Einschübe über Ringe.

A. Die Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$.

Die Einheitengruppe eines Rings. Ist R ein Ring, so bezeichnet man mit R^* die Menge der (bezüglich der Multiplikation) invertierbaren Elemente (also die Menge der $r \in R$, für die es ein $s \in R$ mit $rs = sr = 1$ gibt); dies ist bezüglich der Multiplikation eine Gruppe, man nennt dies die *Einheitengruppe* des Rings R. Ist K ein Körper, so ist $K^* = K \setminus \{0\}$.

Sind R, S Ringe, so ist die Menge $R \times S$ mit komponentenweiser Addition und komponentenweiser Multiplikation wieder ein Ring.

Lemma. *Seien R, S Ringe. Dann ist $(R \times S)^* = R* \times S^*$.*

Beweis: Sei $r \in R, s \in S$. Offensichtlich ist (r, s) genau dann invertierbar, wenn die beiden Elemente $r \in R$ und $s \in S$ invertierbar sind.

Wir interessieren uns für R^* vor allem im Fall $R = \mathbb{Z}/n\mathbb{Z}$ (dabei ist $n \in \mathbb{N}_1$); in diesem Fall besteht $R^* = (\mathbb{Z}/n\mathbb{Z})^*$ gerade aus den Restklassen $\overline{a}$ mit $1 \leq a \leq n$, für die a und n teilerfremd sind (nur für den trivialen Fall $n = 1$, den man aber nicht ausschließen möchte, schreibt man $1 \leq a \leq n$; ist $n \geq 2$, so reicht es, die Elemente a mit $1 \leq a < n$ zu betrachten).

Der chinesische Restsatz. *Seien $m, n \in \mathbb{N}_1$ teilerfremd. Dann liefert die kanonische Abbildung $\overline{a} \mapsto (\overline{a}, \overline{a})$ (für $a \in \mathbb{Z}$) einen Ring-Isomorphismus*

$$\boxed{\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.}$$

(Achtung: wir haben dreimal $\overline{a}$ geschrieben, aber dies hat drei verschiedene Bedeutungen: es handelt sich um die Restklassen modulo mn, modulo m und schließlich modulo n.)

Beweis: Die Zuordnung $\overline{a} \mapsto (\overline{a}, \overline{a})$ ist offensichtlich wohldefiniert (das ist als erstes zu verfizieren, sonst würde die Aussage überhaupt keinen Sinn machen) und sie liefert einen Ring-Homomorphismus (ebenfalls offensichtlich). Sie ist injektiv, denn ist a durch m und durch n teilbar (also $(\overline{a}, \overline{a}) = (\overline{0}, \overline{0})$), so ist a durch mn teilbar, da m, n teilerfremd sind. Nun sind die Mengen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ aber gleichmächtig (beides sind Mengen mit mn Elementen), also ist jede injektive Abbildung auch surjektiv.

Wichtig ist hier vor allem: *Die kanonische Abbildung $\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ist surjektiv.* Man kann dies folgendermaßen formulieren: *Sind die Gleichungen*

$$X \equiv b \mod m \quad \textit{und} \quad X \equiv c \mod n$$

mit $b, c \in \mathbb{Z}$ lösbar, so ist auch das Gleichungssystem

$$X \equiv b \mod mn \quad \textit{und} \quad X \equiv c \mod mn$$

in $\mathbb{Z}$ lösbar.

Die Euler'sche ϕ-Funktion. Sei $\phi(n)$ die Anzahl der natürlichen Zahlen a mit $1 \leq a \leq n$ und $(a, n) = 1$. (Erinnerung: sind m, n natürliche Zahlen, so bezeichnet (m, n) den ggT; die Euler'sche ϕ-Funktion zählt also die zu n teilerfremden Zahlen a mit $1 \leq a \leq n$). Wichtig für uns sind die folgenden beiden Situationen, wo man mit der Euler'schen ϕ-Funktion zu tun hat:

(a)

$$\boxed{|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)}$$

(b) *Ist C_n eine zyklische Gruppe der Ordnng n, so ist die Erzeugendenanzahl von C_n gleich $\phi(n)$:*

$$\boxed{|\{h \in C_n \mid \langle h \rangle = C_n\}| = \phi(n)}$$

Wähle ein erzeugendes Element g von $G = C_n$. Die Elemente der Form g^a mit $1 \leq a \leq n$ sind paarweise verschieden und liefern genau die Elemente von G. Nun gilt aber: Genau dann erzeugt g^a die Gruppe G, wenn $(a, n) = 1$ gilt. Die Zuordnung $a \mapsto g^a$ liefert also eine Bijektion zwischen der Menge $\{a \mid 1 \leq a \leq n, (a, n) = 1\}$ und der Menge der Erzeugenden von C_n.

Zur Berechnung von $\phi(n)$ brauchen wir zwei Rechenregeln:

Lemma. *Es gilt:*
(a) *Seien $n, m \in \mathbb{N}_1$ mit $(m, n) = 1$. Dann ist $\phi(nm) = \phi(n)\phi(m)$.*
(b) *Ist p eine Primzahl und $e \in \mathbb{N}_1$, so ist $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.*

(Warnung: Die Eigenschaft (a) wird in der Zahlentheorie "Multiplikativität" der Funktion ϕ genannt, in der Algebra dagegen nennt man nur dann eine Funktion f multiplikativ, wenn $f(mn) = f(m)f(n)$ für **alle** m, n gilt und nicht nur für **teilerfremde** m, n, wie im Fall der Euler'schen ϕ-Funktion!)

Beweis von (a): Dies folgt direkt aus dem chinesischen Restsatz.

Beweis von (b): Die Anzahl der Zahlen zwischen 1 und p^e, die durch p teilbar sind, ist gerade p^{e-1}, denn dies sind die Zahlen der Form pm mit $1 \leq m \leq p^{e-1}$. Eine Zahl a ist aber genau dann zu p^e teilerfremd, wenn sie nicht durch p teilbar ist. Demnach ist die Anzahl der Zahlen zwischen a mit $1 \leq a \leq p^e$ mit $(a, p^e) = 1$ gerade $p^e - p^{e-1}$.

Also gilt folgende Regel: Sind $p_1, \ldots, p_t$ paarweise verschiedene Primzahlen und sind $e_1, \ldots, e_t \in \mathbb{N}_1$, so ist

$$\boxed{\phi(p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}) = p_1^{e_1-1} p_2^{e_2-1} \cdots p_t^{e_t-1} \cdot (p_1 - 1)(p_2 - 1) \cdots (p_t - 1).}$$

Beispiel: $\phi(90\,000) = \phi(2^4 3^2 5^4) = 2^3 3^1 5^3 \cdot 1 \cdot 2 \cdot 4 = 24\,000$.

B. Das formale Ableiten von Polynomen.

Sei K ein Körper, $K[T]$ der Polynomring in einer Variablen. Für $f = \sum_{i=0}^{n} c_i T^i$ definiert man $f' = \sum_{i=1}^{n} i c_i T^{i-1}$ und nennt dies die *Ableitung* von f. Man rechnet nach: Sind $f, g \in K[T]$, so gilt $(fg)' = f'g + fg'$. Daraus folgt: Sind $f, g \in K[T]$ und ist g^t mit $t \in \mathbb{N}_1$ ein Teiler von f, so ist g^{t-1} ein Teiler von f'. Insbesondere gilt: Hat f eine doppelte Nullstelle α, so ist α Nullstelle von f'.

Lemma. *Sei $f \in K[T]$ ein nicht-konstantes Polynom mit $f' = 0$. Dann ist die Charakteristik von K eine Primzahl p und es gibt ein Polynom $g \in K[T]$ mit* $f(T) = g(T^p)$ (das heißt: Ist $f = \sum_{t=0}^{n} c_t T^t$ mit $c_t \in K$, und ist $c_t \neq 0$, so ist p ein Teiler von t).

Beweis: Sei $f(T) = \sum_{t=0}^{n} a_t \cdot tT^t$ mit $a_n \neq 0$ und $n \geq 1$. Nach Definition ist $f' = \sum_{t=1}^{n} a_t \cdot tT^{t-1}$. Sei also $f' = 0$. Aus $a_n \neq 0$ und der Tatsache, daß der Koeffizient $a_n \cdot n$ von T^{n-1} Null ist, folgt, daß die Charakteristik von K eine Primzahl p und p ein Teiler von n ist. Auch für jeden anderen Koeffizienten a_t mit $a_t \neq 0$ folgt aus $a_t \cdot t = 0$, daß p ein Teiler von t ist. Setzen wir $b_s = a_{ps}$, für $s \geq 0$, so erhalten wir mit $g(T) = \sum_{s \geq 0} b_s T^s$ ein Polynom in $K[T]$ mit $g(T^p) = f(T)$.

