§2. Einige Anwendungen der Galoistheorie

2.1 Theorem (Fundamentalsatz der Algebra): Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

Beweis: $\mathbb{C}$ ist definiert als $\mathbb{R}(i) = \mathbb{R}[i]$, wobei $\mathbb{R}$ wie in der Analysis durch Cauchy-Folgen definiert ist, d.h. durch die nicht-algebraische Eigenständigkeit.

Der Beweis verwendet zwei Eigenschaften von $\mathbb{R}$:

(1) $f(x) \in \mathbb{R}[x]$ mit ungeradem Grad hat eine Nullstelle in $\mathbb{R}$

(2) Jede positive reelle Zahl hat eine Quadratwurzel

Begründung von (1) und (2):

Sei $f(x) = \sum_{j=0}^{n} a_j x^j$ mit $a_n \neq 0$, also $f(x) = a_n x^n \left(1 + \sum_{j=0}^{n-1} \frac{a_j}{a_n} \cdot x^{j-n}\right)$ $\quad x \neq 0$

Für $|x| \gg 0$ werden die Werte $\quad$ ↑ jetzt als Funktion betrachtet

von $|f(x)|$ also auch sehr groß. Ist n ungerade $\Rightarrow f(x)$ nimmt beliebig große und beliebig kleine Werte an, wegen der Vollständigkeit von $\mathbb{R}$ (Zwischenwertsatz) also auch den Wert 0. $\Rightarrow$ (1)

(2) bedeutet: $\mathbb{R}_{\geq 0}$ ist das Bild der Funktion $f(x) = x^2$. Auch das folgt wieder aus dem Zwischenwertsatz.

Jetzt kommt der (algebraische) Hauptteil des Beweises:

Sei $L/\mathbb{C}$ algebraisch. zz $L = \mathbb{C}$. Wir können auch $L/\mathbb{C}$ endlich annehmen sowie $L/\mathbb{C}$ normal, warum?, auch $L/\mathbb{R}$ normal (kann vorausgesetzt werden.

Sei $[L:\mathbb{R}] = 2^k \cdot m$ mit m ungerade und $k \geq 1$.

$[L:\mathbb{C}] \cdot [\mathbb{C}:\mathbb{R}]$

Sei $G = Gal(L/\mathbb{R})$, also $|G| = 2^k \cdot m$.

Sylowsätze $\Rightarrow \exists\, H \subset G$ mit $|H| = 2^k$ warum?

Galoiskorrespondenz $\Rightarrow \mathbb{R} \subset L^H \subset L$ mit $[L:L^H] = |H| = 2^k \Rightarrow [L^H:\mathbb{R}] = m$

$\mathrm{char}(L^H) = 0 \Rightarrow L^H$ separabel, also kann der Satz vom primitiven Element angewandt werden $\Rightarrow \exists a: L^H = \mathbb{R}(a)$, mit Minimalpolynom $f(x) = m_{a,\mathbb{R}}(x)$.

$f(x)$ hat Grad $m = [L^H:\mathbb{R}]$ und ist irreduzibel.

(1) $\Rightarrow$ f hat eine Nullstelle in $\mathbb{R}$ – aber f ist irreduzibel

$\Rightarrow f$ ist linear $\Rightarrow m=1$ und $L^4=\mathbb{R}$

$\Rightarrow [L:\mathbb{R}]=2^k$ und zu zeigen ist $k=1$

Aus (2) folgt, daß jede komplexe Zahl eine Quadratwurzel hat:

Sei $z=x+iy$ mit $x,y\in\mathbb{R}$. Dann ist $z=(a+bi)^2$ mit

$$a^2=\frac{1}{2}x\pm\frac{1}{2}\sqrt{x^2+y^2} \quad \text{und} \quad b^2=-\frac{1}{2}x\pm\frac{1}{2}\sqrt{x^2+y^2}$$

und a und b existieren nach (2). nachprüfen (oder Polarkoordinaten benutzen)

Daraus folgt: $\mathbb{C}$ hat keine Erweiterungen $L/\mathbb{C}$ mit $[L:\mathbb{C}]=2$. warum?

Also ist $[L:\mathbb{C}]=2^{k-1}$ mit $k\geq 2$, mindestens vom Grad 4, oder schon $L=\mathbb{C}$.

Wieder mit den Sylowsätzen folgt: Es existiert eine Untergruppe $U<\mathrm{Gal}(L/\mathbb{C})$ mit Ordnung $|U|=2^{k-2}$.

