

Thomas Kahle terminplaner4.dfn.de/algebra2-augu

(a.7) Zettelblätter

PLW: malte

(1. Übung: Do, 11.04.) ↳ weder null berichtet, aber $2x$ pro Übung was verstehen!
↳ alles optional und am Ende mündliche Prüfung.

zurückpro C:

GCR-314 ("Pi-Raum")

Literatur: Dummit/Foote: Abstract Algebra (dick)
Rotman "Galois Theory" (dünn)

I. GALOISTHEORIE - WIE SIE, WESHALB, WARUM?

In der Schule lernen wir, die quadratische Gleichung $ax^2 + bx + c = 0$ zu lösen. Es gilt: $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Diese Seite wurde im 9. Jhd. von persischen Mathematikern bewiesen. Diese Seite wurde im 9. Jhd. von persischen Mathematikern bewiesen. Diese Seite wurde im 9. Jhd. von persischen Mathematikern bewiesen. Diese Seite wurde im 9. Jhd. von persischen Mathematikern bewiesen.

Auch für die allgemeine kubische Gleichung $ax^3 + bx^2 + cx + d = 0$ gibt es Lösungsformeln, die "Cardanoformeln": $x_1 = -\frac{b}{3a} + \sqrt[3]{-\frac{1}{2}\left(\frac{2b^3}{27a^3} - \dots\right)} + \sqrt[3]{\dots}$

Auch für Grad 4 gibt es Lösungsformeln, die sehr komplizierter sind.

Es ist nicht unbedingt überwältig, dass Lösungen existieren, sondern dass sie durch Formeln ausgedrückt werden können, die nur $+, -, \cdot, /, \sqrt{\quad}, \dots$ und die Koeffizienten verwenden. (anfangs z.B. Greuzeitetraktus) Zu Beginn des 19. Jhd. waren keine solchen Formeln für Grad 5 oder höher bekannt und Abel realisierte, dass keine solchen Formeln existieren. "Wie" kann es keine Formeln? könnte eventuell auch die Gestalt der Formel von den konkreten Koeffizienten abhängen? Dann brauchte man unendlich viele Formeln (evtl. unendlichviele). In Wirklichkeit ist alles viel schlimmer, denn es gibt komplexe Polynome wie z.B. $x^5 - 4x + 2$, deren Nullstellen sich nicht mit Hilfe von algebraischen Formeln wie oben ausdrücken lassen.

19. Jhd.
Évariste Galois
Niels Henrik Abel

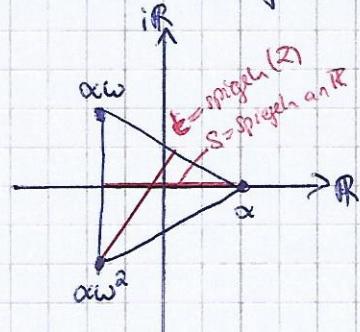
Évariste Galois beschäftigte sich mit der Frage, warum keine Formeln existieren können. Seine wichtige Idee war, die Symmetrien der Nullstellen von Polynomen zu betrachten. Heute bedeutet Symmetrie oft Gruppentheorie, aber die gab es damals noch nicht. Moderner Wiss.: Galoistheorie ist eine Verbindung zwischen Körpertheorie und Gruppentheorie.

Gruppen gibt es erst seit etwa 1840

Lösen von Polynomgleichungen

Bsp.: Die Symmetrien von $x^3 - 2 = 0$. (in \mathbb{C}) → hat lt. Fundamentalsatz der Algebra 3 Lösungen. (Analogie ist hier ein Zufall)

Wir arbeiten über \mathbb{C} . Es gibt 3 Lösungen: $\alpha = \sqrt[3]{2} \in \mathbb{R}$.
Sei $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ eine dritte Einheitswurzel, also $\omega^3 = 1$.
Die Nullstellen sind $\alpha, \alpha\omega, \alpha\omega^2$ (merke: $(\alpha\omega)^3 = \alpha^3 \omega^3 = \alpha^3 = 2$, ähnlich wie $\alpha\omega^2$). Sie bilden ein gleichseitiges Dreieck in der Gauß-Ebene:



Dieses Dreieck hat geometrische Symmetrien:

3 Spiegelungen und 3 Rotationen (um $\frac{2}{3}\pi, \frac{4}{3}\pi, \frac{6}{3}\pi = 0$)
Algebraisch ergibt sich die Diedergruppe $D_3 = \{S, t, ts, ts, (ts)^2, (ts)^3 = id\}$ zu lösen mit Faktorstufenpunkten
↑ Dies ist die Rotation um $\frac{2}{3}\pi$.

Was hat das mit den Nullstellen von $x^3 - 2 = 0$ zu tun?

Bei der Galoistheorie geht es also um zahlentheoretische Symmetrien.
Dafür etwas Theorie:

Def. 1.1 Sei K ein Körper. Ein Teilkörper von K ist eine Teilmenge, die unter den induzierten Operationen abgeschlossen ist.
(d.h., auf die Teilmenge erweitert)

Bsp.: \mathbb{Q} Teilkörper von \mathbb{R} und \mathbb{R} Teilkörper von \mathbb{C} , $\mathbb{Q} \cup \{\sqrt{2}\}$ ist kein Teilkörper von \mathbb{R} , da $1+\sqrt{2} \notin \mathbb{Q} \cup \{\sqrt{2}\}$.

F adjungiert β "

Def. 1.2 Ist F ein Teilkörper von K und $\beta \in K$, dann ist $F(\beta)$ der kleinste Teilkörper von K , der sowohl F als auch β enthält, d.h. falls $F' \subseteq K$ ein Teilkörper ist, der selbst F und β enthält, dann gilt $F(\beta) \subseteq F'$.
Bew. Man kann sich $F(\beta)$ auch als Abschluss der $F \cup \{\beta\}$ unter den Körperoperationen vorstellen.

- Wir nutzen auch $F(\beta_1, \dots, \beta_n)$ für den kleinsten Teilkörper, der F und β_1, \dots, β_n enthält

Bsp.: $\mathbb{R}(i) = \mathbb{C}$ $\mathbb{Q}(\sqrt{2}) \supsetneq \mathbb{Q}$, aber $\mathbb{Q}(\sqrt{2})$ ist viel kleiner als \mathbb{R} .
 $\mathbb{Q}(2) = \mathbb{Q}$ Umg: $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. \rightarrow Vektorraum mit dim 2 über \mathbb{Q} , lineare Algebra-Aufgabe

Zurück zu $x^3 - 2$.

Wir betrachten $K = \mathbb{Q}(\alpha, \omega)$. Da K ein Körper ist, gilt $\alpha, \omega \in K \Rightarrow \alpha \omega \in K$, $\alpha \omega^2 \in K$, d.h. K erhält alle Lösungen von $x^3 - 2 = 0$.
Da $\mathbb{Q}(\alpha) \neq \mathbb{Q}$ und $\mathbb{Q}(\omega) \neq \mathbb{Q}$, ist K der kleinste Körper, der alle Nullstellen enthält. Die Symmetrien, die wir betrachten wollen, sind Körperisomorphismen.

Beh.: $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega^2)$ sind gleich (als Teilkörper von \mathbb{Q}).

Grund: $\alpha, \omega^2 \in \mathbb{Q}(\alpha, \omega) \Rightarrow \mathbb{Q}(\alpha, \omega^2) \subseteq \mathbb{Q}(\alpha, \omega)$
und $\alpha, \omega = \omega^2 \cdot \omega^2 \in \mathbb{Q}(\alpha, \omega^2) \Rightarrow \mathbb{Q}(\alpha, \omega^2)$.

Spiegelung an \overline{t} : $\mathbb{Q}(\alpha, \omega) \rightarrow \mathbb{Q}(\alpha, \omega^2)$ ist bijektiv,

also ein Isomorphismus.

$\alpha \mapsto \alpha$

$\omega \mapsto \omega^2$

(Da $s(0) = 0$, $s(1) = 1$ auch)

$s(\mathbb{Q}) = \mathbb{Q}$) und weiterhin festgelegt durch die Definition als Homomorphismus.)

Ein weiterer Körperisomorphismus ist t : $\mathbb{Q}(\alpha, \omega) \rightarrow \mathbb{Q}(\alpha \omega, \omega^2) \stackrel{\text{Umg analog zu } s}{=} \mathbb{Q}(\alpha, \omega)$

$\alpha \mapsto \alpha \omega$

$\omega \mapsto \omega^2$

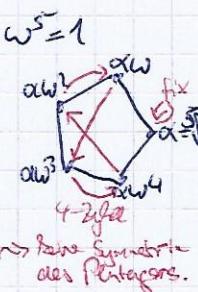
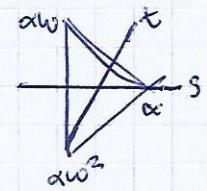
Man prüft nach: Die Isomorphismen s, t erzeugen auch die D₆.

Z.B. s bildet α auf $\alpha \omega^2$ ab und ω auf $\omega^4 = \omega$. Man kann prüfen:
 $(ts)^3 = tssts = id$.

Wenn das immer so wäre, wäre Galoistheorie ein Teil der Ebenengeometrie, aber im Allgemeinen findet man neue abgesetzte Symmetrien (d.h. Körperisomorphismen). Für $x^5 - 2$ erhält man ein Pentagon. Die geometrische Symmetrie in \mathbb{C} ist D_{10} , die Diedergruppe, aber es gibt neue Körperisomorphismen, die die Nullstellen permutieren. (z.B. die roten Pfeile links)
Später sehen wir: $x^p - 2$ (für p prim) erlaubt $P(p-1)$ abgesetzte Symmetrien und $2p$ geometrische (D_{2n}); für $p=3$ erhält man jeweils 6.

“Die Tafel schnurrt beim Würzen”

“Wer kommt auf die Idee, einen Schwarm zu impfignieren?”



II Polynome, Wurzeln, Körpererweiterungen

- Polynome in einer Unbestimmten x mit Koeffizienten in einem Körper K bilden selbst einen Ring, den Polynomring $K[x]$. K adjungiert x
- $K[x]$ ist kommutativ mit Eins und hat keine Nullteiler (d.h. $f, g \in K[x] \rightarrow f \cdot g = 0 \Rightarrow f=0 \text{ oder } g=0$) $\Rightarrow K[x]$ ist ein Integritätsbereich.
- Polynome haben einen Grad $\deg(f)$. Es gilt $\deg(f \cdot g) = \deg(f) + \deg(g)$
- Division mit Rest: $f, g \in K[x]$ dann existieren eindeutige $q, r \in K[x]$ mit $f = g \cdot q + r$ mit $\deg(r) < \deg(g)$. \leftarrow wichtig für Beweise
- Division mit Rest gibt es auch im allgemeinen Fall $R[x]$, wobei R ein Integritätsbereich ist, z.B. $\mathbb{Z}[x]$, oder $R = K[y]$, dann $R[x] \cong K[x,y]$
- Begriff aus \mathbb{Z} werden auch in $K[x]$ verwendet:
 $f | g$ ("f teilt g") $\Leftrightarrow \exists h \in R$ mit $h \cdot f = g$ für $f, g \in \mathbb{Z}$ oder $f, g, h \in K[x]$
- ggT und kgV existieren, Lemma von Bezout: $\text{ggT}(f, g) = a \cdot f + b \cdot g$ für geeignete $a, b \in \mathbb{Z} / K[x]$.
- $K[x]$ ist ein euklidischer Ring, d.h. der euklidische Algorithmus funktioniert.
 Aber: $K[x, y]$ ist kein euklidischer Ring.

Ringe ohne
Identität
heißen auch
Ringe...

- wenn $f \neq 0$

f ist "algebraisches
Objekt", daher
"Wurzel" statt
"Nullstelle".

Def. 2.1 Sei $f = a_0 + a_1 x + \dots + a_d x^d \in K[x]$. Eine Wurzel von f in K ist ein $\alpha \in K$ mit $f(\alpha) = a_0 + a_1 \alpha + \dots + a_d \alpha^d = 0$.

Bem. Existenz von Wurzeln hängt von K ab: $x^2 + 1 \in \mathbb{Q}[x]$ hat keine Wurzeln.
 $x^2 + 1 \in \mathbb{C}[x]$ hat 2 Wurzeln, i.e.

Es gilt: Ein $\alpha \in K$ ist Wurzel von $f \in K[x] \Leftrightarrow (\alpha - \alpha) | f$.

Beweis: Divisionsalgorithmus.

Jeder f mit $\deg(f) = n$ hat höchstens n Wurzeln. Bew: Induktion.

Bsp.: $x^2 + 3x + 2 \in \mathbb{Z}_5$ hat 4 Wurzeln: 1, 2, 4, 5 \rightsquigarrow da \mathbb{Z}_5 kein Körper ist.

$f \in K$ bzw. $\deg(f) = 0$

Def. 2.2 Ein nicht-konstantes Polynom $f \in K[x]$ ist irreduzibel, falls aus $f = g \cdot h$ folgt $\deg(g) = 0$ oder $\deg(h) = 0$.

(wenn)

Falls $f = g \cdot h$ mit $\deg(g) > 0$ und $\deg(h) > 0$, so spricht man von einer reduziblen Faktorisierung von f . Dann heißt f reduzibel. Bew: In $R[x]$ ist eine mittelnormale Faktorisierung auch $f = g \cdot h$ mit $\deg(g) = 0$, aber g null-invertierbar in R .
Bsp.: $2(x^2 + 1) \in \mathbb{Z}[x]$ ist reduzibel; $2(x^2 + 1) \in \mathbb{Q}[x]$ ist irreduzibel.

Oft ist es wichtig Irreduzibilität über verschiedenen Körpern zu unterscheiden. Wenn sagt dann: f ist (ir)reduzibel über K .

Achtung: Keine Wurzeln über $K \not\Rightarrow$ irreduzibel. Bsp.: $(x^2 + 1)^2$ ist reduzibel über \mathbb{Q} , aber hat keine Wurzeln.

Irreduzibel $\not\Rightarrow$ keine Wurzeln. Bsp.: $(x-1)$ ist irreduzibel mit Wurzel 1 über \mathbb{Q} . Aber: irreduzibel und $\deg \geq 2 \Rightarrow$ keine Wurzeln.

Es ist oft wichtig zu entscheiden, ob ein gegebenes $f \in K[x]$ irreduzibel ist.

- Falls $\deg(f) \leq 3$ gilt: Keine Wurzeln \Rightarrow irreduzibel.

Bsp.: $K = \mathbb{F}_2$ (endlicher Körper mit 2 Elementen) $= \mathbb{Z}/2\mathbb{Z}$ und $f = x^4 + x + 1 \in K[x]$.

f hat keine Wurzeln (denn $f(0), f(1) \neq 0$). Falls $f = g \cdot h$, so ist $\deg f = \deg g + \deg h$. Da f keine Wurzeln hat und mittelnormale Fak-

Jeder endliche Körper hat
Ordnung Prim-
zahlpotenz,
 $\#K \Rightarrow p^n$
 $\#K = p^n$ \Rightarrow primzahlpotenz

"Bihomische Formel":
 $(a+b)^2 = a^2 + b^2$
 Freshman's Dream
 für endliche Körper.

torisierung gewünscht, betrachte nur $\deg g = \deg h = 2$.
 Alle Polynome von Grad 2: $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$
 $x \cdot x, x \cdot (x+1), (x+1)^2$ \Leftrightarrow irreduzibel

Aber: $f \neq (x^2 + x + 1)^2 \Rightarrow f$ ist irreduzibel

(Haupt-)
Mit gesuchtem
Koeffizienten in $\mathbb{Q}[x]$
multiplizieren -
ist $\mathbb{Z}[x]$.

Der wichtigste Körper für die Galoistheorie ist \mathbb{Q} . — unsere Baseline
Irreduzibilität über \mathbb{Q} kann auf Irreduzibilität über \mathbb{Z} zurückgeführt werden.
Lemma von Gauß: $f \in \mathbb{Z}[x]$ ist irreduzibel genau dann, wenn
 (1) f ist irreduzibel in $\mathbb{Q}[x]$, und Bsp.: $2(x^2+1)$, reduzibel
da teilerbar durch 2 (p.f.m.).
 (2) f ist nicht durch eine Primzahl teilbar.

Satz 2.3 (Eisenstein-Kriterium)

Sei $f \in \mathbb{Z}[x]$, $f = c_n x^n + \dots + c_1 x + c_0$, $c_n \neq 0$. Wenn eine Primzahl p existiert mit $p | c_i$ für $i = 0, \dots, n-1$
 - $p \nmid c_n$ (Leitkoeffizient)
 - $p \nmid c_0$, dann ist f irreduzibel über \mathbb{Q} . \rightarrow Dies ergibt sich mit Lemma von Gauß

"Wie genere
Aktion passiert
zwischen \mathbb{Q} und
 \mathbb{R} , das verschwundet
Möglichkeit seit
1000 Jahren
rausgefunden...
gibt es \mathbb{R} überlapt?"

Bsp.: $x^n - p$ für p prim ist irreduzibel \Rightarrow Es existieren über \mathbb{Q} irreduzible
Polynome von beliebigem Grad. (über \mathbb{R} und \mathbb{C} nicht!)

Reduktions-test: verwendet von CAS zur Bestimmung von Irreduzibilität.
Manchmal helfen auch Reduktionen. Sei R ein Integritätsbereich, K ein Körper und $\alpha: R \rightarrow K$ ein Ringhomomorphismus (z.B. $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$).

Dann ist $\alpha^*: R[x] \rightarrow K[x]$ definiert durch

$\sum_{i=0}^n c_i x^i \mapsto \sum_{i=0}^n \alpha(c_i) x^i$ auch ein Ringhomomorphismus.
Sei $f \in R[x]$ mit $\deg(\alpha^*(f)) = \deg(f)$ (Leitkoeffizient bleibt bestehen)

und $\alpha^*(f)$ ist irreduzibel über K .

Dann existiert in $R[x]$ keine Faktorisierung $f = g \cdot h$ mit $\deg(g) > 0$ und $\deg(h) > 0$. (was fast, bis auf multiplizität mit nullstellenfrei, irreduzibel ist).

Bsp.: Typische Anwendung: $R = \mathbb{Z}$, $K = \mathbb{Z}/p\mathbb{Z} (= \mathbb{F}_p)$.

$$f = 8x^3 - 6x - 1 \in \mathbb{Z}[x].$$

Reduktion mod 5: $\alpha^*(f) = 3x^3 + 4x + 4 \in \mathbb{F}_5[x]$, $\deg(\alpha^*(f)) = 3$.

Einsetzen von allen Elementen von \mathbb{F}_5 ergibt keine Wurzel \Rightarrow irreduzibel über \mathbb{F}_5 .

Weiterhin kann f nicht faktorisierbar als Grenzschl. Polynom, d.h.

f ist auch irreduzibel über \mathbb{Z} und damit mit inversen auch über \mathbb{Q} .

Achtung: Der Reduktions-test ist keine Charakterisierung, selbst wenn alle Primzahlen betrachtet werden: $x^4 + 1$ ist irreduzibel über \mathbb{Q}/\mathbb{Z} , aber reduzibel in $\mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p .

Ein weiterer Trick: Verde einen Isomorphismus auf $\mathbb{Z}[x]$ an, in der Hoffnung, dass z.B. Eisenstein auf das Bild von f anwendbar ist (z.B. "fliegt um + ...").

Bsp.: $\mathbb{Z}[x] \rightarrow \mathbb{Z}[x]$ für $n \in \mathbb{Z}$ beliebig.

$$x \mapsto x+n$$

Sei p prim: $f = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \dots + x^{p-1}$ (Φ_p , der p -te Kreis-Binomialkoeffizient Teilungspolymer)

Behar: f ist irreduzibel.

Beweis: Betrachte $\frac{(x+1)^p - 1}{(x+1)^p - 1} = f(x+1) = \frac{kP + (P)_1 x^{p-1} + \dots + p x^{p-1} - 1}{x} = x^{p-1} + p x^{p-2} + \dots + (P)_2 x + p$

Mit Eisenstein folgt dann $f(x+1)$ ist irreduzibel $\Rightarrow f$ ist irreduzibel, da $x \mapsto x+1$ einen Isomorphismus von $\mathbb{Z}[x]$ definiert.

Satz 2.4 $K[x]$ ist ein faktorieller Ring, d.h. jedes $f \in K[x]$ lässt sich in bis auf Umordnung eindeutiger Weise als $f = \lambda \cdot g_1 \cdots g_r$ mit $\lambda \in K$ und g_i monisch und irreduzibel schreiben.
(einfachster 1)

Bsp.: $x^4 - 4 = (x^2 + 2)(x^2 - 2) \in \mathbb{R}[x] = (x^2 + 2)(x - \sqrt{2})(x + \sqrt{2}) \in \mathbb{R}[x]$
 $= (x - \sqrt{2}i)(x + \sqrt{2}i)(x - \sqrt{2})(x + \sqrt{2}) \in \mathbb{C}[x]$,
 d.h. die eindeutige Faktorisierung hängt vom Körper ab.

Ist $R \subseteq L$ ein Teilkörper eines Körpers L , so nennt man das Paar L, R eine Körpererweiterung und schreibt L/R (nicht als Faktoring gemeint, geht auch gar nicht, da Körper (fast) keine (dele) Ideale), gesprochen " L über R ". In jeder Körpererweiterung ist L ein R -Vektorraum. Der Grad der Erweiterung L/R ist $[L:R] = \dim_R L$ (L als R -Vektorraum).

Eine Körpererweiterung der Form $R(\beta)$ für ein $\beta \in L$ heißt einfach, und β heißt primitiv Element.

Achtung: Existiert ein primitiv Element ist nicht unbedingt offensichtlich!

Bsp.: Ist $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq R$ einfach? Ja! $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

" \supseteq " ist klar, da $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \ni \sqrt{2} + \sqrt{3}$.

" \subseteq ": $(\sqrt{2} + \sqrt{3})^2 = 2\sqrt{2} + 3 \cdot 2 \cdot \sqrt{3} + 3 \cdot 3 \cdot \sqrt{2} + 3\sqrt{3} = 4\sqrt{2} + 9\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, also auch $2\sqrt{2} = 4\sqrt{2} + 9\sqrt{3} - 9(\sqrt{2} + \sqrt{3}) \Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$

$\mathbb{Q}(\sqrt{2} + \sqrt{3})$

Def. 2.5 Sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt algebraisch über K falls ein $f \in K[x]$ existiert mit $f(\alpha) = 0$, d.h. α ist eine Wurzel von f . Falls kein solches f existiert, heißt α transzendent. Die Erweiterung L/K heißt algebraisch, falls jedes $\alpha \in L$ algebraisch über K ist, und erfüllt, falls $[L:K] = \dim_K L < \infty$.

Bsp.: $-\sqrt{2}$ ist algebraisch über \mathbb{Q} , $\sqrt[3]{\sqrt{3} + \sqrt{2}}$ auch.

- e und π sind transzendent über \mathbb{Q} .
- π ist über algebraisch über $\mathbb{Q}(\pi)$, da $f = x - \pi$ dann π als Wurzel hat.
- i ist algebraisch und endlich über \mathbb{R} ($\dim_{\mathbb{R}} \mathbb{C} = 2$, i ist primitiv).
- \mathbb{R} ist weder algebraisch noch endlich über \mathbb{Q} . (\mathbb{R} = mysteriöses algebraisches Objekt)
- Die algebraischen Zahlen über \mathbb{Q} d.h. alle Elemente von \mathbb{R} die algebraisch über \mathbb{Q} sind, bilden einen abzählbaren Teilkörper von \mathbb{R} , der algebraisch über \mathbb{Q} , aber keine endliche Erweiterung ist.
- endlich \Rightarrow algebraisch, wie wir bald sehen.

