiplikation auf sich selbst*
(4) Sei G eine Gruppe, $X := G$, $W(g)(x) = w(g, x) := xg^{-1}$. *$G$ operiert durch Rechtsmultiplikation auf sich selbst*
(5) Sei G eine Gruppe, $X := G$, $W(g)(x) = w(g, x) := gxg^{-1}$. *$G$ operiert durch Konjugation auf sich selbst*

Oft ist die Operation klar aus dem Kontext, man schreibt dann einfach gx für $W(g)(x)$.

Definition 6.4. Für beliebiges $x \in X$ definiert man die *Isotropiegruppe von x* als

$$G_x := \{g \in G \mid w(g, x) = x.$$

Ein Element $x \in X$ heißt *Fixpunkt*, falls $G_x = G$, d. h. $w(g, x) = x$ für alle $g \in G$. Die Wirkung W ist *treu*, falls Kern $(W : G \to \mathrm{Perm}(X)) = \{e\}$, d. h. $\forall g \in G \setminus \{e\} \exists x \in X : \; w(g, x) \neq x$.

Es gibt treue Abbildungen mit Fipunkten. Beispiel: Die Operation von $\mathrm{GL}(n, \mathbb{R})$ auf $\mathbb{R}^n$ ist treu und besitzt genau einen Fixpunkt, nämlich 0.

Satz 6.5 (Cayley). *Jede Gruppe ist isomorph zu einer Untergruppe einer Permutationsgruppe.*

Beweis. Wir betrachten wieder die Linkswirkung von G, $W : G \to \mathrm{Perm}(G)$, $W(g)(h) := gh$. Zu zeigen ist die Injektivität von W. Sobald wir wissen, dass W injektiv ist, liefert uns W einen Isomorphismus von G nach Bild$W \leq \mathrm{Perm}(G)$.

Sei also $g \in$ Kern W, d. h. $W(g) = \mathrm{Id}_G$. Insbesondere gilt dann also $W(g)(e) = \mathrm{Id}_G(e) = e$. Dies ist aber per definitionem von W gleich $ge = g$. Also $g = e$. □

[1]Achtung: Skriptnummerierung anders als in Vorlesung, zB. Vorlesung 6.5= Skript 6.7

Beispiel: Sei G eine endliche Gruppe, $n := \mathrm{ord}(G)$. Nach der obigen Bemerkung ist dann $\mathrm{Perm}(G) \cong \mathrm{Perm}(\{1, 2 \ldots, n\} = \mathcal{S}_n$. Jede endliche Gruppe ist also isomorph zu einer Untergruppe von einer symmetrischen Gruppe $\mathcal{S}_n$.

Vollständiges Verständnis aller Permutationsgruppen = vollständiges Verständnis aller Gruppen

Definition 6.6. Sei G Gruppe, $x \in G$ und w eine Gruppenwirkung. Die Menge

$$Gx := \{w(g, x) \,|\, g \in G\}$$

heißt *Orbit* oder *Bahn* von x unter der Wirkung w.

Lemma 6.7.

$$y \in Gx$$

ist eine Äquivalenzrelation auf der Menge X.

Beweis. Reflexivität: $x = w(e, x)$, also gilt $\forall x \in X : \quad x \in Gx$.

Symmetrie: Sei $y \in Gx$. Es gibt also ein $g \in G$ mit $y = w(g, x)$. Dann gilt $w(g^{-1}, y) = w(g^{-1}, w(g, x)) = w(g^{-1}g, x) = w(e, x) = x$. Also ist $x \in Gy$.

Transitivität: Sei $x \in Gy$ und $y \in Gz$. Es gibt also $g, h \in G$, so dass $x = w(g, y)$ und $y = w(h, z)$. Es folgt $x = w(g, y) = w(g, w(h, z)) = w(gh, z)$. Daraus folgt $x \in Gz$. □

Lemma 6.8.

$$\#G_x \cdot \#(Gx) = \#G$$

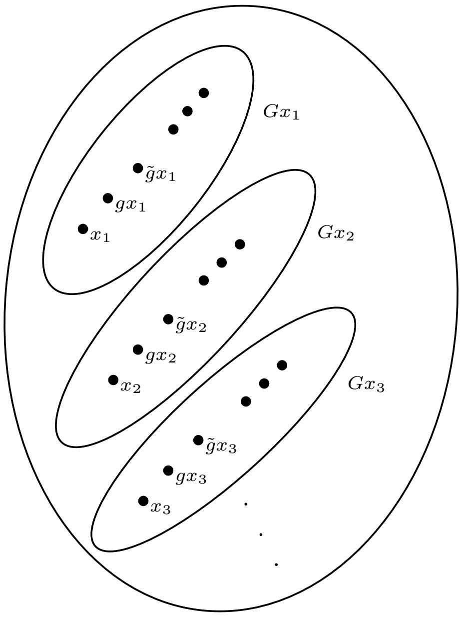
Beweis später.

Lemma 6.9 (Bahnengleichung)**.** *Sei w eine Operation von G auf X, und sei B die Menge aller Bahnen, d.h. $B := \{Gx | x \in X\}$. Dann gilt*

$$\#X = \sum_{Gx \in B} \#Gx.$$

Achtung: jede Bahn ergibt in dieser Summe nur einen Summand. Es ist damit nicht $\sum_{x \in X} \#Gx$ gemeint!

Beweis.



X ist die disjunkte Vereinigung der Gx aus B:

$$X = \dot{\bigcup_{Gx \in B}} Gx.$$

□

7. Nebenklassen und Faktorgruppen

Sei nun G eine Untergruppe und H eine Untergruppe. Wir betrachten die Gruppen-Operation von H auf G durch Links-Multiplikation

$$H \times G \to G, \qquad (h, g) \mapsto hg.$$

Die Bahn von x unter dieser Operation ist $Hx := \{hx | h \in H\}$, und wird die *Rechtsnebenklasse von* x genannt. Für $x, y \in G$ gilt also

$$x \in Hy \quad \Leftrightarrow \quad Hx = Hy \quad \Leftrightarrow \quad Hx \cap Hy \neq \emptyset \quad \Leftrightarrow \quad y \in Hx \quad \Leftrightarrow \quad xy^{-1} \in H.$$

Da $H \to G$, $h \mapsto hx$ injektiv ist, gilt $\#Hx = \mathrm{ord}(H)$. Wir definieren den Linksquotienten von G durch H:

$$H \backslash G := \{Hx | x \in G\}.$$

Wir nennen dann $(G : H) := \#(H \backslash G)$ den *(Links)-Index von* H *in* G.

Beispiel: Ist V ein Vektorraum mit Untervektorraum U, so betrachten wir die Gruppe $G = V$, versehen mit der Verknüpfung $+$. Dann ist $U\backslash V$ der Quotientenvektorraum.

Satz 7.1 (Lagrange)**.** *Ist $H \subset G$ eine Untergruppe, so gilt*

$$\mathrm{ord}(G) = \mathrm{ord}(H)(G : H).$$

Wie liest man diese Gleichung, wenn eine Menge unendlich groß ist?

Entweder als Mächtigkeiten. Oder mit den Konventionen $\forall n \in \mathbb{N}$

$$n \cdot \infty = \infty \cdot n = \infty \qquad \infty \cdot \infty = \infty.$$

Beweis. Wir wenden Lemma 6.9 an.

$$\mathrm{ord}(G) = \#G = \sum_{Hx \in H\backslash G} \#Hx = (G : H)\mathrm{ord}H$$

□

Nun betrachten wir die Operation durch Rechts-Multiplikation:

$$H \times G \to G, \qquad (h, g) \mapsto gh^{-1}.$$

Die Bahn von x ist dann $xH := \{xh^{-1} | h \in H\} = \{xh | h \in H\}$, die Linksnebenklasse von x. Und $G/H := \{xH | x \in G\}$ ist der Rechtsquotient.

$$x \in yH \quad \Leftrightarrow \quad xH = yH \quad \Leftrightarrow \quad y^{-1}x \in H.$$

Lemma 7.2.

$$\#(G/H) = \#(H\backslash G)$$

(Rechtsindex gleich Linksindex)

Beweis. Die Abbildung $i : G \to G$, $g \mapsto g^{-1}$ ist bijektiv, denn $i \circ i = \mathrm{Id}$. (Achtung: Sie ist kein Gruppenhomomorphismus, denn $i(xy) = i(y)i(x)$.) Man überprüft $i(xH) = Hx^{-1}$ und $i(Hx) = x^{-1}H$. Sie bildet also Rechstnebenklassen auf Linksnebenklassen in bijektiver Weise aufeinander ab. Insbesondere $\#(G/H) = \#(H\backslash G)$ □

Wir sagen von jetzt ab „Index von H in G" an Stelle von „Rechtsindex" oder „Linksindex".

Lemma 7.3. *Sei H eine Untergruppe von G.*

$$gH = Hg \quad \forall g \in G \qquad \Leftrightarrow \qquad gH \subset Hg \quad \forall g \in G \qquad \Leftrightarrow \qquad H \text{ ist Normalteiler von } G$$

Beweis. Wir formen um

$$gH \subset Hg \quad \Leftrightarrow \quad \forall h \in H : \; gh \in Hg \quad \Leftrightarrow \quad \forall h \in H : \; ghg^{-1} \in H.$$

Wir erhalten also: $gH \subset Hg$ für alle $g \in G$ genau dann, wenn $H \trianglelefteq G$.

Wir haben den rechten $\Leftrightarrow$-Pfeil gezeigt.