$\Rightarrow \exists$ Kette von Erweiterungen

$$\underbrace{\mathbb{R}}_{2}\subset\underbrace{\mathbb{C}}_{d}\subset\underbrace{L^U}_{2^{k-2}}\subset L \qquad \Rightarrow \underset{[L^U:\mathbb{C}]}{d}=2 \quad \lightning$$

$\Rightarrow$ Es bleibt nur der Fall $L=\mathbb{C}$. $\square$

Sei L/K eine Körpererweiterung. Eine K-Basis von L kann man induktiv über eine Kette von zwischen Körpern bestimmen wie? oder indem man ein primitives Element findet und dann?
Galoistheorie liefert noch eine andere Möglichkeit:

2.2 Theorem: Sei K ein unendlicher Körper, L/K eine Galois-Erweiterung mit Galoisgruppe $Gal(L/K) = G = \{\sigma_1 = id, \sigma_2, \dots, \sigma_n\}$. Dann gibt es ein $a \in L$, sodaß $\sigma_1(a) = a, \sigma_2(a), \dots, \sigma_n(a)$ eine K-Basis von L ist.
Eine solche Basis wird Normalbasis von L über K genannt.
(Der Satz gilt auch für K endlich, aber mit einem anderen Beweis.)

Der Beweis von 2.2 verwendet eine Technik aus der Darstellungstheorie von Gruppe, die zuerst eingeführt wird. Danach folgt dann der Beweis von 2.2.

Sei K ein Körper und G eine Gruppe. Die Menge $K^G = \{f: G \to K \text{ Abbildung}\}$ ist ein K-Vektorraum durch $(f+g)(x) := f(x) + g(x)$ für $x \in G$ und $(\lambda f)(x) := \lambda \cdot f(x)$ nachprüfen

2.3 Definition: Eine Abbildung $\chi: G \to K^* = K^\times$ (= inv.bare Elemente) heißt Charakter (von G), wenn χ multiplikativ ist: $\chi(xy) = \chi(x) \cdot \chi(y)$ $\forall x, y \in G$. und $\chi(1_G) = ?$

"chi"

↑ das ist ein Spezialfall der Definition in der Darstellungstheorie

2.4 Proposition: Seien $\chi_1, \dots, \chi_n$ paarweise verschiedene Charaktere.
Dann sind $\chi_1, \dots, \chi_n$ linear unabhängige Elemente von K^G.
Beweis: Angenommen $\chi_1, \dots, \chi_n$ sind linear abhängig.
$\Rightarrow \exists r$ minimal sodaß $\chi_1, \dots, \chi_r$ linear abhängig sind, o.B.d.A (wenn nötig, neu indizieren)
Falls $r = 1$: $\exists c_1 \neq 0 \in K$ mit $c_1 \chi_1 = 0$, d.h. $c_1 \chi_1(g) = 0$ $\forall g \in G$
$\Rightarrow \chi_1 = 0$, aber $\chi_1: G \to K^*$ ↯
Also muß $r \geq 2$ sein. $\exists c_1, \dots, c_r \in K: \sum_{j=1}^{r} c_j \chi_j = 0$, alle $c_j \neq 0$ (da r minimal)
$\chi_1, \dots, \chi_r$ sind paarweise verschiedene Abbildungen
$\Rightarrow \exists h \in G: \chi_1(h) \neq \chi_r(h)$

$$\sum_{j=1}^{r} c_j \chi_j = 0 \Rightarrow \forall g \in G: \; 0 = \sum_{j=1}^{r} c_j \chi_j(hg) = \sum_{j=1}^{r} c_j \chi_j(h)\chi_j(g)$$

$$\overset{\forall g}{\Rightarrow} \quad 0 = \Big(\sum_{j=1}^{r} c_j \chi_j(g)\Big)\cdot \chi_r(h) = \sum_{j=1}^{r} c_j \chi_r(h)\chi_j(g)$$

Subtrahieren

$$\Rightarrow \qquad 0 = \sum_{j=1}^{r-1} c_j \big(\chi_j(h) - \chi_r(h)\big)\chi_j(g) \quad \forall g \in G$$

r minimal $\Rightarrow \chi_1, \dots, \chi_{r-1}$ linear unabhängig $\Rightarrow 0 = c_j(\chi_j(h) - \chi_r(h)) \; \forall j$,

insbesondere $0 = c_1 \underbrace{(\chi_1(h) - \chi_r(h))}_{\neq 0} \neq 0$ ↯ □

Das ist allgemein sehr nützlich, um Gruppen zu untersuchen. Nur hilft es durch die folgenden Konsequenzen weiter:

2.5 Korollar: Sei K ein Körper, $\sigma_1, \dots, \sigma_n \in \mathrm{Aut}(K)$ paarweise verschieden. Dann sind $\sigma_1, \dots, \sigma_n \in K^K$ linear unabhängig (über K).