Satz 2.6 Sei K ein Körper und $f \in K[x]$ irreduzibel. Dann existiert eine Körpererweiterung L/K , in der f eine Wurzel hat. (wir fragen ob eine Wurzel konstruierbar)

Beweis: $K[x]/\langle f \rangle$ ist dieser Körper. Die Wurzel von f ist $x + \langle f \rangle$.

~~da $\langle f \rangle$ ein Ideal~~ $\text{Bew. } f$ irreduzibel ist Seite Einschränkung, denn von einem $\text{es gibt ein Element}$ einfache Wurzel eines irreduziblen Faktors $\text{wie } K[x]$ aufzutragen.

In einem Hauptidealring erzeugen die irreduziblen Elemente stets maximale Ideale.

aber: $\mathbb{Z}[x]$, also Polynome über einem Ring kein Hauptidealring: $\mathbb{Z}[x]^2 \subsetneq \langle x^2 \rangle$ Multiplication in diesem Körper: Elemente sind Restklassen mod $\langle f \rangle$. Finde Repräsentanten durch Polynomdivision. $K[x] \rightarrow K[x]/\langle f \rangle$, repräsentiert durch $g \mapsto g + \langle f \rangle$

Bsp.: $x^3 - 2 = f$, $K = \mathbb{Q}$. $L = \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ ist ein Körper.

$\bar{x} := x + \langle x^3 - 2 \rangle$ (Repräsentant, Bild von x in den Quotienten)

$$\bar{x} \cdot \bar{x} = \bar{x}^2, \bar{x} \cdot \bar{x} \cdot \bar{x} = x^3 + \langle x^3 - 2 \rangle = 2 + \langle x^3 - 2 \rangle.$$

$$x^3 - 2 \equiv 0 \pmod{\langle x^3 - 2 \rangle}$$

Polynomdivision $g, f \in K[x]$: $\exists! q, r$ mit $g = q \cdot f + r$ und $\deg(r) < \deg(f)$.

Bsp.: Sei $f = x^2 - 2x + 2 \in \mathbb{R}[x]$. Wurzeln sind $\alpha_{1,2} = 1 \pm i$, also ist f irreduzibel über \mathbb{R} , d.h. $K = \mathbb{R}[x]/\langle f \rangle$ ist ein Körper. Behauptung $K = \mathbb{C}$.
 Sei $\varepsilon_{x+i} : \mathbb{R}[x] \rightarrow \mathbb{C}$ der Einbettungsmorphismus. Dann ist $\ker \varepsilon_{x+i} = \langle f \rangle$,
 $f \mapsto f(1+i)$ denn f ist der Grad und $\mathbb{R}[x]$ ist
 (Isomorphiebzl.) $\mathbb{R}[x]/\langle f \rangle \cong \text{Im } (\varepsilon) = \mathbb{C}$, dann ε_{x+i} ist surjektiv: Hauptidealding.
 (Sei $a+bi \in \mathbb{C}$ beliebig. Es gilt $\varepsilon_{x+i}(a+b+bx) = a+b+(1+i) = a+b_i$, also ε_{x+i} surjektiv
 und $\mathbb{R}[x]/\langle f \rangle \cong \mathbb{C}$.
 (Die "normale" Behauptete Konstruktion von $\mathbb{C} = \mathbb{R}[x]/\langle x^2+1 \rangle$ funktioniert genauso.)

Adjungieren einer Wurzel erzeugt eine endliche Erweiterung.
Satz 2.7 Sei $f \in K[x]$ irreduzibel vom Grad d , und $L = K[x]/\langle f \rangle$ sei
 $\Theta = x + \langle f \rangle$ (das Bild von x in L). Dann ist $\{\Theta^0, \Theta^1, \dots, \Theta^{d-1}\}$ eine
 Basis von L über K . hsBereiche ist $[L:K] = d$ und $L = \{a_0 + a_1 \Theta + \dots + a_{d-1} \Theta^{d-1}\}$.

Beweisidee: Das Bild von $p \in K[x]$ in $K[x]/\langle f \rangle$ ist repräsentiert vom Rest
 bei Polynomdivision durch $f \rightarrow$ Angegebene Basis Spannt auf.
 Lineare Unabhängigkeit folgt, da f jedes Polynom, welches in $K[x]/\langle f \rangle$ auf
 Null abbildet, teilt. Jedes solche Polynom hat also Grad $\geq d$.
Merke: In $K[x]/\langle f \rangle$ mit f irreduzibel kann $f = x^d + a_{d-1}x^{d-1} + \dots + a_0$
 als Ersetzungsergel $\Theta^d = a_{d-1}\Theta^{d-1} + \dots + a_0$ genutzt werden.

Man könnte fragen: Welche Wurzel von f wurde in $K[x]/\langle f \rangle$ adjungiert?
 Antwort: Körpertheorie kann die verschiedenen Wurzeln eines irreduziblen f nicht
 unterscheiden. (Alle Wurzeln sind gleich)

Satz 2.8 Sei $f \in K[x]$ irreduzibel, und L eine Erweiterung von K , die eine
 Wurzel α von f enthält. Dann ist $K(\alpha) \cong K[x]/\langle f \rangle$.

Beweis: Sei $\varPhi : K[x] \rightarrow K(\alpha)$. Da $f \in \ker \varPhi$, erhalten wir einen induzierten
 (Ring) $a \mapsto a(\alpha)$ ^{Restklassenring} ^{"algebraische Wurzel"}
 Homomorphismus, den wir auch \varPhi nennen: $\varPhi : K[x]/\langle f \rangle \rightarrow K(\alpha)$ ^{wie definiert,} ^{da $f(\alpha) = 0$}
 Linker steht ein Körper. Ein Ringhomomorphismus $a + \langle f \rangle \mapsto a(\alpha)$
 zwischen Körpern ist injektiv oder Null (denn Ker ist ideal, und Körper haben nur zwei Ideale).
 $\Rightarrow \varPhi$ ist ein Isomorphismus auf sein Bild.
 Da $\varPhi(x) = \alpha$, ist \varPhi surjektiv, also Isomorphismus. \square

Bsp.: $f = x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel (z.B. Eisenstein-Kriterium).

$\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ ist ein "reeller" Körper.

$\mathbb{Q}(\sqrt[3]{2}(-\frac{1}{2} + i\frac{\sqrt{3}}{2}))$ ist kein reeller Körper, aber beide sind isomorphe zu
 $\mathbb{Q}[x]/\langle x^3 - 2 \rangle$ und damit auch isomorph zueinander (diese Isomorphismen
 wollen wir betrachten!).

Satz 2.9 Sei $\varphi: K \rightarrow K'$ ein Isomorphismus von Körpern. Sei weiter $p \in K[x]$ irreduzibel und $p' \in K'[x]$ das Bild unter dem induzierten Isomorphismus $\varphi: K[x] \rightarrow K'[x]$. Sei α eine Wurzel von p (in einer geeigneten Erweiterung von K) und β eine Wurzel von p' . Dann existiert ein Isomorphismus $\theta: K(\alpha) \rightarrow K'(\beta)$, der φ erweitert (d.h. $\theta|_K = \varphi$ (eingeschränkt auf K)). $\alpha \mapsto \beta$

Beweis: Durch.

Proposition 2.10 Sei α algebraisch über K . Dann existiert ein eindeutiges monischer irreduzibles Polynom $m_{\alpha, K} \in K[x]$, dessen Wurzel α ist. Es gilt: α ist Wurzel von einem $f \in K[x]$ genau dann, wenn $m_{\alpha, K} \mid f$.

Beweis: Wähle monische Erzeuger von $\text{Ker}(K[x] \rightarrow K(\alpha))$. \square

Daraus folgt: Sei L/K eine Körpererweiterung und α algebraisch sowohl über L als auch K . Dann gilt: $m_{\alpha, L} \mid m_{\alpha, K}$. Grund: α ist eine Wurzel von $m_{\alpha, K} \in L[x]$ teiler in $L[x]$

Def. 2.11 Das Polynom $m_{\alpha, K}$ in Prop. 2.10 heißt Minimalpolynom von α über K . Sein Grad heißt Grad von α über K .

In besondere gilt für α algebraisch über K : $K(\alpha) \cong K[x]/(m_{\alpha, K})$ und $[K(\alpha):K] \leq \deg(m_{\alpha, K})$. (Bew.) \rightarrow Bsp.: $R(i) \cong R[x]/(x^2+1) \cong \mathbb{C}$ und $\deg(x^2+1) = [C : \mathbb{R}] = 2$!

Satz 2.12 Jede endliche Körpererweiterung ist algebraisch.

Beweis: Sei $n = [L:K]$ und $\alpha \in L$ beliebig. Die Menge $\{\alpha, \alpha^2, \dots, \alpha^n\}$ ist linear abhängig über K , d.h. $\exists \lambda_0, \dots, \lambda_n \in K$ (nicht alle Null): $\sum_{i=0}^n \lambda_i \alpha^i = 0$. Dann hat $f = \sum_{i=0}^n \lambda_i x^i \in K[x]$ die Wurzel α , also ist α algebraisch. \square

Bsp.: Quadratische Erweiterungen (in Charakteristik $\neq 2$).

Sei K ein Körper mit char(K) $\neq 2$ und L eine Erweiterung von K vom Grad 2.

Sei $\alpha \in L/K$ und $m_{\alpha, K} = x^2 + bx + c$ sein Minimalpolynom. Außerdem gilt $K(\alpha) = L$, da $K(\alpha) \subseteq L$ ein 2D-Unterraum und dim _{K} $L = 2$.

Die quadratische Lösungsformel (pq-Formel) gilt in jedem Körper der Charakteristik $\neq 2$: $(*) \alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ und $b^2 - 4c$ ist kein Quadrat in K , da $\alpha \notin K$.

Das Symbol $\sqrt{b^2 - 4c}$ ist eine Kurzschreibweise für eine Wurzel von $x^2 - b^2 + 4c \in L[x]$.

Es gilt: $K(\alpha) = K(\sqrt{b^2 - 4c})$.

" \subseteq ": Da $\alpha \in K(\sqrt{b^2 - 4c})$, also $K(\alpha) \subseteq K(\sqrt{b^2 - 4c})$.

" \supseteq ": $\pm (2\alpha + b) = \pm \sqrt{b^2 - 4c} \in K(\alpha)$.

Die Rechnung war wohlgeklärt von α , d.h. jede Grad-2-Erweiterung von K ist von der Form $K(\sqrt{D})$, wobei die "Diskriminante" $D \in K$

kein Quadrat ist. Da jede Erweiterung dieser Form auch Grad 2 hat, ergibt sich eine Charakterisierung.

\Rightarrow Ringe, Körper, K - und F -Vektorräume gleichzeitig

Satz 2.13 (Satz von Turm). Sei $F \subseteq K \subseteq L$ ein Turm von Teilkörpern. Dann gilt: $[L:F] = [L:K] \cdot [K:F]$. (Gilt aus, falls einige davon 0 sind mit $0 \cdot x = 0$ usw.)

Beweisidee: Falls L/K und K/F endlich und $\alpha_1, \dots, \alpha_m$ eine K -Basis von L und β_1, \dots, β_n eine F -Basis von K sind, dann ist $\{\alpha_i \beta_j \mid i=1, \dots, m, j=1, \dots, n\}$ eine F -Basis von L .

Diese Basis spannt auf, denn: sei $x \in L$. Dann ist $x = \sum_{i=1}^m a_i \alpha_i$ für gewisse $a_i \in K$ und $x = \sum_{i=1}^m \sum_{j=1}^n b_{ij} \beta_j \alpha_i$ mit $b_{ij} \in F$, d.h. a_i, b_{ij} spannen auf.

Lineare Unabhängigkeit und $\dim = \infty$: Obige. \square

Bsp für die Annahme: Beh.: $\mathbb{Q}(\sqrt[3]{2}) \not\subseteq \mathbb{J}\mathbb{Z}$; da $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2$
 (wobei der bereit darunterliegt) und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$
 aber aus $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})$
 folgt der Widerspruch $2 \mid 3$. \square

Bsp.: Sei $\sqrt[6]{2} \in \mathbb{R}$ die positive reelle sechste Wurzel aus 2.

Da $x^6 - 2$ irreduzibel ist (Eisenstein), $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$
 Minimalpolynom Da $(\sqrt[6]{2})^2 = \sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$ gilt, gilt $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$.

Das Minimalpolynom von $\sqrt[6]{2}$ über $\mathbb{Q}(\sqrt{2})$ hat Grad 3
 und ist also gleich $x^3 - \sqrt{2}$.

A priori wäre es schwer zu entscheiden, ob dieses Polynom in $\mathbb{Q}(\sqrt{2})[x]$ irreduzibel ist.

$$\begin{array}{c} x^3 - \sqrt{2} \\ \text{es gilt: } 3 \end{array}$$

Bsp.: Hat man eine endlich erzeugte Körpererweiterung $K(\alpha_1, \dots, \alpha_n)$, d.h. \dim , und alle α_i sind algebraisch über K , so ergibt sich ein Turm:

$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_\ell = K(\alpha_1, \dots, \alpha_n)$ mit $K_i = K_{i-1}(\alpha_i)$.

Der Grad $[K_i : K_{i-1}]$ ergibt sich aus dem Minimalpolynom von α_i über K_{i-1} .

Sei $n_i = [K(\alpha_i) : K]$ der Grad von α_i über K . Dann gilt

$$[K(\alpha_1, \dots, \alpha_n) : K] \leq \prod_{i=1}^{\ell} n_i.$$

Eine Basis muss obwohl konstruiert werden ($K(\alpha_1, \alpha_2) \subset K(\alpha_1)(\alpha_2)$).

Satz 2.11 Eine Erweiterung L/K ist endlich genau dann, wenn $L = K(\alpha_1, \dots, \alpha_n)$ für algebraische (Überk) $\alpha_1, \dots, \alpha_n \in L$.

Beweis: " \Leftarrow " Direkt vor den Satz im Bsp. gezeigt.

" \Rightarrow " Falls L/K endlich ist, sei $\alpha_1, \dots, \alpha_n$ eine K -Basis von L .

Dann ist $[K(\alpha_i) : K] \leq [L : K]$ (fakt sogar!) $\underset{\text{denn auch } L \text{ endlich}}{\text{dann auch } \alpha_i \text{ endlich}}$

Also sind alle α_i algebraisch und es gilt $L = K(\alpha_1, \dots, \alpha_n)$. \square

Es folgt: Die algebraischen Elemente (über K) in einer Körpererweiterung L/K bilden einen Teilkörper von L , denn $\alpha \pm \beta, \alpha \cdot \beta, \alpha/\beta$ ($\beta \neq 0$) sowie α^{-1} sind alle Elemente von $K(\alpha, \beta)$, also algebraisch über K falls α und β algebraisch über K sind.

Bsp.: $\mathbb{Q} \subseteq \mathbb{C}$ sind die algebraischen Elemente über \mathbb{Q} :

$x^n - 2$ ist für alle $n \geq 2$ irreduzibel über $\mathbb{Q} \Rightarrow [\mathbb{Q} : \mathbb{Q}] \geq n \nmid 2$.
 \rightsquigarrow d.h. \mathbb{Q} keine endliche Körpererweiterung.

Ferner ist \mathbb{Q} abzählbar (denn $\mathbb{Q}, \mathbb{Q}[x]$ abzählbar und Vereinigung abzählbarer Mengen abzählbar).

\Rightarrow Praktisch keine reelle Zahl ist algebraisch (zufällig gezogen quasi). Allerdings ist es für einzelne Zahlen sehr schwer nachzuweisen, dass sie nicht algebraisch sind (z.B. π oder e).

Zettel und
Liniel =
"Mathematik des
zweiten Bandes"

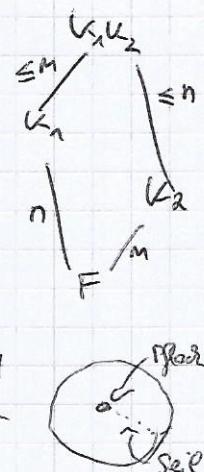
Def. 2.15 Seien K_1 und K_2 Teilkörper eines Körpers L . Das Kompositum K_1K_2 von K_1 und K_2 ist der kleinste Teilkörper von L , der sowohl K_1 als auch K_2 enthält. - hängt vom Körper L nicht ab; (es muss aber so ein L geben).

Prop. 2.16 Sei ein K_1/F und K_2/F endliche Erweiterungen und alle enthalten in einem Körper L . Dann ist $[K_1K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$.

Beweis. Sei $\alpha_1, \dots, \alpha_n$ eine F -Basis von K_1 und β_1, \dots, β_m eine F -Basis von K_2 . Dann ist $K_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$. Die $\alpha_i\beta_j$ spannen K_1K_2 sicher als F -Vektorraum auf; können aber linear abhängig sein. \Rightarrow

Falls m und n in Prop. 2.16 teilerfremd sind, dann hat man Gleichheit:

$$[K_1K_2 : F] = [K_1 : F] \cdot [K_2 : F]. \quad \text{Graed: } [K_1K_2 : F] \text{ ist immer durch } n \text{ und } m \text{ teilbar, also auch durch das kgV von } m \text{ und } n. \text{ Falls } \text{ggT}(m, n) = 1, \text{ also } [K_1K_2 : F] \geq [K_1 : F][K_2 : F] = n \cdot m.$$



3. Konstruktionen mit Zirkel und Lineal

Setting: Landvermessung anno 1000 BC.

Werkzeuge: Pflöcke und Seile. Damit konnte man (bereits bekannte Längen replizieren (2 Pflöcke ins Seil legen), (o) Geraden und Kreise konstruieren. Heutzutage: Zirkel und unmarkierter Lineal.

Die klassischen griechischen Konstruktionsprobleme:

- I) Die Verdopplung des Würfels: Konstruktion zu gegebenem Würfel - Quadrat geht einen mit genau doppeltem Volumen.
- II) Die Dreiteilung des Winkels: Einen gegebenen Winkel in drei gleiche Teile teilen. - Zweitelpung geht (Risektion)
- III) Die Quadratur des Kreises: Zu gegebenem Kreis ein Quadrat mit gleichen Flächeninhalt konstruieren.

"das kennen sie aus ihrem Mathelehrbuch"

Abschreiten im Algebra:

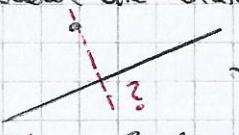
$1 \in \mathbb{R}$ sei eine Basislänge oder Maßeinheit. $a \in \mathbb{R}$ sind andere Längen. Frage: Welche $a \in \mathbb{R}$ sind konstruierbar, d.h. irgendwo in der Konstruktion nach endlich vielen Schritten messbar.

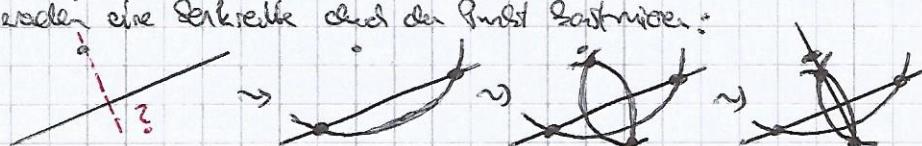
Ein Punkt $(x, y) \in \mathbb{R}^2$ ist konstruierbar, falls x und y konstruierbar sind.

Welche Konstruktionen sind möglich?

- 1) 2 gegebene Punkte durch eine Gerade verbinden,
- 2) Den Schnittpunkt von 2 (nicht-parallel) Geraden bestimmen,
- 3) Einen Kreis mit gegebenem Mittelpunkt und Radius konstruieren,
- 4) Schnittpunkte von Kreisen mit Kreisen und Kreisen mit Geraden bestimmen.

Mit diesen Operatoren kann man viele "stumpftechnische" Konstruktionen aufführen:

- Ein Lot fällen:  zu einer Geraden und einen Punkt nicht auf der Geraden eine Senkrechte durch den Punkt konstruieren:



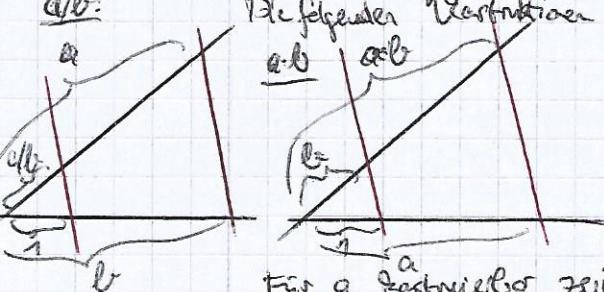
- Mittelpunkt von Strecken finden
- Winkel zweiteln
- Tangent an einem geg. Kreispunkt konstruieren
- einen Punkt an einer Geraden spiegeln
- Parallele zu geg. Gerade durch geg. Punkt konstruieren
- zu 3 nicht kollinearen Punkten einen Kreis konstruieren, der sie enthält

Damit erhält man:

Jede rationale Zahl ist konstruierbar.

Bem: Für gegebene a, b ist $a+b$ mit dem Zirkel konstruierbar.

Die folgenden Konstruktionen geben ab und $\frac{a}{b}$:



- 1) Markiere 1 auf einer Geraden
- 2) Markiere b auf zweiter Geraden durch gleichen Nullpunkt
- 3) Konstruiere parallele rote Geraden.

Quadraturwurzeln sind konstruierbar:

Für a konstruierbar, zeichne Kreis mit Durchmesser $1+a$ (I),
(II) eine Senkrechte durch P (Parallele zur Torgede)
(III) Ja ergibt sich als Höhe, da

$$\begin{array}{l} \text{Diagramm: Ein rechteckiger Kasten mit den Seiten } 1 \text{ und } a. \text{ Eine Diagonale verbindet die Ecken } 1 \text{ und } a. \text{ Der Hypotenuse ist } \sqrt{1+a^2}. \\ (1+a)^2 = y^2 + z^2 = a^2 + x^2 + z^2 + 1 = 1 + a^2 + 2x^2 \\ 1 + a^2 + 2a = 1 + a^2 \Rightarrow x^2 = a \end{array}$$

\Rightarrow Die konstruierbaren Zahlen bilden einen Teilkörper von \mathbb{R} , der alle Quadraturwurzeln enthält, aber nicht mehr "spielt", was wir schon konstruiert haben.

Prop. 3.1 Falls ein $a \in \mathbb{R}$ aus einem Körper $K \subseteq \mathbb{R}$ mit Zirkel und Lineal konstruiert werden kann, so gilt: $[K(a):K] = 2^l$ für ein $l \geq 0$. "quadratische Radikulare lösen".

Beweis: Wir analysieren Konstruktionen 1)-4):

1)-2), d.h. Schnittpunkte von Geraden, sind durch lineare Gleichungen bestimmt, also über jeden K lösbar. (diese Punkte muss ich sie konstruiert haben)

Die Zirkelkonstruktionen 3)-4) lösen quadratische Gleichungen:

z.B. der Schritt von 2 Kreisen: $\{(x,y) \mid (x-l)^2 + (y-k)^2 = r^2\}$ ist auch der Schritt eines Kreises mit einer Geraden, $\{(x-l')^2 + (y-k')^2 = r'^2\}$ Subtrahiere

dazu die vektorielle Gleichung von der zweiten: $= \{(x,y) \mid (x-l)^2 + (y-k)^2 = r^2\}$
Dies ergibt quadratische Gleichungen für x und y .

$$\begin{cases} (x-l)^2 + (y-k)^2 = r^2 \\ (x-l')^2 + (y-k')^2 = r'^2 \end{cases} \quad \begin{cases} \text{lineare Gleichung} \\ x^2 - 2lx + l^2 + y^2 - 2ky + k^2 = r^2 \\ x^2 - 2l'x + l'^2 + y^2 - 2k'y + k'^2 = r'^2 \end{cases}$$

\rightarrow Alle konstruierbaren Punkte sind Lösungen von quadratischen Gleichungen mit Koeffizienten in bereits konstruierbaren Zahlen, d.h. in Grad 2-Erweiterungen enthalten. Erweiterungsgrade sind multiplikativ, also gilt die Aussage. \square

Satz 3.2 Die klassischen griechischen Konstruktionsprobleme II), III), IV) sind mit Zirkel und Lineal nicht lösbar.