C. Der Quotientenkörper eines nullteilerfreien kommutative Rings.

Sei R ein nullteilerfreier kommutativer Ring. Betrachte die Menge Q' der Paare $(r, s) \in R^2$ mit $s \neq 0$ und definiere auf Q' eine Äquivalenzrelation $\sim$ wie folgt

$$(r, s) \sim (r', s') \iff rs' = r's$$

(offensichtlich ist $\sim$ reflexiv und symmetrisch; nachzurechnen ist, daß $\sim$ auch transitiv ist). Mit $\mathrm{Quot}(R)$ bezeichnen wir die Menge $Q'/\sim$ der Äquivalenzklassen; die Äquivalenzklasse, die das Element (r, s) enthält, wird üblicherweise in der Form $\frac{r}{s}$ geschrieben. Auf der Menge $\mathrm{Quot}(R)$ definiert man eine Addition und eine Multiplikation wie folgt:

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}, \quad \text{und} \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

(zu zeigen ist, daß dies wohl-definiert ist!). Es gilt: *Mit diesen Operationen ist* $\mathrm{Quot}(R)$ *ein Körper,* man nennt ihn den *Quotientenkörper* von R. *Die Elemente der Form* $\frac{r}{1}$ *in* $\mathrm{Quot}(R)$ *bilden einen Unterring R', der zu R isomorph ist* (dabei wird der kanonische Isomorphismus $R \to R'$ durch $r \mapsto \frac{r}{1}$ gegeben), *der Unterring R' erzeugt* $\mathrm{Quot}(R)$ *als Körper. Ist K ein Körper, der R als Unterring enthält, so ist der von R erzeugte Unterkörper von K zu* $\mathrm{Quot}(R)$ *isomorph.* All dies zeigt man genauso wie im klassischen Spezialfall $R = \mathbb{Z}$ mit $\mathrm{Quot}(R) = \mathbb{Q}$.

Insbesondere brauchen wir diese Konstruktion im Fall des Polynomrings $R = K[T]$ mit Koeffizienten in einem Körper K. Man nennt den Quotientenkörper $\mathrm{Quot}(K[T])$ den *Körper der rationalen Funktionen mit Koeffizienten in K* und schreibt $K(T)$ statt $\mathrm{Quot}(K[T])$.

D. Faktorielle Ringe (I).

Um zu entscheiden, ob ein vorgebenes Polynom mit Koeffizienten in einem Körper K irreduzibel ist, benötigen wir Hilfsmittel. Arbeiten wir zum Beispiel mit

dem Körper $K = \mathbb{Q}$ der rationalen Zahlen, und ist ein Polynom in $\mathbb{Q}[T]$ gegeben, so können wir durch Multiplikation mit einer von Null verschiedenen ganzen Zahl erreichen, daß alle Koeffizienten in $\mathbb{Z}$ liegen, und dann in $\mathbb{Z}[T]$ arbeiten.

Erinnerung: Sei R ein nullteilerfreier kommutativer Ring. Ein Element $p \in R \setminus \{0\}$ heißt *irreduzibel*, falls einerseits p nicht invertierbar ist und falls andererseits aus $p = p_1 p_2$ folgt, daß p_1 oder p_2 invertierbar ist. Zwei irreduzible Elemente p, q heißen *assoziiert*, falls es ein invertierbares Element $r \in R$ gibt mit $p = rq$. Der Ring R heißt *faktoriell*, falls gilt:

(1) (Existenz) Jedes nicht-invertierbare Element a läßt sich als Produkt $a = p_1 p_2 \cdots p_n$ mit irreduziblen Elementen p_i (und $n \geq 1$) schreiben,

(2) (Eindeutigkeit) Ist $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ mit irreduziblen Elementen p_i, q_i, so gilt $n = m$ und es gibt eine Permutation σ von $\{1, \ldots, n\}$ mit: $p_{\sigma(i)}$ ist zu q_i assoziiert, für $1 \leq i \leq n$.

(falls also die kommutative Halbgruppe $H = (R \setminus \{0\}, \cdot)$ eine Halbgruppe mit eindeutiger Primfaktorzerlegung ist).

Wir wissen: $\mathbb{Z}$ ist faktorieller Ring, jeder Körper ist ein faktorieller Ring (trivialerweise). Ist K ein Körper, so ist der Polynomring $K[T]$ in einer Variablen T faktoriell. Allgemeiner gilt der folgende Satz (Gauß): *Ist R faktoriell, so auch $R[T]$*. Der Beweis soll später noch gebracht werden.

Sei R faktoriell. Ein Polynom $f \neq 0$ in $R[T]$ heißt *primitiv,* wenn der ggT der Koeffizienten gleich 1 ist.

Lemma von Gauß. *Sei R faktorieller Ring. Seien g, h primitive Polynome. Dann ist auch $g \cdot h$ primitiv.*

Beweis: Sei $g = \sum_{i=0}^{n} a_i T^i$ und $h = \sum_{j=0}^{m} b_j T^j$, mit $a_i, b_j \in R$, also $f = \sum_{i=0}^{n+m} c_k T^k$ mit $c_k = \sum_{i+j=k} a_i b_j$.

Sei p irredzibel. Sei p ein Teiler von $a_0, a_1, \ldots, a_{s-1}$ aber kein Teiler von a_s. Sei p ein Teiler von $b_0, b_1, \ldots, b_{t-1}$ aber kein Teiler von b_t. Dann ist p kein Teiler von c_{s+t}, denn

$$c_{s+t} = \sum_{i+j=s+t, i<s} a_i b_j + a_s b_t + \sum_{i+j=s+t, i>s} a_i b_j$$

und p teilt die ersten s Summanden und die letzten t Summanden, aber nicht den mittleren Summanden. Zu jedem irreduziblen Element p gibt es ein derartiges s und ein derartiges t, denn g, h sind primitiv. Also gibt es mindestens einen Koeffizienten von $g \cdot h$, der nicht durch p teilbar ist. Also ist $g \cdot h$ primitiv.

Sei R faktorieller Ring, sei $K = \mathrm{Quot}(R)$ der Quotientenkörper. Jedes von Null verschiedene Polynom in $f \in K[T]$ läßt sich ziemlich eindeutig in der Form $f = c \cdot f_1$ mit $c \in K$ und $f_1 \in R[T]$ primitiv schreiben - ist $f = c_1 \cdot f_1 = c_2 \cdot f_2$, so unterscheiden sich c_1 und c_2 nur durch ein in R invertierbares Element. Insbesondere gilt: Ist $g \in K[T]$ ein normiertes Polynom, so gibt es ein von Null verschiedenes Element $a \in R$ und ein primitives Polynom $g_1 \in R[T]$ mit $g = \frac{1}{a} g_1$.

Folgerung (heißt ebenfalls **Lemma von Gauß.**) *Sei K ein Körper und R ein Unterring von K. Seien f, g, h Polynome in $K[T]$ mit $f = g \cdot h$. Sind f, g normierte Polynome deren Koeffizienten zu R gehören, so ist auch h ein normiertes Polynom mit Koeffizienten in R.*

Beweis: Sei K' der Quotientenkörper von R, dies ist offensichtlich ein Unterkörper von K. Da f, g Polynome mit Koeffizienten in K' sind, gilt dies auch für h (denn wir können mit dem Euklid'schen Algorithmus in $K[T]$ den ggT von f, g bestimmen und erhalten das Polynom g; da alle Koeffizienten von f, g zu K' gehören, arbeitet der Euklid'sche Algorithmus nur mit Koeffizienten in K', demnach sieht man: das Polynom h hat Koeffizienten in K'. Und natürlich ist mit f und g auch h normiert.

Sei nun $g = \frac{1}{a} \cdot g_1$ und $h = \frac{1}{b} \cdot h_1$ mit primitive Polynomen g_1, h_1 in $R[T]$ und $a, b \in R \setminus \{0\}$. Es ist $f = \frac{1}{ab} g_1 h_1$ und $g_1 h_1$ ist primitiv, also ist $\frac{1}{ab} \in R$ invertierbar, also sind a, b beide in R invertierbar. Dies bedeutet aber, daß alle Koeffizienten von g und h zu R gehören.

II. Körper.

1. Definitionen.

Körpererweiterungen. Ist $K = (K, +, \cdot)$ ein Körper und $K' \subseteq K$ eine Teilmenge, die bezüglich $+, \cdot$ selbst ein Körper ist, so nennt man $K' = (K', +\cdot)$ einen *Unterkörper* von K, und K einen *Oberkörper* von K'; und spricht in diesem Fall von der *Körpererweiterung* $K' \subseteq K$. Ist K' ein Unterkörper von K und K'' ein Unterkörper von K', so nennt man K' einen *Zwischenkörper* der Körpererweiterung $K'' \subseteq K$. Ein *Körperturm* $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ ist eine Folge von Körpererweiterungen $K_{i-1} \subseteq K_i$, $1 \leq i \leq n$.

Ist K ein Unterkörper des Köpers L, so ist L (in kanonischer Weise) ein K-Vektorraum (bezüglich der gegebenen Addition auf L, wobei man als Skalarmultiplikation $K \times L \to L$ die Einschränkung der Multiplikation $L \times L \to L$ nimmt). Die Dimension von L als K-Vektorraum bezeichnen man als den *Grad* der Körpererweiterung, und man schreibt $[L : K] = \dim_K L$.

Gradsatz. *Seien $K \subseteq L \subseteq M$ Körpererweiterungen, so gilt*

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

Genauer gilt: *Ist $(a_i)_i$ eine K-Basis von L und $(b_j)_j$ eine L-Basis von M, so ist $(a_i b_j)_{i,j}$ eine K-Basis von M.*

Beweis: Jedes Element $c \in M$ kann als endliche Linearkombination $c = \sum_j \beta_j b_j$ mit $\beta_j \in L$ geschrieben werden. Schreibe nun $\beta_j = \sum_i \alpha_{ij} a_i$ mit $\alpha_{ij} \in K$. Einsetzen liefert: $c = \sum_j \beta_j b_j = \sum_j \sum_i \alpha_{ij} a_i b_j$, also ist die Menge der Elemente $a_i b_j$ ein Erzeugendensystem des K-Vektorraums M. Sind nun Koeffizienten $\lambda_{ij} \in K$ gegeben mit $\sum_{i,j} \lambda_{ij} a_i b_j = 0$, so klammern wir: $\sum_j \big(\sum_i \lambda_{ij} a_i\big) b_j = 0$. Der Koeffizient $\sum_i \lambda_{ij} a_i$ von b_j gehört zu L; da $(b_j)_j$ eine L-Basis von M ist, folgt $\sum_i \lambda_{ij} a_i = 0$ für alle j. Aus der Tatsache, daß $(a_i)_i$ eine K-Basis von L ist, folgern wir $\lambda_{ij} = 0$ für alle i (und natürlich alle j).