Ist das nicht ein Widerspruch zu $\mathrm{Hom}_K(K,K) \simeq K$ als K-Vektorraum?

Beweis: Einschränkung von $\sigma_i : K \to K$ auf $\sigma_i : K^* \to K^*$ definiert einen Charakter von K^*. Diese Charaktere sind auch paarweise verschieden, also folgt die Behauptung aus 2.4. □ Details nochprüfen

2.6 Korollar: Sei $L|K$ eine separable Erweiterung vom Grad n und $\sigma_1, \dots, \sigma_n$ die verschiedenen K-Homomorphismen von L in $\bar{K}$. Seien $v_1, \dots, v_n \in L$, n verschiedene Elemente. Dann gilt:

$v_1, \dots, v_n$ bilden eine K-Basis von $L \Leftrightarrow \det\big((\sigma_i(v_j))_{ij}\big) \neq 0$.

Beweis: Seien $v_1, \dots, v_n$ keine Basis, also linear abhängig warum?

$\Rightarrow \exists \lambda_1, \dots, \lambda_n \in K$, nicht alle 0, sodaß $\sum_{j=1}^{n} \lambda_j v_j = 0$

$$\Rightarrow \forall i: \; 0 = \sigma_i\Big(\sum_{j=1}^{n} \lambda_j v_j\Big) = \sum_{j=1}^{n} \lambda_j \underbrace{\sigma_i(v_j)}_{\text{Spalte in } (\sigma_i(v_j))_{ij}}$$

$$\Rightarrow \det\big((\sigma_i(v_j))_{ij}\big) = 0$$

Seien $v_1, \dots, v_n$ eine K-Basis von L, zz $\det((\sigma_i(v_j))_{i,j}) \neq 0$.
Angenommen $\det((\sigma_i(v_j))_{i,j}) = 0$. Dann sind die Zeilen der Matrix $(\sigma_i(v_j))_{i,j}$ linear abhängig $\Rightarrow \exists \lambda_1, \dots, \lambda_n \in K$, nicht alle 0, so daß

$$\sum_{i=1}^{n} \lambda_i \sigma_i(v_j) = 0 \quad \forall\, 1 \leq j \leq n$$

Behauptung: sogar $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$

Denn: Für $\mu_1, \dots, \mu_n \in K$ gilt mit $v = \sum_{j=1}^{n} \mu_j v_j$ (also für jedes $v \in L$): (warum?)

$$\left(\sum_{i=1}^{n} \lambda_i \sigma_i\right)(v) = \sum_{i,j=1}^{n} \lambda_i \mu_j \sigma_i(v_j) = \sum_{j=1}^{n} \mu_j \left(\sum_{i=1}^{n} \lambda_i \sigma_i(v_j)\right) = 0$$

$\Rightarrow$ die Charaktere $\sigma_i : L^* \longrightarrow \bar{K}$ sind linear abhängig $\lightning$ (Widerspruch wozu?) $\square$

Beweis von Theorem 2.2 (Existenz von Normalbasen):
Gesucht ist ein $a \in L$ mit $\det(\sigma_i(\sigma_j(a))_{i,j}) \neq 0$. Dann folgt aus Korollar 2.6, daß die $\sigma_j(a)$ eine Basis von L über K bilden.
Nach dem Satz vom primitiven Element $\exists b \in L: L = K(b)$, eine einfache Erweiterung. Sei $f = m_{b,K}$ das Minimalpolynom von b.
Sei $b_i := \sigma_i(b)$ für $i = 1, \dots, n$. Die b_i sind Nullstellen von ~~f~~ $m_{b,K}$ und sie sind paarweise verschieden. warum?
$\deg f = [L:K] = n \Rightarrow f(x) = \prod_{i=1}^{n} (x - b_i)$
Die einfache Erweiterung $L = K(b)$ hat K-Basis $1, b, b^2, \dots, b^{n-1}$. Daraus können wir nicht schliessen, daß die b_i eine Basis bilden. Da es im Allgemeinen viele primitive Elemente gibt, wäre $a = b$ eine zu optimistische Wahl. Gesucht ist eine Konstruktion, die $b_1, \dots, b_n$ als Input hat und daraus neue Vektoren produziert, die mit Korollar 2.6 als Basis nachgewiesen werden können.
Für $1 \leq j \leq n$ sei $g_j := \prod_{i \neq j} \frac{x - b_i}{b_j - b_i} \in L[x]$, Polynome mit Koeffizienten in L

Dann gilt $g_j(b_i) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ nachprüfen

Behauptung: $g_1 + \dots + g_n = 1$, konstantes Polynom (*)

Begründung: $\deg g_i \leq n-1 \ \forall i$, also $\deg(g_1 + g_2 + \dots + g_n - 1) \leq n-1$,
aber $(g_1 + \dots + g_n - 1)(b_i) = 0$ für $b_1, \dots, b_n$, d.h. n verschiedene Nullstellen
$\Rightarrow g_1 + \dots + g_n - 1 = 0$ ✓

Sei $\sigma \in G = Gal(L/K)$, $c \in L$ und $h \in L[x]$. Dann ist $\sigma^*(h)(\sigma(c)) = \sigma(h(c))$
warum?