Beweis (Schluss): Zur Verdopplung des Winkels müste man die Kantenlänge $3\sqrt{2}$ konstruieren, aber $3\sqrt{2}$ ist in keinem Grad 2 Erweiterung von \mathbb{Q} enthalten.

Zur Dreiteilung des Winkels will man mit gegebenen $\cos \theta$ und $\cos \theta/3$ konstruieren, z.B. $\theta = 60^\circ$ kann nicht dreigeteilt werden. Es gilt $\cos \theta = \frac{1}{2}$.

Es gilt: (Chebyschev-Polygone!)

$$\cos \theta = \cos 3 \cdot \theta/3 = 4 \cos^3 \theta/3 - 3 \cos \theta/3. \text{ Sei } \beta = \cos 20^\circ.$$

$$\text{Dann gilt: } 4\beta^3 - 3\beta - \frac{1}{2} = 0 \quad | \cdot 2$$

$$\Leftrightarrow (2\beta)^3 - 3(2\beta) - 1 = 0 \text{ ist ein irreduzibles Eudides Polynom in } 2\beta.$$

$\Rightarrow 2\beta$ ist nicht konstruierbar $\Rightarrow \beta$ ist nicht konstruierbar.

Zur Quadratur des Kreises: Hier müsste man π konstruieren. Das ist nicht mal algebraisch über \mathbb{Q} , also nicht konstruierbar. \square

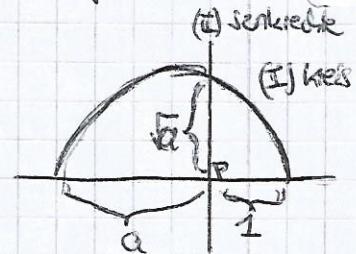
Bem.: $-\cos \theta$ (für ganzzahlige θ in Grad) ist konstruierbar $\Leftrightarrow \theta$ ist durch 3 teilbar.

Grund: Formel für $\cos 3^\circ$ ist explizit bekannt.

- Konstruktion des regulären n -Ecks - primäre Primzahlen etc.

(Bsp. 6537-Eck: konstruierbar)

Bibliothek Göttingen: Konstruktionsvorstüft von Gauß ("Koffer-Buch")



IV. ZERFALLUNGSKÖRPER

Wir haben in Kapitel II mittels $K(\alpha) = \frac{K[x]}{(f)}$ eine Wurzel eines irreduziblen Polynoms f an K adjungiert. Jetzt betrachten wir alle Wurzeln.

Def. 4.1 Ein Zerfallungskörper eines $f \in K[x]$ ist eine Erweiterung L/K , in der f in Linearfaktoren zerfällt und so, dass füher seinen edleren Teilkörper von L zerfällt (der Glanz sei die Körper).

Bsp.: $x^3 - 1 \in \mathbb{Q}[x]$ zerfällt über \mathbb{C} , aber der Zerfallungskörper ist $\mathbb{Q}(\omega)$ für $\omega \in \mathbb{C}$ eine primitive dritte Einheitswurzel.

Jedes $f \in K[x]$ hat einen Zerfallungskörper, da sukzessive Wurzeln adjungiert werden können und dabei der Grad sinkt. So bekommt man keine Eindeutigkeit, aber nur Eindeutigkeit bis auf Isomorphie später (verbesserter Satz 2.9).

Zunächst diskutieren wir einen Effekt in Charakteristik $p > 0$.

Def. 4.2 Sei $f \in K[x]$ ein Polynom und $f = \lambda \cdot g_1 \cdots g_s$ sei eine irreduzible Zerlegung über K (d.h. $\lambda \in K$, g_i irreduzibel und monisch). Dann heißt f separabel, falls kein g_i mehrfache Wurzeln hat (in irgendwelchen Erweiterungen von K bzw. in einer Erweiterung von K , die alle Wurzeln von f enthält).

→ f kann mehrere Wurzeln haben, aber die g_i müssen nicht g_i mehrfach auf.

Ein g_i hat mehrfache Wurzeln, falls es eine Wurzel mit seiner Ableitung teilt oder falls $\text{ggT}(g_i, g'_i) \neq 1$. Aber: g_i irreduzibel und $\deg(g_i) < \deg(f)$ ist ein "leeres Ergebnis".
 $x^d \mapsto dx^{d-1}$
 $1 \mapsto 0$

In Charakteristik 0 ist jedes nichtkonstante Polynom separabel, aber in Charakteristik $p > 0$ kann $g'_i = 0$ auch gelten, wenn g_i nicht konstant ist. (z.B. x^p)

Ein Körper K heißt perfekt, falls jedes nicht konstante Polynom separabel ist.

Bem.: $\text{char}(K) = 0 \Rightarrow K$ perfekt
 $|K| < \infty \Rightarrow K$ perfekt ← nicht offensichtlich

Bsp.: $K[t] \rightsquigarrow K(t) = \left\{ \frac{f}{g} \mid f, g \in K[t], g \neq 0 \right\}$ $\frac{f}{g} \in K \Leftrightarrow f \cdot \bar{g} = \bar{f} \cdot g$

- "Das ist im Prinzip das einzige Beispiel, wo das gemacht"

Sei $K = \mathbb{F}_p(t)$ der Körper der rationalen Funktionen mit Koeffizienten in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p prim. In $K[x]$ sei $f = x^p - t$. Wir sehen gleich: f ist irreduzibel. Sei L der Zerfallungskörper von f .

In Charakteristik p (geg. α eine Wurzel von f , $\alpha \in L$) gilt:

$$(x - \alpha)^p = x^p - \alpha^p = x^p - t, \text{ d.h. } \alpha \text{ ist } p\text{-te Nullstelle von } f. \quad \text{Es gibt nur eine Einheitswurzel!}$$

Da die irreduzible Zerlegung eindeutig ist, folgt, dass f irreduzibel über K ist, da keine Potenz $(x - \alpha)^k$ mit $k < p$ in $K[x]$ liegt.

Es gilt: $f' = p \cdot x^{p-1} = 0$, wie oben bemerkt. ($\text{char} = p$), also ist f inseparabel.

Def. 4.3 Sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt separabel, falls α transzendent ist oder ein separables Minimalkörpern hat.

Die Erweiterung L/K ist separabel, falls jedes $\alpha \in L$ separabel ist.

Bem. Sei L/K eine Körpererweiterung. Dann heißt $K_S = \{\alpha \in L \mid \alpha \text{ separabel über } K\}$ der separabile Abschluss von K in L . Das ist ein Teilkörper von L . Ein Element $\alpha \in L$ heißt inseparabel, falls sein Minimalpolynom über K nach α als $(K - \alpha)^m$ faktoriert (in einem Zerfallungskörper, z.B.p.).

"Die Deter auf
einer CD sind
Unterlizenzen von
Polymeren."

Eine Erweiterung L/K heißt rein inseparabel, falls jedes $\alpha \in L$ rein inseparabel ist.
Dann gilt: L/K_S ist rein inseparabel und K_S/K ist separabel.
Die Grade dieser Erweiterungen erfüllen aufeinander folgende Formeln.

Satz 4.4 Sei $\varphi: K \rightarrow K'$ ein Isomorphismus von Körpern. Sei $f \in K[x]$ und $f' \in K'[x]$ das Bild unter dem induzierten Isomorphismus $\varphi: K[x] \rightarrow K'[x]$.
Sei L ein Zerfällungskörper von f und L' ein Zerfällungskörper von f' . ($f' = \sum_{i=0}^d \varphi(a_i)x^i$)
(i) Dann existiert ein Isomorphismus $\alpha: L \rightarrow L'$, der φ erweitert
(d.h. $\alpha|_K = \varphi$ (ingeschränkt auf K)).
(ii) Ist f separabel, so gilt es genau $[L:K]$ solche Erweiterungen α .

Beweisstrategie: Satz 2.9: $K(\alpha) \cong K'(\beta)$... induktiv nutzen.

$$\frac{[L:K]}{[L':K']} = \frac{1}{\frac{[K(x):K]}{[K'(x'):K']}} = \frac{1}{1} = 1$$

Beweis i): Induktion nach dem Grad $n = [L:K]$. Der Isomorphismus $\varphi: K[x] \rightarrow K'[x]$ bildet irreduzible Zerlegungen auf irreduzible Zerlegungen ab. D.h. f zerfällt über $K \Leftrightarrow f'$ zerfällt über K' .

In diesem Fall setze $\alpha = \varphi$. Satz gilt für $n=1$.

Induktionsannahme: Der Satz gilt für alle Grade $< n$.

Sei $n \geq 2$. Da f nicht zerfällt existiert ein irreduzibler Faktor p von f mit Grad ≥ 2 . Sei $p' \in K'[x]$ das Bild von p unter φ , $\alpha \in L$ eine Wurzel von p und $\beta \in L'$ eine Wurzel von p' . Beide Sätze 2.9 haben uns einen Isomorphismus $\varphi: K(\alpha) \rightarrow K'(\beta)$, der $\varphi: K \rightarrow K'$ erweitert. Dann gilt:
$$[L:K] = \underbrace{[L:K(\alpha)]}_{< n} \cdot \underbrace{[K(\alpha):K]}_{\geq 2} \quad (\text{Satz von Turm}).$$

Nach Induktionsannahme existiert ein $\alpha: L \rightarrow L'$, welches φ und damit auch φ erweitert. Also gilt (i).

Zu ii): Induktion nach $n = [L:K]$. Falls $n=1$, ist $\alpha=\text{id}$ die einzige Möglichkeit. Falls $n > 1$, sei $f = p \cdot g$ mit $p \in K[x]$ irreduzibel vom Grad ≥ 2 . Sei α eine Wurzel von p , und $\alpha: L \rightarrow L'$ eine Erweiterung von φ . $\alpha(\alpha) = \beta \in L'$ ist eine Wurzel von $p' = \varphi(p) \in K'[x]$.

Da p und damit p' separabel ist, hat es genau $d = \deg p$ verschiedene Wurzeln in L' . Also existiert in Satz 2.9 genau d Isomorphismen $\psi: K(\alpha) \rightarrow K'(\beta)$, die φ erweitern. (ψ ist auch über $K(\alpha)$ ein Zerfällungskörper von f und genau L' von f' über $K'(\beta)$).

Per Induktionsannahme und $[L:K(\alpha)] = [L:K]/d$ hat jeder der d Isomorphismen ψ noch $[L:K(\alpha)] = [L:K]/d$ Erweiterungen zu $\alpha: L \rightarrow L'$. Insgesamt hat also φ genau $[L:K]$ Erweiterungen. \square

Folgerungen. - Je zwei Zerfällungskörper eines $f \in K[x]$ sind isomorph. Dazu wählt man im Satz $\varphi = \text{id}_K$.

- Moore's Theorem: Je zwei endliche Körper der Ordnung $q = p^n$ sind isomorph. Beweisidee: Zeige, dass der Körper mit $q = p^n$ Elementen der $\mathbb{F}_p[x]$ mit $x^q - x \in \mathbb{F}_p[x]$ st. Dieses Polynom hat alle Elemente von \mathbb{F}_q als Wurzeln.

II. DIE GALOISGRUPPE

Wir machen die Analogie aus Kapitel I formal und schreiben:

Ebene Geometrie	Galoistheorie
Polygone P	Polynom $f \in K[x]$
Ebene	Zerfällskörper von f L/K
Erben von P	Wurzeln von f
Lineare Transformationen	Automorphismen von L
orthogonale Transformationen	Autonelemente von L , die K punktweise fixieren
Symmetriegruppe von P	Galoisgruppe von f
reguläres P	irreduzibles f

Algebra II

09.05.2019

Def. 5.1 Sei L/K eine Körpererweiterung. Die Galoisgruppe der Erweiterung ist $\text{Gal}(L/K) = \{ \text{Automorphismen von } L, \text{ die } K \text{ punktweise fixieren} \}$

Bem. $\text{Gal}(L/K)$ ist eine Untergruppe von $\text{Aut}(L)$
 "punktweise fixieren": $\forall x \in K, \sigma \in \text{Gal}(L/K): \sigma(x) = x$

Satz 5.2 Sei L der Zerfällskörper von $f \in K[x]$. Wenn f in L n verschiedene Wurzeln hat, dann ist $\text{Gal}(L/K)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n .

Beweis: Sei $X = \{\alpha_1, \dots, \alpha_n\}$ die Menge der Wurzeln von f in L .
 Nach Aufgabe 1.5 ist $\sigma(X) = X$ für jedes $\sigma \in \text{Gal}(L/K)$. Die so definierte Abbildung $i: \text{Gal}(L/K) \rightarrow S_n$ (wobei jede Permutation von $\alpha_1, \dots, \alpha_n$ mit der Permutation von $1, \dots, n$ identifiziert wird), ist ein Gruppenhomomorphismus.
 Um zu zeigen, dass i injektiv ist, müssen wir zeigen, dass aus $\sigma(\alpha_i) = \alpha_i$ für $i = 1, \dots, n$ folgt, dass $\sigma = \text{id}_L$, was aus Satz 3.1 folgt. \square Hint: $\sigma: K(\alpha_i) \longrightarrow K(\alpha_i)$

Bem. Satz 5.2 zeigt, dass $|\text{Gal}(L/K)| \leq n!$

Bsp. Zerfällskörper von $x^2 + 1$ über \mathbb{R} ist \mathbb{C} und $|\text{Gal}(\mathbb{C}/\mathbb{R})| \leq 2 = 2$ folgt, da $(z \mapsto \bar{z}) \in \text{Gal}(\mathbb{C}/\mathbb{R})$. $\varphi: \mathbb{C} \longrightarrow \mathbb{K}$

Satz 5.3 Sei $f \in K[x]$ separabel (kein irreduzibler Faktor hat wiederholte Wurzeln) und L/K sein Zerfällskörper. Dann gilt: $|\text{Gal}(L/K)| = [L:K]$.

Beweis: Satz 4.4 mit $K = K'$, $\varphi = \text{id}_K$, $L = L'$ liefert, dass es $[L:K]$ Erweiterungen der Identität auf K' zu einem Isomorphismus von L gibt. Dies sind genau die Elemente von $\text{Gal}(L/K)$.

Bsp.: $f = x^3 - 1 \in \mathbb{Q}[x]$ ist separabel als Polynom über \mathbb{Q} . f zerfällt über \mathbb{Q} als $f = (x-1)(x^2+x+1)$. Sei L der Zerfällskörper. Sei w eine Kreisteilungspolynom von Grad 2 primitive dritte Einheitswurzel, z.B. $w = e^{\frac{2\pi i}{3}}$ in \mathbb{C} . Eine, die alle Einheitswurzeln erzeugt, also insb. nicht 1. Dann hat $L = \mathbb{Q}(w)$ den Erweiterungsgrad 2 über \mathbb{Q} (da $\text{min}_{\mathbb{Q}}(w) = x^2 + x + 1$):

Also $|\text{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 2$. Das zweite Element ist die komplexe Konjugation, und bildet ω auf $\bar{\omega} = \omega^2$ ab.

Bsp.: Sei $f = x^3 - 2 \in \mathbb{Q}[x]$. Die Wurzeln sind $\alpha, \omega\alpha, \omega^2\alpha$ mit $\omega = \sqrt[3]{-1} \in \mathbb{R}$

Der Zerfallkörper ist $L = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega)$.

f ist irreduzibel über \mathbb{Q} (Kriterium) und (rekon ferner) α ist eine Wurzel, d.h. $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ (nach $m_{\alpha,\mathbb{Q}} = x^3 - 2$).

Aber: $\mathbb{Q}(\alpha) \neq L$ da $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. (aber $L \not\subseteq \mathbb{R}$)
 $\Rightarrow [L:\mathbb{Q}(\alpha)] > 1 (= 1$ soweit gleich)

vgl.

Aus Satz 5.2 und 5.3 erhalten wir:

$$\begin{aligned} \text{1. Vorausg., } |\text{Gal}(L/\mathbb{Q})| &= [L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}] \leq 3 \cdot 1 = 3. \\ \text{Analogie zu D}_6 \text{ (Geometrie). } &\Rightarrow L/\mathbb{Q}(\alpha) \text{ ist quadratisch, } > 1 = 3 \quad \text{Satz 5.2} \\ &\text{also } [L:\mathbb{Q}(\alpha)] = 2, \text{ und } \text{Gal}(L/\mathbb{Q}) \text{ ist } D_3. \text{ (zufällig auch } D_6). \end{aligned}$$

Lemma 5.4 Sei $F \subseteq K \subseteq L$ ein Turm von Körpererweiterungen. Sei weiter K der Zerfallskörper eines $f \in F[x]$. Für jedes $\sigma \in \text{Gal}(L/F)$ ist $\sigma|_K \in \text{Gal}(K/F)$.

↪ permutiert K intern, bildet nicht auf separabel K/F

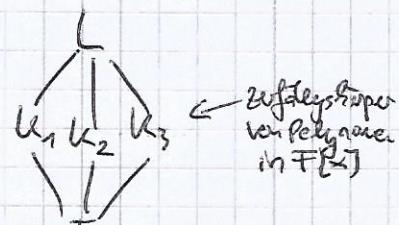
Beweis: Es genügt zu zeigen: $\sigma(K) = K$. Seien $\alpha_1, \dots, \alpha_n$ die resturzellen Wurzeln von f . Dann gilt $K = F(\alpha_1, \dots, \alpha_n)$. Es gilt $\sigma(F) = F$ (da $\sigma \in \text{Gal}(L/F)$) und $\sigma(\{\alpha_1, \dots, \alpha_n\}) = \{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$. Damit $\sigma(K) = \sigma(F(\alpha_1, \dots, \alpha_n)) = F(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \supseteq F(\alpha_1, \dots, \alpha_n) = K$. \square
da $K(\alpha_1\beta) = K(\beta\alpha_1) = K(\alpha_1\beta)$

Das Lemma eröffnet eine "Sortierungsgelegenheit" aus.

Ein $\sigma \in \text{Gal}(L/F)$ permutekt jeden Zerfallskörper zwischen L und F intern. (wobei z.B. nicht vertauscht)

(So ein σ versucht" vorzusehen nicht die "Innen" K_1, K_2, K_3)

Falls L selbst ein Zerfallskörper ist, erhalten wir Einschätzungen von Quotienten von $\text{Gal}(L/F)$:



Satz 5.5 Sei $F \subseteq K \subseteq L$ ein Turm von Körpererweiterungen und K/F der Zerfallskörper von $f \in F[x]$ und L der Zerfallskörper von $g \in F[x]$. \square Unterkapitel zu Lemma 5.4.

Dann ist $\text{Gal}(L/K)$ ein Normalteiler in $\text{Gal}(L/F)$ und

$$\frac{\text{Gal}(L/F)}{\text{Gal}(L/K)} \cong \text{Gal}(K/F).$$

Beweis: Definiere $\Psi: \text{Gal}(L/F) \rightarrow \text{Gal}(K/F)$. (gilt Dank Lemma 5.4)

$$\sigma \mapsto \sigma|_K$$

Ψ ist ein Gruppenhomomorphismus: $(\sigma_1 \circ \sigma_2)|_K = \sigma_1 \circ \sigma_2|_K = \sigma_1|_K \circ \sigma_2|_K$, da $\sigma_2(K) = K$. Kern besteht aus Automorphismen σ von L mit $\sigma|_K = \text{id}_K$, also genau $\text{Gal}(L/K) \Rightarrow$ Also ist dies ein Normalteiler.

Nach Satz 4.4 kann jedes $\Psi \in \text{Gal}(K/F)$ zu einem $\sigma \in \text{Gal}(L/F)$ erweitert werden. Also ist Ψ surjektiv und der Isomorphiesatz (Vorlesung) liefert

$$\frac{\text{Gal}(L/F)}{\text{Gal}(L/K)} \cong \text{Gal}(K/F). \quad \square$$

Bem.: Warum wurden K und L als Zerfallskörper angenommen?

- Für Lemma 5.4 benötigt man K/F als Zerfallskörper; sonst kann man Ψ nicht so definieren.

- Für die Surjektivität von Ψ haben wir Satz 4.4 und damit L/F Zerfallskörper genutzt. (Dies impliziert, dass L/K auch Zerfallskörper ist, nämlich von g aufgesetzt als $g \in K[x]$). Falls L/F kein Zerfallskörper ist, bleibt $\text{Gal}(L/F)$ unbestimmt und $\frac{\text{Gal}(L/F)}{\text{Gal}(L/K)}$ ist nur eine Untergruppe von $\text{Gal}(K/F)$.

Ausblick auf
Kategorienlehre =
 $G \rightarrow H$
bijektiv
 \downarrow
 $G/\text{ker } \varphi \rightarrow H/\varphi$
"Quotienten" "Untergruppen"

(Jemand versteht den Raum.)
geflüxt
"bleibt doch hier!"

Weil dieses Konzept so wichtig ist, definieren wir:

Def. 5.6 Eine Erweiterung L/K heißt Galoiserweiterung, falls L Zerfallskörper eines separaten $f \in K[x]$ ist.

"Abel war so
bif, dass
oblig klein
geschriften wird.
Der wurde adjektiv,
hinter. Das ist
der griechische, adjektiv,
hinter zu nennen!"

Bsp. Wieder $f = x^3 - 2 \in \mathbb{Q}(x)$. Notation wie oben, $L = \mathbb{Q}(\alpha, \omega)$ Zerfallskörper.
 $\text{Gal}(L/\mathbb{Q}) = S_3$. Betrachte der Turm $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq L$.

\Rightarrow Satz: $\text{Gal}(L/\mathbb{Q}(\omega)) \cong \text{Gal}(L/\mathbb{Q}) = S_3$. Zerfallskörper

$$\text{und } \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \frac{\text{Gal}(L/\mathbb{Q})}{\text{Gal}(L/\mathbb{Q}(\omega))}$$

↑
= S_3 , hat
ordnung 6
↑
muss nach Lagrange
ordnung = 3 haben

Wir haben oben festgestellt: $x^3 - 2$ ist irreduzibel über $\mathbb{Q}(\omega)$, da es keine Wurzeln hat.

$\Rightarrow L/\mathbb{Q}(\omega)$ ist Galois $\Rightarrow [L : \mathbb{Q}(\omega)] = |\text{Gal}(L/\mathbb{Q}(\omega))|$.

Also ist der Isomorphismus $\mathbb{Z}_2 \cong S_3/A_3$:
Der Erzeuger von $\text{Gal}(L/\mathbb{Q}(\omega))$ ist definiert durch $\sigma(\omega) = \omega$
 $\sigma(\alpha) = \alpha\omega$.

Algebra II

10.05.2019

$(x^n - c)$ hat die Wurzeln $\sqrt[n]{c}, \sqrt[n]{cw}, \dots, \sqrt[n]{cw^{n-1}}$.

Def. 5.7 Sei $n \geq 2$ und K ein Körper. Eine n -te Einheitswurzel ist ein $\lambda \in K$ oder $\notin K$ mit $\lambda^n = 1$. Die n -ten Einheitswurzeln bilden unter Multiplikation eine Gruppe. Eine n -te Einheitswurzel ist primitiv, falls sie Erzeuger der Gruppe aller n -ten Einheitswurzeln von K ist.