Sei $K \subseteq L$ eine Körpererweiterung, sei $a \in L$.
Sei $K[a]$ der kleinste Unter**ring** von L, der K und und a enthält.
Sei $K(a)$ der kleinste Unter**körper** von L, der K und und a enthält.

Sind Elemente $a_1, \ldots, a_m$ in L gegeben, so setzt man

$$K[a_1, \ldots, a_m] = K[a_1, \ldots, a_{m-1}][a_m]$$

und

$$K(a_1, \ldots, a_m) = K(a_1, \ldots, a_{m-1})(a_m).$$

Natürlich sind $K[a_1, \ldots, a_m]$ der kleinste Unterring und $K(a_1, \ldots, a_m)$ der kleinste Unterkörper von L, die die Elemente $a_1, \ldots, a_m$ enthalten.

Algebraische Elemente Sei $K \subseteq L$ eine Körpererweiterung. Ein Element $a \in L$ heißt *algebraisch über* K, falls es ein Polynom $0 \neq f \in K[T]$ mit $f(a) = 0$ gibt, andernfalls heißt *a transzendent über* K. Ist $a \in L$ algebraisch über K, so nennt man **das** normierte Polynom $f \in K[T]$ mit $f(a) = 0$ und kleinstmöglichem Grad das *Minimalpolynom von a über* K (daß es nur ein einziges normiertes Polynom $f \in K[T]$ mit $f(a)$ und kleinstmöglichem Grad geben kann, sieht man wie folgt: Sind $f, g \in K[T]$ mit $f(a) = 0 = g(a)$, und ist h der ggT von f und g, so ist wegen der Bézout'schen Gleichung auch $h(a) = 0$). *Das Minimalpolynom f eines Elements $a \in L$ über K ist irreduzibel,* denn ist $f = gh$, so folgt aus $0 = f(a) = g(a)h(a)$ und der Nullteilerfreiheit von L, daß $g(a) = 0$ oder $h(a) = 0$ gilt. Und es gilt: *Das Minimalpolynom f von a über K ist das einzige normierte irreduzible Polynom in $K[T]$ mit Nullstelle a.*

Erinnerung: Da L ein kommutativer Ring ist, der K als Unterring enthält, ist die Auswertungsabbildung ϵ_a: $K[T] \to L$ mit $\epsilon_a(f) = f(a)$ für $f \in K[T]$ ein Ring-Homomorphismus, dessen Bild $K[a]$ ist. Offensichtlich gilt: *Genau dann ist ϵ_a injektiv, wenn a transzendent ist,* denn die Injektivität bedeutet gerade, daß das Nullpolynom das einzige Polynom in $K[T]$ ist, das a als Nullstelle hat.

Lemma. *Sei $K \subseteq L$ eine Körpererweiterung. Ist $a \in L$ algebraisch über K mit Minimalpolynom f über K und ist* grad $f = n$, *so bilden die Elemente* $1, a, a^2, \ldots, a^{n-1}$ *eine K-Basis von $K[a]$, und $K[a]$ ist ein Körper.* Es ist demnach $K(a) = K[a]$.

Beweis: Die Elemente $1, a, a^2, \ldots, a^{n-1}$ sind linear unabhängig über K, denn sind Koeffizienten $\lambda_i \in K$ gegeben, mit $\sum_{i=0}^{n-1} \lambda_i a^i = 0$, so ist a Nullstelle des Polynoms $g(T) = \sum_{i=0}^{n-1} \lambda_i T^i$. Da aber g kleineren Grad als das Minimalpolynom f hat, muß g das Nullpolynom sein: also gilt $\lambda_i = 0$ für alle $0 \leq i \leq n-1$.

Sei K' der von den Elementen a^i mit $0 \leq i < n$ aufgespannte K-Unterraum von L. Wir zeigen als erstes, daß K' ein Unterring (und demnach gleich $K[a]$) ist: Es ist zu zeigen, daß K' abgeschlossen unter der Multiplikation ist. Sei $f = T^n + \sum_{i=0}^{n-1} c_i T^i$ mit $c_i \in K$. Wegen $f(a) = 0$ gilt also

$$a^n = \sum_{i=0}^{n-1} (-c_i) a^i \in K'.$$

Wir sehen also: $a \cdot K' \subseteq K'$. Mit Induktion folgt nun, daß K' alle Potenzen von a enthält: denn ist $a^m \in K'$, so ist $a^{m+1} = a \cdot a^m \in a \cdot K' \subseteq K'$. Daraus folgt aber mit Hilfe des Distributivgesetzes, daß K' ein Unterring ist.

Als Unterring von L ist $K' = K[a]$ nullteilerfrei. Um zu zeigen, daß $K[a]$ ein Unterkörper ist, betrachte ein von Null verschiedenes Element $b \in K[a]$. Die Multiplikationsabbildung ϕ_b: $K[a] \to K[a]$ (definiert durch $\phi_b(c) = bc$) ist K-linear

(wegen des Distributivgesetzes und der Kommutativität der Multiplikation) und injektiv (wegen der Nullteilerfreiheit), also auch surjektiv, denn $K[a]$ ist ein endlichdimensionaler Vektorraum. Insbesondere finden wir ein $b' \in K[a]$ mit $\phi_b(b') = 1$, also $bb' = 1$. Dies zeigt, daß $K[a]$ ein Körper ist.

Lemma. *Sei $K \subseteq L$ eine Körpererweiterung, sei $a \in L$. Die folgenden Eigenschaften sind äquivalent:*

(i) *a ist algebraisch über K,*
(ii) *$K[a] = K(a)$,*
(iii) *$[K(a) : K]$ ist endlich,*
(iv) *Es gibt einen Zwischenkörper $K \subseteq K' \subseteq L$ mit $[K' : K]$ endlich und $a \in K'$.*

Beweis: (i) $\Longrightarrow$ (ii), (iii) wurde gerade gezeigt. (iii) $\Longrightarrow$ (iv) ist trivial: nimm $K' = K(a)$.

Sei nun (ii) gegeben. Wäre a transzendent über K, so würde die Auswertungsabbildung ϵ_a: $K[T] \to L$ mit $\epsilon_a(f) = f(a)$ für $f \in K[T]$ einen Ring-Isomorphismus $K[T] \to K[a]$ liefern. Der Ring $K[T]$ ist aber sicher kein Körper, denn keines der Polynome vom Grad ≥ 1 ist invertierbar. Ist $K[a]$ zu $K[T]$ isomorph, so ist natürlich auch $K[a]$ kein Körper, also $K[a] \neq K(a)$.

Es bleibt zu zeigen: (iv) $\Longrightarrow$ (i). Es gebe also einen Zwischenkörper $K \subseteq K' \subseteq L$ mit $[K' : K]$ endlich und $a \in K'$. Sei $[K' : K] = n$. Da K' ein Unterring von L ist mit $a \in K'$, gehören die Elemente $1, a, a^2, \ldots, a^n$ zu K' und wegen $[K' : K] = n$ sind sie linear abhängig über K. Sei etwa $\sum_{i=0}^{n} \lambda_i a^i = 0$, wobei nicht alle Koeffizienten λ_i Null sind. Setze $f(T) = \sum_{i=0}^{n} \lambda_i T^i$. Dies ist ein von Null verschiedenes Polynom mit $f(a) = 0$. Also ist a algebraisch.

Folgerung. *Sei $K \subseteq L$ eine Körpererweiterung. Die Menge der Elemente von L, die algebraisch über K sind, bildet einen Unterkörper von L.* Das heißt: Sind $a, b \in L$ algebraisch über K, so sind auch die Elemente $-a, a+b, ab$ algebraisch über K; ist $a \neq 0$ algebraisch über K, so ist auch $\frac{1}{a}$ algebraisch über K.

Beweis. Betrachte den Körperturm

$$K \subseteq K[a] \subseteq K[a, b].$$

Da a algebraisch über K ist, ist $[K[a] : K]$ endlich. Auch b ist algebraisch über K, sei g das Minimalpolynom von b über K. Da $g \in K[T] \subseteq K[a][T]$ ein von Null verschiedenes Polynom mit $g(b) = 0$ ist, ist b algebraisch über $K[a]$ und demnach ist auch $[K[a, b] : K[a]]$ endlich. Der Gradsatz besagt, daß $[K[a, b] : K]$ endlich ist, demnach ist jedes Element in $K[a, b]$ algebraisch über K. Da $K[a, b]$ ein Körper ist, gehören die Elemente $-a, a+b, ab$ zu $K[a, b]$, sind also algebraisch über K; ist $a \neq 0$, so liegt auch $\frac{1}{a} \in K[a, b]$ und ist demnach ebenfalls algebraisch über K.