Wir rechnen ähnlich wie oben nach

$$Hg \subset gH \quad \Leftrightarrow \quad g^{-1}hg \in H \quad \Leftrightarrow \quad g^{-1}H \subset Hg^{-1}.$$

Es folgt: $Hg \subset gH \ \forall g \in G$ ist genau dann wahr, wenn $gH \subset Hg \ \forall g \in G$. Der linke $\Leftrightarrow$-Pfeil folgt. $\square$

Die Abbildung $\pi : G \to G/H$, $g \mapsto gH$ bezeichnet man oft als *kanonische Projektion von G nach G/H.*

Gesucht: Schöne, natürliche Gruppenstruktur auf G/H bzw. $H\backslash G$.

Satz 7.4. *Sei $(G, \bullet)$ eine Gruppe, und H eine Untergruppe von G.*

Genau dann, wenn H ein Normalteiler von G ist, gibt es eine Verknüpfung $\circ : G/H \times G/H \to G/H$, so dass das Diagramm

$$\begin{tikzcd} G \times G \arrow[r, "\bullet"] \arrow[d, "\pi \times \pi"] & G \arrow[d, "\pi"] \\ G/H \times G/H \arrow[r, "\circ"] & G/H \end{tikzcd}$$

kommutiert.

Diese Verknüpfung ist dann offensichtlich assoziativ, eH ist ein neutrales Element und das Inverse von gH ist $g^{-1}H$. Also ist dann $(G/H, \circ)$ eine Gruppe.

Beweis. Angenommen, solch ein Verknüpfung ist definierbar, dann muss auf Grund der Kommutativität des Diagramms bereits gelten:

$$xH \circ yH = xyH \quad \forall x, y \in G \tag{7.5}$$

Wir versuchen also die Verknüpfung durch (7.5) zu definieren. Wir müssen deshalb fragen: Wann ist die durch (7.5) definierte Verknüpfung wohldefiniert?

Zu üperprüfen ist also: Sei $xH = \tilde{x}H$ und $yH = \tilde{y}H$. Ist dann auch $xyH = \tilde{x}\tilde{y}H$?

1. Fall: Sei H nicht normal. Das heißt, es gibt ein $g \in G$ und ein $h \in H$ mit $ghg^{-1} \notin H$. Wir setzen $x := h$, $\tilde{x} := e$, $y := \tilde{y} := g^{-1}$. Es folgt $xH = H = \tilde{x}H$ und $yH = \tilde{y}H$. Wäre die Verknüpfung wohldefiniert, dann müsste also $hg^{-1}H = g^{-1}H$ gelten, was wiederum äquivalent zu der falschen Aussage $ghg^{-1} \in H$ ist. Also ist die Verknüpfung in diesem Fall nicht wohldefiniert.

2. Fall: Sei $H \trianglelefteq G$. Behauptung: Dann ist die Verknüpfung wohldefiniert.

Sei $xH = \tilde{x}H$ und $yH = \tilde{y}H$. Zu zeigen: $xyH = \tilde{x}\tilde{y}H$, oder äquivalent dazu $(\tilde{x}\tilde{y})^{-1}xy \in H$.

Setze $h_1 := \tilde{x}^{-1}x \in H$ und $h_2 := \tilde{y}^{-1}y \in H$. Dann gilt

$$(\tilde{x}\tilde{y})^{-1}xy = \tilde{y}^{-1}\tilde{x}^{-1}xy = \underbrace{\tilde{y}^{-1}h_1\tilde{y}}_{\in H}\underbrace{h_2}_{\in H} \in H.$$

Also ist durch (7.5) eine Verknüpfung $\circ$ wohldefiniert und das Diagramm kommutiert offensichtlich.

□

Nachtrag:

Beweis von Lemma 6.8. Sei w eine Wirkung von G auf X. Wir notieren gx für $w(g,x)$. Für ein festes $x \in X$ betrachten wir die Abbildung

$$j_x : G \to Gx, \qquad g \mapsto g.$$

Sie ist offensichtlich surjektiv. Es gilt $j_x(g) = j_x(\tilde{g})$ gdw $gx = \tilde{g}x$ gdw $\tilde{g}^{-1}gx = x$ gdw $\tilde{g}^{-1}g \in G_x$ gdw $gG_x = \tilde{g}G_x$. Wir erhalten also eine Bijektion J_x, so dass das Diagramm

$$\begin{tikzcd}
G \arrow[r, "j_x"] \arrow[d, "\pi"'] & Gx \\
G/G_x \arrow[ur, "J_x"'] &
\end{tikzcd}$$

komutiert. Es folgt $\#Gx = \#(G/G_x) = (G : G_x)$ und der Satz von Lagrange sagt dann

$$\#G = (G : G_x)\#G_x = \#Gx\#G_x.$$

□

8. Homomorphiesatz und Isomorphiesätze

Die Sätze dieses Abschnitts gelten in leicht veränderter Form auch, wenn wir überall Gruppen durch K-Vektorräume ersetzen Untergruppen und Normalteiler durch Untervektorräume ersetzen und von Homomorphismen von Vektorräumen reden.

Satz 8.1 (Homomorphiesatz). *Ist $f : G \to H$ ein Homomorphismus von Gruppen und ist N ein Normalteiler von G mit $N \subset \mathrm{Kern}\ f$, dann gibt es genau einen Homomorphismus $\bar{f} : G/N \to H$, so dass*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
G/N \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

kommmutiert. Hierbei ist wiederum $\pi : G \to G/N$ die kanonische Projektion. Außerdem gilt $\mathrm{Kern}\ \bar{f} = \pi(\mathrm{Kern}\ f)$. *Die Abbildung $\bar{f}$ ist also genau dann injektiv, wenn* $N = \mathrm{Kern}\ f$.

Beweis. Wenn es solch eine Abbildung $\bar{f}$ gibt, so muss gelten

$$\forall g \in G : \ \bar{f}(gN) = f(g). \tag{8.2}$$

Da jedes Element in G/N von der Form gN ist, wird durch (8.2) jedem Element (mindestens) ein Element in H zugeordnet. Wir wollen zeigen, dass diese Zuordnung auch wohldefiniert ist. Hierfür ist zu zeigen:

$$gN = \tilde{g}N \quad \Rightarrow \quad f(g) = f(\tilde{g}).$$

Wir rechnen:

$$\begin{aligned} & f(g) = f(\tilde{g}) \quad \Leftrightarrow \quad f(g)^{-1}f(\tilde{g}) = e \quad \Leftrightarrow \quad f(g^{-1}\tilde{g}) = e \\ \Leftrightarrow \quad & g^{-1}\tilde{g} \in \mathrm{Kern}\ f \quad \Leftarrow \quad g^{-1}\tilde{g} \in N \quad \Leftrightarrow \quad gN = \tilde{g}N. \end{aligned} \tag{8.3}$$

Es folgt, dass $\bar{f}$ wohldefiniert ist. Offensichtlich ist $\bar{f}$ dann ein Homomorphismus von Gruppen. Die restlichen Aussagen sind offensichtlich. □

Man sieht in dem Beweis sogar noch mehr: im Fall $N = \mathrm{Kern}\ f$ wird aus dem $\Leftarrow$-Pfeil in (8.3) ein $\Leftrightarrow$-Pfeil. Also ist in diesem Fall sogar $\bar{f}$ injektiv. Es folgt:

Folgerung 8.4. *Ist $f : G \to H$ ein Homomorphismus, dann gibt es genau einen Isomorphismus $\bar{f} : G/\mathrm{Kern}\ f \to \mathrm{Bild} f$, so dass*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
G/\mathrm{Kern}\ f \arrow[r, "\overline{f}"] & \mathrm{Bild} f \arrow[u]
\end{tikzcd}$$

kommutiert.

Satz 8.5 (1. Isomorphiesatz)**.** *Sei G Gruppe, $H \leq G$, $N \trianglelefteq G$. Dann ist $HN := \{hn \,|\, h \in H,\ n \in N\}$ eine Untergruppe von G und $N \trianglelefteq HN$ und $H \cap N \trianglelefteq H$. Es gibt genau eine Abbildung $I_1 : H/H \cap N \to HN/N$ so dass*

$$\begin{tikzcd}
H \arrow[r, "\mathrm{incl}"] \arrow[d, "\pi"'] & HN \arrow[d, "\pi"] \\
H/H \cap N \arrow[r, "I_1"] & HN/N
\end{tikzcd}$$

kommutiert und I_1 ist ein Isomorphismus von Gruppen.

Beweis. $e \in HN$ und es gilt $\forall h, \tilde{h} \in H\ \forall n, \tilde{n} \in N$:

$$hn\tilde{h}\tilde{n} = h\tilde{h}\underbrace{\tilde{h}^{-1}n\tilde{h}}_{\in N}\tilde{n} \in HN$$

$$(hn)^{-1} = (\underbrace{hnh^{-1}}_{=:\hat{n} \in N}h)^{-1} = h^{-1}\hat{n}^{-1}.$$

Also ist HN nicht-leer und abgescholssen unter Multiplikation und Inversenbildung.

$N \trianglelefteq HN$ ist dann offensichtlich, ebenso $H \cap N \leq H$.