- Bem.:
- Diese Gruppe ist also zugleich (beweisen wir später).
 - In \mathbb{C} gibt es n -te Einheitswurzeln und eine primitive ist $e^{\frac{2\pi i}{n}}$.
 - Die Gruppe der Einheitswurzeln ist zugleich Anzahl der Erzeuger ist $\phi(n)$, die euklidische Phi-Funktion (Anzahl von Zahlen $\geq 1, < n$ mit $\gcd(n, k) = 1$).
 - Für jeden Ring R setzen wir $R^* = \{r \in R \mid r \text{ ist invertierbar in } R\}$ für die Multiplikativen Gruppe von R . Wir brauchen das nur für $K^* = K \setminus \{0\}$, die multiplikative Gruppe eines Körpers und $\mathbb{Z}/n\mathbb{Z}^*$ die Einheitsgruppe von $\mathbb{Z}/n\mathbb{Z}$ als Ring

$\mathbb{Z}/n\mathbb{Z}$ $\xrightarrow{2\pi i}$

$\mathbb{Z}/n\mathbb{Z}$ $\xrightarrow{\text{Addition}}$
 $\mathbb{Z}/n\mathbb{Z}$ $\xrightarrow{\text{Multiplikation}}$

Satz 5.8 Sei K ein Körper und $L = K(\omega)$ für ω eine primitive n -te Einheitswurzel. Dann ist $\text{Gal}(L/K)$ eine Untergruppe von $\mathbb{Z}/n\mathbb{Z}^*$ und insbesondere abgeschlossen. \rightsquigarrow da sind dann alle Unterguppen abgeschlossen!

Beweis: Sei $\sigma \in \text{Gal}(L/K)$. σ ist durch das Bild $\sigma(\omega)$ eindeutig bestimmt.

Es gilt: $\sigma(\omega) = \omega^i$ für ein i , welches modulo n eindeutig ist, dann σ muss ω auf eine ordene Wurzel von $x^n - 1$ abbilden. (L ist dieser Zerfallskörper)
Schreibe σ_i für dieses σ . Da σ ein Automorphismus ist, muss ω^i auch eine primitive n -te Einheitswurzel sein. Also $\text{ggT}(i, n) = 1$, d.h. $\sigma_i \in \text{Gal}(L/K)$

Ist ein "Gruppenendomorphismus".

Sei $\Psi: \text{Gal}(L/K) \rightarrow \mathbb{Z}/n\mathbb{Z}^*$. Ψ ist ein Homomorphismus.

$$\sigma_i \mapsto \overline{i}$$

$$\sigma_i \circ \sigma_j(\omega) = \sigma_i(\omega^j) = (\omega^j)^i = \omega^{ji} = \Psi(\sigma_i \circ \sigma_j) = \overline{j} \cdot \overline{i} = \overline{j \cdot i} = \Psi(\sigma_i) \circ \Psi(\sigma_j)$$

Eine n -te Einheitsgruppe

Übung 3.1

Ψ ist injektiv: $\Psi(\alpha) = \bar{1}$ bedeutet $\alpha(\omega) = \omega \Rightarrow \alpha = \text{id.}$ \square
 (also $\text{Ker } \Psi = \{\text{id}\}$)

Dene-Kunz: Beachte Unterschied zwischen der multiplikativen Gruppe der n -ten Einheitswurzeln und $\text{Gal}(L/K)$. Die eine ist zyklisch ($\cong \mathbb{Z}/n\mathbb{Z}$), die zweite nur abelsch ($\text{var var } \mathbb{Z}/n\mathbb{Z}^*$), z.B. $\mathbb{Z}/8\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, die "kleine Viergruppe".
 - Es gibt eine Art Verzerrung vor Satz 5.8. Der Satz von Kneser-Lieber sagt, dass jede endliche Gruppe mit abelscher Galoisgruppe in einer zyklischen Erweiterung L/K mit $\text{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}^*$ enthalten ist. (Beweis braucht mehr Technik.)

(Zeta)

Bsp: Sei p prim. Dann ist $\zeta_p = e^{\frac{2\pi i}{p}}$ eine primitive p -te Einheitswurzel über \mathbb{Q} .
 Das Minimalpolynom von ζ_p ist das p -te Kreisteilungspolynom $\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + 1$ mit $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = p-1$. Da alle weiteren Einheitswurzeln p -te Potenzen von ζ_p sind, ist $\mathbb{Q}(\zeta_p)$ der Zerfallskörper \rightarrow Galoiskörper. Also $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$.
 $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ ist eine Untergruppe des Ordnung $p-1$ in $\mathbb{Z}/p\mathbb{Z}^*$ weder aus Ordnung $p-1$ hat, d.h. $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}^*$, in diesem Fall also zyklisch.

Bem. $\mathbb{Z}/p\mathbb{Z}^*$ ist zyklisch, da es die multiplikative Gruppe eines endlichen Körpers ist. Es gilt sogar: sei K Körper. Jede endliche Untergruppe von K^* ist zyklisch.

Beweisidee: $G \subseteq K^*$ endliche Untergruppe mit $|G| = n$. Sei C eine zyklische zyklische Untergruppe von G mit Ordnung $d \mid n$ (Lagrange). Sei $x \in C$ ein Erzeuger von $C \Rightarrow x^d = 1$ gilt in G . Angenommen es gibt eine weitere Untergruppe ($\neq C$) von G mit Ordnung d . Dann gibt es mindestens $d+1$ Elemente von G , die $x^d = 1$ erfüllen. Dies ist unmöglich, da $x^d = 1$ in K höchstens d Wurzeln hat. G hat also für jeden Teiler der Gruppenordnung höchstens eine zyklische Untergruppe. Daraus folgt aber: G ist zyklisch nach Übungsbett 3.

Wir räumen uns den Auflösen durch Radikale $\sqrt[n]{\dots}$ und untersuchen jetzt $x^n - c$ für $c \in K$.

1. inj. Homomorphismus!

Satz 5.9 Angenommen, ein Körper K enthält alle n -ten Einheitswurzeln. Sei $f = x^n - c \in K[x]$ und L der Zerfallskörper von f . Dann existiert eine Injektion $\text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$. Diese ist surjektiv genau dann, wenn f irreduzibel ist.

Beweis: Sei $\omega \in L$ eine primitive n -te Einheitswurzel und α eine Wurzel von f .
 Dann gilt $\alpha^n = c$ und $\{\alpha, \alpha\omega, \alpha\omega^2, \dots, \alpha\omega^{n-1}\}$ ist die Menge der Wurzeln von f .
 Jedes $\sigma \in \text{Gal}(L/K)$ ist bestimmt durch die Exponenten i in $\sigma(\alpha) = \alpha\omega^i$.
 Setze: $\Psi: \text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$. Sei $\sigma \in \text{Gal}(L/K)$.
 $\sigma \mapsto i$

$$\Psi(\sigma)(\alpha) = \Psi(\sigma(\alpha)) = \Psi(\alpha\omega^i) = \alpha\omega^i \cdot \omega^i = \alpha\omega^{2i} \Rightarrow \Psi(\sigma \circ \sigma) = \bar{i} + \bar{i} = \bar{i} = \Psi(\sigma)\Psi(\sigma).$$

\bar{i} läuft w in K fix
und $\Psi(\sigma) < \omega^n$

$\Rightarrow \Psi$ ist ein Homomorphismus

$\Rightarrow \Psi$ ist injektiv nach Übung 3.1.

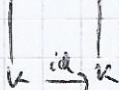
Ψ ist surjektiv genau dann, wenn $\text{Gal}(L/K)$ transitiv auf der Menge der Wurzeln ist, d.h. für je zwei Wurzeln λ, μ existiert ein $\sigma \in \text{Gal}(L/K)$ s.d. $\sigma(\lambda) = \mu$.

Wir zeigen, dass ist der Fall genau dann, wenn f irreduzibel ist.

Ang., f ist irreduzibel und λ, μ 2 Wurzeln von f , dann erweitern wir mit (Satz 2.9) die Identität auf K (s. links). Dann ist $K(\lambda) = K(\mu) = L$, also $\sigma \in \text{Gal}(L/K)$ mit $\sigma(\lambda) = \mu \Rightarrow \text{Gal}(L/K)$ transitiv.

Angenommen $\text{Gal}(L/K)$ nicht transitiv und $f \neq g \cdot h$, bei λ eine Wurzel von g
 $\Rightarrow \lambda$ keine Wurzel von h , da $\text{ggT}(g, h) = 1$. mit $\text{ggT}(g, h) = 1$. (dies geht)

• die Wurzeln sind
als Wurzeln mit
unterschiedl.
 $\hookrightarrow K(\lambda) \cong K(\mu)$



Sei $\alpha \in \text{Gal}(L/K)$ mit $\alpha(1) \neq 1$ Wurzel von h . Dies ist ein Widerspruch, da α die Wurzeln von g und h jeweils intern permuteert. \square

Korollar S.10 Sei p prim, K ein Körper, der eine primitive p -te Einheitswurzel enthält, L der Zerfälligkeitkörper von $f = x^p - c \in K[x]$, dann zerfällt f schon über K ($\text{Gal}(L/K) = \{\text{id}\}$) oder $\text{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis. $\mathbb{Z}/p\mathbb{Z}$ hat nur die triviale und $\mathbb{Z}/p\mathbb{Z}$ als Untergruppen. \square

Bem. Die Annahme über die p -ten Einheitswurzeln in K ist nicht nötig; aber dann muss man was beweisen.

Beobachtungen: - Zwischenkörper in einer Galoiserweiterung haben mit Quotienten und Unterguppen zu tun (Satz 5.5 + Bsp. $x^3 - 2$).

- Bei Adjunktion von Einheitswurzeln und anderen n -ten Wurzeln treten abelsche Galoigruppen auf.

Dies führt auf die Definition: Eine Gruppe G ist auflösbar, wenn eine Kette von Normalteilen $\{\text{id}\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq G$ existiert, so dass H_i/H_{i-1} abelsch ist.

Algebra II

16.05.2019

6 AUFLÖSABRE GRUPPEN

Viele El., um nicht abdrucken
/ sie Gruppen zu verteilen

diese Kette
 $H_0 \trianglelefteq G$ gibt es
immer obw.
 $G/H_0 = G$ null
muss nicht abelsch!

Def. 6.1 Sei G eine endliche Gruppe. G heißt auflösbar, falls eine Kette von Normalteilen $\{\text{id}\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = G$ existiert, so dass H_i/H_{i-1} abelsch ist für alle $i = 1, \dots, n$.

Bsp.: - G abelsch mit $\{\text{id}\} \trianglelefteq G$

- D_{2n} Niederguppe = Symmetriegruppe des regulären n -Ecks.
Die Kette $\{\text{id}\} \trianglelefteq \{\text{Rotationen}\} \trianglelefteq G \rightarrow G/\{\text{Rotationen}\} \cong \mathbb{Z}_{2n}$ abelsch.
da Rotationen zyklisch. ($\{\text{Rotationen}\} / \{\text{id}\}$ zyklisch)

Nicht-Beispiele: - Eine Gruppe G ist einfach, falls $\{\text{id}\}$ und G ihre einzigen Normalteile sind. Falls G nicht bereits abelsch (also G zyklische Gruppe von Primzahlordnung) ist es sicher nicht auflösbar ("Antithese" zu auflösbar).

Man kann systematisch testen, ob ein G auflösbar ist. Dafür benötigen wir Kommutatoren.

Def. 6.2 Sei G eine Gruppe und $x, y \in G$. Der Kommutator von x und y ist insb. $xyx^{-1}y^{-1} \in G$, und nicht als $[x, y]$. Die Kommutatoruntergruppe von G ist $G' = \langle [x, y] \mid x, y \in G \rangle$ die von allen Kommutatoren erzeugte Untergruppe. Wir schreiben ad hoc G' für die Kommutatoruntergruppe von G .

Lemma 6.3 $G' \trianglelefteq G$.

Bew. Sei $c \in G'$ ein Kommutator, $g \in G$,
 $gcg^{-1}c^{-1}$ ist Kommutator; $c^{-1} \in G' \Rightarrow geg^{-1} \in G'$.
 $\Rightarrow G'$ normal in G , da die Kommutatoren G' erzeugen. \square

$$gcg^{-1}c^{-1} \in G' \xrightarrow{c \in G'} geg^{-1} \in G'$$

$$H \trianglelefteq G \Leftrightarrow ghg^{-1} \in H \forall g \in G$$

aber: wenn man Elemente von H kennt,
reicht es das für die zu zeigen,
denn dann kann ghg^{-1} entdeckt.
 $h = h_1 h_2$
 $\Rightarrow gh_1 h_2 g^{-1} = gh_1 g^{-1} gh_2 g^{-1}$

Lemma 6.4 Sei H ein Normalteiler in G . Dann ist G/H abelsch gdw. G' in H enthalten ist, $G' \subseteq H$.

Bew. Falls G/H abelsch ist, so gilt für $x, y \in G$: $xyH = yxH$

$$\begin{aligned} \text{Falls } G' \subseteq H, \text{ f\"agt nach (dritten)} \\ \text{Isomorphismus: } G/H \cong G/G'/H/G', \end{aligned}$$

und das G/G' bereits abelsch ist, ist auch G/H abelsch. \square

Verein: $G' \trianglelefteq G$ ist ein Normalteiler mit abelschen Quotienten. Nutze dies, um die Kette in einer Auflösung iterativ zu konstruieren.

Def. 6.5 Die n -te Kommutatorgruppe einer Gruppe ist $G^{(n)} := G^{(n-1)'} \cap G^{(0)} = G$.

Satz 6.6 G ist auflösbar genau dann, wenn $G^{(n)} = \{\text{id}\}$ für ein n .

Bew. Ang., G ist auflösbar und $G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_n = \{\text{id}\}$ eine Auflösung, d.h. H_i/H_{i+1} abelsch. Wir zeigen per Induktion nach i , dass $G^{(i)} \subseteq H_i$. Dann folgt $G^{(n)} = \{\text{id}\}$.

Für $i=0$ gilt $G^{(0)} = H_0 = G$.

Angenommen $G^{(i)} \subseteq H_i$. Dann ist $G^{(i+1)} = G^{(i)'} \subseteq H_i'$. Da H_i/H_{i+1} abelsch ist, gilt Lemma 6.4, dass $H_i' \subseteq H_{i+1}$ und damit auch $G^{(i+1)} \subseteq H_{i+1}$.

Falls $G^{(n)} = \{\text{id}\}$, so ist $G = G^{(0)} \triangleright G^{(1)} \triangleright \dots \triangleright G^{(n)} = \{\text{id}\}$ eine Auflösung von G . \square

Satz 6.7 Wenn G auflösbar ist, dann sind es auch alle Untergruppen und Quotienten von G .

Bew. Sei $H \subseteq G$ eine Untergruppe. Dann gilt: $H' \subseteq G' \subseteq \dots \subseteq H^{(n)} \subseteq G^{(n)}$. Falls

$G^{(n)} = \{\text{id}\}$ für ein n , gilt auch $H^{(n)} = \{\text{id}\}$ für dieses n . Also ist H auflösbar.

Angenommen $\varphi: G \rightarrow K$ ist surjektiv, d.h. K ist ein Quotient von G ($G/\ker \varphi \cong \text{im } \varphi = K$).

Bew.: $\varphi(G') = K'$ (also: φ ist surjektiv in K'). (Beweis)

Sei dazu $uv^{-1}v^{-1}$ ein Kommutator in K . Seien $x, y \in G$ mit $\varphi(x) = u, \varphi(y) = v$.

Dann ist $\varphi(xyx^{-1}y^{-1}) = uvu^{-1}v^{-1}$, also ist jeder Kommutator in K (also erzeugt K'). Bild eines Kommutators in G .

Induktiv: $\varphi(G^{(n)}) = K^{(n)}$. Falls $G^{(n)} = \{\text{id}\}$, folgt $K^{(n)} = \{\text{id}\}$, also K auflösbar. \square

Aufgabe I

Wir best\"igen jetzt den Korrespondenzsatz: G Gruppe, $K \trianglelefteq G$. $G^* = G/K$, $S^* \subseteq G^*$

1) Es existiert genau ein S mit $K \subseteq S \subseteq G$ s.d. $S/K = S^*$.

2) S^* normal $\Rightarrow S$ normal

3) $[G^*: S^*] = [G: S]$

4) $T^* \trianglelefteq S^* \Rightarrow T \trianglelefteq S$; $S^*/T^* \cong S/T$.

\hookrightarrow Untergruppe im Quotienten

Satz 6.8 Sei G eine Gruppe und $H \trianglelefteq G$ Normalteiler. Falls G/H und H auflösbar sind, so ist auch G auflösbar.

Beweis: Sei $G/H = G^* = G_0^* \triangleright G_1^* \triangleright \dots \triangleright G_n^* = \{\text{id}\}$ eine Auflösung von G/H .

Nach dem Korrespondenzsatz gibt es eine Kette von Normalteichern in G :

$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = H$ mit $G_i/G_{i+1} \cong G_i^*/G_{i+1}^*$ abelsch.

Da H auflösbar ist existieren Normalteiler $H = H_0 \triangleright H_1 \triangleright \dots \triangleright H_n = \{\text{id}\}$ mit H_i/H_{i+1} abelsch. Zusammensetzen der beiden Ketten ergibt eine Auflösung von G . \square

Für die Auflösbarkeit von Gleichungen müssen wir die Auflösbarkeit von S_n untersuchen.

Fakten: - Jede endliche Gruppe ist Untergruppe einer S_n (Satz von Cayley).

- In jeder S_n hat man den Normalteiler $A_n = \{\text{gerade Permutationen}\}$

$\Rightarrow \text{Ker}(\text{sgn}: S_n \rightarrow \{\pm 1\}, \cdot)$.

- Jede Untergruppe vom L-dex 2 ist ein Normalteiler. Anzahl Transpositionen

- Die A_n wird von 3-Zyklen erzeugt (die kleinsten freien Permutationen).

Beweis: Sei $\alpha \in A_n$. Dann ist $\alpha = \gamma_1 \dots \gamma_m$ mit m gerade und $\gamma_1 \dots \gamma_m$ Transpositionen.

- Betrachte $T_i T_{i+1}$ für $i=1, 2, \dots$. Falls T_i nicht das Inlet, etwa $T_i = (a\ b)$, $T_{i+1} = (a\ c) : (ab)(ac) = (a\ c\ b)$. Falls T_i, T_{i+1} das Inlet, nenne $(ab)(cd)$, $= (ab)(bc)(bc)(cd) = (b\ c\ b)(bac) \Rightarrow$ jede Permutation ist Produkt von 3-Zykeln. \square
- $S_n' = A_n$: Grund: S_n/A_n abelsch $\Rightarrow S_n' \subseteq A_n$ (Lemma 6.4).
Z.z. $A_n \subseteq S_n'$. Wir zeigen, dass jeder 3-Zykel (Träger von A_n) ein Kommutator ist.
Sei $\alpha = (i\ j\ k)$. Dann gilt $\alpha^2 = (i\ k\ i) = (i\ j)(i\ k)$. Damit auch $\alpha^4 = \alpha = (i\ j)(i\ k)(i\ j)(i\ k)$ ein Kommutator. $\Rightarrow A_n = S_n'$.
- $A_n \subseteq S_n$ ist die einzige Untergruppe vom Index 2. Sei $H \subseteq S_n$ mit $[S_n : H] = 2$.
 $\Rightarrow H \subseteq S_n$ Normalteiler. Da S_n/H abelsch (\mathbb{Z}_2) $\Rightarrow A_n = S_n' \subseteq H$. Aber $|A_n| = \frac{|S_n|}{2}$, also $|A_n| = |H| \Rightarrow A_n = H$. \square

- Konjugation in S_n' : $\gamma = (i_1\ i_2 \dots i_k)$ ein k -Zykel in S_n' . Sei $\alpha \in S_n'$ beliebig.
Es gilt: $\alpha \gamma \alpha^{-1} = (\underset{\alpha \text{ als Funktion}}{\alpha(i_1)} \dots \alpha(i_k))$. Insb. ist $\alpha \gamma \alpha^{-1}$ wieder ein k -Zykel.
Beweis: Falls $j = \alpha(i_l)$ für ein l , so gilt: $\alpha \gamma \alpha^{-1}(j) = \alpha(i_{l+1})$ ($l+1$ ist nach γ zu rechnen)
Falls $j \neq \alpha(i_l)$ für alle $l=1, \dots, k$:
 $\gamma \alpha^{-1}(j) = \alpha^{-1}(j) \Rightarrow \alpha \gamma \alpha^{-1}(j) = \alpha^{-1}(\alpha(j)) = j \quad \square$
Man sieht: Je zwei k -Zykeln sind konjugiert zueinander:
 $\gamma = (i_1 \dots i_k), \gamma' = (i'_1 \dots i'_k)$. Dann ergibt sich für jedes $\alpha \in S_n'$ mit
 $\alpha(i_l) = i'_l : \alpha \gamma \alpha^{-1} = \gamma'$.
- S_5 hat 20 3-Zykeln und diese sind auch in A_5 je paarweise zueinander konjugiert.
Beweis: Es gilt offensichtlich $10 = \binom{5}{3}$ 3-Zykeln in S_5 . Seien $\gamma, \gamma', \gamma''$ 3-Zykeln in S_5 . W.z.b. $\exists \alpha \in A_5$ mit $\gamma \alpha \alpha^{-1} = \gamma'$ (es findet α).
Erstmal $\alpha = (1\ 2\ 3)$. Sei $C_{S_5}(\alpha) = \{\alpha \in S_5 : \alpha \alpha^{-1} = \alpha\}$
"Stabilisator der Konjugaten" $= \{\alpha \in S_5 : \alpha \alpha^{-1} = \alpha\}$
Dann gilt: $[S_5 : C_S(\alpha)] = 20$, da alle 3-Zykeln in S_5 konjugiert sind.
(Orbit-Stabilisator-Lemma) $|O(\gamma)| = [G : G_x] = |G| / |G_x|$, wobei G auf x wirkt mit $O(x)$ Orbitsgröße, $G_x \subseteq G$ Stabilisator von x)
 $\rightarrow C_S(\alpha) = 6$. Hier sind 6 Elemente in $C_S(\alpha)$.
 $\underbrace{\{1, \alpha, \alpha^2, (4\ 5), \alpha(4\ 5), \alpha^2(4\ 5)\}}$. Davor sind $1, \alpha, \alpha^2 \in A_5$.
gerade ungerade
Damit ist $C_A(\alpha) := \{\alpha \in A_5 \mid \alpha \alpha^{-1} = \alpha\}$ von der Ordnung 3. Nach Orbit-Stabilisator-Lemma: $[A_5 : C_A(\alpha)] = |A_5| / |C_A(\alpha)| = 60 / 3 = 20$. Also werden alle 3-Zykeln durch Konjugation von $\alpha = (1\ 2\ 3)$ mit jedem $\alpha \in A_5$ erreicht.

Satz 6.9 Die Gruppe A_5 ist einfach, d.h. $\{id\}$ und A_5 sind die einzigen Normalteiler.

- Beweis: Sei $\{id\} \neq H \subseteq A_5$ ein Normalteiler, und $id \neq \alpha \in H$. In A_5 gibt es nur 3 mögliche Zyklendekompositionen: 3-Zykel, Produkt von 2 Transpositionen, 5-Zykel.
-Falls α ein 3-Zykel ist, folgt da H Normalteiler, $\alpha \alpha^{-1} \in H$ also $\alpha \in A_5$.
Damit sind alle 3-Zykeln (= Einzige von A_5) in $H \Rightarrow A_5 \subseteq H \Rightarrow A_5 = H$.
-Falls $\alpha = (1\ 2\ 3\ 4) = (1\ 2)(3\ 4)$. Sei $\tau = (1\ 2)(3\ 5)$. Damit gilt:
 $\tau \alpha \tau^{-1} = (\tau(1) \tau(2))(\tau(3) \tau(4))$ hier braucht man die 5, obwohl $\alpha \in A_5$
 $= (1\ 2)(4\ 5) \in H$

$$H \ni \tau \alpha \tau^{-1} \alpha^{-1} = (3\ 5\ 4). \text{ Also enthält } H \text{ ein } 3\text{-Zykel } \Rightarrow H = A_5 \text{ wie oben.}$$

- Bei aufmerksamer Betrachtung ist dies der allgemeine Fall von Produkten von 2 Transpositionen.
- Ist $\alpha = (1\ 2\ 3\ 4\ 5)$, sei $\tau = (1\ 3\ 2)$. $\tau \alpha \tau^{-1} = (3\ 1, 2\ 4\ 5)$ - konjugiert in S_5 oder
 $\tau \alpha \tau^{-1} \alpha^{-1} = (1\ 3\ 4)$. Also folgt wie oben $H = A_5$, o.B.d.A. $\Rightarrow A_5$ ist einfach. \square

die Beschränkung der Menge
der Möglichkeiten
des allgemeinen Fälls

Satz 6.10 S_n ist auflösbar, wenn $n \leq 4$ und nicht auflösbar, wenn $n \geq 5$ ist.