Beispiel. Von besonderem Interesse ist die Körpererweiterung $\mathbb{Q} \subset \mathbb{C}$. Die komplexen Zahlen, die algebraisch über $\mathbb{Q}$ sind, nennt man *algebraische Zahlen,* sie bilden einen Unterkörper $\mathbb{A}$ von $\mathbb{C}$, den *Körper der algebraischen Zahlen.* Beachte: Wie man in der Vorlesung Analysis I lernt, ist der Körper $\mathbb{R}$ und demnach auch der Körper $\mathbb{C}$ überabzählbar. Man zeigt recht einfach, daß es nur abzählbar viele algebraische Zahlen geben kann: Jede algebraische Zahl ist Nullstelle eines von Null verschiedenen Polynoms in $\mathbb{Q}$, es gibt aber nur abzählbar viele Polynome in $\mathbb{Q}$ und jedes Polynom hat nur endlich viele Nullstellen: insgesamt gibt es also nur abzählbar viele Nullstellen von Polynomen mit Koeffizienten in $\mathbb{Q}$.

Im allgemeinen ist es gar nicht einfach, von einer vorgegebenen komplexen Zahl zu zeigen, daß sie nicht algebraisch (also "transzendent") ist. Es ist bekannt, daß die Kreiszahl π und die Euler'sche Zahl e transzendente Zahlen sind, für einen Beweis sei auf JACOBSON: Basic Algebra I, verwiesen.

2. Adjunktion einer Wurzel von f

Sei K ein Körper, sei f ein irreduzibles Polynom in $K[T]$. Wir suchen einen Oberkörper von K, in dem f eine Nullstelle hat. (Ist K zum Beispiel Unterkörper des Körpers $\mathbb{C}$ der komplexen Zahlen, so wissen wir, daß f in $\mathbb{C}$ eine Nullstelle hat. Ganz anders sieht es aber aus, wenn wir zum Beispiel mit $K = \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl p arbeiten - bisher kennen wir überhaupt keine echten Oberkörper von $\mathbb{Z}/p\mathbb{Z}$. Da wir sehr leicht irreduzible Polynome vom Grad ≥ 2 über $\mathbb{Z}/p\mathbb{Z}$ konstruieren können, erhalten wir durch die nun folgende "Kronecker-Konstruktion" die Möglichkeit, neue endliche Körper zu konstruieren.)

Die Kronecker-Konstrukion: Adjunktion einer Wurzel eines irreduziblen Polynoms. Sei also K ein Körper und $f \in K[T]$ ein Polynom vom Grad $n \geq 1$. Die Menge $fK[T] = \{fg \mid g \in K[T]\}$ ist ein Unterraum des K-Vektorraums $K[T]$, die Polynome $1, T, T^2, \ldots, T^{n-1}$ bilden eine Komplementärbasis für diesen Unterraum. Bilde den Faktorraum $L = K[X]/fK[T]$. Ist $g \in K[T]$, so bezeichnen wir die Restklasse $g + fK[T]$ einfach mit $\overline{g}$. Derartige Restklassen können wir vermöge

$$\overline{g_1} \cdot \overline{g_2} = \overline{g_1 g_2}$$

multiplizieren: zu zeigen ist, daß dies wohldefiniert ist, daß also für Polynome g_1, g_2, q_1, q_2 mit $\overline{g_1} = \overline{q_1}$ und $\overline{g_2} = \overline{q_2}$ folgt $\overline{g_1 g_2} = \overline{q_1 q_2}$. Aber dies rechnet man sofort nach: Aus $\overline{g_i} = \overline{q_i}$ folgt $g_i - q_i = fh_i$ für Polynome $h_i \in K[T]$ und es ist $g_1 g_2 - q_1 q_2 = (g_1 - q_1)g_2 + q_1(g_2 - q_2) = f(h_1 g_2 + q_1 h_2)$. Man verifiziert sofort, daß die so definierte Multiplikation assoziativ ist, daß die Restklasse des konstanten Polynoms 1 ein Einselement ist, und daß das Distributivgesetz für die Addition und diese neu definierte Multiplikation gilt. Also ist L ein Ring. Man nennt ihn den *Restklassenring von $K[T]$ modulo f.*

Beachte: In jeder Restklasse $\overline{g}$ gibt es genau ein Polynom vom Grad echt kleiner n, nämlich den Rest von g der beim Teiler durch f bleibt. Man könnte also als Grundmenge von L auch die Menge der Polynome g vom Grad $\operatorname{grad} g < n$ nehmen. Man addiert sie wie üblich. Beim Multiplizieren von g_1 und g_2 bildet man zuerst das übliche Produkt $g_1 g_2$ und teilt dann durch f mit Rest: der Rest ist das gesuchte Produkt. Insbesondere bilden die konstanten Polynome (oder ihre Restklassen) einen zu K isomorphen Unterkörper in L; wir werden K immer mit diesem Unterkörper identifizieren.

Ist nun f ein irreduzibles Polynom, so ist L sogar ein Körper. Dies folgt aus der Bezout'schen Gleichung: Ist $\overline{g} \neq 0$, so ist also g ein Polynom, das nicht durch f teilbar ist. Dann ist der ggT von f und g das Einselement, es gibt also Polynome h und q mit $1 = hf + qg$. Wir sehen also: $\overline{1} = \overline{q} \cdot \overline{g}$ (der Summand $\overline{h} \cdot \overline{f}$ ist ja gleich $\overline{0}$), demnach ist $\overline{q}$ das zu $\overline{g}$ inverse Element.

Betrachte die Restklasse $\overline{T}$ von T. Es gilt $f(\overline{T}) = 0$, dies besagt, daß $\overline{T}$ in L eine Nullstelle des Polynoms f ist: genau, was wir suchen. Wir wollen dies explizit

nachrechnen. Sei $f(T) = \sum_{i=0}^{n} \alpha_i T^i$. Wir betrachten nun die Auswertungsabbildung

$$\epsilon_{\overline{T}} : K[T] \longrightarrow K[T]/fK[T] \quad \text{mit} \quad \epsilon(T) = \overline{T}.$$

Ganz allgemein gilt: Ist R ein kommutativer Ring, mit K als Unterring, und ist $r \in R$, so ist ϵ_r: $K(T) \to R$ durch $\epsilon_r(g) = g(r)$ definiert; ist dabei $g(T) = \sum_{i=0}^{m} a_i T^i$, so ist $g(r) = \sum_{i=0}^{m} a_i r^i$. Für $R = K[T]/fK[T]$, $r = \overline{T}$ und $f = g$ bedeutet dies:

$$\epsilon_{\overline{T}}(f) = \sum\nolimits_{i=0}^{n} \alpha_i \overline{T}^i.$$

Da wir die Elemente $\alpha_i \in K$ mit den Restklassen $\overline{\alpha_i}$ identifizieren, ist

$$\sum\nolimits_{i=0}^{n} \alpha_i \overline{T}^i = \sum\nolimits_{i=0}^{n} \overline{\alpha_i}\, \overline{T}^i \overset{(*)}{=} \overline{\sum\nolimits_{i=0}^{n} \alpha_i T^i} = \overline{f} = \overline{0}\,,$$

dabei haben wir bei $(*)$ verwandt, daß $\overline{\ }$ ein Ring-Homomorphismus ist.

Die Konstruktion von $K[T]/fK[T]$ entspricht natürlich völlig der Konstruktion der Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}_1$. Ganz allgemein gilt: Ist R ein euklid'scher Ring und $r \neq 0$ nicht invertierbar, so kann man auf der Menge der möglichen Reste modulo r eine Ringstruktur definieren, den "Restklassenring R/rR modulo r". Der Ring R/rR ist genau dann ein Körper, wenn r in R ein Primelement ist.

Der allgemeine Rahmen, um mit "Restklassenringen" zu arbeiten, sind (zweiseitige) "Ideale" in Ringen. Dabei heißt eine Teilmenge I eines Rings R ein *Ideal,* wenn I eine Untergruppe bezüglich der Addition ist und wenn zusätzlich gilt: Ist $x \in I$ und $r \in R$, so gehören rx und xr zu I. Diese Ideale sind gerade die Kerne von Ring-Homomorphismen: Ist η: $R \to S$ ein Ring-Homomorphismus, so ist die Menge $\{r \in R \mid \eta(r) = 0\}$ (wie üblich nennt man dies den "Kern" von η) ein Ideal. Umgekehrt gilt: Ist I ein Ideal in R, so induziert die Multiplikation von R eine Multiplikation auf der Menge der Restklassen R/I (dies ist die Restklassengruppe $(R,+)/(I,+)$, die wir im Abschnitt über Gruppen eingeführt haben): schreibt man $\overline{r} = r + I$ für die Restklasse von r modulo I, so ist die Multiplikation auf R/I durch $\overline{r_1} \cdot \overline{r_2} = \overline{r_1 r_2}$ definiert — wie oben ist ganz allgemein zu zeigen, daß diese Multiplikation wohl-definiert ist (und dafür braucht man gerade die Idealeigenschaft von I). Daß man auf diese Weise einen Ring R/I erhält, ist nicht überraschend: die Gesetze wie Assoziativität, Distributivität übertragen sich bei derartigen Faktorbildungen.