Der Homomorphismus $H \to HN \to HN/N$, $h \mapsto hN$ ist surjektiv (denn $\forall h \in H \forall n \in N$ repräsentieren hn und h dasselbe Element in G/N) und der Kern dieses Homomorphismus ist

$$\{h \in H \,|\, hN = N\} = \{h \in H \,|\, h \in N\} = N \cap H.$$

Also ist $N \cap H$ ein Normalteiler und der 1. Isomorphiesatz folgt dann aus dem Homomorphiesatz. $\square$

Satz 8.6 (2. Isomorphiesatz)**.** *Sei G eine Gruppe, $N \leq H \trianglelefteq G$ mit $N \trianglelefteq G$. Dann kann man H/N als Normalteiler in G/N auffassen. Die eindeutige Abbildung $I_2 : G/H \to (G/N)/(H/N)$, für die*

$$\begin{tikzcd} G \arrow[r] \arrow[d] & G/N \arrow[d] \\ G/H \arrow[r, "I_2"] & (G/N)/_{(H/N)} \end{tikzcd}$$

kommutiert, ist ein Gruppenisomorphismus,

Beweis. Offensichtlich $N \trianglelefteq H$. Der Kern des Homomorphismus $H \to G \to G/N$, $h \mapsto hN$ ist

$$\{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = N.$$

Mit dem Homomorphiesatz erhalten wir einen Monomorphismus $H/N \to G/N$, mit Hilfe dessen wir H/N mit seinem Bild $M(H/N)$ identifizieren. Also $(H/N) \leq G/N$. Man prüft nach: $\forall h \in H\, \forall g \in G$:

$$gN\, hN\, (gN)^{-1} = ghg^{-1}\, N \in H/N,$$

also ist $H/N \trianglelefteq G/N$.

Ein $g \in G$ liegt genau dann im Kern des Epimorphismus $G \to G/N \to (G/N)/(H/N)$, wenn $gN \in H/N$, d.h. gdw es ein $h \in H$ gibt mit $gN = hN$. Wegen $N \subset H$ ist dies wiederum zu $g \in H$ äquivalent. Der Kern von $G \to G/N \to (G/N)/(H/N)$ ist somit H und der Homomorphiesatz ergibt den 2. Isomorphiesatz. $\square$

9. Mehr über zyklische Gruppen und über $\mathbb{Z}/n\mathbb{Z}$

Wdh: Eine Gruppe G ist
zyklisch
$\Leftrightarrow$ sie wird einem Element erzeugt wird, d. h. $\exists g \in G : \quad G = \langle g \rangle$.
$\Leftrightarrow$ Es existiert ein Epimorphismus $\mathbb{Z} \to G$

Lemma 9.1. *Sei G eine endliche Gruppe und sei* $\mathrm{ord}(p)$ *eine Primzahl. Dann ist G zyklisch.*

Beweis. Sei $a \in G$, $a \neq e$. Nach dem Satz von Lagrange gilt $\mathrm{ord}(a)|p$, aber wegen $a \neq e$ gilt $\mathrm{ord}(a) \neq 1$, also $\mathrm{ord}(a) = p$. Somit gilt auch $\mathrm{ord}(\langle a \rangle) = p = \mathrm{ord}(G)$, also $G = \langle a \rangle$. □

Wir wissen bereits: G ist Untergruppe von $\mathbb{Z}$ genau dann, wenn es ein $n \in \mathbb{N}_0$ gibt mit $G = n\mathbb{Z} = (n) = \langle n \rangle$.

Lemma 9.2. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Beweis. Sei H eine Untergruppe der zyklischen Gruppe G. Sei $f : \mathbb{Z} \to G$ ein Epimorphismus. Dann ist $f^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$, also $f^{-1}(H) = k\mathbb{Z}$ für ein $k \in \mathbb{Z}$. Dann ist $f|_{k\mathbb{Z}} : k\mathbb{Z} \to G$ ein Homomorphismus mit Bild H. Die Komposition

$$\begin{array}{ccc} \mathbb{Z} & \to & k\mathbb{Z} \to H \\ r & \mapsto & kr \to f(kr) \end{array}$$

ist ein Epimorphismus. Also ist H zyklisch. □

Beispiele: Die Untergruppen von $\mathbb{Z}/6\mathbb{Z}$ sind $\{\bar{0}\} \cong \mathbb{Z}/\mathbb{Z}$, $\{\bar{0}, \bar{3}\} \cong \mathbb{Z}/2\mathbb{Z}$, $\{\bar{0}, \bar{2}, \bar{4}\} \cong \mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ selbst.

Allgemein: die Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ sind die Gruppen der Form $\langle \bar{k} \rangle$, $k|n$. Es gilt $\mathrm{ord}(\langle \bar{k} \rangle) = \mathrm{ord}(k) = n/k$. Wir haben gezeigt:

Korollar 9.3. *In einer zyklischen Gruppe von Ordung n gibt es zu jedem $d|n$ genau eine Untergruppe der Ordung d.*

□

Chinesischer Restsatz.
Betrachte nun die Abbildung $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $x \mapsto (x \mod n, x \mod m)$ mit $n, m \in \mathbb{N}$. Offensichtlich ist dies ein Gruppenhomorphismus und es gilt:

$$a \in \text{Kern } \phi \quad \Leftrightarrow \quad m|a \text{ und } n|a \quad \Leftrightarrow \quad \mathrm{kgV}(n,m)|a \quad \Leftrightarrow \quad a \equiv 0 \mod \mathrm{kgV}(n,m).$$

Somit $\phi(a) = \phi(b)$ genau dann, wenn $a \equiv b \mod \mathrm{kgV}(n,m)$.

Es gibt also genau eine Abbildung ψ, so dass

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, "\phi"] \arrow[ddd, "\pi"'] & & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\
& x \arrow[r, mapsto] \arrow[d, mapsto] & (x \mod n, x \mod m) \\
& x \mod kgV(n,m) & \\
\mathbb{Z}/kgV(n,m)\mathbb{Z} \arrow[uuurr, "\psi"'] & &
\end{tikzcd}$$

kommutiert und ψ ist ein Monomorphismus von Gruppen. Nun ist aber $\mathrm{ord}(\mathbb{Z}/n\mathbb{Z}) = n$. Wenn n und m teilerfremd sind ($\mathrm{ggT}(n,m) = 1$), dann ist $\mathrm{kgV}(n,m) = nm$, somit also $\mathrm{ord}(\mathbb{Z}/\mathrm{kgV}(n,m)\mathbb{Z}) = \mathrm{ord}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$. Im Fall $\mathrm{ggT}(n,m) = 1$ ist somit ψ ein Isomorphismus.

Satz 9.4 (Chinesischer Restsatz). *Falls* $\mathrm{ggT}(n,m) = 1$*, dann ist* $\mathbb{Z}/nm\mathbb{Z}$ *isomorph zu* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*.*

Bemerkung: Mit analogen Methoden zeigt man, dass dieser Isomorphismus nicht nur ein Isomorphismus von Gruppen, sondern sogar ein Isomorphismus von Ringen ist.

Beispiele:
(1) $\mathbb{Z}/45\mathbb{Z}$ ist isomorph zu $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, der Isomorphismus ist gegeben durch $x \mod 45 \mapsto (x \mod 5, x \mod 9)$.
(2) $\mathbb{Z}/4\mathbb{Z}$ ist nicht isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Angenommen es gäbe solch einen Isomorphismus $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Da $\bar{1}$ Ordung 4 hat, müsste auch $\phi(\bar{1})$ Ordnung 4 haben. Alle Elemente in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ haben aber Ordnung ≤ 2. Widerspruch.

Anwendung: Berechnen Sie alle Lösungen $x \in \mathbb{Z}$ der Gleichung

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 4 \mod 9 \end{aligned}$$

Bestimme zunächst eine ganzzahlige Lösung von $a5 + b9 = 1$. Dies ist zum Beispiel $a = 2$, $b = -1$. (Euklidischer Algorithmus)
Ansatz

$$x = 5k + 2 = 9r + 4$$

mit $k, r \in \mathbb{Z}$. Also $5k - 9r = 2$. Eine spezielle Lösung ist also $k = 2a = 4$, $r = -2b = 2$. Somit ist $x = 22$ eine spezielle Lösung des inhomogenen Gleichungssystems. Die gesamte Lösungsmenge erhält daraus unter Betrachtung des homogenen Gleichunngsystems

$$\begin{aligned} x &\equiv 0 \mod 5 \\ x &\equiv 0 \mod 9 \end{aligned}$$

Der chinesische Restsatz besagt, dass die Lösungen hiervon alle $x \equiv 0 \mod 45$ sind. Die Lösungsmenge des inhomomgenen Systems ist also

$$\{22 + 45k \,|\, k \in \mathbb{Z}\}.$$

Der chinesische Restsatz besagt zum Beispiel, dass man $\mathbb{Z}/60\mathbb{Z}$ isomorph zum Produkt $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ist. Der folgende Satz besagt, dass man jede endlich erzeugte abelsche Gruppe so ähnlich zerlegen kann.

Satz 9.5 (Hauptsatz der endlich erzeugten abelschen Gruppen)**.** *Sei G eine endlich erzeugte, abelsche Gruppe. Dann gibt es Primzahlen $p_1, \dots, p_k$ und $n_0, n_1, \dots, n_k \in \mathbb{N}$, so dass G als* **Gruppe** *isomorph zu*

$$\mathbb{Z}^{n_0} \times (\mathbb{Z}/{p_1}^{n_1}\mathbb{Z}) \times (\mathbb{Z}/{p_2}^{n_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/{p_k}^{n_k}\mathbb{Z})$$

ist. Diese Zerlegung ist bis auf Reihenfolge eindeutig.

Man beachte: die p_i müssen nicht paarweise verschieden sein.

Die Zahl n_0 heißt *Rang von G*.

Beweis des Satzes später.