Bew. Falls $n \leq 4$, so hat S_n eine Untergruppe, die isomorphe zu S_3 ist.

Da jede Untergruppe einer auflösbarer Gruppe auflösbar ist genügt es, S_4 und S_5 zu betrachten.
S₄ zu betrachten: redundant (Beweis ist V) Normal und abelsch (da Index 2) Normal und abelsch (da Index 2)

Eine Auflösung von S_4 ist: $\{id\} \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$, wobei $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mit $V = \{id, (12)(34), (14)(23), (13)(24)\}$

ad (2): $|A_4| = 12$, Koyngesetz erhält die Zyklenstruktur, Winkelt alle Produkte von Transpositionen $\Rightarrow V \trianglelefteq S_4$ und $V \trianglelefteq A_4$. A_4/V hat Ordnung $12/4 = 3$ $\Rightarrow A_4/V \cong \mathbb{Z}_3$ und A_4/V zyklich.

Falls S_5 auflösbar, so ist A_5 als Untergruppe auflösbar; aber A_5 ist einfach und nicht selbst abelsch, also ist A_5 nicht auflösbar. \square

7. Auflösbare Gleichungen

Def. 7.1 Eine Erweiterung L/K heißt rein vom Typ m, falls $L = K(\alpha)$ für ein $\alpha \in L$ mit $\alpha^m \in K$. Ein Turm $K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_t$ heißt auflösbar, falls jede Erweiterung $L_i/L_{i-1}, i=1 \dots t$ rein ist. In diesem Fall heißt auch L_t/K auflösbar. Ein $f \in K[x]$ heißt durch Radikale auflösbar, falls eine auflösbare Erweiterung L/K existiert, die einen Zerfällungskörper von f enthält.

"wir haben jetzt ausreichende Praktiziertheit"

Bsp.: $f = x^2 + bx + c \in \mathbb{C}[x]$. Sei $K = \mathbb{Q}(b, c)$ und $L = K(\sqrt{b^2 - 4c})$.

Dann ist L/K rein vom Typ 2 und L der Zerfällungskörper von f . (Abhängig von b und c) (aber alle die gleiche Galoisgruppe!)

Bsp.: $f = x^3 + qx + r \in \mathbb{C}[x]$ und $K = \mathbb{Q}(q, r)$. Sei $L = K(\sqrt[3]{\frac{q^2}{2} + \frac{4r^3}{27}})$ rein vom Typ 2) und $L_2 = L_1(y)$ mit $y^3 = \frac{1}{2}(-r + \sqrt[3]{\frac{q^2}{2} + \frac{4r^3}{27}})$ (rein vom Typ 3 über L_1). Die Wurzeln von f sind $x_1 = y + z$, $x_2 = w_1y + w_2z$, $x_3 = w_2y + w_1z$, wobei $z = \frac{-q}{3y} \in L_2$ und $w = e^{\frac{2\pi i}{3}}$. Sei $L_3 = L_2(w)$ rein vom Typ 3 (das ist null der Galoisgrad!).

Der Zerfällungskörper von f ist sicher in L_3 enthalten, also ist f auflösbar.

Achtung: Es ist möglich und nötig, dass die "Turmspitze" L größer als der Zerfällungskörper ist. Zum Beispiel könnte ein f wie in Beispiel 2 3 reelle Wurzeln haben.

Dann ist der Zerfällungskörper in \mathbb{R} enthalten \rightarrow Konkrete Auflösungen hängen von Koeffizienten ab.

Lemma 7.2 Sei K ein Körper der Charakteristik 0 und $f \in K[x]$ durch Radikale auflösbar. Sei L der Zerfällungskörper von f .

- 1) Es existiert ein auflösbarer Turm $K = R_0 \subseteq R_1 \subseteq \dots \subseteq R_t$ so dass $L \subseteq R_t$ und R_t ist Zerfällungskörper eines $g \in K[x]$ (also R_t/K eine Galoiserweiterung), und L_i/R_{i-1} ist rein vom Primzahltyp p_i .
- 2) Falls K alle p_i -ten Einheitswurzeln für alle $i=1, \dots, t$ enthält, so ist L/K auflösbar.

Lemma 7.2 K Körper, $\text{char}(K)=0$; $f \in K[x]$ auflösbar; L Zerfallskörper von f über K .

- 1) Existiert Auflösung $K = R_0 \subset R_1 \subset \dots \subset R_\ell$ mit $L \subseteq R_\ell \subseteq R$ und Zerfallskörper (via aus dem Polynom) von R_i/R_{i-1} von Primzahltyp ($\Leftrightarrow R_i \cong R_{i-1}(\alpha)$, mit $\alpha \in R_{i-1}$ für ein p_i prim, d.h. in α lösen nur $x^p = c$)
- 2) Falls R alle p_i -ten Einheitswurzeln enthält, so ist $\text{Gal}(L/K)$ auflösbar.

Beweis: 1) f auflösbar \Rightarrow Es existiert eine Auflösung $K = R_0 \subset R_1 \subset \dots \subset R_\ell$ mit $L \subseteq R_\ell$. Galoisgruppe $\text{Gal}(L/K)$ permutiert über R_i ($i=1, \dots, \ell$). Da R_ℓ über K endlich ist, existieren $\alpha_1, \dots, \alpha_n \in R_\ell$ mit $K(\alpha_1, \dots, \alpha_n) = R_\ell$. Sei R'_ℓ der Zerfallskörper des Galoisspalts der Minimalpolynome der α_i . σ_i kompositum mit transp.
Die σ_i permutieren die Wurzeln des Minimalpolynome der α_i transitiv. $R'_\ell = R_{\ell-1}(\sqrt[n]{c})$

Jedes $\sigma_i(R_\ell)$ ist auflösbar ($\sigma_i(R_\ell)$ ist auflösbar über $\sigma_i(R_{\ell-1})$, da:

Falls $(x^{n_i} - c_i)$ gleich verhält wie von $R_{\ell-1}$ zu R_ℓ zu können, dann $x^{n_i} - \sigma_i(c_i) \Rightarrow \sigma_i(R_{\ell-1})$ für $\sigma_i(R_{\ell-1})$ zu $\sigma_i(R_\ell)$. Man kann zeigen, dass Vierpotenz von über K auflösbar
Körper ist auflösbar. \Rightarrow Auflösung von f erledigt ℓ -fach in einem Zerfallskörper.

Potenzialtypen erreicht man durch Verfeinerung des Auflösung. Falls L/K eine Erweiterung ist und $\alpha \in L$ mit $\alpha^m \in K$ und $m = p \cdot n$ mit p prim, dann ist $K \subseteq K(\alpha^m) \subseteq L$ ein Zwischenkörper und $K \subseteq K(\alpha^m)$ ist rein von Typ p . Also gilt 1).

ad 2): Sei $K = R_0 \subset R_1 \subset \dots \subset R_\ell$ eine Auflösung wie in 1). Sei $G_i = \text{Gal}(R_i/R_{i-1})$. Nach Annahme enthält K und damit auch jedes R_i alle p_i -ten Einheitswurzeln.

Also ist jedes R_i ein Zerfallskörper über R_{i-1} . Also gilt Satz 5.5 über Erweiterungen von Zerfallskörpern ausreichend: $\text{Gal}(L/F)/\text{Gal}(L/K) \cong \text{Gal}(K/F)$
Wir erhalten eine Kette von Normalteilen

$\text{Gal}(R_\ell/K) = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_\ell = \{\text{id}\}$. Die Gradienten sind

$$G_i/G_{i+1} = \text{Gal}(R_i/R_{i+1}) \cong \text{Gal}(R_{i+1}/R_i). \quad \text{Nach Satz 5.9 sind die}$$

Quotienten Untergruppen von $\text{Gal}(R_i/R_{i+1})$, also zyklisch, also abelsch. $\Rightarrow \text{Gal}(R_\ell/K)$ ist auflösbare Gruppe.

Satz 5.5 für $K \subseteq L \subseteq R_\ell$ gibt, dass $\text{Gal}(L/K)$ als Quotient einer auflösaren Gruppe auch auflösbar ist. \square

Sylow-Satz

Man kann mit Gruppentheorie die Annahme "K enthält alle p_i -ten Einheitswurzeln" loswerden.

Nach einem Satz von Gauss sind Einheitswurzeln nichts durch Radikale ausdrückbar.

Satz 7.3 (Abel-Ruffini) Das Polynom $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist nicht durch Radikale auflösbar.

Beweis: f ist irreduzibel nach Eisenstein. Sei L/\mathbb{Q} der Zerfallskörper und $G = \text{Gal}(L/\mathbb{Q})$. Sei $\alpha \in L$ eine Wurzel von f . Dann ist $(\mathbb{Q}(\alpha):\mathbb{Q}) = 5$. Nach dem Satz von Cauchy gibt es in G ein Element der Ordnung 5, also einen 5-Zykel.

$$f'(x) = 5x^4 - 4.$$

Da $f(-\sqrt[4]{4}) > 0$ und $f(\sqrt[4]{4}) < 0$, hat f nach Zwischenwert-Theorem 3 reelle Nullstellen.

\Rightarrow Die Komplexe-Konjugationen eingeschränkt auf L verteilen die 2 komplexe konjugierten Nullstellen α und $\bar{\alpha}$ und ist damit eine Transposition in G .

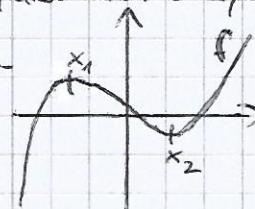
Beh: Falls $H = \langle \alpha, \tau \rangle \leq S_5$ mit α ein 5-Zykel und τ Transposition, so gilt $H = S_5$.

ObdA sei $\alpha = (1 2 3 4 5)$ und $\tau = (a b)$ mit $a < b$. Es gilt: $\alpha^b \cdot \tau \cdot \alpha^{-b} = b$.

α^{b-a} ist auch ein 5-Zykel: $\alpha^{b-a} = (a b \dots)$. Nochmal neu nummerieren gibt

$$\alpha^{b-a} = (1 2 3 4 5), \tau = (1 2). \quad \text{Dann gilt } \alpha^{k(b-a)} \tau \alpha^{-k(b-a)} = (k+1 \ k+2)$$

für alle k (Vorabin b gleich nach S_5).



z-2
z-1
z
z+1
z+2
z+3
z+4
z+5
z+6
z+7
z+8
z+9
z+10
z+11
z+12
z+13
z+14
z+15
z+16
z+17
z+18
z+19
z+20
z+21
z+22
z+23
z+24
z+25
z+26
z+27
z+28
z+29
z+30
z+31
z+32
z+33
z+34
z+35
z+36
z+37
z+38
z+39
z+40
z+41
z+42
z+43
z+44
z+45
z+46
z+47
z+48
z+49
z+50
z+51
z+52
z+53
z+54
z+55
z+56
z+57
z+58
z+59
z+60
z+61
z+62
z+63
z+64
z+65
z+66
z+67
z+68
z+69
z+70
z+71
z+72
z+73
z+74
z+75
z+76
z+77
z+78
z+79
z+80
z+81
z+82
z+83
z+84
z+85
z+86
z+87
z+88
z+89
z+90
z+91
z+92
z+93
z+94
z+95
z+96
z+97
z+98
z+99
z+100
z+101
z+102
z+103
z+104
z+105
z+106
z+107
z+108
z+109
z+110
z+111
z+112
z+113
z+114
z+115
z+116
z+117
z+118
z+119
z+120
z+121
z+122
z+123
z+124
z+125
z+126
z+127
z+128
z+129
z+130
z+131
z+132
z+133
z+134
z+135
z+136
z+137
z+138
z+139
z+140
z+141
z+142
z+143
z+144
z+145
z+146
z+147
z+148
z+149
z+150
z+151
z+152
z+153
z+154
z+155
z+156
z+157
z+158
z+159
z+160
z+161
z+162
z+163
z+164
z+165
z+166
z+167
z+168
z+169
z+170
z+171
z+172
z+173
z+174
z+175
z+176
z+177
z+178
z+179
z+180
z+181
z+182
z+183
z+184
z+185
z+186
z+187
z+188
z+189
z+190
z+191
z+192
z+193
z+194
z+195
z+196
z+197
z+198
z+199
z+200
z+201
z+202
z+203
z+204
z+205
z+206
z+207
z+208
z+209
z+210
z+211
z+212
z+213
z+214
z+215
z+216
z+217
z+218
z+219
z+220
z+221
z+222
z+223
z+224
z+225
z+226
z+227
z+228
z+229
z+230
z+231
z+232
z+233
z+234
z+235
z+236
z+237
z+238
z+239
z+240
z+241
z+242
z+243
z+244
z+245
z+246
z+247
z+248
z+249
z+250
z+251
z+252
z+253
z+254
z+255
z+256
z+257
z+258
z+259
z+260
z+261
z+262
z+263
z+264
z+265
z+266
z+267
z+268
z+269
z+270
z+271
z+272
z+273
z+274
z+275
z+276
z+277
z+278
z+279
z+280
z+281
z+282
z+283
z+284
z+285
z+286
z+287
z+288
z+289
z+290
z+291
z+292
z+293
z+294
z+295
z+296
z+297
z+298
z+299
z+300
z+310
z+320
z+330
z+340
z+350
z+360
z+370
z+380
z+390
z+400
z+410
z+420
z+430
z+440
z+450
z+460
z+470
z+480
z+490
z+500
z+510
z+520
z+530
z+540
z+550
z+560
z+570
z+580
z+590
z+600
z+610
z+620
z+630
z+640
z+650
z+660
z+670
z+680
z+690
z+700
z+710
z+720
z+730
z+740
z+750
z+760
z+770
z+780
z+790
z+800
z+810
z+820
z+830
z+840
z+850
z+860
z+870
z+880
z+890
z+900
z+910
z+920
z+930
z+940
z+950
z+960
z+970
z+980
z+990
z+1000
z+1010
z+1020
z+1030
z+1040
z+1050
z+1060
z+1070
z+1080
z+1090
z+1100
z+1110
z+1120
z+1130
z+1140
z+1150
z+1160
z+1170
z+1180
z+1190
z+1200
z+1210
z+1220
z+1230
z+1240
z+1250
z+1260
z+1270
z+1280
z+1290
z+1300
z+1310
z+1320
z+1330
z+1340
z+1350
z+1360
z+1370
z+1380
z+1390
z+1400
z+1410
z+1420
z+1430
z+1440
z+1450
z+1460
z+1470
z+1480
z+1490
z+1500
z+1510
z+1520
z+1530
z+1540
z+1550
z+1560
z+1570
z+1580
z+1590
z+1600
z+1610
z+1620
z+1630
z+1640
z+1650
z+1660
z+1670
z+1680
z+1690
z+1700
z+1710
z+1720
z+1730
z+1740
z+1750
z+1760
z+1770
z+1780
z+1790
z+1800
z+1810
z+1820
z+1830
z+1840
z+1850
z+1860
z+1870
z+1880
z+1890
z+1900
z+1910
z+1920
z+1930
z+1940
z+1950
z+1960
z+1970
z+1980
z+1990
z+2000
z+2010
z+2020
z+2030
z+2040
z+2050
z+2060
z+2070
z+2080
z+2090
z+2100
z+2110
z+2120
z+2130
z+2140
z+2150
z+2160
z+2170
z+2180
z+2190
z+2200
z+2210
z+2220
z+2230
z+2240
z+2250
z+2260
z+2270
z+2280
z+2290
z+2300
z+2310
z+2320
z+2330
z+2340
z+2350
z+2360
z+2370
z+2380
z+2390
z+2400
z+2410
z+2420
z+2430
z+2440
z+2450
z+2460
z+2470
z+2480
z+2490
z+2500
z+2510
z+2520
z+2530
z+2540
z+2550
z+2560
z+2570
z+2580
z+2590
z+2600
z+2610
z+2620
z+2630
z+2640
z+2650
z+2660
z+2670
z+2680
z+2690
z+2700
z+2710
z+2720
z+2730
z+2740
z+2750
z+2760
z+2770
z+2780
z+2790
z+2800
z+2810
z+2820
z+2830
z+2840
z+2850
z+2860
z+2870
z+2880
z+2890
z+2900
z+2910
z+2920
z+2930
z+2940
z+2950
z+2960
z+2970
z+2980
z+2990
z+3000
z+3100
z+3200
z+3300
z+3400
z+3500
z+3600
z+3700
z+3800
z+3900
z+4000
z+4100
z+4200
z+4300
z+4400
z+4500
z+4600
z+4700
z+4800
z+4900
z+5000
z+5100
z+5200
z+5300
z+5400
z+5500
z+5600
z+5700
z+5800
z+5900
z+6000
z+6100
z+6200
z+6300
z+6400
z+6500
z+6600
z+6700
z+6800
z+6900
z+7000
z+7100
z+7200
z+7300
z+7400
z+7500
z+7600
z+7700
z+7800
z+7900
z+8000
z+8100
z+8200
z+8300
z+8400
z+8500
z+8600
z+8700
z+8800
z+8900
z+9000
z+9100
z+9200
z+9300
z+9400
z+9500
z+9600
z+9700
z+9800
z+9900
z+10000
z+10100
z+10200
z+10300
z+10400
z+10500
z+10600
z+10700
z+10800
z+10900
z+11000
z+11100
z+11200
z+11300
z+11400
z+11500
z+11600
z+11700
z+11800
z+11900
z+12000
z+12100
z+12200
z+12300
z+12400
z+12500
z+12600
z+12700
z+12800
z+12900
z+13000
z+13100
z+13200
z+13300
z+13400
z+13500
z+13600
z+13700
z+13800
z+13900
z+14000
z+14100
z+14200
z+14300
z+14400
z+14500
z+14600
z+14700
z+14800
z+14900
z+15000
z+15100
z+15200
z+15300
z+15400
z+15500
z+15600
z+15700
z+15800
z+15900
z+16000
z+16100
z+16200
z+16300
z+16400
z+16500
z+16600
z+16700
z+16800
z+16900
z+17000
z+17100
z+17200
z+17300
z+17400
z+17500
z+17600
z+17700
z+17800
z+17900
z+18000
z+18100
z+18200
z+18300
z+18400
z+18500
z+18600
z+18700
z+18800
z+18900
z+19000
z+19100
z+19200
z+19300
z+19400
z+19500
z+19600
z+19700
z+19800
z+19900
z+20000
z+20100
z+20200
z+20300
z+20400
z+20500
z+20600
z+20700
z+20800
z+20900
z+21000
z+21100
z+21200
z+21300
z+21400
z+21500
z+21600
z+21700
z+21800
z+21900
z+22000
z+22100
z+22200
z+22300
z+22400
z+22500
z+22600
z+22700
z+22800
z+22900
z+23000
z+23100
z+23200
z+23300
z+23400
z+23500
z+23600
z+23700
z+23800
z+23900
z+24000
z+24100
z+24200
z+24300
z+24400
z+24500
z+24600
z+24700
z+24800
z+24900
z+25000
z+25100
z+25200
z+25300
z+25400
z+25500
z+25600
z+25700
z+25800
z+25900
z+26000
z+26100
z+26200
z+26300
z+26400
z+26500
z+26600
z+26700
z+26800
z+26900
z+27000
z+27100
z+27200
z+27300
z+27400
z+27500
z+27600
z+27700
z+27800
z+27900
z+28000
z+28100
z+28200
z+28300
z+28400
z+28500
z+28600
z+28700
z+28800
z+28900
z+29000
z+29100
z+29200
z+29300
z+29400
z+29500
z+29600
z+29700
z+29800
z+29900
z+30000
z+31000
z+32000
z+33000
z+34000
z+35000
z+36000
z+37000
z+38000
z+39000
z+40000
z+41000
z+42000
z+43000
z+44000
z+45000
z+46000
z+47000
z+48000
z+49000
z+50000
z+51000
z+52000
z+53000
z+54000
z+55000
z+56000
z+57000
z+58000
z+59000
z+60000
z+61000
z+62000
z+63000
z+64000
z+65000
z+66000
z+67000
z+68000
z+69000
z+70000
z+71000
z+72000
z+73000
z+74000
z+75000
z+76000
z+77000
z+78000
z+79000
z+80000
z+81000
z+82000
z+83000
z+84000
z+85000
z+86000
z+87000
z+88000
z+89000
z+90000
z+91000
z+92000
z+93000
z+94000
z+95000
z+96000
z+97000
z+98000
z+99000
z+100000
z+101000
z+102000
z+103000
z+104000
z+105000
z+106000
z+107000
z+108000
z+109000
z+110000
z+111000
z+112000
z+113000
z+114000
z+115000
z+116000
z+117000
z+118000
z+119000
z+120000
z+121000
z+122000
z+123000
z+124000
z+125000
z+126000
z+127000
z+128000
z+129000
z+130000
z+131000
z+132000
z+133000
z+134000
z+135000
z+136000
z+137000
z+138000
z+139000
z+140000
z+141000
z+142000
z+143000
z+144000
z+145000
z+146000
z+147000
z+148000
z+149000
z+150000
z+151000
z+152000
z+153000
z+154000
z+155000
z+156000
z+157000
z+158000
z+159000
z+160000
z+161000
z+162000
z+163000
z+164000
z+165000
z+166000
z+167000
z+168000
z+169000
z+170000
z+171000
z+172000
z+173000
z+174000
z+175000
z+176000
z+177000
z+178000
z+179000
z+180000
z+181000
z+182000
z+183000
z+184000
z+185000
z+186000
z+187000
z+188000
z+189000
z+190000
z+191000
z+192000
z+193000
z+194000
z+195000
z+196000
z+197000
z+198000
z+199000
z+200000
z+201000
z+202000
z+203000
z+2

$\Rightarrow H = \langle \sigma_i, \tau \rangle$ erhält alle Transpositionen der Form $(i \ i+1)$, $i=1, \dots, n-1$. Diese erzeugen S_n . Also ist $\text{Gal}(L/\mathbb{Q}) = S_n$. Damit ist f nach Lemma 7.2 nicht auflösbar. \square

Bem. Abel und Ruffini haben nur ausgeschlossen, dass es einheitliche Formeln für alle Wurzeln von Koeffizienten eines Grad-5-Polynoms gibt. Satz 7.3 ist stärker, da für ein konkretes Polynom keine Formeln existieren können.

Berechnung von Galoisgruppen über \mathbb{Q}

Bei $f = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Q}[x]$ mit Wurzeln $\alpha_1, \dots, \alpha_n \in \mathbb{C}$.

Def. 7.4 Die Diskriminante von f ist $D = \prod_{i,j} (\alpha_i - \alpha_j)^2$.

Man kann zeigen:

- $D = 0 \Rightarrow f$ reduzibel
- Die Diskriminante ist ein symmetrisches Polynom in den Wurzeln.
 \Rightarrow Alle $\sigma \in \text{Gal}(L/\mathbb{Q})$, wobei L Beifeldkörper von f , fixieren $D \Leftrightarrow D \in \mathbb{Q}$.
- D kann als Polynom in den Koeffizienten von f geschrieben werden.
- $\sqrt{D} = \prod (\alpha_i - \alpha_j) \in L$. Es gilt $\sigma \in \text{Gal}(L/\mathbb{Q})$ ist in $A_n \Leftrightarrow \sigma(\sqrt{D}) = \sqrt{D}$.
- Für ganzalgebraisches irreducibles f ist die Diskriminante in $\mathbb{Z}[\frac{1}{2}\sigma_0]$.