Behauptung: $\forall j: g_j = \sigma_j^*(g_1)$.

Begründung (recycle das vorige Argument!):
$\sigma_j^*(g_1)(b_j) = \sigma_j^*(g_1)(\sigma_j(b_1)) = \sigma_j(g_1(b_1)) = \sigma_j(1) = 1$
und für $i \neq j$ $\exists k \neq 1: b_i = \sigma_j(b_k)$ und $\sigma_j^*(g_1)(b_i) = \sigma_j(g_1(b_k)) = \sigma_j(0) = 0$
weiter wie oben ✓ Details?

Aus $g_j = \sigma_j^*(g_1)$ folgt $\forall u \in K: g_j(u) = \sigma_j^*(g_1(u)) = \sigma_j(g_1(u))$ – dieses
Element muß nicht in K liegen.

Unser Ziel: Finde ein $u \in K$ mit $\det(\sigma_i(\underbrace{\sigma_j(g_1(u))}_{g_j(u)})) = \underbrace{\det(\sigma_i(g_j(u)))}_{u} \neq 0$
Dann können wir $a := g_1(u)$ wählen
und sind fertig, wegen 2.6.
$\det(\sigma_i^*(g_j)(u))$

Ein einziges ureicht.

Aber $\det(\sigma_i^*(g_j)) \in L[x]$, ein Polynom. Also gibt es zwei Fälle:
Entweder ist $\det(\sigma_i^*(g_j))$ das Nullpolynom, dann ist unsere Strategie
gescheitert. Oder $\det(\sigma_i^*(g_j)) \neq 0 \Rightarrow \exists u \in K: \det(\sigma_i^*(g_j)(u)) \neq 0$
warum?

Sei $A := (\sigma_i^*(g_j))_{ij} \in Mat(n \times n, L[x])$

Behauptung: $\det(A) \neq 0$

Beweis: Für $i \neq j$ ist $g_i g_j(b_k) = 0 \ \forall k$ warum?

f war definiert als $\prod_u (x - b_u) \Rightarrow f \mid g_i g_j$, d.h. $g_i g_j \equiv 0 \pmod f$ für $i \neq j$
(**)

Aus (*) $g_1 + \dots + g_n = 1$ folgt $g_i(g_1 + \dots + g_n) = g_i$

$\Rightarrow g_i^2 \equiv g_i \pmod f \ \forall i$ (***)

Wir wollen zeigen, daß $\det(A) \neq 0$. Genauso können wir zeigen:
Für $B := A \cdot A^t$ gilt $\det(B) \neq 0$. Wir werden zeigen:
↑ transponiert
$\det(B) \equiv 1 \pmod f$

Sei also $B = A \cdot A^t$, $B = (b_{ij})$ mit

$$b_{ij} = \sum_{k=1}^{n} \sigma_i^*(g_k)\sigma_j^*(g_k) = \sum_{k=1}^{n} (\sigma_i\sigma_k)^*(g_1)(\sigma_j\sigma_k)^*(g_1)$$ nachprüfen

$\sigma_i\sigma_k$ ist wieder ein Gruppenelement, Bezeichnung: $\sigma_i\cdot\sigma_k = \sigma_{m(i,k)}$,

also $(\sigma_i\sigma_k)^*(g_1) = \sigma^*_{m(i,k)}(g_1) = g_{m(i,k)}$

das ist nur umständliche Buchhaltung, aber trotzdem genau nachzuprüfen

$$\Rightarrow b_{ij} = \sum_{k=1}^{n} g_{m(i,k)}\, g_{m(j,k)}$$

Für $i \neq j$ ist $\sigma_i\sigma_k \neq \sigma_j\sigma_k \;\forall k \Rightarrow m(i,k) \neq m(j,k)$

$$\overset{(**)}{\Rightarrow} b_{ij} \equiv 0 \pmod{f}$$

Für $i = j$ $\overset{(**)\text{ und }(*)}{\Longrightarrow}$ $b_{ii} \equiv \sum_{k=1}^{n} g^2_{m(i,k)} = 1 \pmod{f}$