Die Bedeutung der Kronecker-Konstruktion I. *Die Restklasse $\overline{T}$ in $L = K[T]/fK[T]$ ist eine Nullstelle von f und sie erzeugt L über K.* Also gilt: *Es ist $[L : K]$ eine Körpererweiterung, die von einer Nullstelle von f erzeugt wird.*

Eindeutigkeitssatz. *Sei K ein Körper, sei $f \in K[T]$ ein irreduzibles Polynom. Für $i = 1, 2$ seien $K \subseteq L_i$ Körpererweiterungen und $\alpha_i \in L_i$ sei eine Nullstelle von f. Dann sind die Körper $K[\alpha_1]$ und $K[\alpha_2]$ isomorph.*

Genauer: *Es gibt einen* **und nur einen** *Körper-Isomorphismus η: $K[\alpha_1] \to K[\alpha_2]$ mit $\eta(c) = c$ für jedes $c \in K$ and $\eta(\alpha_1) = \alpha_2$.*

Insbesondere gilt also: *Ist $K \subseteq L$ eine Körpererweiterung, ist $\alpha \in L$ algebraisch über K mit Minimalpolynom f über K, so gibt es einen (und nur einen) Körperisomorphismus η: $K[T]/\langle f\rangle \to K[\alpha]$ mit $\eta(c) = c$ für alle $c \in K$ und $\eta(\overline{T}) = \alpha$.*

Beweis: Sei $K \subseteq L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit Minimalpolynom f über K. Die Auswertungsabbildung ϵ: $K[T] \to L$ mit $g \mapsto g(\alpha)$ ist ein Ring-Homomorphismus mit Bild $K[\alpha]$. Wegen $f(\alpha) = 0$ wird f, aber auch jedes Vielfache von f auf Null abgebildet. Wir erhalten demnach einen Ring-Homomorphismus $K[T]/\langle f\rangle \to L$ durch $\overline{g} \mapsto g(\alpha)$. Zu zeigen ist hier, daß diese Zuordnung wohldefiniert ist, aber es ist $\overline{g_1} = \overline{g_2}$, also $g_2 = g_1 + hf$ für ein Polynom h, so ist $g_2(\alpha) = g_1(\alpha) + h(\alpha)f(\alpha) = g_1(\alpha)$. Wir erhalten demnach einen Ring-Homomorphismus η: $K[T]/\langle f\rangle \to L$ mit $\eta(c) = c$ für alle $c \in K$ und $\eta(\overline{T}) = \alpha$. Es bleibt zu zeigen, daß η injektiv ist. Dafür braucht man, daß $K[T]/\langle f\rangle$ ein Körper ist. Denn es gilt ganz allgemein:

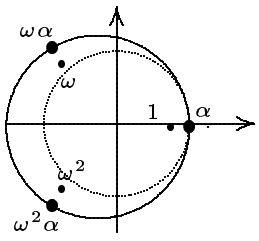
Lemma. Ist ϕ: $K \to R$ ein Ring-Homomorphismus, wobei K ein Körper und $R \neq 0$ ist, so ist ϕ injektiv.

Beweis: Ist $c \neq 0$ in K, so ist $\phi(c) \neq 0$, denn es gibt $c^{-1} \in K$ und also folgt aus $c \cdot c^{-1} = 1$ daß gilt $\phi(c) \cdot \phi(c^{-1}) = \phi(c \cdot c^{-1}) = \phi(1_K) = 1_R$; also ist $\phi(c)$ in R invertierbar und demnach sicher nicht Null.

> Wir haben hier die Injektivität gezeigt, ohne den Begriff eines "Ideals" zu verwenden. Üblicher Beweis: Der Kern eines Ring-Homomorphismus ist ein Ideal. Der Kern von ϕ ist also ein Ideal im Körper K. Die einzigen Ideale eines Körpers K sind K und 0. Wäre der Kern von ϕ gleich K, so wäre $\phi(1_K) = 1_R = 0$ und demnach $R = 0$, im Widerspruch zur Voraussetzung. Also ist der Kern gleich 0, also ist ϕ injektiv.

Beispiel: Sei $f = T^3 - 2 \in \mathbb{Q}[T]$, sei $\alpha = \sqrt[3]{2}$, dies ist offensichtlich eine Wurzel von f. Sei $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, dies ist eine primitive dritte Einheitswurzel, also sind auch $\omega\alpha$ und $\omega^2\alpha$ Wurzeln von f, es gilt also

$$f = (T - \alpha)(T - \omega\alpha)(T - \omega^2\alpha).$$



Da $\alpha, \omega\alpha$ und $\omega^2\alpha$ Wurzeln von f sind, sehen wir, daß die Körper $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\omega\alpha]$ und $\mathbb{Q}[\omega^2\alpha]$ isomorph sind, und zwar können wir auch entsprechende Isomorphismen explizit angeben.

Interpretation. Sei also $K \subseteq L$ eine Körpererweiterung, sei $\alpha \in L$ algebraisch über K mit Minimalpolynom f über K, der Grad von f sei n. Dann sind die Elemente $1, \alpha, \ldots, \alpha^{n-1}$ linear unabhängig, und das Polynom f drückt gerade aus, daß α^n sich als Linearkombination der Potenzen $1, \alpha, \ldots, \alpha^{n-1}$ schreiben läßt. Wir sehen also: als K-Vektorraum hat $K[\alpha]$ die Basis $1, \alpha, \ldots, \alpha^{n-1}$, und die Multiplikation ist eindeutig durch f bestimmt — und natürlich hat $K[T]/\langle f\rangle$ als K-Vektorraum

die Basis $1, \overline{T}, \ldots, \overline{T}^{n-1}$ und hier ist nun die Multiplikation gerade so gemacht, daß $\overline{f} = \overline{0}$ gilt.

Noch einmal: **Eindeutigkeitssatz.** *Sei η: $K_1 \to K_2$ ein Köperisomorphismus, dies liefert einen Isomorphismus $K_1[T] \to K_2[T]$, den wir ebenfalls mit η bezeichnen (also $\eta(\sum_{i=0}^n c_i T^i) = \sum_{i=0}^n \eta(c_i) T^i$ für $c_i \in K$, $0 \le i \le n$). Sei $f_1 \in K_1[T]$ ein irreduzibles Polynom und $f_2 = \eta(f_1)$. Für $i = 1, 2$ seien $K_i \subseteq L_i$ Körpererweiterungen und $\alpha_i \in L_i$ sei jeweils Nullstelle von f_i. Dann sind die Körper $K_1[\alpha_1]$ und $K_2[\alpha_2]$ isomorph.*

Genauer: *Es gibt einen* **und nur einen** *Körper-Isomorphismus $\overline{\eta}$: $K_1[\alpha_1] \to K_2[\alpha_2]$ mit $\overline{\eta}(c) = \eta(c)$ für jedes $c \in K_1$ and $\overline{\eta}(\alpha_1) = \alpha_2$.*

Die Bedeutung der Kronecker-Konstruktion II: Konstruktion von Oberkörpern durch Vorgabe von irreduziblen Polynomen.

Beispiel: Konstruktion eines Körpers mit 4 Elemente. Verwende $k = \mathbb{F}_2$ und $f = X^2 + X + 1$.

Die Bedeutung der Kronecker-Konstruktion III: (später): Konstruktion von Körper-Automorphismen.

3. Normalität von Körpererweiterungen.

Der Zerfällungskörper eines Polynoms. Sei K ein Körper, $f \in K[T]$ ein Polynom vom Grad mindestens 1. Wir haben gesehen, daß wir immer einen Oberkörper L von K konstruieren können, in dem f eine Nullstelle besitzt. Dies bedeutet allerdings nicht, daß f über L in Linearfaktoren zerfällt, sondern nur, daß f dort mindestens **eine** Nullstelle besitzt. Was wir wollen: Gegeben ist ein Polynom $f \in K[T]$. Gesucht ist ein Erweiterungskörper von K, in dem f in Linearfaktoren zerfällt. Ist also $K \subseteq L$ eine Körpererweiterung und $f \in K[T]$ ein normiertes Polynom, so nennt man L einen *Zerfällungskörper* von f über K, falls f über L in Linearfaktoren zerfällt, etwa $f = \prod_{i=1}^n (T - \alpha_i)$ und $L = K[\alpha_1, \ldots, \alpha_n]$ gilt.

Beobachtung. Sei $K \subseteq L$ eine Körpererweiterung, sei $\alpha \in L$ algebraisch über K mit Minimalpolynom f.

- Es ist also f irreduzibel über K,
- Über L besitzt f die Nullstelle α, hat also die Form $f = (T - \alpha) \cdot g$.

Frage: Was weiß man über g? Im allgemeinen **nichts.** Insbesondere braucht f über L nicht in Linearfaktoren zu zerfallen.

Beispiel: $K = \mathbb{Q}$, $f = T^3 - 2$, $L = \mathbb{Q}[\alpha]$ und $\alpha = \sqrt[3]{2}$. Dann gilt

$$T^3 - 2 = (T - \alpha) \cdot g \quad \text{mit} \quad g = T^2 + \alpha T + \alpha^2.$$

(Daß g die angegebene Form hat, kann man auf ganz verschiedene Weisen zeigen: multipliziert man $T^2 + \alpha T + \alpha^2$ mit $T - \alpha$, so erhält man offensichtlich $T^3 - a$, dies ist der erste Beweis. Oder auch: $g = (T - \omega\alpha)(T - \omega^2\alpha)$, und ausmultiplizieren liefert das gewünschte Ergebnis.) Beachte: $g \in L[T]$ ist irreduzibel, denn $L \subset \mathbb{R}$, aber die beiden Wurzeln $\omega\alpha$ und $\omega^2\alpha$ liegen nicht in $\mathbb{R}$.

Satz (Existenz und Eindeutigkeit eines Zerfällungskörpers). *Sei K Körper, $f \in K[T]$ normiertes Polynom. Dann gibt es einen Zerfällungskörper L*

von f über K. Sind $K \subseteq L_1$ und $K \subseteq L_2$ Zerfällungskörper von f, so gibt es einen Isomorphismus η: $L_1 \to L_2$ mit $\eta(c) = c$ für alle $c \in K$. **Warnung:** Meist gibt es nicht nur einen solchen Isomorphismus! Ist $f = \prod_{i=1}^{n}(T - \alpha_i)$ in L_1 und $f = \prod_{i=1}^{n}(T - \beta_i)$ in L_2, so gibt es eine Permutation σ von $1, 2, \ldots, n$ mit $\eta(\alpha_i) = \beta_{\sigma(i)}$. Fixiert man eine derartige Permutation, so gibt es **höchstens einen** Isomorphismus mit dieser Eigenschaft.