Man kann diesen Satz mit eher elementaren Methoden zeigen (siehe z.B. [**2**]). Wir werden aber im Rahmen der Modul-Theorie den Elementarteiler-Satz zeigen, aus dem der obige Hauptsatz als Spezialfall folgt.

Bemerkung: $(\mathbb{Q}, +)$ und $(\mathbb{Q}/\mathbb{Z}, +)$ sind abelsch, aber nicht endlich-erzeugt. Sie sind nicht Produkt von zyklischen Gruppen.

Kleiner Fermatscher Satz.
Betrachte nun $\mathbb{Z}/n\mathbb{Z}$. Sei $m \in \mathbb{Z}$ gegeben.

$\bar{m}$ ist invertierbar in $\mathbb{Z}/n\mathbb{Z}$
$\Leftrightarrow$ es gibt ein Inverses $\bar{b}$ von $\bar{m}$, d.h. $\bar{m}\bar{b} = \bar{1}$
$\Leftrightarrow$ die Gleichung $an + bm = 1$ besitzt eine ganzzahlige Lösung
$\Leftrightarrow$ n und m sind teilerfremd.

$\bar{m}$ invertierbar $\Leftrightarrow$ $\bar{m}$ ist weder Null noch ein Nullteiler.

$(\mathbb{Z}/n\mathbb{Z})^*$ ist eine (multiplikative) Gruppe. Sie ist im allgemeinen **nicht** zyklisch. Beispiel: $(\mathbb{Z}/8\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Die Funktion $\phi : \mathbb{N} \to \mathbb{N}$, $\phi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ heißt *Eulersche ϕ-Funktion*.

Sei $\operatorname{ord}(\bar{x})$ die (multiplikative) Ordnung von $\bar{x}$ in $(\mathbb{Z}/n\mathbb{Z})^*$. Der Satz von Lagrange besagt

$$\operatorname{ord}(\bar{x})|\operatorname{ord}((\mathbb{Z}/n\mathbb{Z})^*) = \phi(n).$$

Also gilt $\bar{x}^{\operatorname{ord}(\bar{x})} = \bar{1}$, also auch $\bar{x}^{\phi(n)} = \bar{1}$.

Wir haben gezeigt:

Satz 9.6 (Kleiner Satz von Fermat)**.** *Seien $n \in \mathbb{N}$, $x \in \mathbb{Z}$ mit* $\operatorname{ggT}(n, x) = 1$*. Dann gilt*

$$x^{\phi(n)} \equiv 1 \mod n.$$

□

Anwendungen: Kryptographie. Public-Key-Verfahren.

Korollar 9.7. *Sei $p \in \mathbb{N}$ prim. Dann gilt für alle $x \in \mathbb{Z}$*

$$x^p \equiv x \mod p.$$

Beweis des Korollars. Wenn x von p geteilt wird, dann gilt $x \equiv 0 \mod p$, also auch $x^p \equiv 0 \mod p$.

Falls p nicht x teilt, besagt der obige Satz:

$$x^{\phi(p)} \equiv 1 \mod p.$$

Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, gilt $\phi(p) = p-1$. Multiplizieren von $x^{p-1} \equiv 1$ mit x ergibt die Behauptung. □

10. Innere Automorphismen und Zentrum

Sei G eine Gruppe.

Es wirke G auf sich selbst durch Konjugation

$$C : G \to \operatorname{Perm}(G), \qquad g \mapsto c_g$$

wobei $c_g : G \to G$, $h \mapsto ghg^{-1}$. Die Abbildung c_g ist ein Automorphismus von G: die Bijektivität ist klar, und es gilt $\forall h, \tilde{h} \in G$:

$$c_g(h\tilde{h}) = gh\tilde{h}g^{-1} = ghg^{-1}g\tilde{h}g^{-1} = c_g(h)c_g(\tilde{h}).$$

Ein Automorphismus $\alpha \in \operatorname{Aut}(G)$ heißt *innerer Automorphismus*, falls es ein $g \in G$ gibt mit $\alpha = c_g$. Die Menge der inneren Automorphismen, $\operatorname{Inn}(G)$ ist also das Bild von C. Insbesondere $\operatorname{Inn}(G) \leq \operatorname{Aut}(G)$. Ist α ein beliebiger Automorphismus, dann gilt $\alpha \circ c_g \circ \alpha^{-1} = c_{\alpha(g)}$, somit gilt $\operatorname{Inn}(G) \trianglelefteq \operatorname{Aut}(G)$.

Den Kern von C nennen wir das *Zentrum von G*

$$Z(G) := \operatorname{Kern} C = \{z \in G \,|\, c_z = \operatorname{Id}_G\} = \{z \in G \,|\, zg = gz \,\forall g \in G\}.$$

Offensichtlich $Z(G) \trianglelefteq G$.

Sei $x \in G$. Die Isotropiegruppe von x nennt man in diesem Fall den *Zentralisator*

$$Z_{\{x\}} = \{z \in G \mid zx = xz\} \leq G.$$

Es gilt dann $Z = \cap_{x \in G} Z_{\{x\}}$. Ferner $c_g(Z_{\{x\}}) = Z_{\{c_g(x)\}}$.

Die Bahn $Gx = \{c_g(x) \mid g \in G\}$ nennt man *Konjugationsklasse von x*. Falls $x \in Z$, dann $G = \{x\}$. Falls $x \in G \setminus Z$, dann ist Gx ganz in $G \setminus Z$ enthalten und besitzt mindestens zwei Elemente. Wir schreiben also alle Bahnen in $G \setminus Z$ als $Gx_1, \ldots, Gx_r$. Dann gilt $\#Gx_i = \#(G/Z_{\{x_i\}}) = (G : Z_{\{x_i\}})$. Die Bahnengleichung (Lemma 6.9) ergibt den Satz.

Satz 10.1 (Klassengleichung)**.** *Sei G eine endliche Gruppe mit Zentrum Z und seien $Gx_1, \ldots, Gx_r$ die Bahnen der Konjugations-Wirkung auf $G \setminus Z$. Dann gilt:*

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

□

11. Der Normalisator

Sei G eine Gruppe und S eine Teilmenge. Wir definieren den *Normalisator von S ind G* als

$$N_S := \{x \in G \mid xS = Sx\}.$$

Beispiel: Sei S eine Untergruppe von G. Dann gilt

$$N_S = G \quad \Leftrightarrow \quad S \triangleleft G.$$

Sei $X := \mathcal{P}(G)$ die Potenzmenge von G, d. h. $s \in X$. Wir definieren auf X eine Operation von G: Sei $g \in G$, $A \in X = \mathcal{P}(G)$,

$$w(g, A) := gAg^{-1} = \{c_g(a) \mid a \in A\}.$$

Die Isotropiegruppe von S dieser Operation ist der Normalisator N_S. Insbesondere ist N_S eine Untergruppe von G. Ist S eine Untergruppe, dann ist N_S die größte Untergruppe von G, die S als Normalteiler enthält. Sei wieder S ein Untergruppe. Dann ist S genau dann ein Fixpunkt von w, wenn S ein Normalteiler von G ist.

12. Die Sätze von Sylow

Ziel: bessere Kenntnis endlicher Gruppen. Wir schreiben in diesem Abschnitt alle Gruppen multiplikativ mit neutralem Element e.

Achtung: im Fall der Gruppe $G = (\mathbb{Z}/m\mathbb{Z}, +)$ bedeutet dies für $g = \bar{a}$, $h = \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ $gh = \overline{a+b}$, $e = \bar{0}$, $g^k = \overline{ka}$, d.h. für $g = \bar{1}$

$$g^k = e \quad \Leftrightarrow \quad m|k.$$

Definition 12.1. Sei p eine Primzahl. Eine Gruppe H heißt *p-Gruppe*, falls es eine Zahl $k \in \mathbb{N}$ gibt mit $\operatorname{ord}(H) = p^k$.
Sei G eine endliche Gruppe. Eine Untergruppe $H \leq G$ heißt p-Sylow-Gruppe, falls H eine p-Gruppe ist und falls $p \not| (G : H)$.

Beispiel: $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ sind p-Gruppen

Beispiel: Die Symmetriegruppe eines Quadrats in der Ebene hat 8 Elemente und ist somit eine 2-Gruppe.

Beispiel: Sei $p \not| \operatorname{ord}(G)$. Dann ist $\{e\}$ eine p-Sylow-Gruppe.

Beispiel: Sei G abelsch. Dann besagt Satz 9.5:

$$G \cong (\mathbb{Z}/{p_1}^{n_1}\mathbb{Z}) \times (\mathbb{Z}/{p_2}^{n_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/{p_k}^{n_k}\mathbb{Z})$$

mit p_i prim. Wir nehmen an, dass $p = p_1 = p_2 = \cdots = p_r$ und $p \neq p_i$ für alle anderen p_i. Dann ist

$$\mathbb{Z}/{p_1}^{n_1}\mathbb{Z} \times (\mathbb{Z}/{p_2}^{n_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/{p_r}^{n_r}\mathbb{Z}) \times \{e\} \times \{e\} \times \cdots \times \{e\} = \{g \in G \,|\, \exists k \in \mathbb{N} : \; g^{p^k} = e\}$$

die einzige p-Sylow-Gruppe von G.