Satz 7.5. Für jede Primzahl p mit $p \nmid D$ ist die Galoisgruppe von $\bar{f} \in \mathbb{F}_p[x]$ eine Untergruppe der Galoisgruppe von f über \mathbb{Q} .

Zusammen mit

Satz 7.6 Die Galoisgruppe eines jeden $\bar{f} \in \mathbb{F}_p[x]$ istzyklisch.

erhält man viele Informationen über die Zyklustruktur von Elementen von $\text{Gal}(L/\mathbb{Q})$.

Wenn z.B. \bar{f} mod p in irreducibile Polynome mit Graden d_1, \dots, d_k zerfällt,
so gibt es in $\text{Gal}(L/\mathbb{Q})$ ein Element mit der Zyklustruktur $\sigma = (d_1\text{-zykl.}) \cdot (d_2\text{-zykl.}) \cdot \dots \cdot (d_k\text{-zykl.})$.

f. Semidirekte Produkte

Das semidirekte Produkt nimmt 2 Gruppen H und K und bildet eine neue Gruppe G , in der H und K Untergruppen sind. Im Gegensatz zum direkten Produkt $H \times K$ ist beim semidirekten Produkt nur eine der beiden Gruppen ein Normalteiler. Insbesondere muss G nicht abelsch sein, auch wenn H und K es sind.

Betrachte die folgende Situation: G Gruppe, $H, K \subseteq G$ sind Untergruppen und $H \trianglelefteq G$, und $H \cap K = \{1\}$. Annahme von $H \trianglelefteq G$ zeigt, dass $HK = \{hk \mid h \in H, k \in K\} \subseteq G$ (eine Teilmenge ist) (s. Algebra I).

$$\text{Zum Produkt in } HK: h_1 k_1 h_2 k_2 = \underbrace{h_1}_{\in H} \underbrace{k_1 h_2^{-1}}_{\in H, \text{ da } H \trianglelefteq G} \underbrace{k_2}_{= k_2 \in H} = h_3 k_3 \in HK \quad (*).$$

Das semidirekte Produkt erfordert diese Situation nur aus H und K .

Beobachtungen: k_3 ist als Produkt in K nur aus K definiert. h_3 ist ein Produkt in H von h_1 und dem Element $k_1 h_2 k_2^{-1}$. Letzteres nutzt die Gruppenoperation in G , welche wir nicht zur Verfügung haben (würde mit G konstruieren).

Wenn wir das Element $k_1 h_2 k_2^{-1} \in H$ abstrakt beschreiben, dann definiert (*) eine Gruppenoperation auf der Menge HK . H soll ein Normalteiler sein, also muss G und insb. K auf H durch Konjugation: $h \in H, k \in K: koh = khk^{-1} \in H$

Dann wird (*) zu $h_1 (k_1 h_2) (k_1 k_2^{-1}) \quad (**)$.

Die Konjugation kann aufgefasst werden als Homomorphismus von K nach $\text{Aut}(H)$: $\varphi: K \rightarrow \text{Aut}(H)$. (φ ist) linigt von φ definiert eine Gruppenoperation.

Satz f.1 Seien H, K Gruppen und $\varphi: K \rightarrow \text{Aut}(H)$ ein Homomorphismus, d.h. K wirkt mit \circ auf H . Sei $G = \{(h, k) \mid h \in H, k \in K\}$ und $(h_1, k_1)(h_2, k_2) = (h_1 \cdot (k_1 \circ h_2), k_1 k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2)$.

Dann gilt:

- (1) G ist eine Gruppe.
- (2) $H \cong \{(h, 1) \mid h \in H\}, K \cong \{(1, k) \mid k \in K\}$
- (3) $H \trianglelefteq G$
- (4) $H \cap K = \{1\}$
- (5) $\forall k \in K, h \in H: khk^{-1} = koh = \varphi(k)(h)$

Bew. Übung.

Die Gruppe G in Satz f.1 heißt das semidirekte Produkt von H und K entlang φ und wird mit $H \rtimes_{\varphi} K$ oder $H \rtimes_{\varphi} K$ bezeichnet.

(Erstellen: $H \rtimes K$, da $H \trianglelefteq G$)

Bew. - φ ist trivial gel. $H \rtimes_{\varphi} K = H \times K$ gel. $K \trianglelefteq H \rtimes K$ ($= \text{id}$)

- Falls G Gruppe und H, K Untergruppen und $H \trianglelefteq G$ und $H \cap K = \{1\}$, dann ist $HK \cong H \rtimes_{\varphi} K$ mit $\varphi = \text{Konjugation in } G$.

Bsp.: Sei H eine abelsche Gruppe und $K = \mathbb{Z}/2\mathbb{Z} = \langle s \rangle$ zyklisch von Ordnung 2. Sei $\varphi: K \rightarrow \text{Aut}(H)$. Für H zyklisch von Ordnung n ergibt sich

$$s \mapsto (h \mapsto h^{-1}) \quad H \rtimes_{\varphi} K \text{ von Ordnung } 2n. \text{ Welche Gruppe ist es?}$$

Elemente (r^i, s^j) mit $i \in \{0, \dots, n-1\}, j \in \{0, 1\}$.

$$\begin{aligned} \text{Ord } (r^i, s^j)(r^{i'}, s^{j'}) &= \left(r^i \varphi(s^j)(r^{i'}), s^j s^{j'} = s^{i+j} \right) \\ &= \begin{cases} (r^{i+i'}, s^{i+j'}) & \text{falls } j=0 \\ (r^{i-i'}, s^{i+j'}) & \text{falls } j=1 \end{cases} \end{aligned}$$

Merk: $D_{2^n} = \{r^i s^j \mid 0 \leq i \leq n-1, 0 \leq j \leq 1\}$ mit Relationen $r^n = s^2 = 1, sr = r^{-1}s$.

$$sr = (1, s)(r, 1) = (1, r^{-1}, s) = r^{-1}s.$$

Man sieht: D_{2^n} ist ein semidirektes Produkt von zyklischen Gruppen. ($D_{2^n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$)

Bsp.: Galoisgruppe von $x^p - 2$, p prim und $p \neq 2$. (über \mathbb{Q})... zeta
Der Zerfällungskörper ist $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ mit $\zeta_p^p = 1$ (ζ_p = primitive pte Einheitswurzel). Sei $G = \text{Gal}(L/\mathbb{Q})$. Satz 5.3: $|G| = [L:\mathbb{Q}]$ ist endlich, da $\leq p!$, da Wurzeln permutiert werden.

Wir kennen 2 Zwischenkörper: $\mathbb{Q}(\sqrt[p]{2})$ und $\mathbb{Q}(\zeta_p)$ und $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$ und $[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}] = p$. Also ist $|G| = [L:\mathbb{Q}]$ durch p und $p-1$ teilbar.
Da p prim, $|G| \geq p(p-1)$. Aber $x^p - 2 \in \mathbb{Q}(\zeta_p)[x]$ zerfällt über L vollständig, also ist $[L:\mathbb{Q}(\zeta_p)] \leq p$, da das Mindestpolynom von $\sqrt[p]{2}$ über $\mathbb{Q}(\zeta_p)$ $x^p - 2$ teilt.
 $\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(\zeta_p) \subseteq L$, also $|G| = p(p-1)$.

ZB: verstecken uns Elemente von G , als Permutationen von $\{\sqrt[p]{2}, \zeta_p\sqrt[p]{2}, \dots, \zeta^{p-1}\sqrt[p]{2}\}$.
Wählt jede der $p!$ Permutationen taucht auf!

Um Elemente zu finden, bedenkt wir: Ein Automorphismus von L ist auch durch die Bilder von ζ_p und $\sqrt[p]{2}$ bestimmt. \rightarrow Untergruppen per Satz von Cauchy Sodrin.
 \rightarrow Satz 5.5 anwenden.

(d.h. für ein Element in G ist: komplexe Ordnung: $\sigma_a: L \rightarrow L^a$ für geeignetes $a \in \mathbb{N}$. Das gilt $K = \{\sigma_a : a=1, 2, \dots, p-1\} \subseteq G$. $\sqrt[p]{2} \mapsto \zeta_p^a \sqrt[p]{2}$
 K istzyklisch von Ordnung $p-1$. $K \cong \text{Gal}(\mathbb{Q}(\zeta_p):\mathbb{Q})$.

Nach Satz 5.5 ist $K \cong \text{Gal}(L:\mathbb{Q}) / \text{Gal}(L:\mathbb{Q}(\zeta_p))$.

Ein $\tau \in \text{Gal}(L:\mathbb{Q}(\zeta_p))$ muss ζ_p fixieren und die Wurzeln von $x^p - 2$ perm. tuzieren.

$\tau_b: L \rightarrow L$, $b=0, \dots, p-1$. Das gibt eine zyklische Untergruppe
 $\sqrt[p]{2} \mapsto \zeta_p^b \sqrt[p]{2}$ $H \subseteq G$ der Ordnung p .

Es gilt: $H \cap K = \{\sigma_1 = \zeta_p^0 = 1\}$.

Ortsmittel? zu K : $\tau_b \sigma_a \tau_b^{-1}: h \mapsto h^a$
 $\sqrt[p]{2} \mapsto \zeta_p^{-b} \sqrt[p]{2} \mapsto (\zeta_p^a)^b \sqrt[p]{2} \mapsto \zeta_p^{ab} \sqrt[p]{2}$
 $\mapsto \zeta_p^{(b-a)p} \sqrt[p]{2} \neq \sqrt[p]{2}$ für $a \neq 1$.
 $\Rightarrow \tau_b \sigma_a \tau_b^{-1} \notin K$ für $a \neq 1$. (d.h. G mit abelsch.)

zu H : $\sigma_a \tau_b \sigma_a^{-1}: h \mapsto h$
 $\sqrt[p]{2} \mapsto \text{andere Wurzel von } x^p - 2 \} \in H$.

wg. Ordnung
 $\Rightarrow G = HK = H \rtimes K$ mit Gruppenoperation: $(\sigma_1, \tau_1)(\sigma_2, \tau_2) = (\sigma_1 \tau_1 \sigma_2 \tau_1^{-1}, \tau_1 \tau_2)$.

Teil II - Kategorientheorie

Literatur: S. MacLane: "Categories for the Working Mathematician" (geeignet)
 S. Awodey: "Category Theory" (Besser geeignet)

3. Was ist Kategorientheorie?

Kategorientheorie ist eine Art abstrakte Algebra der Abbildungen mit der Komposition als eine Art Produkt.

Ideengeschichtliches: Felix Kleins Erlanger Programm: Verstelle mathematische Objekte durch ihre Symmetrien und Transformationen zwischen ihnen.

Formalierung zunächst 1945 von Eilenberg + MacLane. Fand sofort Nutzen in der Vereinheitlichung, Formalisierung und Verallgemeinerung von algebraischer Topologie und homologischer Algebra. Ab 1950: Grothendieck schafft weitreichenden Ausbau der aufgebauten Geometrie mit Hilfe von Kategorien. Seit 1970 überall zu finden: Informatik, Linguistik, Philosophie, Gewerbeschaffen.

Grund: Objekte und Abbildungen müssen ihrer sind überall.

"Theorie der
geordneten
Grafiken mit
Komposition"

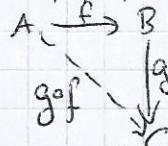
"der Grothendieck
nur noch interessante
als Galois"

"Seine Mutter war
Fotografin und
sein Vater war
Amaranthus"

Bsp: Mengen: Seien A, B, C, D Mengen. $A \xrightarrow{f} B$ ist eine Silbe wobei $f: A \rightarrow B$.

Dann existiert

gof .



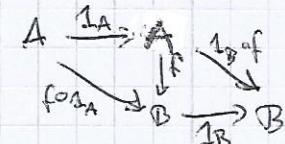
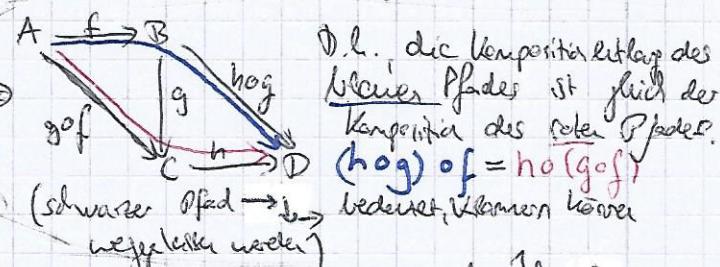
Die Komposition ist assoziativ: \Rightarrow

Außerdem hat jede Menge eine identische Abbildung $1_A: A \rightarrow A$ mit der Eigenschaft

$$f \circ 1_A = 1_B \circ f \quad \forall f: A \rightarrow B.$$

(Insbesondere ist das nicht über einzelne Elemente definiert!) \Rightarrow

Das erfordert nun in der Kategorientheorie zwei Axiome.

Algebra II

13.06.2019

Def. 9.1 Eine Kategorie besteht aus:

- Objekten A, B, C, \dots
 - Pfeilen f, g, h, \dots
 - Für jeden Pfeil f zwei Objekte $\text{dom}(f)$ – Domäne, Definitionsbereich
 $\text{cod}(f)$ – Kodomäne, Bildbereich
- Wir schreiben: $f: A \rightarrow B$ oder $A \xrightarrow{f} B$ falls $A = \text{dom}(f)$ und $B = \text{cod}(f)$.
- Für je zwei Pfeile $f: A \rightarrow B$ und $g: B \rightarrow C$ (d.h. $\text{cod}(f) = \text{dom}(g)$) existiert ein Pfeil $g \circ f: A \rightarrow C$, genannt die Verknüpfung oder Komposition von f und g .
 - Für jedes Objekt A gibt es einen Pfeil $1_A: A \rightarrow A$, genannt die Identität auf A .

z.B. Mengen
 z.B. Abbildungen

Diese Ordnung erfüllen die folgenden Eigenschaften:

- Assoziativgesetz: $\forall f: A \rightarrow B, g: B \rightarrow C, h: C \rightarrow D: h \circ (g \circ f) = (h \circ g) \circ f$
- 1_A ist eine Identität, d.h. $\forall f: A \rightarrow B: f \circ 1_A = f = 1_B \circ f$.

Bem. Eine Kategorie ist erstmal sicher, was diese Axiome erfüllt. Wir können auch die Mengeltheorie verlassen, d.h. alle Objekte oder alle Pfeile müssen keine Menge bilden, und die Objekte selbst müssen keine Mengen sein.

oder Menge
 besteht aus
 Standardauf vor,
 dass die Mengen-
 lebe zusammen-
 bricht"

- Bsp.: - Sets: die Kategorie der Mengen mit Abbildungen als Pfeilen
 - Sets_{fin}: die Kategorie der endlichen Mengen mit Abbildungen als Pfeilen
 Die zweite ist eine Einschränkung der ersten. Solche Einschränkungen gibt es häufig.
 Man kann auf die Pfeile einschränken, z.B. ist die Verknüpfung von injektiven Abbildungen injektiv + bijektiv + surjektiv, also sind endliche Mengen mit injektiven Abbildungen auch eine Kategorie.

- strukturierte Mengen und ihre Homomorphismen:
 Gruppen + Homomorphismen, Vektorräume über einem festen Körper + lineare Abbildungen,
 Graphen + Graphhomomorphismen ($f: G \rightarrow H : \{v, w\} \in E(G) \mapsto \{f(v), f(w)\} \in E(H)$)
- ein Objekt \mathbb{R} mit stetigen Funktionen als Pfeilen
- topologische Räume mit stetigen Abbildungen
- differenzierbare Mannigfaltigkeiten mit glatten Abbildungen (Halbordnung)
- partiell geordnete Mengen + ordnungsverhaltende Abbildungen (Pos, partially ordered set)

Alle diese Kategorien nennt man konkret, da ihre Objekte Mengen sind und ihre Pfeile Abbildungen. Ein nicht-konkretes Beispiel:

- Die Kategorie Rel hat als Objekte Mengen und als Pfeile lineare Relationen, d.h. ein Pfeil $A \rightarrow B$ ist eine beliebige Teilmenge von $A \times B$, und $1_A = \{(a, a) | a \in A\} \subseteq A \times A$, und für $R \subseteq A \times B$ und $S \subseteq B \times C$ ist $S \circ R = \{(a, c) | \exists b \in B : (a, b) \in R \wedge (b, c) \in S\} \subseteq A \times C$.

Witzige Kategorien:

- 1: $*$ ist die Kategorie mit einem Objekt " $*$ " und nur einem Pfeil 1_* .
- 2: $* \rightarrow \square$ hat 2 Objekte $*$ und \square und einen Pfeil $* \rightarrow \square$ sowie 2 Identitäten 1_* und 1_{\square} .
- 3: $* \rightarrow \square$ hat 3 Objekte und $* \rightarrow \square$ muss als Komposition erfordern.

- 0 hat keine Objekte und keine Pfeile.

Wenn man witzige Kategorien als Pfeildiagramme zeichnet, lässt man Identitäten und "unnötige" Kompositionen weg.

Bsp.: $A \xrightleftharpoons[g]{f} B$ hat unendlich viele Pfeile $gof, gofogof, \dots$

\Rightarrow In der Kategorientheorie dreht sich alles um die Pfeile.
 Die Pfeile zwischen Kategorien sind die Funktoren.

Def. 3.2 Seien \mathcal{C} und \mathcal{D} Kategorien. Ein Funktator $F: \mathcal{C} \rightarrow \mathcal{D}$ ist eine Zuordnung von Objekten von \mathcal{C} zu Objekten von \mathcal{D} und Pfeilen von \mathcal{C} zu Pfeilen von \mathcal{D} , sodass

- 1) $F(f: A \rightarrow B) = F(f) : F(A) \rightarrow F(B)$
- 2) $F(1_A) = 1_{F(A)}$
- 3) $F(gof) = F(g) \circ F(f)$

für alle Objekte A, B von \mathcal{C} und Pfeile $f, g \in \mathcal{C}$.

Bsp.: Jede Kategorie \mathcal{C} hat einen identischen Funktator $1_{\mathcal{C}}$, der alles auf sich selbst abbildet.

Nach Prüfung des Argumentationsgeistes erhält man

Cat = Kategorie aller Kategorien mit Funktoren als Pfeilen.

"Sie haben sie einen
Turing-vollständigen
Computer?"

"Stem ist einfach
ein Stern"
"Stem, Box und
Dreieck"

Bsp.: (Forts.)

- Eine Quasiordnung oder (Präordnung) ist eine Halbordnung ohne Antisymmetrie, d.h. eine binäre Relation $p \leq q$ auf einer Menge P , die reflexiv und transitiv ist, d.h. $p \leq p + p \in P$ und $p \leq q \wedge q \leq r \Rightarrow p \leq r$. Jede Quasiordnung ist eine Kategorie mit der Objektmenge P mit Pfeilen $p \rightarrow q \Leftrightarrow p \leq q$.
- Reflexivität \Rightarrow Existenz von 1_p , Transitivität \Rightarrow Komposition von Pfeilen.
- Insbesondere ist jede partiell oder total geordnete Menge auch eine Kategorie.
(Dies ist nicht passt, denn Passt hat partiell geordnete Mengen selbst als Objekte.)

Ein Beispiel aus der Logik / theoretischen Informatik:

Die Kategorie der Beweise, wo Objekte Aussagen sind, d.h. logische Formeln, deren Wahrheitswert zugeordnet werden kann. Pfeile sind logische Ableitungen, d.h. Beweise. Dies ist endlich assoziativ und hat Identitäten (jede Aussage beweist sich selbst). Es gibt zwischen zwei Objekten oft mehrere Pfeile, da es mehrere Beweise für eine Proposition geben kann. \Rightarrow Grundlage des λ -Kalküls.

„die Informatik hat die Logik verdeckt“

Andere Beispiel: Hask die Kategorie der Haskell-Datentypen. Objekte sind Datentypen wie `Bool`, `List Bool`, ...; und Pfeile sind berechenbare Funktionen (diese sind vollständig typisiert).

„schreien Sie die größte Zahl auf, um Port 1!“
⇒ Busy Beaver
(BusyBeaver (1))

Diese Kategorie der Beweise und Hask hängen zusammen über den Coqu-Howard-Isomorphismus. Dieser sagt aus: Aussagen $\xrightarrow{\text{1:1}}$ Datentypen
Formelle Beweise $\xrightarrow{\text{1:1}}$ Implementierung von Datentypen.

Funktionen sind auch Datentypen
 $f : \text{Bool} \rightarrow \text{Bool}$
Datentyp in Hask

\Rightarrow HOTT: Homotopytyptheorie als neue Grundlage der Mathematik?
(statt Mengenlehre).

„dann müssen Sie erstmal in Oxford in Logik prawnien“

Wenden wir uns wieder algebraischen Beispielen zu.

Bsp.: Ein Monoid ist eine Menge M mit einer binären Operation $\circ : M \times M \rightarrow M$ und einer Einheit $u \in M$ so dass $\forall x, y, z \in M. (x \circ y) \circ z = x \circ (y \circ z)$ und $u \circ x = x \circ u = x$. (wie Gruppe ohne Inverse).

Es gibt Monoide sind genau die Kategorien mit nur einem Objekt. Die Elemente des Monoids sind die Pfeile von einem Objekt zu sich selbst.

Monoide: $-(\mathbb{N}, +, 0)$

(also auch Gruppe)
 $\text{Home}(X, X) = \{f : X \rightarrow X \text{ Abbildungen}\}$
 (allgemein: falls C Kategorie und $A \in C$ ein Objekt,
 $\text{Home}(A, A) = \{Pfeile A \rightarrow A \text{ in } C\}$ ist ein Monoid)

Algebra II

„die heutige Wirkung und gespannt von der weitesten, spannendsten Kategorien-Kette“

Monoide: $\text{Men} =$ Kategorie der Monoide mit Monoidhomomorphismen als Pfeilen

Jedes Monoid ist selbst eine Kategorie mit nur einem Objekt.

Monoidhomomorphismen sind genau die Funktoren zwischen Monoide (gesehen als Kategorien).

Seien (M, \circ, u) und (N, \times, v) Monoide. Ein Monoidhomomorphismus oder Funktor ist eine Abbildung $h : M \rightarrow N$ mit $h(u) = v$, $h(m_1 \circ m_2) = h(m_1) \times h(m_2) \quad \forall m_1, m_2 \in M$.

Man könnte sagen: Kategorien verallgemeinern Monoide auf mehr als ein Objekt.
(und Funktoren verallgemeinern Monoidhomomorphismen).

Wir verallgemeinern nun weitere Begriffe aus der Algebra.

Def. 9.3: Sei \mathcal{C} eine Kategorie. Ein Pfeil $f: A \rightarrow B$ heißt Isomorphismus, falls in \mathcal{C} ein $g: B \rightarrow A$ existiert mit $g \circ f = 1_A$ und $f \circ g = 1_B$. Falls ein Isomorphismus $f: A \rightarrow B$ existiert, nennen wir A und B isomorphe ($A \cong B$).

Bem.: Das g in Def. 9.3 ist eindeutig und wird mit f^{-1} bezeichnet ("Invers von f ").
Wir haben nicht verändert, dass A und B Mengen und f eine Abbildung sind. Dies ist eine "abstrakte", kategorientheoretische Definition.

Damit kann man definieren: Eine Gruppe ist eine Kategorie mit genau einem Objekt, in der jeder Pfeil ein Isomorphismus ist. Ein Gruppenisomorphismus ist ein Funktor zwischen Gruppen.

Satz 9.4 (Cayley): Jede Gruppe ist isomorph zu einer Untergruppe einer Permutationsgruppe.