Insgesamt also: modulo f hat B Diagonaleinträge 1
und außerhalb der Diagonale 0

Also: $B \equiv$ Einheitsmatrix $\pmod{f}$

$\Rightarrow \det(B) \equiv 1 \pmod{f}$ – also nicht 0

$\Rightarrow 0 \neq \det(B) = \det(A)\det(A^t) \Rightarrow \det(A) \neq 0$ □

Die dritte Anwendung betrifft geometrische Konstruktionen mit Zirkel und Lineal. In Algebra wurde definiert:
Sei $0,1 \in M \subset \mathbb{C} = \mathbb{R}^2$. $Kon(M) := \{p \in \mathbb{R}^2 : p$ ist aus M in endlich vielen Schritten mit Zirkel und Lineal konstruierbar$\}$
Dann wurde gezeigt: $Kon(M)$ ist ein Körper, genauer ein Teilkörper von $\mathbb{C}$, und enthält $\mathbb{Q}$ als Teilkörper, sogar $\mathbb{Q}(M \cup \bar{M})$ als Teilkörper.
($\bar{\ }$ komplexe Konjugation)
Die entscheidende Charakterisierung von Konstruierbarkeit ist dann:
Eine komplexe Zahl $z \in \mathbb{C}$, als Punkt in $\mathbb{R}^2$ verstanden, ist genau dann aus M konstruierbar, wenn es eine Kette von Körpererweiterungen gibt

$$\mathbb{Q}(M \cup \bar{M}) = L_0 \subset L_1 \subset \dots \subset L_r \quad (\text{für ein } r \in \mathbb{N})$$

so daß $z \in L_r$ und $\forall j : [L_j : L_{j-1}] \leq 2$.
Daraus erhält man z.B. die Unmöglichkeit der Würfelverdopplung.
Diese Beweise brauchen keine Galoistheorie, sondern nur die allgemeine Theorie der Körpererweiterungen.
Mit Galoistheorie kann man weitere Unmöglichkeitsfragen und - wie im folgenden Beispiel - die Unmöglichkeit einer Konstruktion sogar genau charakterisieren.

Sei $M = \{0,1\}$, also $\mathbb{Q}(M \cup \bar{M}) = \mathbb{Q}$, $n \in \mathbb{N}$, $n \geq 2$.
Problem: Kann man mit Zirkel und Lineal ein regelmäßiges n-Eck konstruieren?
Anders gesagt: Sind die n-ten Einheitswurzeln $\zeta_n = e^{2\pi i/n}$ aus $M = \{0,1\}$ aus mit Zirkel und Lineal konstruierbar? Hängt das von n ab?
$n = 2, 3, 4, 5, 6$: relativ leicht
Gauss (1796): geht nicht für $n = 7$, aber für $n = 17$
Das Problem muss also so formuliert werden: Für welche n ist ζ_n mit Zirkel und Lineal konstruierbar?

Die bisherigen Unmöglichkeitsbeweise zeigten immer, daß der Grad einer Körpererweiterung keine Zweierpotenz war, also eine bestimmte Zahl nicht konstruierbar ist. Für eine Charakterisierung braucht man auch die Umkehrung. Das ist ein Beitrag der Galoistheorie.

2.7 Proposition: Sei $0,1 \in M \subset \mathbb{C}$, $K = \mathbb{Q}(M \cup \bar{M})$, $z \in \mathbb{C}$ algebraisch über K, $f \in K[X]$ das Minimalpolynom von z und $L > K$ der Zerfällungskörper von f. Sei $[L:K]$ eine Potenz von 2. Dann ist $z \in \mathrm{Kon}(M)$.

Beweis: L/K ist eine Galoiserweiterung, also $|G| = [L:K]$ für $G = \mathrm{Gal}(L/K)$, d.h. $|G|$ ist eine Zweierpotenz.

In Algebra wurde (z.B. mit der Klassengleichung) gezeigt: Für jede Primzahl p und jede p-Gruppe P ist das Zentrum $Z(P)$ nicht-trivial. $P/Z(P)$ ist wieder eine p-Gruppe, also erhält man induktiv eine Kette von Normalteilern.

Für $G = \mathrm{Gal}(L/K)$ also: $\{id_L\} = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_r = G$ mit $|N_j / N_{j-1}| = 2$, für alle j. Details der Konstruktion dieser "Normalreihe"?

Die Bijektion β im Hauptsatz der Galoistheorie macht daraus eine Kette von Körpererweiterungen (welcher Körper ist $\beta(N_j)$?)

$$K = L_0 \subset L_1 \subset \dots \subset L_r = L$$

mit $[L_{i+1} : L_i] = 2$. Folglich ist $z \in \mathrm{Kon}(M)$. □

Wie wird die in Algebra gegebene Charakterisierung durch 2.7 verbessert?