Lemma 12.2. *Sei p eine Primzahl und $G \ncong \{e\}$ eine p-Gruppe. Dann teilt p die Ordnung von Z. Insbesondere $Z \neq \{e\}$. Es gibt in Z Elemente von Ordnung p.*

Beweis. Sei $\operatorname{ord}(G) = p^k$. Es gilt

$$x \notin Z \quad \Leftrightarrow \quad \#Gx \leq 2 \quad \Leftrightarrow \quad (G : Z_{\{x\}}) \leq 2.$$

Nach dem Satz von Lagrange ist $(G : Z_{\{x_i\}})$ ein Teiler von p^k. Also $p|(G : Z_{\{x_i\}})$. Somit folgt aus der Klassengleichung $p|\operatorname{ord}(Z)$. Also auch $Z \neq \{e\}$. Sei $a \in Z$, $a \neq \{e\}$. Dann ist $\operatorname{ord}(a) = p^r$ mit $r \in \{1, 2, \ldots, k\}$. Dann ist auch $a' := a^{p^{r-1}}$ in Z und $\operatorname{ord}(a') = p$. $\square$

Proposition 12.3. Diese Proposition wurde in der Vorlesung zunächst übersprungen und wird nach hinten verschoben.

Theorem 12.4 (Frobenius)**.** *Sei G eine endliche Gruppe und p^k eine Potenz der Primzahl p mit $p^k|\operatorname{ord}(G)$. Sei s die Anzahl der Untergruppen $H \leq G$ mit $\operatorname{ord}(H) = p^k$. Dann gilt*

$$s \equiv 1 \mod p.$$

Insbesondere gibt es mindestens eine Untergruppe von Ordnung p^k.

Anwendung: Wähle k maximal. Dann besagt das Theorem, dass mindestens eine p-Sylow-Gruppe in G existiert, und die Anzahl der p-Sylow-Gruppen ist $\equiv 1 \mod p$.

Um das Theorem zu zeigen, zeigen wir zunächst das folgende Lemma:

Lemma 12.5. *Angenommen die Voraussetzungen des Theorems gelten. Sei $n := \operatorname{ord}(G)$. Dann gilt:*

$$s \equiv \binom{n-1}{p^k-1} \mod p.$$

Beweis von „Lemma ⇒ Theorem“. Zu zeigen ist nur noch

$$\binom{n-1}{p^k-1} \equiv 1 \mod p. \tag{12.6}$$

für alle $n, k \in \mathbb{N}$ und Primzahlen p mit $p^k|n$. Nach Korollar 9.3 gibt es genau eine Untergruppe von $\mathbb{Z}/n$ von Ordnung p^k, Wir wenden nun das Lemma auf $G = \mathbb{Z}/n$ an und erhalten Gleichung (12.6) für die gegebenen n, k, p. □

Beweis des Lemmas. Wie in [**1**, Abschnitt 5.2 Sylow-Gruppen, Lemma 7].

Lemma 12.7. *Es sei G eine endliche Gruppe, $H \leq G$ eine p-Untergruppe, $S \leq G$ eine p-Sylow-Gruppe. Dann existiert $g \in G$ mit*

$$H \leq gSg^{-1}.$$

Beweis. Wie in [**1**, Abschnitt 5.2 Sylow-Gruppen, Lemma 9].

Korollar 12.8. *Sei G eine endliche Gruppe. Dann sind alle p-Sylow-Gruppen konjugiert, d.h. für zwei p-Sylow-Gruppen S_1 und S_2 gibt es ein $g \in G$ mit $S_1 = gS_2g^{-1}$.*

□

Lemma 12.9. *Sei G eine endliche Gruppe und N_S der Normalisator einer p-Sylow-Gruppe in G. Dann ist die Anzahl aller p-Sylow-Gruppen in G gleich $(G : N_S)$.*

Beweis. Wie in [**1**, Abschnitt 5.2 Sylow-Gruppen, Lemma 10].

Wir fassen zusammen:

Theorem 12.10 (Sylowsche Sätze)**.** *Sei G eine endliche Gruppe und p eine Primzahl.*

(1) *Die Anzahl s der p-Sylow-Gruppen in G erfüllt*

$$s|\operatorname{ord}(G) \qquad \textit{und} \qquad s \equiv 1 \mod p.$$

(2) *Je zwei p-Sylow-Gruppen sind zueinander konjugiert.*
(3) *Jede p-Untergruppe ist in einer p-Sylow-Gruppe enthalten.*

Satz 12.11. *Sei G eine Gruppe der Ordnung pq, wobei p und q Primzahlen sind mit $p < q$, $p \not| (q-1)$. Dann ist G zyklisch.*

PROPOSITION 12.12. *Sei G eine Gruppe mit sei Inn(G) zyklisch. Dann ist G abelsch, d.h. Inn$(G) = \{\mathrm{Id}\}$.*

Daraus folgt auch: Jede Gruppe mit zyklischer Automorphismengruppe ist abelsch.

Beweis. Schreibe kurz $Z := Z(G)$. Wir wissen bereits $G/Z \cong \mathrm{Inn}(G)$. Angenommen G/Z werde von der gZ, $g \in G$ erzeugt, d. h. $G/Z = \{g^k Z \mid k \in \mathbb{Z}\}$. Beliebige $h_1, h_2 \in G$ kann man also in der Form $h_1 = g^k z$, $h_2 = g^m w$ mit $k, m \in \mathbb{Z}$ und $z, w \in Z$ schreiben.

$$h_1 h_2 = g^k z g^m w = g^k g^m z w = g^{k+m} z w$$
$$h_2 h_1 = g^m w g^k z = g^m g^k w z = g^{k+m} z w$$

Also ist G abelsch. □

PROPOSITION 12.13. *Sei G eine Gruppe der Ordnung p^2, p Primzahl. Dann ist $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Wir zeigen zunächst, dass G abelsch ist. Aufgrund von Lemma 12.2 gilt $p|\mathrm{ord}(Z(G))$. Also ist $\mathrm{ord}(G/Z(G)) = (G : Z(G)) = p^2/\mathrm{ord}(Z(G)) \in \{1, p\}$. Also ist $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ (siehe Lemma 9.1) oder $G = Z(G)$. In beiden Fällen ist G/Z zyklisch und somit G abelsch, also tritt nur der Fall $G = Z$ auf.

Wir unterscheiden wieder zwei Fälle. Erster Fall: Es gebe ein $x \in G$ mit $\mathrm{ord}(x) = p^2$. Dann erzeugt x bereits G. Zweiter Fall: für alle $x \in G \setminus \{e\}$ gilt $\mathrm{ord}(x) = p$. Wähle ein derartiges $x \in G$ und ein $y \in G \setminus \langle x \rangle$. Dann ist $y\langle x \rangle$ ein nichttriviales Element in $G/\langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$ und erzeugt somit $\mathbb{Z}/p\mathbb{Z}$. Es folgt $y^r \in \langle x \rangle$ gdw $p|r$. Also ist $x^k y^r \neq e$ im Fall $p \not| r$. Im Fall $p|r$ baechate man $\mathrm{ord}(y) = p$, also $x^k y^r = x^r$ somit ist der Kern der Abbildung $\mathbb{Z} \times \mathbb{Z} \to G$, $(k, l) \mapsto x^k y^l$, gleich $p\mathbb{Z} \times p\mathbb{Z}$. Wir erhalten einen Monomorphismus $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to G$ und da $\mathrm{ord}/G) = p^2$ ist dieser Monomrphismus auch surjektiv. □

13. Semidirekte Produkte und exakte Sequenzen

DEFINITION 13.1. Seien G und H Gruppen und $\phi : H \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus. Wir versehen die Menge $G \rtimes H$ mit dem folgenden Produkt

$$\begin{array}{rcl} \bullet : (G \times H) \times (G \times H) & \to & (G \times H) \\ (g, h) \bullet (\tilde{g}, \tilde{h}) & := & (g\phi(h)(\tilde{g}), h\tilde{h}) \end{array}$$

Die Menge $G \times H$ versehen mit der Multiplikation $\bullet$ nennen wir *semi-direktes Produkt $G \rtimes_\phi H$* oder $G \rtimes H$.

Das semi-direkte Produkt ist eine Gruppe:
Assoziativität:

$$[(g,h) \bullet (\tilde{g},\tilde{h})] \bullet (\hat{g},\hat{h}) = (g\phi(h)(\tilde{g}), h\tilde{h}) \bullet (\hat{g},\hat{h}) = (g\phi(h)(\tilde{g})\phi(h\tilde{h})(\hat{g}), h\tilde{h}\hat{h})$$
$$= (g\, \underbrace{\phi(h)(\tilde{g}\phi(\tilde{h})(\hat{g}))}_{\phi(h)(\tilde{g})\phi(h)\phi(\tilde{h})(\hat{g})}, h\tilde{h}\hat{h}) = (g,h) \bullet (\tilde{g}\phi(\tilde{h})(\hat{g}), \tilde{h}\hat{h}) = (g,h) \bullet [(\tilde{g},\tilde{h}) \bullet (\hat{g},\hat{h})]$$

(e,e) ist linksneutrales

$$(e,e) \bullet (g,h) = (e\phi(e)(g), eh) = (g,h).$$

Und $(\phi(h^{-1})(g^{-1}), h^{-1})$ ist Linksinverses von (g,h).

$$((\phi(h^{-1})(g^{-1}), h^{-1}) \bullet (g,h) = (\underbrace{\phi(h^{-1})(g^{-1})\phi(h^{-1})(g)}_{\phi(h^{-1})(e)=e}, h^{-1}h) = (e,e)$$

Also ist nach Proposition 1.2 $G \rtimes H$ mit der Multiplikation $\bullet$ eine Gruppe.

Offensichtlich ist $H \to G \rtimes H$, $h \mapsto (e,h)$ ein Gruppenmonomorphismus, als ist das Bild kanonisch isomorph zu H.