Beweis: Die Cayley-Darstellung einer Gruppe G ist die Wirkung von G (als Gruppe) auf G (als Menge) via $\tilde{g}: G \rightarrow G$. Dies ist für jedes $g \in G$ eine Bijektion, die \tilde{g}^{-1} die Umkehrabbildung $h \mapsto gh^{-1}$ ist.
Das definiert einen Homomorphismus $i: G \rightarrow \tilde{G} \subseteq \text{Sym}(G)$.

$$\begin{array}{c} g \mapsto \tilde{g} \\ \text{Bew.: } i \text{ ist ein Isomorphismus und die Umkehrabbildung ist } j: \tilde{G} \rightarrow G \quad \leftarrow \text{einheit in } G \\ \text{Es gilt } i \circ j = 1_{\tilde{G}} \text{ und } j \circ i = 1_G: \\ \text{in der Kategorie der Gruppen} \\ i \circ j: \tilde{G} \rightarrow \tilde{G} \quad j \circ i: G \rightarrow G \quad \text{eineindeutige Funktion} \\ \tilde{g} \mapsto \tilde{g}(u) = g \quad \text{da } g(u) = g \quad g \mapsto (h \mapsto gh^{-1})(u) \quad \square \end{array}$$

Bem.: Man beachte die verschiedenen Arten von Isomorphismen im Beweis: Permutationen von Mengen sind Isomorphismen in Sets und invertierbare Gruppenhomomorphismen sind Isomorphismen in Groups (die Kategorie aller Gruppen).

Gruppen sind spezielle Kategorien und tatsächlich lässt sich der Satz von Cayley allgemein formulieren:

Satz 9.5: Sei \mathcal{C} eine Kategorie, in der die Pfeile eine Menge bilden. Dann ist \mathcal{C} isomorph (in Cat) zu einer konkreten Kategorie, d.h. einer Kategorie, in der die Objekte Mengen und die Pfeile Abbildungen sind.

Beweisidee: Betrachte die Cayley-Darstellung $\tilde{\mathcal{C}}$ von \mathcal{C} : Sie hat als Objekte die Mengen $\tilde{\mathcal{C}} = \{f \in \mathcal{C} \mid \text{cod } f = C\} = \{f: X \rightarrow C \text{ in } \mathcal{C} \text{ mit } X \text{ beliebig}\}$ für jedes Objekt C in \mathcal{C} .

Pfeile von $\tilde{\mathcal{C}}$ sind: $\tilde{g}: \tilde{\mathcal{C}} \rightarrow \tilde{\mathcal{D}}$ definiert für jedes $f: X \rightarrow C$ gilt: $\tilde{g}(f) = g \circ f$ für jeden Pfeil $g: C \rightarrow D$ in \mathcal{C} .

Man prüft, dass die Cayley-Darstellung $i: \mathcal{C} \rightarrow \tilde{\mathcal{C}}$ ein invertierbarer Funktor, also ein Isomorphismus in Cat ist. \square

Der Begriff "konkrete Kategorie" soll eigentlich eine Unterscheidung zwischen vorgelehrten bzw. abstrakten Kategorien ermöglichen. Der Satz sagt: Die Unterscheidung gibt es nicht. Die abstrakte und konkrete Version einer gegebenen Kategorie können nur mit Mitteln unterscheiden werden, die außerhalb der Kategorientheorie liegen. Diese Unterschiede betreffen also nicht die (Struktur des) Pfeile in der Kategorie.

(Analogie: TH kann als Verallgemeinerung von \mathbb{Q} oder als Menge Dedekindscher Schnitte gesehen werden, reelle Analysis kann den Unterschied nicht "sehen".)

Falls die Objekte Mengen sind, dann können wir mit Elementen arbeiten: in einer konkreten Kategorie z.B. wir testen, ob $(f: A \rightarrow B) \models (g: A \rightarrow B)$ via $f(x) = g(x) \forall x \in A$.

Dieses Prinzip kann man auch mit Pfeilen darstellen.

Idee dazu: Ein verallgemeinertes Element eines Objektes A ist ein Pfeil $x : T \rightarrow A$ für ein spezielles Testobjekt T mit der Eigenschaft $(f \circ x = g \circ x \quad \forall x : T \rightarrow A) \Rightarrow f = g$. Später mehr zu solchen terminalen Objekten T .

Def. 9.6 Seien \mathcal{C} und \mathcal{D} Kategorien. Das Produkt $\mathcal{C} \times \mathcal{D}$ ist die Kategorie mit Objekten (C, D) mit C Objekt in \mathcal{C} und D Objekt in \mathcal{D} und Pfeilen $(f, g) : (C, D) \rightarrow (C', D')$ für jedes Paar von Pfeilen $f : C \rightarrow C'$ in \mathcal{C} und $g : D \rightarrow D'$ in \mathcal{D} .

Identität und Komposition sind komponentenweise definiert:

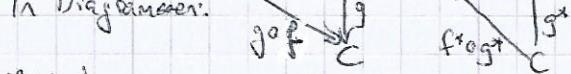
$$\mathbf{1}_{(C,D)} = (\mathbf{1}_C, \mathbf{1}_D) \text{ und } (f,g) \circ (f',g') = (f \circ f', g \circ g').$$

Bem. Man hat 2 Projektionsfunktionen: $\mathcal{C} \xleftarrow{\pi_1} \mathcal{C} \times \mathcal{D} \xrightarrow{\pi_2} \mathcal{D}$
mit $\pi_1(C, D) = C$, $\pi_2(C, D) = D$
 $\pi_1(f, g) = f$, $\pi_2(f, g) = g$.

Bsp.: In Sets ist dies das kartesische Produkt und in Groups das direkte Produkt.

Def. 9.7 Sei \mathcal{C} eine Kategorie. Die duale Kategorie \mathcal{C}^{op} hat die gleichen Objekte wie \mathcal{C} und genau einen Pfeil $f^* : D \rightarrow C$ für jeden Pfeil $f : C \rightarrow D$ in \mathcal{C} . (Also ist \mathcal{C}^{op} einfach \mathcal{C} mit allen Pfeilen umgedreht.)

Es gilt dabei $(\mathbf{1}_C)^* = \mathbf{1}_C$ und $(g \circ f)^* = f^* \circ g^*$. in \mathcal{C} : $A \xrightarrow{f} B$ in \mathcal{C}^{op} : $A \xleftarrow{f^*} B$
für jedes C in \mathcal{C} $\downarrow g$ $\downarrow g^*$



Viele Dualitätsbegriffe in der Mathematik

lassen sich ausdrücken als "eine Kategorie ist (teileins) duale Kategorie einer anderen Kategorie".

Bsp.: VektorenDualität ist ein Funktor, der alle Pfeile umdreht.

10. Freie Kategorien und universelle Eigenschaften

"wir definieren jetzt
Freiheit"

In der Algebra bedeutet "frei", dass keine Relationen gelten außer den automatisch geforderten, z.B. in einer freier abelscher Gruppe gelten nur Erzeugerrelationen wie $ug = gu = g$ und Verknüpfungsrelationen $xy = yx$. Wir drücken dieses "sonst keine Relationen" kategorientheoretisch aus. (Zunächst für Monoid)

Def. 10.1

Ein Alphabet A ist eine Menge von Buchstaben $A = \{a, b, c, \dots\}$.

Ein Wort über A ist eine endliche Folge von Buchstaben aus A , z.B. algebra, xyz, quetz.

Das leere Wort ist $-$.

Der Kleene-Abschluss von A ist $A^* = \{\text{Worte über } A\}$.

Die Konkatenation ist eine binäre Operation $A^* \times A^* \rightarrow A^*$
 $(w, w') \mapsto ww'$.

Zusammen mit der Einheit $-$ ist A^* ein Monoid – das freie Monoid über A .

- Alphabet $A = \{a, b, \dots\}$ Buchstaben

- A^* ist das Monoid der Wörter bestehend aus Buchstaben mit Konkatenation als Operation und dem leeren Wort - als Einheit.
das freie Monoid über A .

Es gibt offensichtlich eine Injektion $i: A \rightarrow A^*$. Die Bilder von i erzeugen A^* als Monoid, d.h. jeder Wert ist eine ... $x \mapsto x$... Konkatenation von Buchstaben.
Zusätzlich ist A^* frei d.h. alle Relationen $a_1 \dots a_k = a_1' \dots a_k'$ gelten nur, wenn sie aus den Monoidrelationen folgen. Wir machen diesen Begriff präzise.

- Jedes Monoid N ist auch eine Menge, die wir mit $|N|$ bezeichnen.
- jeder Monoidhomomorphismus $f: M \rightarrow N$ ist eine Abbildung von Mengen, die wir mit $|f|: |M| \rightarrow |N|$ bezeichnen.

Diese Zuweisungen definieren den vergesslichen Funktor $\text{U}: \text{Mon} \rightarrow \text{Sets}$, der die Monoidstruktur vergisst.

Die Forderung, dass etwas was auf Buchstaben von A darf ist, inklusive einer

(def.) Homomorphismus:
S. theoretische
Informatik, wo
wir nur Zeichen
abbilden!
(das wird in
Proof einfach
behauptet)

Def. 10.2 Die universelle Eigenschaft des freien Monoids $M(A)$ über der Menge A ist:
es existiert eine Abbildung $i: A \rightarrow |M(A)|$ und für jedes Monoid N und
jede Abbildung $f: A \rightarrow |N|$ ein eindeutiger Homomorphismus $\bar{f}: M(A) \rightarrow N$ mit
 $|\bar{f}| \circ i = f$.

In Diagrammen:
 $\text{Mon}: M(A) \xrightarrow{i} |M(A)|$; "lift"
 $\text{Sets}: |M(A)| \xrightarrow{\bar{f}} |N|$
 $\uparrow i \quad \uparrow \bar{f}$
 A

Prop. 10.3 A^* hat die universelle Eigenschaft (UE) des freien Monoids über A .

Beweis: Die Abbildung i wurde oben definiert.

Angenommen, $f: A \rightarrow |N|$ bildet A in ein beliebiges Monoid N ab (als Menge).

Wir müssen $\bar{f}: A^* \rightarrow N$ konstruieren. Seien

$$\bar{f}(-) = u_N \in \text{Endet in } N$$

$f(a_1 \dots a_k) = f(a_1) \dots f(a_k)$ (Produkt in N) \bar{f} ist schon ein Monoidhomomorphismus mit $(\bar{f} \circ i)(a) = f(a) \forall a \in A$.

Zur Eindeutigkeit von \bar{f} : Sei $g: A^* \rightarrow N$ ein weiterer Homomorphismus mit $g(a) = f(a) \forall a \in A$ ($d.h. g \circ i = f$).

Dann ist $g(a_1 \dots a_k) = g(a_1) \dots g(a_k) = f(a_1) \dots f(a_k) = \bar{f}(a_1 \dots a_k)$ für $a_1, \dots, a_k \in A$ beliebig. $\Rightarrow g = \bar{f}$. \square

Bem: Die universelle Eigenschaft präzisiert 2 Begriffe:

- "A erzeugt A^* " ist ausgedrückt in der Eindeutigkeit von \bar{f} , da, wenn zu-sätzliche Elemente in A^* existieren würden, Eindeutigkeit für \bar{f} auf diesen Elementen besteht, denn das gegebene f fixt nur die Bilder von A .
- " A^* ist frei" ist Kodiziert in der Existenz von \bar{f} für jeder Monoid N , denn jede Relation zwischen den Wörtern von A^* muss in jedem N vorkommen - aber keine Relation außer den Monoidrelationen kommt in allen Monoiden vor.

Wir nutzen die \rightarrow Prop. 10.4 Das freie Monoid $M(A)$ auf einer Menge A ist eindeutig. (hier auf Isomorphe)

Beweis: Seien M, N Monide und $i: A \rightarrow |M|$ und $j: A \rightarrow |N|$ je-

Wells mit der universellen Eigenschaft (UE) des freien Monoids. $\text{Mon}: M \xrightarrow{i} |M| \xrightarrow{\bar{i}} M$

$|M|$ die UE hat, existiert zu j ein $\bar{j}: |M| \rightarrow |N|$ mit $|\bar{j}| \circ i = j$.

$|N|$ die UE hat, existiert zu i ein $\bar{i}: |N| \rightarrow |M|$ mit $|\bar{i}| \circ j = i$. $\text{Sets}: |M| \xrightarrow{\bar{i} \circ j} |N| \xrightarrow{\bar{i}} M$

...
 i
 j
 \bar{i}
 \bar{j}
 $\bar{i} \circ j$
 A

Beweis: ... Komposition liefert einen Homomorphismus $\bar{i} \circ \bar{j}: M \rightarrow M$ mit $(\bar{i} \circ \bar{j}) \circ i = i$.
 Da 1_M die gleiche Eigenschaft hat ($1_M \circ i = i$) und die reziproke Abbildung
 in der UE vor M eindeutig ist, gilt $1_M = \bar{i} \circ \bar{j}$.
 Das gleiche Argument mit vertauschten Rollen liefert $\bar{j} \circ \bar{i} = 1_N$. ("mutatis mutandis")
 insgesamt also $M \cong N$. \square

Bem. Der Isomorphismus $\bar{j}: M \rightarrow N$ ist eindeutig mit der Eigenschaft $(\bar{j}) \circ i = j$.

Bsp.: freies Monoid auf einem Erzeuger ist, bis auf Isomorphie, $(N, +, 0)$.

Das Prinzip der freien Konstruktion kann von Kategorien (Kategorien mit nur einem Objekt) auf Kategorien verallgemeinert werden. Die Rolle von Mengen als unterliegenden Strukturen wird dann von gerichteten Graphen (Pfeildiagrammen) gespielt.

Zu jedem solchen Graphen G gibt es eine freie Kategorie $\mathcal{C}(G)$, in der die Pfeile von G vorkommen (Objekte sind die Vertices) und alle Pfeile, die nicht enden, damit $\mathcal{C}(G)$ eine Kategorie wird, aber sonst nichts.

Der vergleichende Functor hat den Typ $1: \text{Cat} \rightarrow \text{Graphs}$ und die universelle Eigenschaft ist: Es existiert ein Homomorphismus von gerichteten Graphen $i: G \rightarrow |\mathcal{C}(G)|$ und für jede Kategorie \mathcal{D} und Homomorphismus $f: G \rightarrow |\mathcal{D}|$ ein Functor $\tilde{f}: \mathcal{C}(G) \rightarrow \mathcal{D}$ mit $|f| \circ i = f$.

Bsp.: - Die freie Kategorie auf einem Graphen mit einem Vertex ist das freie Monoid auf der Menge der Pfeile.
 - Die freie Kategorie auf dem Graphen ist die einzige Kategorie $\mathbb{1}$.

11. Kategorientheoretische Abstraktionen

Wir sehen lange vertraute Konstruktionen der Mathematik im Kontext der Kategorientheorie.

Def 11.1 Sei \mathcal{C} eine Kategorie. Ein Pfeil $f: A \rightarrow B$ in \mathcal{C} ist

- ein Monomorphismus oder mono, falls $\forall g, h: C \rightarrow A$ beliebige Pfeile end, so gilt $f \circ g = f \circ h \Rightarrow g = h$ d.h. falls f linksinjizierbar ist, weil
- ein Epimorphismus oder epi, falls $\forall g, h: B \rightarrow C$ gilt:

$$g \circ f = h \circ f \Rightarrow g = h, \text{ d.h., falls } f \text{ rechtsinjizierbar ist.}$$

Man schreibt manchmal $f: A \hookrightarrow B$ oder $f: A \twoheadrightarrow B$ für $f: A \rightarrow B$ mono, (links, Pfeilverkürzung)
 oder $f: A \rightarrow B$ für $f: A \rightarrow B$ epi.

In Sets gilt f ist mono $\Leftrightarrow f$ injektiv.

Beweis: Sei $f: A \hookrightarrow B$ mono. Seien $a, a' \in A$ und $a \neq a'$. Sei $\{x\}$ eine beliebige einel元ige Menge. Betrachte die Abbildungen $\bar{a}: \{x\} \rightarrow A$ und $\bar{a}': \{x\} \rightarrow A$.
 Sicher ist $\bar{a} \neq \bar{a}'$ (als Pfeile in Sets).

Da f mono, $f \circ \bar{a} \neq f \circ \bar{a}'$, also $(f(\bar{a}(x)) = f(a) \neq f(\bar{a}'(x)) = f(a')) \Rightarrow f$ injektiv.

Falls f injektiv ist und $g, h: C \rightarrow A$ mit $g \neq h$, dann existiert ein $c \in C$ mit $g(c) \neq h(c)$.

Da f injektiv ist, also $f(g(c)) \neq f(h(c))$, also $f \circ g \neq f \circ h$, also f mono. \square - neutrale Verkopplung

"Berechnungsweise"

$$\begin{array}{ccc} x & \mapsto & a \\ x & \mapsto & a' \end{array}$$

$$\begin{array}{ccc} x & \mapsto & a \\ x & \mapsto & a' \end{array}$$

Algebra III

27.06.2019
 23.7. tl 19.7. ✓
 10.8. Urlaub
 dann 1 Woche da.
 dann Vakanz
 15.8. 2.3.
 13/14.

In Mon und vielen anderen abstrakten Kategorien sind die Monomorphismen genau die injektiven Homomorphismen. Wir diskutieren Mon.
 Sei $h: M \rightarrow N$ ein Monomorphismus in Mon ($h: M \rightarrow N$ mono) $\Rightarrow h \circ f = h \circ g \Rightarrow f = g \quad \forall f, g: X \rightarrow M$.

Betrachte "Elemente" von M : $x: 1 \rightarrow |M|$, wobei $1 = \{*\}$

$$y: 1 \rightarrow |M|$$

eine beliebige einelnechte Menge ist. D.h. universelle Eigenschaft von $M(1)$ gibt Homomorphismen $\bar{x}, \bar{y}: M(1) \rightarrow M$ mit $\bar{x} \neq \bar{y} \Rightarrow \bar{x} \neq \bar{y} \Rightarrow h \circ \bar{x} \neq h \circ \bar{y}$ (als Pfeil $M(1) \rightarrow M(1)$). Also sind die "Elemente" $|h \circ \bar{x}|, |h \circ \bar{y}|: 1 \rightarrow |N|$ verschieden, also $|h|$ mono bzw. injektiv.

Umgekehrt sei $|h|: |M| \rightarrow |N|$ injektiv bzw. mono in Sets. Seien $f, g: X \rightarrow M$ Pfeile in Mon. Falls $f \neq g$, dann ist $|f| \neq |g|: |X| \rightarrow |M| \Rightarrow |h \circ f| \neq |h \circ g|$ (da $|h|$ mono). Damit ist $|h \circ f| = |h \circ g| \neq |h \circ f| \circ |g| = |h \circ g| \Rightarrow h \circ f \neq h \circ g$. ■

In Sets sind die Epimorphismen genau die surjektiven Abbildungen (wie Mon analog zum Beweis für Monomorphismen prüft). In Mon haben wir folgendes Beispiel:
 Sei $i: \mathbb{N} \rightarrow \mathbb{Z}$ die Abbildung von $(\mathbb{N}, +, 0)$ in $(\mathbb{Z}, +, 0)$.

Da $i|_1$ injektiv ist, ist i ein Monomorphismus in Mon.

Behauptung: i ist auch epi.

Wir zeigen: i kann rechts getilgt werden. Seien dazu $f, g: (\mathbb{Z}, +, 0) \rightarrow (\mathbb{N}, +, 0)$

Mit $f \circ i = g \circ i$, d.h. $f|_{\mathbb{N}} = g|_{\mathbb{N}}$. Wir wollen zeigen: $f = g$. Es gilt:

$$f(-n) = f((-1) + (-1) + \dots + (-1)) = f(-1) + f(-1) + \dots + f(-1) \text{ und analog } g(-n) = g(-1) + g(-1) + \dots + g(-1)$$

heißt es genügt zu zeigen $f(-1) = g(-1)$.

$$\begin{aligned} f(-1) &= f(\mathbb{N}) * u = f(-1) * g(\mathbb{N}) = f(-1) * g(1 - 1) = f(-1) * g(1) * g(-1) \\ &= f(1) * f(1) * f(-1) = 1 * g(-1) = g(-1). \end{aligned}$$

Also i epi, obwohl nicht surjektiv.

Proposition 11.2: Jeder Isomorphismus ist sowohl mono als auch epi.

(Vorlesung gilt i.A. nicht, nur in Sets.)

Beweis: Betrachte $A \xrightarrow[y]{\cong} B \xrightarrow{m} C$

Sei m Isomorphismus mit $c = m^{-1}$
 Falls $m \circ x = m \circ y \Rightarrow c \circ m \circ x =$
 $c \circ m \circ y = 1_B \circ x = 1_B \circ y = x = y$.
 und analog für n epi. □

Vie oben gesehen gilt die Umkehrung nicht!

Die Argumente in Prop 11.2 können auch separat betrachtet werden: Falls ein $f: A \rightarrow B$ ein Linksinverses g besitzt, d.h. zu $g: B \rightarrow A$ mit $g \circ f = 1_A$, dann ist f mono, und g epi.

Def 11.3 Ein Monomorphismus heißt split, falls er ein Linksinverses hat.

Epimorphismus

Rechtsinvers

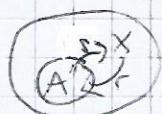
Wenn man Pfeile $r: X \rightarrow A$ und $s: A \rightarrow X$ mit $r \circ s = 1_A$ hat, dann heißt
 r Retraktion von s und s Schnitt von r. Das Objekt A heißt Retract von X.

Bsp: Diese Begriffe kommen aus der Topologie (Studium der Kategorie "Top").

→ einfaches Beispiel:

↓ Einbettung

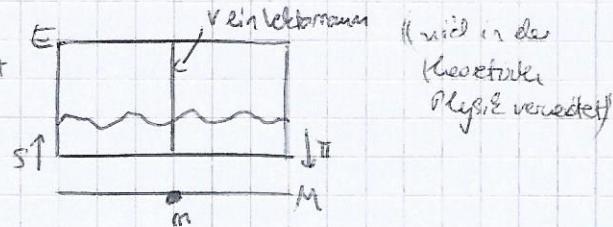
↑ Rückzug / Retraction



In der Kategorie Top der topologischen Räume mit stetigen Abbildungen gilt:

A ist Retrakt von $X \Leftrightarrow$ Jede stetige Abbildung $f: A \rightarrow Y$ lässt sich zu einer stetigen Abbildung $\tilde{f}: X \rightarrow Y$ erweitern ($\tilde{f} = f \circ r$).

Bsp.: Bündel über Mannigfaltigkeiten:
Ein Schnitt s assoziiert zu jedem Punkt von m einen Vektor in V bzw. einen Punkt in E , so dass gilt:
 $\pi \circ s = 1_m$.



Da Funktionenkomposition und Inversitäten erhalten, erhalten sie auch Split-Epi-Kat.
Monomorphismen: $r \circ s = 1_A \Rightarrow f(r) \circ f(s) = 1_{f(A)}$. Aber der vergessliche Funktor $\text{Mon} \rightarrow \text{Sets}$ bildet den Epimorphismus $N \rightarrow Z$ auf den nicht-Epimorphismus $|N| \rightarrow |Z|$ ab.

Bsp.: Jeder Monomorphismus in Sets $f: A \rightarrow B$ mit $A \neq \emptyset$ ist schon Split, d.h. zu einer injektiven Abbildung $f: A \rightarrow B$ gibt es ein Linksmusses $g: B \rightarrow A$ mit $gof = 1_A$.

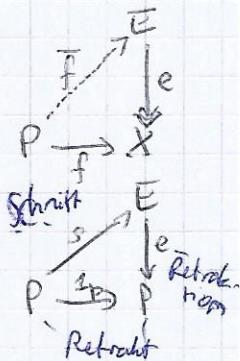
Die Bedingung "Jeder Epimorphismus ist split" kann als verallgemeinerte Auswählaktion gedeutet werden. Sei $e: E \rightarrow X$ epi in Sets. Dann existiert für jedes $x \in X$ "Auswahlrecht" ein mit-leeres Urbild $E_x = e^{-1}(x)$. Ein Schnitt von e ist eine Abbildung $r: X \rightarrow E$ mit $r \circ e = 1_X$, d.h. eine Auswahlfunktion mit $r(x) \in E_x \quad \forall x \in X$.
Sei nun $(E_x)_{x \in X}$ eine Familie von mit-leeren Mengen. Retrakte $E - \{r(x, y) \mid x \in X, y \in E_x\}$. Der Pfeil $e: E \rightarrow X$ ist injektiv (epi).
 $(x, y) \mapsto x$

Ein Schnitt von e ist eine Auswahlfunktion für die Familie $(E_x)_{x \in X}$.