Konstruktion eines Zerfällungskörpers von f, mit Induktion nach dem Grad von f. Ist $\operatorname{grad} f = 1$, so ist K Zerfällungskörper. Sei also $\operatorname{grad} f > 1$. Sei also $f = gh$ und g sei irreduzibel. Adjungiere nach Kronecker zu K eine Wurzel von g, wir erhalten also eine Körpererweiterung $K \subseteq L$ und eine Wurzel $\alpha_1 \in L$ von f mit $L = K[\alpha_1]$. Es gibt also in $L[T]$ eine Faktorisierung $g = (T - \alpha) \cdot q$, also ist $f = (T - \alpha_1) \cdot q \cdot h$, dabei ist $q \cdot h \in L[T]$. Nach Induktion besitzt $q \cdot h$ über L einen Zerfällungskörper M, also gilt $L \subseteq M$, $q \cdot h = \prod_{i=2}^{n}(T - \alpha_i)$ und $M = L[\alpha_2, \ldots, \alpha_n]$. Insgesamt haben wir:

$$f = g \cdot h = (T - \alpha_1) \cdot q \cdot h = (T - \alpha_1) \prod_{i=2}^{n}(T - \alpha_i),$$

und

$$M = L[\alpha_2, \ldots, \alpha_n] = (K[\alpha_1])[\alpha_2, \ldots, \alpha_2] = K[\alpha_1, \ldots, \alpha_n].$$

Also ist M Zerfällungskörper.

Eindeutigkeit: Ebenfalls induktiv.

Noch einmal: **Eindeutigkeitssatz.** *Sei η: $K_1 \to K_2$ ein Köperisomorphismus, dies liefert einen Isomorphismus $K_1[T] \to K_2[T]$, den wir ebenfalls mit η bezeichnen (also $\eta(\sum_{i=0}^{n} c_i T^i) = \sum_{i=0}^{n} \eta(c_i) T^i$ für $c_i \in K$, $0 \leq i \leq n$). Sei $f_1 \in K_1[T]$ ein irreduzibles Polynom und $f_2 = \eta(f_1)$. Für $i = 1, 2$ seien $K_i \subseteq L_i$ Körpererweiterungen, und es sei L_i ein Zerfällungskörper von f_i über K_i. Dann gibt es einen Körperisomorphismus η': $L_1 \to L_2$ mit $\eta'(c) = \eta(c)$ für $c \in K_1$.* Sind $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f_1 in L_1 und $\alpha'_1, \ldots, \alpha'_n$ die Nullstellen von f_2 in L_2, so gibt es eine Permutation σ von $1, 2, \ldots, n$ mit $\eta(\alpha_i) = \alpha'_{\sigma(i)}$.

Normalitätssatz. *Sei $K \subseteq L$ eine Körpererweiterung. Sei L Zerfällungskörper eines Polynoms $f \in K[T]$. Dann gilt: Jedes irreduzible Polynom in $K[T]$, das in L eine Nullstelle hat, zerfällt über L in Linearfaktoren.*

Beweis: Sei also L Zerfällungskörper des Polynoms $f = \prod_{i=1}^{n}(T - \alpha_i) \in K[T]$ mit $\alpha_1, \ldots, \alpha_n \in L$. Sei $g \in K[T]$ irreduzibel, sei β eine Nullstelle von f in L. Sei $L \subseteq L'$ ein Zerfällungskörper von g über L (es ist ja $g \in K[T] \subseteq L[T]$. Wir zeigen, daß alle Nullstellen von g in L' schon in L liegen, daß also $L = L'$ gilt (und demnach g in L in Linearfaktoren zerfällt). Sei β' eine Nullstelle von g in L'. Betrachte die Unterkörper $K[\beta]$ und $K[\beta']$ von L'. Es gibt einen Isomorphismus η: $K[\beta] \to K[\beta']$ mit $\eta(c) = c$ für alle $c \in K$ und $\eta(\beta) = \beta'$. Betrachte nun die Zerfällungskörper von f über $K[\beta]$ und über $K[\beta']$ (es ist ja $\eta(f) = f$). Es gibt also einen Körperisomorphismus

$$\eta'\colon K[\beta][\alpha_1, \ldots, \alpha_n] \longrightarrow K[\beta'][\alpha_1, \ldots, \alpha_n].$$

Der linke Körper ist aber nichts anderes als L. Die Bilder der α_i unter η' sind von der Form $\alpha_{\sigma(i)}$ für eine Permutation σ, also wird der rechte Körper von K und den Elementen $\alpha_1, \ldots, \alpha_n$ erzeugt und ist demnach ebenfalls gleich L. Also ist $\beta' \in L$.

Eine Körpererweiterung $K \subseteq L$ heißt *normal*, wenn jedes irreduzible Polynom in $K[T]$, das in L eine Nullstelle besitzt, über L in Linearfaktoren zerfällt. (Daß es normale Körpererweiterungen gibt, ist eigentlich ganz überraschend. Aber wie wir gesehen haben: Jeder Zerfällungskörper L eines Polynoms mit Koeffizienten in K ist über K normal. Und Zerfällungskörper kann man ganz einfach konstruieren!)

Ist $f \in K[T]$, so bezeichnen wir mit $\mathcal{Z}_K(f)$ einen Zerfällungskörper von f über K (es sei daran erinnert, daß Zerfällungskörper bis auf Isomorphie eindeutig bestimmt sind). Ist ein Oberkörper L von K gegeben, über dem f in Linearfaktoren zerfällt, so werden wir $\mathcal{Z}_K(f)$ als Unterkörper von L realisieren: $\mathcal{Z}_K(f)$ ist dann der kleinste Unterkörper von L, der alle Wurzeln von f enthält. (Insbesondere denken wir hier an den Fall $K = \mathbb{Q}$ und $L = \mathbb{C}$: Zerfällungskörper von Polynomen $f \in \mathbb{Q}$ werden wir immer als Unterkörper von $\mathbb{C}$ interpretieren.)

4. Beispiel: Endliche Körper.

Sei K ein endlicher Körper, sei $|K| = q$. Da der Primkörper zu K ebenfalls endlich sein muß, ist die Charakteristik von K eine Primzahl, also ist $\mathbb{Z}/p\mathbb{Z}$ ein Unterkörper von K. Nun ist K ein Vektorraum über dem Primkörper, die Dimension sei n (als endlicher Vektorraum ist die Dimension natürlich endlich). Dann gilt also $q = p^n$.

Die Gruppe $K^* = (K^*, \cdot)$ hat die Ordnung $q-1$, also ist die Ordnung eines jeden Elements von K^* ein Teiler von $q-1$, demnach ist $a^{q-1} = 1$ für jedes Element $a \in K^*$ und demnach $a^q = a$ (wir haben $a^{q-1} = 1$ mit a multipliziert). Natürlich erfüllt auch $a = 0$ diese Gleichung, demnach hat das Polynom $T^q - T$ (dies ist ein Polynom in $K[T]$) alle Elemente aus K als Nullstellen: es hat also q paarweise verschiedene Nullstellen und *K ist der Zerfällungskörper dieses Polynoms $T^q - T$ über $\mathbb{Z}/p\mathbb{Z}$.* Als Zerfällungskörpers des Polynoms $T^q - T$ ist K eindeutig bestimmt. Es gilt also: *Bis auf Isomorphie gibt es höchstens einen Körper mit q Elementen.*

Zu zeigen ist noch die Existenz: *Zu jeder Primzahlpotenz q gibt es einen Körper mit q Elementen.* Sei $q = p^n$ für eine Primzahl p. Wir bilden den Zerfällungskörper $L = \mathcal{Z}_{\mathbb{Z}/p\mathbb{Z}}(T^p - T)$ (dieser Körper existiert natürlich) und zeigen, daß er genau q Elemente hat.

Wir zeigen als erstes: In L bilden die Nullstellen von $T^q - T$ einen Unterkörper. Beweis: Sei N die Menge dieser Nullstellen. Ist $\alpha \in N$, so ist auch $-\alpha \in N$, denn aus $\alpha^q = \alpha$ folgt $(-\alpha)^q = (-1)^q \alpha^q = (-1)^q \alpha = -\alpha$ (beachte: für $p = 2$ ist $1 \equiv -1 \mod p$, für p ungerade ist $(-1)^q = -1$). Sind $\alpha, \beta \in N$, so ist auch $\alpha + \beta \in N$ — hier verwendet man ganz essentiell, daß man in Charakteristik p arbeitet: daß $(\alpha + \beta)^q = \alpha^q + \beta^q$ für jede Potenz q von p gilt. Sind $\alpha, \beta \in N$, so ist auch $\alpha\beta \in N$ — dies dagegen verwendet nur die Kommutativität der Multiplikation: $(\alpha\beta)^q = \alpha^q \beta^q$. Insgesamt sehen wir auf diese Weise: N ist ein Unterring von L. Ein Unterring eines Körpers ist aber ein nullteilerfreier kommutativer Ring, und ein endlicher nullteilerfreier kommutativer Ring ist immer ein Körper!

Da N ein Unterkörper von L ist, der alle Nullstellen von $T^q - T$ enthält, gilt $N = L$ (denn als Zerfällungskörper von $T^q - T$ wird L ja über dem Primkörper von der Menge N erzeugt). Dies zeigt: L besteht nur aus den Nullstellen von $T^q - T$.