Offensichtlich ist $G \to G \rtimes H$, $g \mapsto (g,e)$ ein Gruppenmonomorphismus, als ist das Bild kanonisch isomorph zu G.

Bsp: $K^n \rtimes \mathrm{GL}(n,K)$

Lemma 13.2. *Sei G eine Gruppe, N, H Untergruppen mit $N \trianglelefteq G$. Es gelte $G = HN$ und $H \cap N = \{e\}$. Dann ist G isomorph zu $N \rtimes_\phi H$, wobei $\phi : H \to Aut(N)$, $h \mapsto (n \mapsto hnh^{-1})$ die Konjugation ist.*

Beweis. *Nicht ausgefuehrt* □

Definition 13.3. Eine Folge von Gruppen-Homomorphismen

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \cdots \xrightarrow{f_{n-1}} G_n$$

nennt man eine *exakte Sequenz von Gruppen*, wenn für alle $i \in \{1, \ldots, n-1\}$ gilt $\mathrm{Bild}(f_i) \subset \mathrm{Kern}\,(f_{i+1})$. Im Spezialfall $n = 5$ und $G_1 = \{e\} = G_5$ nennt man die Sequenz eine *kurze exakte Sequenz*. Man nennt in diesem Fall auch G_3 eine *Erweiterung von G_4 durch G_2*.

$1 \to G \xrightarrow{f} H \to 1$ ist exakt gdw f ist Isomorphismus.

Sei $H \trianglelefteq G$, dann ist $1 \to H \to H \to G \to G/H \to 1$ eine kurze exakte Sequenz.

Umgekehrt ist $1 \to H \xrightarrow{i} G \to K \to 1$, eine kurze exakte Sequenz, dann ist $i(H) \trianglelefteq G$ und $G/i(H) \cong K$ (Grund: Homomorphiesatz bzw. seine Folgerung).

Ist $f : G \to H$ ein Homorphismus, dann ist $1 \to \mathrm{Kern}\,(G) \to G \to \mathrm{Bild}(f) \to 1$ exakt.

Der 1. Isomorphiesatz besagt dann: ist H eine Untergruppe und N ein Normalteiler von einer Gruppe G, dann ist $1 \to H \cap N \to H \to HN/N \to 1$ eine exakte Sequenz.

Falls die Gruppe K auf H operiert, dann ist auch die Sequenz

$$\begin{array}{rcl} 1 \to H \to & H \rtimes K \to & K \to 1 \\ h \mapsto & (h, e) & \\ & (h, k) \mapsto & k \end{array}$$

exakt.

Definition 13.4. Sei $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ eine kurze exakte Sequenz. Ein *Schnitt* ist ein Homomorphismus $s : K \to G$ gibt mit $\pi \circ s = \mathrm{Id}_K$.

Proposition 13.5. *Eine kurze exakte Sequenz* $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ *hat einen Schnitt genau dann, wenn es eine Wirkung von* K *auf* H *gibt* $\phi : K \to Aut(H)$, *so dass* $G \cong H \rtimes K$, *und der Isomorphismus ist so, dass*

$$\begin{tikzcd}
 & & G \arrow[dr] & & \\
1 \arrow[r] & H \arrow[ur] \arrow[dr] & \circlearrowleft \; \wr\| \; \circlearrowleft & K \arrow[r] & 1 \\
 & & H \rtimes K \arrow[ur] & &
\end{tikzcd}$$

kommutiert.

Beweis. Im Fall $G = H \rtimes K$ definieren wir $s(k) = (e, k)$ und der Fall $G \cong H \rtimes K$ geht so ähnlich.

Sei nun umgekehrt ein Schnitt s gegeben. Dann ist $i(H) \trianglelefteq G$ und $s(K) \leq G$. Sei $g \in i(H) \cap s(K)$. Wir schreiben $g = s(k)$. Wegen $g \in i(H) = \text{Kern } (\pi)$, sehen wir $e = \pi(g) = \pi(s(k)) = k$. Somit $g = e$. Also $i(H) \cap s(K) = \{e\}$.

Sei nun ein beliebiges $g \in G$ gegeben. Betrachte $h := gs(\pi(g^{-1}))$. Berechne $\pi(h) = \pi(g)\pi(s(\pi(g^{-1}))) = \pi(g)\pi(g)^{-1} = e$. Also $h \in \text{Kern } \pi = i(H)$. Setze $z := \pi(g)$, dann folgt $g = hs(z) \in i(H)s(K)$.

Mit Lemma 13.2 folgt dass $G \cong H \rtimes K$ und die Kommutativität des Diagramms. $\square$

KAPITEL 2

Kategorien

KAPITEL 3

Ringe

KAPITEL 4

Körper

10. Einheitswurzeln

Geplant: 1. Stunde, Freitag 30.1.

DEFINITION 10.1. Sei $a \in K$, $n \geq 1$.

Wir sagen: a ist eine n-te Einheitswurzel (EW), gdw $a^n = 1$, gdw a ist NSt von $X^n - 1$.

$E_n(K) := \{a \in \overline{K} \mid a^n = 1\}$ Untergruppe von K^*, zyklisch nach Satz 8.4.

Den kleinsten Körper, der K und alle n-ten Einheitswurzeln von enthält, nennen wir $K_{\sqrt[n]{1}}$.

Beispiel: $K = \mathbb{Q} < \overline{\mathbb{Q}} < \mathbb{C}$, $E_n(\mathbb{Q}) = \{e^{\frac{2\pi ik}{n}} \mid 0 \leq k < n\}$
$\#E_n(K) \leq n$, da $X^n - 1$ höchstens n NSt. $f = X^n - 1$ hat mehrfache NSt in a
$\Leftrightarrow f(a) = 0$ und $f'(a) = 0$
$\Leftrightarrow a^n = 1$ und $na^{n-1} = 0$

Falls $\mathrm{char}(K) \not| n$, dann ist dies äquivalent zu $a^{n-1} = 0$ und $a^n = 1$, was nicht möglich ist. In diesem Fall sind also alle NSt von $X^n - 1$ einfach, und deswegen $\#E_n(K) = n$.

Im Fall $\mathrm{char}(K)|n$ ist jede NSt mehrfach. Sei $p = \mathrm{char}(K) > 0$ und $n = pl$. Dann verschwinden alle Binomialkoeffizienten der Form $\binom{p}{j}$, $0 < j < p$, also

$$(X^l - 1)^p = X^{lp} + (-1)^p = X^n - 1$$

Also $E_n(K) = E_l(K)$. Analog $E_{lp^k}(K) = E_l(K)$. Um $E_n(K)$ zu verstehen, reicht es also, den Fall $\mathrm{char}(K) \not| n$ zu betrachten.

Ab jetzt sei $\mathrm{char}(K) \not| p$**.**

Wir haben also $E_n(K) = \mathbb{Z}/n\mathbb{Z}$.

DEFINITION 10.2. Eine EW $\xi \in E_n(K)$ heißt *primitiv* $\Leftrightarrow \xi$ erzeugt $E_n(K) \Leftrightarrow \xi$ ist Element der Ordnung n in $E_n(K)$.

$Pr_n(K) = \{\xi \in E_n(K) \,|\, \xi \text{ primitiv}\}$. Das Polynom

$$\Phi_n := \prod_{\xi \in Pr_n(K)} (X - \xi) \in K(Pr_n(K))[X]$$

heißt *Kreisteilungspolynom* und ist offensichtlich seprabel und normiert.

Sei $\xi \in Pr_n(K)$. Dann gilt:
$\xi^k \in Pr_n(K) \Leftrightarrow \xi^k$ erzeugt $E_n(K)$
$\Leftrightarrow \bar{k}$ erzeugt $\mathbb{Z}/n\mathbb{Z}$
$\Leftrightarrow \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$
$\Leftrightarrow ggT(k, n) = 1.$

Somit $\deg \Phi_n = \#Pr_n(K) = \#(\mathbb{Z}/n\mathbb{Z})^* = \phi(n)$, wobei ϕ die anfangs der Vorlesung eingeführt Eulersche ϕ-Funktion ist.

$E_n(K) = \dot{\bigcup\limits_{d|n}} Pr_n(K)$, also somit $X^n - 1 = \prod\limits_{\xi \in E_n(K)} (X - \xi) = \prod\limits_{d|n} \prod\limits_{\xi \in Pr_n(K)} (X - \xi) = \prod\limits_{d|n} \Phi_d$.

Da $K \sqrt[n]{1}$ der Zerfällungskörper über K zum Polynom $X^n - 1$ ist, sehen wir, dass die Körpererweiterung$K \leq K \sqrt[n]{1}$ galoissch ist. Für jedes $\xi \in Pr_n(K)$ gilt $K \sqrt[n]{1} = K(\xi)$.

Jedes $\sigma \in \mathrm{Gal}(K(\xi) \geq K)$ lässt $X^n - 1$ invariant, und deswegen ist $\sigma|_{E_n(K)}$ ein Gruppen-Automorphismus von $E_n(K)$. Unter anderem bildet σ dann auch $Pr_n(K)$ bijektiv auf sich selbst ab. Somit ist Φ_n unter σ invariant für alle $\sigma \in \mathrm{Gal}(K(\xi) \geq K)$, also

$$\Phi_n \in (K(\xi))^{\mathrm{Gal}(K(\xi) \geq K)}[X] = K[X].$$

Zwei Elemente der Galois-Gruppe $\sigma, \tau \in \mathrm{Gal}(K_(\xi) \geq K)$ mit $\sigma(\xi) = \tau(\xi)$ sind bereits gleich.