Um 2.7 anzuwenden, muß also $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ bestimmt werden.

2.8 Proposition: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^*| = |\{j : 1 \le j \le n, \ ggT(j,n) = 1\}|$.

($(\mathbb{Z}/n\mathbb{Z})^*$: multiplikativ invertierbare Elemente in $\mathbb{Z}/n\mathbb{Z}$; $ggT(j,n)=1$: d.h. j und n sind teilerfremd)

In der Zahlentheorie wird diese Zahl mit $\varphi(n)$ bezeichnet (Eulersche φ-Funktion).

Aus 2.8 (noch zu beweisen) folgt:

2.9 Theorem: Für $n \geq 2$ ist das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beispiele: 5-Eck und 17-Eck sind konstruierbar, 7-Eck und 9-Eck nicht

Für welche n ist $\varphi(n)$ eine Zweierpotenz? Das ist eine zahlentheoretische Frage.

Spezialfall: $n = p$ Primzahl, also $\varphi(p) = p-1$ warum?

Behauptung: Sei p prim, $p > 2$, $p-1$ eine Zweierpotenz. Dann ist

$$p = 2^{2^n} + 1 \text{ für ein } n \in \mathbb{N}.$$

Beweis: Nach Voraussetzung ist $p = 2^m + 1$ für ein m. Zu zeigen: m ist eine Zweierpotenz, $m = 2^n$ für ein n. Wenn nicht: m hat dann einen ungeraden Teiler $k \geq 3$, d.h. $m = k \cdot \ell$ und daher

$$p = 2^{k\ell} + 1 = \underbrace{(2^\ell + 1)}\,(2^{(k-1)\ell} - 2^{(k-2)\ell} \pm - + 2^{2\ell} - 2^\ell + 1)$$

$1 < 2^\ell + 1 < 2^{k\ell} + 1 \Rightarrow p$ nicht prim $\lightning$

Primzahlen von der Form $2^{2^n}+1 =: F_n$ heißen Fermatsche Primzahlen.

F_0 bis F_4 sind Primzahlen, F_5 bis F_{11} nicht, was danach kommt, weiß man nicht.

2.10 Proposition: $\varphi(n)$ ist genau dann eine Potenz von 2, wenn

$$n = 2^m \cdot p_1 \cdot \ldots \cdot p_r \text{ für ein } m \in \mathbb{N} \text{ und } p_1, \ldots, p_r \text{ paarweise}$$

verschiedene Fermatsche Primzahlen.

Beweis: Sei $n = p_1^{\ell_1} \cdot \ldots \cdot p_r^{\ell_r}$ Primfaktorzerlegung $\Rightarrow$ Zahlentheorie oder Gruppentheorie (abelsche Gruppen)

$\varphi(n) = p_1^{\ell_1 - 1} \cdot \ldots \cdot p_r^{\ell_r - 1} \cdot (p_1 - 1) \cdot \ldots \cdot (p_r - 1)$. $\Rightarrow \varphi(n)$ ist eine Zweierpotenz genau dann, wenn für alle $p_j \neq 2$: $\ell_j = 1$ und $(p_j - 1)$ eine Potenz von 2, d.h. nach der Behauptung oben p_j eine Fermatsche Primzahl. $\square$

Jetzt fehlt noch ein Beweis von Proposition 2.8:

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \text{ für } \zeta_n = e^{2\pi i/n}$$

Sei nfest. $\zeta_n = e^{2\pi i/n}$ ist eine n-te Einheitswurzel, dh. eine Nullstelle von $x^n - 1 \in \mathbb{Q}[x]$. $x^n - 1$ ist nicht irreduzibel, z.B. ist 1 immer eine Nullstelle, wir müssen genauer hinschauen.

Alle n-ten Einheitswurzeln sind von der Form $e^{2\pi i/n \cdot j}$ für $j \in \mathbb{Z}$.

Genauer: $\pi: \mathbb{Z} \to \mathbb{C}$, $j \mapsto e^{2\pi i/n \cdot j}$ ist ein Gruppenhomomorphismus nachprüfen
Addition Multiplikation
dessen Bild genau die n-ten Einheitswurzeln sind.

Der Kern von π ist $n\mathbb{Z}$, also ist $\bar{\pi}: \mathbb{Z}/n\mathbb{Z} \to C_n = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\} \subset \mathbb{C}$ ein Gruppenisomorphismus. Details?

C_n ist zyklisch, erzeugt z.B. von $\pi(1) = \zeta_n$, aber natürlich auch von jedem $\pi(m)$ mit $ggT(n,m) = 1$ (und von keinem anderen $\pi(m)$). warum?