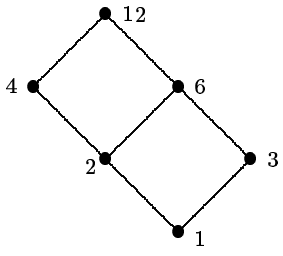
Es bleibt zu zeigen, daß das Polynom $T^q - T$ keine mehrfachen Nullstellen hat (denn dann besteht L genau aus q Elementen). Es ist $T^q - T = T(T^{q-1} - 1)$, und 0 ist keine Nullstelle von $T^{q-1} - 1$, also ist 0 einfache Nullstelle von $T^q - T$. Zu zeigen bleibt also, daß $T^{q-1} - 1$ keine mehrfache Nullstelle hat. Die Ableitung dieses Polynoms ist aber $\overline{q-1}T^{q-2}$, wobei $\overline{q-1}$ die Restklasse von $q-1$ modulo p ist: wichtig ist, daß diese Restklasse nicht $\overline{0}$ ist, aber dies gilt, denn q ist eine Potenz von p. Wegen α von $\overline{q-1} \neq \overline{0}$ hat $\overline{q-1}T^{q-2}$ nur das Nullelement als Nullstelle. Eine mehrfache Nullstelle von $T^{q-1} - 1$ wäre aber Nullstelle der Ableitung $\overline{q-1}T^{q-2}$. Da die die Ableitung aber nur die Null als Nullstelle hat und die Null keine Nullstelle von $T^{q-1} - 1$ ist, sehen wir, daß $T^{q-1} - 1$ keine mehrfachen Nullstellen hat. (Auch ohne abzuleiten läßt sich die Einfachheit der Nullstellen beweisen: Sei α eine Nullstelle von $T^{q-1} - 1$, setze schreibe $g(T) = \sum_{i=0}^{q-2} \alpha^i X^{q-2-i}$, dann ist $T^{q-1} - 1 = (T - \alpha) \cdot g(T)$ (wie man leicht nachrechnet, dabei verwendet man $\alpha^{q-1} = 1$). Da nun $g(\alpha) = (q-1)\alpha^{q-2} \neq 0$ ist, ist α eine einfache Nullstelle.)

Ist q eine Primzahlpotenz, so bezeichnen wir mit $\mathbb{F}_q$ den Körper mit q Elementen (wie wir gezeigt haben, existiert ein solcher Körper und er ist bis auf Isomorphie eindeutig bestimmt).

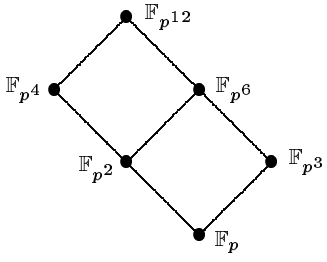
Es sei noch einmal notiert: *In einem endlichen Körper ist* **jedes** *von Null verschiedene Element eine Einheitswurzel.*

Die Unterkörper eines endlichen Körpers. *Seien q, r Primzahlpotenzen. Genau dann ist $\mathbb{F}_q$ isomorph zu einem Unterkörper von $\mathbb{F}_r$, wenn r eine Potenz von q ist.* Ist also $q = p^n$ und $r = (p')^m$, so muß $p = p'$ und n ein Teiler von m sein. *In diesem Fall ist der zu $\mathbb{F}_q$ isomorphe Unterkörper von $\mathbb{F}_r$ die Menge der Nullstellen von $T^q - T$ in $\mathbb{F}_r$.* Beweis: Ist K ein Unterkörper von $\mathbb{F}_r$, der zu $\mathbb{F}_q$ isomorph ist, so ist $\mathbb{F}_r$ ein endlich-dimensionaler K-Vektorraum, die Elementanzahl von $\mathbb{F}_r$ ist demnach eine Potenz von q. Insbesondere sind q, r Potenzen der gleichen Primzahl p, etwa $q = p^n$ und $r = p^m$. Es ist r genau dann eine Potenz von q, wenn n ein Teiler von m ist. In diesem Fall folgt aus $a^q = a$, daß auch $a^r = a$ gilt: dies zeigt, daß der Zerfällungskörper $\mathbb{F}_q$ des Polynoms $T^p - T$ im Zerfällungskörper $\mathbb{F}_r$ des Polynoms $T^r - T$ enthalten ist.

Wir sehen also: *Das Unterkörper-Diagramm des Körpers $\mathbb{F}_{p^n}$ entspricht bijektiv dem Teilerdiagramm von n.* Hier das Beispiel $n = 12$



Teilerdiagramm



Unterkörper von $\mathbb{F}_{p^n}$

Automorphismen endlicher Körper. Sei q eine Potenz von p. Die Abbildung $a \mapsto a^p$ ist ein Körperautomorphismus von $\mathbb{F}_q$, man nennt ihn den *Frobenius-*

Automorphismus F. Die einzigen Elemente von $\mathbb{F}_q$, die unter F invariant bleiben, sind die Elemente des Primkörpers $\mathbb{F}_p$. Beweis: Die Zuordnung $a \mapsto a^p$ ist für jeden Körper multiplikativ, sie ist additiv nur für Körper der Charakteristik p (aber um einen solchen handelt es sich ja bei $\mathbb{F}_q$). Im Fall eines Körpers der Charakteristik p ist diese Abbildung also ein Ring-Homomorphismus. Diese Abbildug ist injektiv, denn aus $a^p = 0$ folgt $a = 0$, da ein Körper nullteilerfrei ist. Als injektive Abbildung $\mathbb{F}_q \to \mathbb{F}_q$ ist F auch surjektiv. Ist $F(a) = a$, also $a^p = a$, so ist a Nullstelle des Polynoms $T^p - T$ und dieses Polynom hat genau p Nullstellen, nämlich die Elemente des Primkörpers.

Die multiplikative Gruppe $\mathbb{F}_q^*$. Wir werden weiter unten sehen, daß jede endliche Untergruppe der multiplikativen Gruppe $(K^*, \cdot)$ eines Körpers K zyklisch ist. Also gilt: *Die Gruppe $\mathbb{F}_q^*$ ist zyklisch.* Ist a ein erzeugendes Element der Gruppe $\mathbb{F}_q^*$, so ist $1, a, a^2, a^3, \ldots, a^{q-2}$ eine Aufzählung der von Null verschiedenen Elemente von $\mathbb{F}_q^*$. Insbesondere gilt: $\mathbb{F}_q = \mathbb{F}_p[a]$.

5. Separabilität.

Sei K ein Körper, sei $f \in K[T]$ irreduzibel. Dann heißt f *separabel*, wenn die Nullstellen von f in einem Zerfällungskörper (und damit in jedem Zerfällungskörper) paarweise verschieden sind. Ein nicht notwendig irreduzibles Polynom heißt separabel, wenn alle irreduziblen Faktoren separabel sind. Statt "nicht-separabel" sagt man meist *inseparabel.* Ist $K \subseteq L$ eine Körpererweiterung, so nennt man $a \in L$ *separabel über K*, wenn das Minimalpolynom von f über K separabel ist.

Zur Analyse der Separabilität von Polynomen kann man das "formale Ableiten" verwenden, siehe den Einschub über Ringe.

Lemma. *Sei K Körper, $f \in K[T]$ irreduzibel. Dann sind äquivalent:*
(i) *f ist nicht separabel über K.*
(ii) $f' = 0$.

Beweis: (ii) $\Longrightarrow$ (i). Sei also $f' = 0$. Es gibt $g \in K[T]$ mit $f(T) = g(T^p)$. Bilde den Zerfällungskörper L_1 von g über K. Über L_1 zerlegt sich $g(T) = \prod(T - \beta_i)$. Sei nun L_2 Zerfällungskörper von $f(T) = \prod(T^p - \beta_i)$ über L_1. In L besitzt also jedes $T^p - \beta_i$ mindestens eine Nullstelle α_i. Es ist demnach $\alpha_i^p = \beta_i$, also ist

$$T^p - \beta_i = T^p - \alpha_i^p = (T - \alpha_i)^p,$$

demnach ist α_i eine p-fache Nullstelle von f. Also ist f nicht separabel über K.

(i) $\Longrightarrow$ (ii). Sei f nicht separabel, dann hat f im Zerfällungskörper L von f eine doppelte Nullstelle α, also ist α Nullstelle von f'. Wir sehen, daß der ggT g der Polynome f und f' nicht 1 ist. Dies gilt unabhängig davon, ob wir f und f' als Polynome in $L[T]$ oder in $K[T]$ betrachten. Nun ist aber $f \in K[T]$ irreduzibel. Da g ein nicht-konstanter Teiler von f ist, muß $g = f$ gelten. Es folgt also: f ist ein Teiler von f'. Da f' kleineren Grad als f hat, ist dies nur möglich für $f' = 0$.

Folgerung 1. *Ist K ein Körper und $f \in K[T]$ ein inseparables irreduzibles Polynom, so ist die Charakteristik von K eine Primzahl p und es gibt ein Polynom $g \in K[T]$ mit $f(T) = g(T^p)$.* Insbesondere teilt p den Grad von f.

Beweis: Dies folgt unmittelbar aus dem Lemma und allgemeinen Überlegungen über das Verschwinden der Ableitung eines Polynoms.