Wir haben also einen injektiven Gruppen-Homomorphismus

$$\mathrm{Gal}(K(\xi) \geq K) \to \mathrm{Aut}(E_n(K)) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Im allgemeinen ist dieser Gruppen-Homomorphismus nicht injektiv, z.B. falls $K = \mathbb{R}$, $n = 5$, dann besteht $\mathrm{Gal}(K(\xi) \geq K)$ aus der Identität und der Konjugation, wohingegen $(\mathbb{Z}/5\mathbb{Z})^*$ vier Elemente besitzt.

Von nun ab sei $\mathrm{char}(K) = 0$, d.h. K habe den Primkörper $\mathbb{Q}$.

Lemma 10.3. *Sei* $\mathrm{char}(K) = 0$. *Dann ist* $\Phi_n \in \mathbb{Z}[X]$.

Beweis. Der Beweis erfolgt über Induktion n.
Induktionsanfang: $\Phi_1 = X - 1$ ist offensichtlich in $\mathbb{Z}[X]$.
Induktionsschritt: Es gelte $\Phi_d \in \mathbb{Z}[X]$ für alle $d < n$. Also ist $\prod\limits_{\substack{d|n \\ d<n}} \Phi_d$ ein normiertes Polynom in $\mathbb{Z}[X]$.

$$\Phi_n \cdot \left(\prod_{\substack{d|n \\ d<n}} \Phi_d \right) = X^n - 1$$

Wenn p ein ganzzahliges Polynom ist und q ein normiertes ganzzahliges Polynom ist, und wenn Polynom-Division durchführen $p = qr + t$, $\deg t < \deg q$, dann sieht man leicht, dass auch r und t wieder ganzzahlig sind. Wir wenden dies für $p = X^n - 1$, $r = \prod_{\substack{d|n \\ d<n}} \Phi_d$, $q = \Phi_n$ und $t = 0$ an. □

Satz 10.4. *Sei* $\mathrm{char}(K) = 0$. *Das Polynom* $\Phi_n \in \mathbb{Z}[X]$ *ist irreduzibel in* $\mathbb{Z}$ *(und damit auch in* $\mathbb{Q}$*).*

Beweis: wird aus Zeitgründen nicht ausgeführt, siehe zB Bosch 4.5 für den recht eleganten Beweis.

Korollar 10.5. *Sei* $\xi \in Pr_n(\mathbb{Q})$. *Dann gilt* $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$.

Korollar 10.6. *Sei* $\xi \in Pr_n(\mathbb{Q})$. *Die Abbildung*

$$\mathrm{Gal}(\mathbb{Q}(\xi) \geq \mathbb{Q}) \to Aut(E_n(\mathbb{Q}))$$

ist surjektiv.

Beweis. Fixiere ein $\xi \in Pr_n(\mathbb{Q})$. Sei $\tau \in \mathrm{Aut}(E_n(\mathbb{Q}))$. Die Abbildung $\mathbb{Z}/n\mathbb{Z} \to E_n(\mathbb{Q})$, $\bar{k} \mapsto \sigma^k$ ist ein Gruppenisomorphismus. Jeder Gruppenautomorphismus von $\mathbb{Z}/n\mathbb{Z}$ ist durch Multiplikation mit einem $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ gegeben. Es gilt somit $ggT(a,n) = 1$, $\xi^a \in Pr_n(\mathbb{Q})$. Somit $\tau(\eta) = \eta^a$ für alle $\eta \in E_n(\mathbb{Q})$. Nach obigem Satz ist das Minimalpolynom von ξ durch Φ_n gegeben. Die Potenz ξ^a ist ebenfalls eine Wurzel von Φ_n.

Auf Grund von 5.1 gibt es desegen genau einen Körperisomorphismus $\sigma : K(\xi) \to K(\xi^a) = K(\xi)$ mit $\sigma|_K = \mathrm{Id}_K$ und $\sigma(\xi) = \xi^a$. Man überprüft leicht, dass dies eine Fortsetzung von τ ist. □

11. Anwendungen der Körpertheorie

Geplant, 2. Stunde, Freitag 30.1.

11.1. Konstruktionen mit Zirkel und Lineal.

Sei M eine Teilmenge von $\mathbb{R}$, $\{0,1\} \subset M$.

Definition 11.1. $x \in \mathbb{R}$ ist konstruierbar aus M, falls es eine Formel für x gibt, die nur aus den Symbolen $+$, $-$, $\cdot$, $/$ und $\sqrt[2]{\ }$ und Elementen von M besteht.
$\mathcal{K}(M)$ sei die Menge aller aus M konstruierbaren Punkte.

Motivation (siehe Saalübung): Sei eine Menge $N \subset \mathbb{R}^2$ gegeben, $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in N$. Definiere

$$M := \left\{ x \,|\, \exists y \text{ mit } \begin{pmatrix} x \\ y \end{pmatrix} \in N \right\} \cup \left\{ y \,|\, \exists x \text{ mit } \begin{pmatrix} x \\ y \end{pmatrix} \in N \right\}$$

Dann gilt: $\begin{pmatrix} a \\ b \end{pmatrix}$ kann aus den Punkten in N mit Hilfe von Zirkel und Lineal konstruiert werden genau dann, wenn $a, b \in \mathcal{K}(M)$.

Offensichtlich $\mathcal{K}(M) = \mathcal{K}(\mathbb{Q}(M))$.

Außerdem ist auch offensichtlich $\mathcal{K}(M)$ ein Körper.

Lemma 11.2. *Sei $0, 1 \in M$. Die reelle Zahl a ist genau dann in $\mathcal{K}(M)$ wenn es ein $k \in \mathbb{N}_{\{}0\}$ und eine Folge von Körpern*

$$\mathbb{Q}(M) = K_0 \leq K_1 \leq \cdot \leq K_k$$

gibt, so dass $a \in K_k$ und $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, k$.

Beweis. Die Elemente von $\mathcal{K}(M)$ sind genau die reellen Zahlen, die man durch endlich viele Operationen

(i) (Grundrechenarten) $+, -, \cdot, /$
(ii) (Wurzelziehen) $\sqrt[2]{}$

erhält. Die grundrechenoperationen sind innerhalb eines Körpers. Durch diese Operationen erhält man also genau den von M erzeugten Körper $K_0 := \mathbb{Q}(M)$. Zieht man eine Wurzel, so erhält man eine Zahl vom Typ $\sqrt{\alpha}$, $\alpha \in \mathbb{Q}(M)^+$. Durch Grundrechenarten erhält man so auch den Körper $K_1 := \mathbb{Q}(M \cup \{\sqrt{\alpha}\})$, der eine Körpererweiterungvon $\mathbb{Q}(M)$ von Grad 2 (oder 1 im trivialen Fall, dass bereits $\sqrt{\alpha} \in K_0$). Wenn wir k nicht-triviale Wurzeln gezogen haben, haben wir eine Körper-kette wie oben beschrieben.

Sei umgekehrt eine Kette von Körpererweiterungen wie oben gegeben. Wir haben in einer Übungsaufgabe gezeigt, dass aus $[K_i : K_{i-1}] = 2$ die Existenz eines $\alpha_i \in K_i$ folgt mit $K_i = K_{i-1}(\alpha_i)$. Wir erhalten somit a aus M durch Hintereinanderausführung der Grundrechenarten und von k-mal Wurzelziehen. □

Es sei ab jetzt immer $M := \{0, 1\}$, schreibe kurz $\mathcal{K} := \mathcal{K}(\{0, 1\})$.

Beispiele.

(1) $a = \sqrt{3 + \sqrt{2}}$ ist konstruierbar. $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{3 + \sqrt{2}}) \geq K_1$,
(2) Delisches Problem der Würfelverdoppelung. Ein Würfel sei gegeben. Kann man daraus einen Würfel mit Volumen mit doppeltem Volumen konstruieren? In anderen Worten $\sqrt[3]{2} \in \mathcal{K}$? Nein: Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $X^3 - 2$, also $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Angenommen es gäbe $\mathbb{Q} = K_0 \leq \cdots \leq K_k$ wie oben. Dann gilt $2^k = [K_k : \mathbb{Q}] = [K_k : \mathbb{Q}(\sqrt[3]{2})]\,[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. Wir erhalten den Widerspruch $3 | 2^k$.
(3) $a = \sqrt[3]{7 + 5\sqrt{2}} \in \mathcal{K}$, denn $a = 1 + \sqrt{2}$. Also Achtung: eine komplizierte Formel kann täuschen und man muss sorgfältig schauen, ob jeweils das Minimalpolynom irreduzibel ist.

THEOREM 11.3 (Gauß). *Für $n \geq 2$ sind äquivalent:*

(1) *Das regelmäßige n-Eck ist konstruierbar*
(2) *$\phi(n)$ ist eine Potenz von 2*
(3) *Es gibt $k \in \mathbb{N}$ und paarweise verschiedene Fermatsche Primzahlen $p_1, \dots, p_r$ mit $n = 2^k p_1 \cdot p_2 \cdots p_r$.*

DEFINITION 11.4. $f_n := 2^{2^n} + 1$ heißt n-te Fermatsche Zahl. Eine Fermatsche Primzahl ist eine Fermatsche Zahl, die prim ist.

Beispiele: $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$ sind prim. Aber 641 teilt f_5. Alle f_i, $5 \leq i \leq 32$ sind nicht prim. Man vermutet, dass f_i für alle $i \geq 5$ nicht prim ist.