Die Restklassen $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ mit $ggT(n,m) = 1$ sind genau die invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$, d.h. die Elemente in $(\mathbb{Z}/n\mathbb{Z})^\times$, wie z.B. aus dem Euklidischen Algorithmus folgt. warum?

Die Bilder $\pi(m) = \zeta_n^m$ heißen <u>primitive Einheitswurzeln</u>, genauer erzeugen C_n.
Die Eulersche φ-Funktion zählt also genau die primitiven Einheitswurzeln.
Bezeichnung: $C_n^\times = \{\zeta_{n,1}, \dots, \zeta_{n,\varphi(n)}\}$ seien die primitiven n-ten Einheitswurzeln.

Unser Ziel ist zu zeigen: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ ist der Grad des Minimalpolynoms von ζ_n, also versuchen wir das zu bestimmen. Es muß ein Teiler von $x^n - 1$ sein.

Kandidat: $\Phi_n(x) := (x - \zeta_{n,1})(x - \zeta_{n,2}) \cdots (x - \zeta_{n,\varphi(n)}) \in \mathbb{C}[x]$.

heißt das <u>n-te Kreisteilungspolynom</u>

Beispiele:

$n = 1$	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$ nachrechnen
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$

Die Koeffizienten sind nicht immer $\in \{0,1,-1\}$. Beispiel: Φ_{105} nachrechnen oder in Bosch Algebra-Buch nachschauen

Behauptung: $\forall n \in \mathbb{N}$ ist $\Phi_n \in \mathbb{Z}[x]$ und normiert.

Beweis: $x^n - 1 = \prod_{\zeta \text{ n-te Einheitswurzel}} (x-\zeta) = \prod_{d|n} \Phi_d = \Phi_n \cdot \prod_{d|n, d<n} \Phi_d$ warum?

$\Rightarrow \Phi_n$ kann rekursiv berechnet werden als $x^n-1 \,/\, \prod_{d|n, d<n} \Phi_d$

x^n-1 und Φ_1 sind normiert, in $\mathbb{Z}[x]$

$\Rightarrow$ alle Φ_d, $d|n$, normiert und in $\mathbb{Z}[x]$ ✓ Division mit Rest nachprüfen

2.11 Theorem: Für jedes n ist das Kreisteilungspolynom $\Phi_n \in \mathbb{Z}[x]$ irreduzibel. Insbesondere ist Φ_n Minimalpolynom aller primitiven n-ten Einheitswurzeln. Außerdem ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

(2.8 ist also damit nachgewiesen)

Beweis: $x^n - 1 = (x-1) \cdot \underbrace{(x^{n-1} + x^{n-2} + \dots + x + 1)}_{\text{Bez: } f_n}$

Spezialfall: $n = p$. $\varphi(p) = p-1$, d.h. f_p hat die richtigen Nullstellen, nämlich die Elemente in $\mathbb{C}_p^\times \Rightarrow \Phi_p = f_p$, nach dem Kriterium von Eisenstein ist $f_p = \Phi_p$ irreduzibel.

Allgemeiner Fall: $\mathbb{C}_n^\times = \{\zeta_n^e : ggT(e,n) = 1, e \in \mathbb{N}\}$

$= \{\zeta_n^{p_1 \cdots p_r} : r \in \mathbb{N}, p_i | n, p_i \text{ prim}\}$ ← nicht notwendig verschiedene Primzahlen

ζ, nicht Zeta

Behauptung: Sei $\zeta \in \mathbb{C}_n^\times$, $m \in \mathbb{Q}[x]$ das Minimalpolynom von ζ, p prim mit $p \nmid n \Rightarrow m$ ist auch das Minimalpolynom von ζ^p, d.h. $m(\zeta^p) = 0$.

Aus der Behauptung folgt das Theorem: Denn dann sind all $\zeta_n^{p_1 \cdots p_r}$ Nullstellen von m, d.h. alle Elemente von $\mathbb{C}_n^\times$ sind Nullstellen von m, aber auch von Φ_n ist Minimalpolynom $\Rightarrow m | \Phi_n$, aber $\deg m \geq \deg \Phi_n \Rightarrow m = \Phi_n$, d.h. Φ_n ist das Minimalpolynom aller $\zeta \in \mathbb{C}_n^\times$