Def. 11.4 Ein Objekt P ist projektiv falls für jeden Epimorphismus $e: E \rightarrow X$ und Pfeil $f: P \rightarrow X$ ein (nicht eindeutig erkenbarer) Pfeil $\tilde{f}: P \rightarrow E$ existiert mit $e \circ \tilde{f} = f$.

Merk: Jedes $f: P \rightarrow X$ kann entlang Epimorphismen geliftet werden.

Beh. falls $e: E \rightarrow P$ ein Epimorphismus ist und P projektiv, dann existiert ein Schnitt, d.h. e ist split. Die Definition sagt: $\exists s: P \rightarrow E$ mit $e \circ s = 1_P$.
(Nicht eindeutig. Schnitte sind Wahlmöglichkeiten, e ist ganz viele.)



Bsp.: - Projektive Objekte lassen mehr abgehende Pfeile zu als beliebige Objekte, sind also "freier" als beliebige Objekte da Relationen die abgehenden Pfeile einschränken.

- Homologistische Algebra: Projektive Auflösungen erlauben cf. Modulen zu verstehen:
 $\text{Mod} \rightarrow \text{Mod} \leftarrow \text{Proj} \leftarrow \text{P}_0 \leftarrow \text{P}_1 \leftarrow \text{P}_2 \leftarrow \dots$ (im \mathcal{C} wie \mathcal{C}_{Mod})

- In Sets ist Glanz des Auswählens jedes Objekt projektiv.
- In vielen algebraischen Strukturen / Kategorien (aber nicht allen Kategorien) sind freie Objekte (nicht definiert) projektiv.
- Die Pfeilartweise hat die Algebra vorangestellt. Ohne projektive Auflösungen hätte man die Klassifizierung der endlichen einfachen Gruppen wohl nicht fortführen können.

Def. 11.5 Sei \mathcal{C} eine Kategorie. Ein Objekt

- 0 in \mathcal{C} ist initial, falls für jedes Objekt C in \mathcal{C} ein eindeutiger Pfeil $0 \rightarrow C$ existiert.
- 1 in \mathcal{C} ist terminal, falls für jedes Objekt C in \mathcal{C} ein eindeutiger Pfeil $C \rightarrow 1$ existiert.

Bem. Dualität: initial in \mathcal{C} entspricht terminal in \mathcal{C}^{op}

Zwang: initiale und terminale Objekte sind (bis auf Isomorphie) eindeutig.

Bsp. - In Sets ist 0 initial und jede endliche Menge ist terminal (es gibt unendliche wie die sind alle isomorphe einzige Kategorien).

- In Cat, der Kategorie aller Kategorien, ist 0 initial und 1 terminal.

- In Groups ist die triviale einkreisige Gruppe sowohl initial als auch terminal. Analog auch für K -Vektorräume und Monide.

- In der Kategorie der Ringe (Kommutativ mit 1) ist \mathbb{Z} initial (da $\mathbb{Z} \rightarrow 0$, also neigt nur was für 0 nicht). Endring, da 0 auf 0 und 1 auf 1 abgesenkt wird. Das terminale Objekt ist der triviale Ring $\{0\}, 1\mathbb{Z}$.

- In einer partiell geordneten Menge ist ein initiales Objekt ein kleinstes Element und ein terminales Objekt ein größtes Element.

Was versteht damit, "Elemente" von Objekten in einer allgemeinen Kategorie zu definieren. In Sets sind Elemente von Mengen $1:1$ mit Pfeilen von endlichen Mengen. Allgemein verwenden wir Pfeile, die von terminalen Objekten ausgehen, zu nutzen.

Notation: in jeder Kategorie \mathcal{C} schreiben wir $\text{Hom}(A, B)$ für die Pfeile $A \rightarrow B$.

In Sets gilt: $X \cong \text{Hom}_{\text{Sets}}(1, X)$ für jede Menge X .

$$(mit X \leftrightarrow \mathbb{I}: 1 \rightarrow X)$$

$$X \mapsto \mathbb{I}$$

In einer Kategorie mit einem terminalen Objekt heißen die Pfeile $1 \rightarrow X$ globale Elemente, Punkte oder Kontakte.

In Sets, Rng und anderen Kategorien (aber nicht allen) sind Pfeile dadurch bestimmt, dass sie auf Punkten tun, d.h. durch ihre Komposition mit Punkten ("einsetzen").

Dann sind f,g: $A \rightarrow B$ gleich genau dann, wenn $f \circ a = g \circ a \forall a: 1 \rightarrow A$.

In Mon gilt dies nicht; da hier $1 = \{*\}$ sowohl initial als auch terminal ist, hat jedes Monid nur einen eindeutigen Punkt $1 \rightarrow M$ (da die Identität fixiert).

Def. 11.6 Ein verallgemeinertes Element eines Objektes A in einer Kategorie \mathcal{C} ist ein Pfeil, der bei A endet, d.h. $X \rightarrow A$ für beliebiges X .

Das genügt, um Pfeile zu unterscheiden:

Sei \mathcal{C} eine Kategorie. $f, g: C \rightarrow D$ seien Pfeile. Dann ist

$$f = g \Leftrightarrow f \circ x = g \circ x \quad \forall x: X \rightarrow C.$$

Beweis. \Rightarrow trivial

$$\nRightarrow f \neq g \Rightarrow f \circ 1_C \neq g \circ 1_C, \text{ also Gegenbeispiel.}$$

Das ist etwas albern, vielleicht sollte man sich auf weniger "Testpfeile" $T \rightarrow C$ für gewisse Testobjekte T einstricken?

In Mon genügen die Pfeile $M(1) \rightarrow M$, um Pfeile zu unterscheiden. ($M(1) \cong \mathbb{N}$)

D.h. f,g: $M \rightarrow M$ zwei Pfeile in Mon. Falls $f=g$, so auch $f \circ t = g \circ t \forall T: M(1) \rightarrow M$.

Andere Richtung Verallgemeinerte Elemente $T: M(1) \rightarrow M$ sind Bilder von \mathbb{N} in M .

Mit der universellen Eigenschaft von $M(1)$ gilt: $|M| \cong \text{Hom}_{\text{Sets}}(1, M) \cong \text{Hom}_{\text{Mon}}(M(1), M)$.

(Falls $f+g: M \rightarrow M$, existiert ein $m \in M$ mit

$$f(m) \neq g(m)$$

Da $f \circ m \neq g \circ m$.) \square

Allgemeine Produkte

Wie verallgemeinern das kartesische Produkt von Mengen.

Für abstrakte Kategorien ergibt sich das komponentenweise definierte direkte Produkt.

Def. 11.7: Sei \mathcal{C} eine Kategorie. Ein Produktdiagramm für Objekte A und B von \mathcal{C} besteht aus einem Objekt P und Pfeilen $A \xleftarrow{p_1} P \xrightarrow{p_2} B$, mit der folgenden universellen Eigenschaft: Falls $\Delta \xleftarrow{x_1} X \xrightarrow{x_2} B$ in \mathcal{C} existiert, dann gibt es einen eindeutigen Pfeil $x: X \rightarrow P$, so dass

$$\text{d.h. } x_1 = p_1 \circ x \text{ und } x_2 = p_2 \circ x.$$

Übung: Produkte sind bis auf Isomorphie eindeutig (zweimal UE anwenden, war ...)

Man schreibt: $P = A \times B$.

Abitung: Die Pfeile führen dazu. Falls $(A \times B, p_1, p_2)$ ein Produkt ist, und $Q \cong A \times B$ mit Isomorphismus $h: A \times B \xrightarrow{\cong} Q$, dann ist $(Q, p_1 \circ h, p_2 \circ h)$ (oder $A \xleftarrow{p_1 \circ h} Q \xrightarrow{p_2 \circ h} B$) auch ein Produktdiagramm.

(Jeder Pfeil, der in der direkten Produkt gilt, ist in Wirklichkeit genau zwei Pfeile $= \text{UE}$)

- Ein Pfeil in das Produkt $X \rightarrow A \times B$ ist ein Paar von Pfeilen $f: X \rightarrow A$ und $g: X \rightarrow B$. D.h., alle Pfeile von $X \rightarrow A \times B$ sind/können als Paare (f_1, f_2) geschaut werden.
- Pfeile aus Produkten $g: A \times B \rightarrow Y$ können als Funktionen mit 2 Argumenten gedeutet werden.

Bsp.: strukt in
als return
value vs.
einzelne
Attribut, und
nur bei Processor
Funktionen

Bsp.: Das kartesische Produkt von Mengen $A \times B = \{(a, b) : a \in A, b \in B\}$ hat das Diagramm $\Delta \xleftarrow{} A \times B \xrightarrow{} B$.

$$a \leftrightarrow (a, b) \leftrightarrow b$$

- Direkte Produkte von Gruppen, Vektorräumen, ...
- Produktkategorie: $\mathcal{C} \leftarrow \mathcal{C} \times \mathcal{D} \rightarrow \mathcal{D}$ analog zum kartesischen Produkt Paare von Objekten, ...
- (s. Anwesen: Lambek-Kalkül und Produktdatentypen)

Produkte müssen nicht existieren.

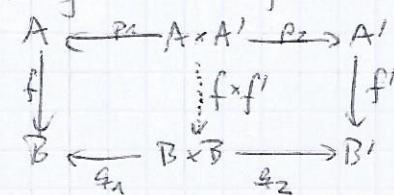
Def. 11.8: Eine Kategorie \mathcal{C} , in der zu je zwei Objekten ein Produkt existiert, heißt Kategorie mit eindimensionalen Produkten.

Zum Beweis: Man kann ternäre Produkte $A \times B \times C$ für drei Objekte und drei Pfeile $A \xleftarrow{p_1} A \times B \times C \xrightarrow{p_2} B \xrightarrow{p_3} C$ über die angegebene universelle Eigenschaft definieren. Dann zeigt man, dass $A \times B \times C \cong (A \times B) \times C$ und $(A \times B) \times C \cong A \times (B \times C)$, auch alle eindimensionalen Produkte.

Pfeile: Sei \mathcal{C} eine Kategorie mit eindimensionalen Produkten und $f: A \rightarrow B$ und $f': A' \rightarrow B'$

Pfeile. Dann existiert ein Pfeil $f \times f': A \times A' \rightarrow B \times B'$, nämlich $f \times f' = (f \circ p_1, f' \circ p_2)$ (denn Pfeile in das Produkt sind Paare von Pfeilen).

Dies bedeutet: Wenn wir für jedes Paar von Objekten ein Produkt wählen, erhalten wir einen



Faktor $\times: \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$. Zum Beweis der Tautorialität wird nur die universelle Eigenschaft verwendet. Man kann über eine universelle Eigenschaft auch allgemein über Mengen indizierte Produkte definieren. Also für I eine Indexmenge, Objekte $X_i: i \in I$ und Pfeile $p_i: \prod_{j \in I} X_j \rightarrow X_i$.

Hom: Sei \mathcal{C} eine Kategorie. Wir schreiben $\text{Hom}(A, B)$ für die Menge der Pfeile von A nach B .
 (A, B) Objekte von \mathcal{C} . Angenommen $\text{Hom}(A, B)$ ist für alle A, B eine Menge.
Dann ist $\text{Hom}(A, \cdot) : \mathcal{C} \rightarrow \text{Sets}$ ein Funktor! Auf Pfeilen $f : B \rightarrow C$ definiere wir dazu $\text{Hom}(A, f) : \text{Hom}(A, B) \rightarrow \text{Hom}(A, C)$

Dann ist $\text{Hom}(A, 1_B) = 1_{\text{Hom}(A, B)}$ und $\text{Hom}(A, g \circ f) = (g \circ f) \circ \text{Hom}(A, f)$. } $\text{Hom}(A, \cdot)$ ist ein Funktor.

Hom steht in enger Beziehung zum Produkt. Falls P ein Objekt ist und $P \xrightarrow{x} A$ und $P \xrightarrow{y} B$ Pfeile in \mathcal{C} sind; dann hat man ein Element $(x_1, x_2) \in \text{Hom}(P, A) \times \text{Hom}(P, B)$. Beide ein Pfeil $x : X \rightarrow P$ hat man 2 Kompositionen
insets $p_1 \circ x = x_1 : X \rightarrow A$ $p_2 \circ x = x_2 : X \rightarrow B$ \Downarrow definiert eine Abbildung $V_X = (\text{Hom}(X, p_1) \times \text{Hom}(X, p_2)) : \text{Hom}(X, P) \rightarrow \text{Hom}(X, A) \times \text{Hom}(X, B)$

Proposition 11.9: Ein Diagramm $A \leftarrow P \rightarrow B$ ist ein Produktdiagramm, also P ein Produkt, genau dann wenn für jedes Objekt X die Abbildung V_X ein Isomorphismus ist.

Beweis: Die universelle Eigenschaft des Produktes sagt genau, dass x aus (x_1, x_2) eindeutig rekonstruierbar ist.

Definition 11.10: Ein Funktor $F : \mathcal{C} \rightarrow \mathcal{D}$ erhält endliche Produkte, falls er jedes Produktdiagramm $A \leftarrow P \rightarrow B$ in \mathcal{C} auf ein Produktdiagramm $F(A) \leftarrow F(P) \rightarrow F(B)$ in \mathcal{D} abbildet.

Bew.: Es genügt zu prüfen: $F(A \times B) \cong F(A) \times F(B)$, so dass $F(p_1) \times F(p_2) : F(A \times B) \rightarrow F(A) \times F(B)$ ein Isomorphismus in \mathcal{D} ist.

Bsp: $\text{Hom}_e(X, \cdot)$ erhält endliche Produkte

- (1): $\text{Mon} \rightarrow \text{Sets}$ (der vergessende Funktor) erhält endliche Produkte

Allgemein kann Hom in der Kategorientheorie abstrakt folgendes Prinzip implementieren:
Ein mathematisches Objekt wird interviert mit Hilfe der Homomorphismen, die am Objekt ankommen oder losgehen.

12. Dualitätsprinzip

Die Dualitäten epi/mono bzw. initial/terminal sind nur die Spitze eines Dualitätsbergs. Dahinter steckt, dass die Axiome der Kategorientheorie invariant unter Umkehr von Pfeilen sind. In der Sprache haben wir Objekte, Pfeile, cod, dom, \circ , 1_A + PL1 (Prädikatelogik 1. Stufe) mit den Axiomen:

$$\begin{aligned} \text{(CT)} \quad & \text{dom}(1_A) = A, \text{cod}(1_A) = A \\ & f \circ 1_{\text{dom}(f)} = f, 1_{\text{cod}(f)} \circ f = f \\ & \text{dom}(f \circ g) = \text{dom}(g), \text{cod}(f \circ g) = \text{cod}(f) \\ & h \circ (g \circ f) = (h \circ g) \circ f \end{aligned}$$

Diese Axiome sind invariant unter der Dualität, die alle Pfeile umdreht, d.h. alle cod durch dom ersetzt, alle dom durch cod ersetzt und alle $f \circ g$ durch $g \circ f$.

Sei Σ eine wohlgeformte Aussage in der (Sprache der) Kategorientheorie und Σ^* ihre duale Aussage.

Satz 12.1: $(\text{CT}) \Rightarrow \Sigma \Rightarrow ((\text{CT}) \Rightarrow \Sigma^*)$
(Falls (CT) Σ beweist, beweist es auch Σ^*). \square

Diese Dualität liefert oft zwei Definitionen/Konzepte/Beweise zum Preis von einem.
 Aber Achtung: Es kann eine völlig andere aussehende Kategorie als \mathcal{C} sein.
 Daher bekommt man aus einem Beweis in \mathcal{C} meistens überraschende Erkenntnisse
 in \mathcal{C}^\perp .

Bsp.: Coproducte. Ein Coproductdiagramm $A \xrightarrow{g_1} Q \xleftarrow{g_2} B$ ist ein Diagramm mit: Für jedes Z mit $A \xrightarrow{z_1} Z \xleftarrow{z_2} B$ existiert ein einziges $u: Q \rightarrow Z$ so dass $z_1 \circ g_1 = u \circ g_1$ und $z_2 \circ g_2 = u \circ g_2$ kommutiert, d.h. $z_1 = u \circ g_1$. Man schreibt $A + B = Q$ und $u = (z_1, z_2)$ für das Coproduct. Als Objekt ist ein Coproduct ein Produkt in der dualen Kategorie.

"jetzt kontrolliert die ganze Sache nicht mehr selbst, weil ich nicht weiß, ob ich Coproduct mit C oder mit \mathcal{C}^\perp schreiben soll"

Bsp.: In Sets ist $A + B = A \cup B$ die disjunkte Vereinigung (d.h. von bedingt $\{(*, a)\} \cup \{(*, b)\}$, also $A \cup B = \{(a, *)\} \cup \{(*, b)\} | a \in A, b \in B\}$ mit $g_1: A \rightarrow A + B$, $g_2: B \rightarrow A + B$ $a \mapsto (a, *)$, $b \mapsto (*, b)$

Beim. Vereinigung wäre nicht universell, da z_1 und z_2 zwei unterschiedliche Bilder für das gleiche Element verlängern.

Das Coproduct ist bis auf Isomorphie eindeutig wegen Pkt 1.2.

In Mon: Proposition 12.2 Seien $M(A)$ und $M(B)$ freie Monoide. Dann gilt

$$M(A) + M(B) = M(A + B).$$

Beweis durch Diagrammjagd mit Häuschen: Betrachte:

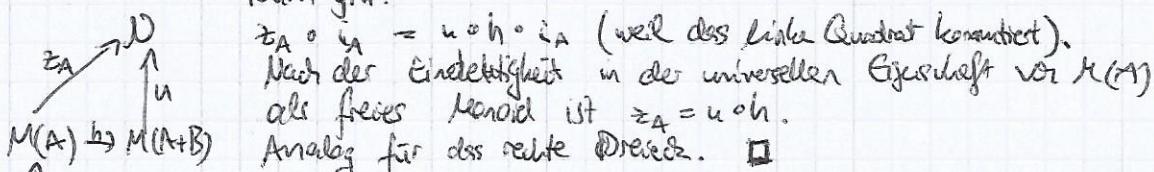
Betrachtung: $M(A+B)$ hat die universelle Eigenschaft des Coproducts von $M(A)$ und $M(B)$. Sei N ein beliebiges Monoid und $z_A: M(A) \rightarrow N$ und $z_B: M(B) \rightarrow N$.

Wir wollen ein einziges $u: M(A+B) \rightarrow N$, so dass die drei Dreiecke kommutieren.

Wegen der universellen Eigenschaft von $M(A)$ und $M(B)$ als freie Monoide und die ~~Quadrat~~-Pfeile $M(A) \rightarrow M(A+B) \leftarrow M(B)$ aus $g_1: A \rightarrow A+B$ und $g_2: B \rightarrow A+B$ eindeutig bestimmt. Wegen der universellen Eigenschaft von $A+B$ als Coproduct ist aus den Pfeilen z_A und z_B ein Pfeil $A+B \rightarrow N$ eindeutig bestimmt.

Wegen der universellen Eigenschaft von $M(A+B)$ als freies Monoid ist damit $u: M(A+B) \rightarrow N$ eindeutig bestimmt.bleibt zu prüfen, ob die drei Dreiecke kommutieren (hier nur links):

Dann gilt:



Achtung: Die Menge $|M(A) + M(B)|$ ist nicht das Coproduct $|M(A)| + |M(B)|$:

Bsp.: - In Groups ist das Coproduct das freie Produkt von Gruppen.
 - In AbGroups, also abelschen Gruppen, ist das Binäre Coproduct isomorph zum Produkt.

Beim. Die Proposition sagt aus: $M: \text{Sets} \rightarrow \text{Mon}$ (freies Monoid "Funktör") erhält endliche Coproducte. \rightsquigarrow dies führt zu Adjunktivitäten:
 Vorsichtiger Tipp: es freies Monoid, M \hookrightarrow runden in R , $V \hookrightarrow \mathbb{Z}$.

$$\begin{array}{c} N \\ \downarrow \\ 2 & \times & x & x \\ 1 & \times & x & x \\ 0 & \times & x & x \\ \hline & 1 & 2 & \dots \end{array}$$

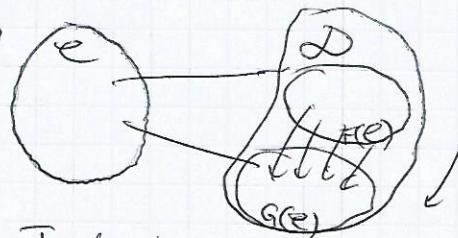
$N + M = M^N$
 Coproduct in Mon
 Coproduct in Sets
 $|M| + |N| = "2M"$

Prüfung: Satz 5.5 + freies Monoid
 letztere hierzu

Def. Seien $F, G: \mathcal{C} \rightarrow \mathcal{D}$ Funktoren. Eine natürliche Transformation ist eine Familie von Pfeilen $\eta_C: F(C) \rightarrow G(C)$ in \mathcal{D} , für jedes Objekt C in \mathcal{C} , so dass gilt $\eta_{C_2} \circ F(f) = G(f) \circ \eta_{C_1}$ für alle Pfeile $f: C_1 \rightarrow C_2$ in \mathcal{C} .

Diagramm:

$$\begin{array}{ccc} f: C_1 \rightarrow C_2 & \text{in } \mathcal{C} & \text{Natürliche Transforma-} \\ & \downarrow \eta_{C_1} \quad \uparrow F(f) & \text{tionen sind 'Pfeile' } \\ & \text{in } \mathcal{D} & \text{zwischen Funktionen:} \\ & \downarrow \eta_{C_2} & \\ G(C_1) & \xrightarrow{G(f)} & G(C_2) \end{array}$$



η_C heißt Komponente von η an C .

Komposition: $\eta: F \rightarrow G$ und $\theta: G \rightarrow H$ natürliche Transformationen.

Dann ist $\theta \circ \eta: F \rightarrow H$ natürliche Transformation.

Funktorenbedingung: $F, G: \mathcal{C} \rightarrow \mathcal{D}$, $\eta: F \rightarrow G$ natürliche Transformation, $H: \mathcal{D} \rightarrow \mathcal{E}$ ein Funktor.

$H\eta: H \circ F \rightarrow H \circ G$ definiert durch $(H\eta)_C = H(\eta_C)$.

Analog, falls $E: \mathcal{B} \rightarrow \mathcal{C}$, so ist $\eta_E: F \circ E \rightarrow G \circ E$ natürliche Transformation mit Komponente $(\eta_E)_B = \eta_{E(B)}$.

Def. (Adjunktion)

Seien \mathcal{C} und \mathcal{D} Kategorien, 2 Funktoren $F: \mathcal{D} \rightarrow \mathcal{C}$, $G: \mathcal{C} \rightarrow \mathcal{D}$, natürliche Transformationen $\nu: 1_{\mathcal{D}} \rightarrow G \circ F$ und $\mu: F \circ G \rightarrow 1_{\mathcal{C}}$,

für die gilt: $\nu F \circ \mu_F = 1_F$ und $\mu_G \circ G\nu = 1_G$.

Dann heißt F linksadjungiert zu G .

G rechtsadjungiert zu F ,

ν Einheit, μ Co-Einheit.

Komponenten von $(\nu F \circ \mu_F)_{\mathcal{D}} = (\nu F)_{\mathcal{D}} \circ (\mu_F)_{\mathcal{D}} = \nu_{F(\mathcal{D})} \circ F(\mu_{\mathcal{D}})$.

$\sim \text{LE FIN} \sim$