Beispiele: Konstruierbar sind das n-Eck für $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, ...$, nicht konstruierbar für $n = 7, 9, 11, 13, 14, 18, 21, ...$

LEMMA 11.5. *Sei $m \in \mathbb{N}$ und $p = 2^m + 1$ prim. Dann ist p eine Fermatsche Primzahl.*

Beweis des Lemmas. Klar für $m = 1$, $p = 3$. Sei $m > 1$, $p = 2^m + 1$. Angenommen m ist nocht von der Form 2^k. Dann gibt es eine ungerade Zahl $r > 1$, die m teilt. Schreibe $m = rt$.

$$p = 2^{rt} + 1 = (2^r + 1)(2^{r(t-1)} - 2^{r(t-2)} \dots + 1).$$

Da beide Faktoren > 1 sind, ist p nicht prim. □

Beweis von Theorem 11.3 (2)⇔(3). Sei $n = q_1^{l_1} \cdots q_r^{l_r}$, wobei $q_1, \dots, q_r$ verschiedene Primzahlen sind. Wir nutzen den chinesischen Restsatz, d.h. $\mathbb{Z}/n\mathbb{Z}$ ist als Ring isomorph zu $\prod_{i=1}^r \mathbb{Z}/q_i^{l_i}\mathbb{Z}$.

$$\phi(n) = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \#\left(\prod_{i=1}^r \mathbb{Z}/q_i^{l_i}\mathbb{Z}\right)^* = \prod_{i=1}^r \#\left(\mathbb{Z}/q_i^{l_i}\mathbb{Z}\right)^* = \prod_{i=1}^r (q_i - 1)q_i^{l_i - 1}.$$

$\phi(n)$ ist also genau dann Zweierpotenz, falls für jedes i gilt: $q_i = 2$ oder q_i ist von der Form $2^m + 1$, und letzeres ist nach dem Lemma gleichbedeutend dazu, dass q_i Fermatsche Priumzahl ist. □

BEMERKUNG 11.6. Folgende Bedingungen sind äquivalent

(1) Das regelmäßige n-Eck ist konstruierbar
(2) $(\cos 2\pi/n, \sin 2\pi/n)$ ist konstruierbar.
(3) $\cos 2\pi/n \in \mathcal{K}$.
(4) $\mathbf{Re}\,\xi \in \mathcal{K}$ für die primitive n-te EW $\xi = e^{2\pi i/n}$.
(5) $\mathbf{Re}\,\xi \in \mathcal{K}$ für all $\xi \in Pr_n(\mathbb{Q})$.

BEMERKUNG 11.7. Sei $\xi \in Pr_n(\mathbb{Q})$, z.B. $\xi = e^{2\pi i/n}$. Sei $n > 2$, also $\xi \notin \mathbb{R}$. Dann $\bar{\xi} = \xi^{n-1} \in \mathbb{Q}(\xi)$. Also auch $\mathbf{Re}\,\xi \in \mathbb{Q}(\xi)$. Somit $\mathbb{Q}(\mathbf{Re}\,\xi) \leq \mathbb{Q}(\xi)$.

Die Zahl ξ ist Nullstelle von $(X-\xi)(X-\bar{\xi}) = X^2 - \mathbf{Re}\,\xi\, X + 1 \in \mathbb{Q}(\mathbf{Re}\,\xi)[X]$ und deswegen gilt

$$[\mathbb{Q}(\xi) : \mathbb{Q}(\mathbf{Re}\,\xi)] = 2.$$

Beweis von Theorem 11.3 (1)⇔(2).
„(1)⇒(2)“:
Aus (1) und Bemerkung 11.6 folgt für $\xi = e^{2\pi i/n}$: $\mathbf{Re}\,\xi \in \mathcal{K}$. Also gibt es nach Lemma 11.2 eine Folge von Körpern $\mathbb{Q} = K_0 \leq \cdots \leq K_k$ mit $[K_i : K_{i-1}] = 2$ und $\mathbf{Re}\,\xi \in K_k$. Wir schließen $\mathbb{Q}(\mathbf{Re}\,\xi) \leq K_k$ und

$$[\mathbb{Q}(\mathbf{Re}\,\xi) : \mathbb{Q}] \mid [K_k : \mathbb{Q}(\mathbf{Re}\,\xi)] \cdot [\mathbb{Q}(\mathbf{Re}\,\xi) : \mathbb{Q}] = 2^k$$

Also ist auch

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}(\mathbf{Re}\,\xi)] \cdot [\mathbb{Q}(\mathbf{Re}\,\xi) : \mathbb{Q}] = 2[\mathbb{Q}(\mathbf{Re}\,\xi) : \mathbb{Q}]$$

eine Potenz von 2.

„(2)⇒(1)“:
Sei $\xi \in Pr_n(\mathbb{Q})$, z.B. $\xi = e^{2\pi i/n}$.

Wie im letzten Abschnitt gezeigt, ist die Erweiterung $\mathbb{Q}(\xi) \geq \mathbb{Q}$ galoissch, und $\mathrm{Gal}(\mathbb{Q}(\xi) \geq \mathbb{Q})$ ist isomorph zur multiplikativen Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$. Insbesondere ist die Galois-Gruppe abelsch und hat $\phi(n)$ viele Elemente. Unter der Annahme von (2) folgt, dass $\phi(n)$ eine Zweierpotenz ist, schreibe $\phi(n) = 2^{k+1}$, $k \in \mathbb{N} \cup \{0\}$.

Wir nutzen nun die Galois-Theorie, insbesondere den Hauptsatz. Der Körper $\mathbb{Q}(\mathbf{Re}\,\xi)$ ist Zwischenkörper von $\mathbb{Q} \leq \mathbb{Q}(\xi)$. Somit ist die Galois-Gruppe $\mathrm{Gal}(\mathbb{Q}(\xi) \geq \mathbb{Q}(\mathbf{Re}\,\xi))$ eine Untergruppe von $\mathrm{Gal}(\mathbb{Q}(\xi) \geq \mathbb{Q})$ und somit ein Normalteiler. Also ist auch $\mathbb{Q}(\mathbf{Re}\,\xi) \geq \mathbb{Q}$ galoissch und

$$\mathrm{Gal}(\mathbb{Q}(\mathbf{Re}\,\xi) \geq \mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\xi) \geq \mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\xi) \geq \mathbb{Q}(\mathbf{Re}\,\xi))}$$

Somit ist $\#\mathrm{Gal}(\mathbb{Q}(\mathbf{Re}\,\xi) \geq \mathbb{Q}) = 2^{k+1}/2 = 2^k$.

Wir setzen nun $G := \mathrm{Gal}(\mathbb{Q}(\mathbf{Re}\,\xi) \geq \mathbb{Q})$. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gibt es $l_1, \ldots, l_r \in \mathbb{N}$ mit $\sum l_i = k$ so dass

$$G \cong \mathbb{Z}/2^{l_1} \times \cdots \times \mathbb{Z}/2^{l_r}.$$

Man überlegt sich leicht, dass G die folgende Eigenschaft (UG) erfüllt ist:

$$(P) \qquad \exists \text{ Untergruppen } \quad G_0 = \{0\} < G_1 < G_2 < \cdots < G_k = G, \quad \#G_i = 2^i.$$

Man überprüft dies zunächst im Fall $G = \mathbb{Z}/2^l$ und überlegt sich dann: Wenn G' und G'' die Eigenschaft (UG) erfüllen (mit G' bzw. G'' an Stelle von G), dann erfüllt auch $G' \times G''$ diese Eigenschaft. [1] Hieraus folgt dann induktiv die Eigenschaft (UG) für die Gruppe G selbst.

Die Gruppen G_i sind alle normal, da G abelsch. Definiere $K_i := (\mathbb{Q}(\mathbf{Re}\,\xi))^{G_i}$, $\mathrm{Gal}(\mathbb{Q}(\mathbf{Re}\,\xi) \geq K_i) = G_i$, $\mathrm{Gal}(K_i \geq \mathbb{Q}) = G/G_i$.

[1] Noch allgemeiner kann man zeigen: Ist $1 \to G' \to G''' \to G'' \to 1$ eine kurze exakte Sequenz von Gruppen, dann erfüllt G''' die Eigenschaft (UG) gdw G' und G'' sie erfüllen.

$K_0 := \mathbb{Q}(\mathbf{Re}\,\xi)$, $K_{i+1} \leq K_i$

$$[K_i : \mathbb{Q}] = \#\mathrm{Gal}(K_i \geq \mathbb{Q}) = \#(G/G_i) = 2^k/2^i = 2^{k-i}$$

Somit

$$[K_i : K_{i+1}] = \frac{[K_i : \mathbb{Q}]}{[K_{i+1} : \mathbb{Q}]} = 2.$$

Nach Lemma 11.2 ist somit $\mathbf{Re}\,\xi$ konstruierbar. □

Bemerkung: Der Beweis von Theorem 11.3 ist konstruktiv. Dies heißt, er liefert nicht nur die Existenz einer Konstruktion, sondern wenn man dem Beweis zeilenweise folgt, auch ein Verfahren, um solch eine Konstruktion zu erlangen. So konnte man eine (theoretische) Methode erlangen, das 17-Eck zu konstruieren. Praktisch sind solche Verfahren aber undurchführbar, da die Dicke des Bleistifts zu große Fehler bewirkt.

Dennoch gab es Leute, die mit viel Mühe die Konstruktion des 257-Ecks und des 65537-Eck ausgearbeitet haben. Ganz amüsant sind die Artikel http://de.wikipedia.org/wiki/65537-Eck und http://de.wikipedia.org/wiki/Johann_Gustav_Hermes.