Also genügt es, die Behauptung zu beweisen. m ist irreduzibel, als Minimalpolynom $\overset{\text{warum}}{\Rightarrow}$ es genügt, $m(\zeta^p)=0$ zu zeigen:
m ist Minimalpolynom von ζ, der eine Nullstelle von x^n-1 ist
$\Rightarrow m(x) \mid x^n-1$, genauer: $\exists h(x) \in \mathbb{Q}[x]$ mit $x^n-1 = m(x)\cdot h(x)$
Aber $x^n-1 \in \mathbb{Z}[x]$ und $m(x)$ normiert $\overset{\text{Details?}}{\Rightarrow} m, h \in \mathbb{Z}[x]$, h normiert
$\zeta^p \in C_n^\times$, wie alle Elemente in C_n ist ζ^p Nullstelle von x^n-1
Falls $m(\zeta^p)\neq 0$ muß also $h(\zeta^p)=0$ gelten.
$\Rightarrow \zeta$ ist Nullstelle von $h(x^p)$, d.h. $x \mapsto x^p \mapsto h(x^p)$, auch ein Polynom in $\mathbb{Z}[x]$
Bez: h_p

m ist Minimalpolynom von $\zeta \Rightarrow m \mid h_p$, d.h. $\exists g$ $h_p = m\cdot g$ für ein $g \in \mathbb{Z}[x]$
$h_p, m, g \in \mathbb{Z}[x] \Rightarrow$ man kann die Koeffizienten modulo p reduzieren,
d.h. $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ anwenden und erhält $\overline{h_p} = \overline{m}\cdot\overline{g}$
$f \mapsto \overline{f}$
h_p, m, g normiert $\Rightarrow \overline{h_p}, \overline{m}, \overline{g}$ alle $\neq 0$ in $\mathbb{F}_p[x]$
In $\mathbb{F}_p$ ist der Frobenius homomorphismus $\mathbb{F}_p \xrightarrow{\text{Frob}} \mathbb{F}_p$, $a \mapsto a^p$ die Identität warum?

$\Rightarrow \overline{h_p}(x) = \overline{h}(x^p) = \overline{h}(x)^p$ warum?
$\overline{m}(x)\cdot\overline{g}(x)$
Also $\overline{m}\cdot\overline{g} = \overline{h}^p$ im euklidischen Ring $\mathbb{F}_p[x]$
$\Downarrow$
faktoriell: eindeutige Primfaktorzerlegung

m ist irreduzibel, aber $\overline{m}$ vielleicht nicht
$\overline{m}$ ist jedenfalls ein Produkt von irreduziblen Faktoren, sei α einer davon
$\Rightarrow \alpha \mid \overline{m} \mid \overline{h}^p \Rightarrow \alpha \mid \overline{h}$
$x^n-1 = m\cdot h \Rightarrow x^n-\overline{1} = \overline{m}\cdot\overline{h}$, das hat den Teiler α^2 warum
$\Rightarrow x^n-\overline{1}$ hat eine mehrfache Nullstelle – das ist noch kein Widerspruch, weil wir ja nicht mehr in Charakteristik 0 sind. Aber $(x^n-\overline{1})' = \overline{n}\,x^{n-1}$ und wegen $p\nmid n$ ist diese Ableitung $\neq 0 \overset{\text{Algebra}}{\Rightarrow}$ es gibt keine mehrfache Nullstelle ζ $\Rightarrow$ Behauptung $\Rightarrow$ 2.11 (und 2.8) $\square$

Das liefert auch Information über die Galoisgruppe:

2.12 Korollar: Die Abbildung $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\chi} (\mathbb{Z}/n\mathbb{Z})^*$
$\psi \longmapsto r$, wenn $\psi(\zeta_n) = \zeta_n^r$

ist ein Isomorphismus von Gruppen.

Ersetzt man $\mathbb{Q}$ durch K mit $\mathrm{char}(K) = 0$, dann ist χ immer noch injektiv.

Beweis: $\mathbb{Q}(\zeta_n)$ enthält alle Nullstellen von $T^n - 1$, ist also der Zerfällungskörper
$\Rightarrow \mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist eine Galoiserweiterung. Ebenso mit K statt $\mathbb{Q}$.
$\psi(\zeta_n)$ ist wieder eine primitive Einheitswurzel $\Rightarrow r \in (\mathbb{Z}/n\mathbb{Z})^*$ χ ist multiplikativ
$\psi(\zeta_n) = \zeta_n^1 \Rightarrow \psi = \mathrm{id}$, das Bild von ζ_n legt ψ fest warum nachprüfen
$\Rightarrow \chi$ ist injektiv
Für $K = \mathbb{Q}$ gilt $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$
$\Rightarrow \chi$ Isomorphismus □

was kann bei Kstatt $\mathbb{Q}$ passieren, so daß χ nicht surjektiv ist?

Eine weitere Anwendung der Galoistheorie folgt im nächsten Kapitel.