Folgerung 2. *Ist die Charakteristik von K eine Primzahl p und ist die Abbildung $x \mapsto x^p$ surjektiv, so ist jedes Polynom über K separabel.*

Beweis: Sei $f \in K[T]$ irreduzibel und inseparabel. Nach der Folgerung 1 gibt es ein normiertes Polynom $g \in K[T]$ mit $f(T) = g(T^p)$. Sei α eine Nullstelle von f im Zerfällungskörper. Sei $g(T) = \sum_{s\geq 0} b_s T^s$ mit Koeffizienten $b_s \in K$. Nach Voraussetzung gibt es zu jedem b_s ein $c_s \in K$ mit $b_s = c_s^p$, also ist $g(T) = \sum_{s\geq 0} c_s^p T^s$. Es ist

$$0 = f(\alpha) = g(\alpha^p) = \sum\nolimits_{s\geq 0} c_s^p \alpha^{ps} = \left(\sum\nolimits_{s\geq 0} c_s \alpha^s\right)^p,$$

dabei haben wir verwandt, daß p die Charakteristik ist. Es folgt, daß α Nullstelle des normierten Polynoms $h(T) = \sum_{s\geq 0} c_s T^s$ ist. War n der Grad des Polynoms f, so ist der Grad von h gerade $\frac{n}{p}$ und damit echt kleiner als n. Dies widerspricht der Tatsache, daß f das Minimalpolynom von α ist.

Insbesondere gilt: *Ist K ein endlicher Körper, so ist jedes Polynom $f \in K[T]$ separabel.* Denn ist p die Charakteristik von K, so ist die Abbildung $K \to K$ mit $x \mapsto x^p$ ein Ring-Homomorphismus (sie ist mit Addition und Multiplikation verträglich), dessen Kern Null ist (denn aus $x^p = 0$ folgt $x = 0$, da K nullteilerfei ist. Eine injektive Abbildung einer endlichen Menge in sich ist aber immer surjektiv.

Folgerung 3. *Es sei die Charakteristik von K eine Primzahl p und es sei die Abbildung $x \mapsto x^p$ nicht surjektiv. Ist $a \in K$ nicht im Bild dieser Abbildung, so ist das Polynom $T^p - a$ nicht separabel.*

Beweis: Sei L der Zerfällungskörper von $f(T) = T^p - a$, sei α eine Nullstelle von f in L, es ist also $\alpha^p = a$ und demnach $f(T) = T^p - a = T^p - \alpha^p = (T - \alpha)^p$, wegen Charakteristik p. Wir sehen also, daß α p-fache Nullstelle von f ist.

Beispiel. Sei k ein Körper der Charakteristik $p > 0$, sei $k[X]$ der Polynomring in einer Variablen X mit Koeffizienten in k, sei $L = k(X)$ der zugehörige Quotientenring.

Sei K der von X^p erzeugte Unterkörper. Wir zeigen: *Es ist $1, X, \ldots, X^{p-1}$ eine K-Basis von L, insbesondere ist $[L : K] = p$.*

Bezeichnen wir mit R den von k und den Potenzen X^{pi} mit $i \in \mathbb{N}_0$ erzeugten Unterring von L, so läßt sich jedes $c \in K$ in der Form $c = \frac{f}{g}$ mit $f, g \in R$ schreiben. Wir zeigen: *Die Polynome $1, X, \ldots, X^{p-1}$ sind über K linear unabhängig.* Sei also $\sum_{i=0}^{p-1} c_i X^i = 0$ mit $c_i \in K$, sei etwa $c_i = \frac{f_i}{g_i}$, mit $f_i, g_i \in R$. Wir können annehmen (Erweitern, um als Nenner den sogenannten Hauptnenner zu erhalten), daß $g_i = g$ für alle i gilt. Multiplizieren wir die Gleichung $\sum_{i=0}^{p-1} c_i X^i = 0$ mit g, so erhalten wir $\sum_{i=0}^{p-1} f_i \cdot X^i = 0$, dies ist eine Gleichheit im Polynomring $k[X]$, also sind alle Koefizienten des linken Summenpolynoms Null. Nun ist aber $f_i \in R$, dieses Polynom hat also von Null verschiedene Koeffizienten nur für Indizes, die durch p teilbar sind, entsprechend hat $f_i \cdot X^i$ von Null verschiedene Koeffizienten nur für Indizes, die kongruent i modulo p sind. Bei der Summenbildung können sich keine von Null verschiedenen Indizes wegheben - also gilt $f_i = 0$ für alle i. Dies wollten wir zeigen.

Da X^p zu K gehört, sehen wir: $[L : K] = p$ und auch L entsteht aus K durch Adjunktion von X, und das Minimalpolynom von X über K ist $T^p - X^p$. (Hier heißt es aufpassen, denn die bisher verwandte Notation kann hier leicht zu

Mißverständnissen führen: Da L aus K durch Adjunktion von X entsteht, könnten wir $L = K[X]$ schreiben, man muß aber beachten, daß hier $K[X]$ nicht den Polynomring über K, sondern eine p-dimensionale Körpererweiterungen beschreibt. Eigentlich kann es keine Verwirrung geben, denn wenn wir den Polynomring über K bilden, dürfen wir als Variablenbezeichnen keinen Buchstaben verwenden, der schon beim Arbeiten mit K eine Bedeutung hat, also ist es nicht möglich, X als Variablennamen zu nehmen (denn X^p bezeichnet ja ein Element von K); stattdesen können wir aber (wie wir das oben getan haben) als Variablennamen T nehmen. Der Ausdruck $T^p - X^p$ ist also ein ganz normales Polynom der Form $T^p - a$ im Polynomring $K[T]$ (dabei ist $a = X^p \in K$); da dies das Minimalpolynom eines Elements des Erweiterungskörpers L über K ist, ist dies ein irreduzibles Polynom. Wir haben also ein irreduzibles Polynom der Form $T^p - a \in K[T]$ gefunden. Da die Charakteristik von K die Primzahl p ist, ist dies ein inseparables Polynom (genauer: wie kennen ja eine Nullstelle dieses Polynoms, nämlich $X \in L$, und wegen $T^p - X^p = (T - X)^p$ sehen wir, daß X eine p-fache Nullstelle dieses Polynoms ist.)

6. Galois-Theorie.

Wir beschäftigen uns nun mit Automorphismen eines Körpers L (das heißt: mit Körperautomorphismen). Die Menge aller Automorphismen von L bezeichnen wir mit $\operatorname{Aut} K$, dies ist (bezüglich der Hintereinanderschaltung) eine Gruppe, die *Automorphismengruppe des Körpers* K. Ist S eine Menge von Automorphismen von L, so interessiert man sich für die Menge der Elemente $a \in L$, die unter allen Automorphismen in S fixiert werden, man nennt dies die *Invarianten* von S,

$$\operatorname{Inv} S = \{a \in L \mid \eta(a) = a \quad \text{für alle} \quad \eta \in S\}.$$

Es ist offensichtlich, daß $\operatorname{Inv}(S)$ ein Unterkörper von L ist.

Erster Hauptsatz. *Sei G eine endliche Gruppe von Körperautomorphismen eines Körpers L. Dann gilt:*

$$\boxed{[L : \operatorname{Inv} G] = |G|}$$

Beweis: Wir zeigen als erstes: *Sei $|G| = n$. Dann sind je $n+1$ Elemente von L über K linear abhängig* (also $[L : K] \leq |G|$).

Seien also $u_1, \ldots, u_{n+1} \in L$. Sei $G = \{\eta_1, \eta_2, \ldots, \eta_n\}$. Betrachte das lineare homogene Gleichungssystem

$$(*) \qquad \sum_{j=1}^{n+1} \eta_i(u_j) X_j = 0 \quad \text{mit} \quad 1 \leq i \leq n.$$

Insgesamt haben wir n Gleichungen und $n+1$ Unbekannte, es gibt also eine von Null verschiedene Lösung, also ein $0 \neq (c_1, \ldots, c_{n+1}) \in L^{n+1}$. Wir wählen eine derartige Lösung mit minimaler Anzahl von Koeffizienten, die von Null verschieden sind. Wir können voraussetzen, daß $c_1 \neq 0$ gilt (Vertauschung der u_j und entsprechend der X_j) und daß sogar $c_1 = 1$ gilt (Skalarmultiplikation: das Gleichungssystem ist homogen).

Für jedes i haben wir also gegeben:

$$\sum_{j=1}^{n+1} \eta_i(u_j)c_j = 0.$$

Wenden wir $\eta \in G$ auf diese Gleichung an, so erhalten wir

$$\sum_{j=1}^{n+1} \eta\eta_i(u_j)\eta(c_j) = 0,$$

für jedes i. Es ist also $(\eta(c_1), \ldots, \eta(c_{n+1}))$ ebenfalls eine Lösung des Gleichungssystems $(*)$. (Wegen $G = \{\eta\eta_1, \ldots, \eta\eta_n\}$ sind hier nur die Gleichungen vertauscht.) Da es sich um ein homogenes Gleichungssystem handelt, sind die Differenzen zweier Lösungen wieder Lösungen, also ist mit $(c_1, \ldots, c_{n+1})$ und $(\eta(c_1), \ldots, \eta(c_{n+1}))$ auch

$$(c_1 - \eta(c_1), \ldots, c_{n+1} - \eta(c_{n+1})) = (0, c_2 - \eta(c_2), \ldots, c_{n+1} - \eta(c_{n+1}))$$

eine Lösung des Gleichungssystems; dabei erhalten wir die Null rechts wegen $c_1 = 1$ und $\eta(1) = 1$. Wir erhalten also eine Lösung mit weniger von Null verschiedenen Koeffizienten. Wegen der Minimalitätswahl müssen nun **alle** Komponenten Null sein, also gilt $\eta(c_i) = c_i$ für alle $1 \leq i \leq n$ und alle $\eta \in G$. Dies besagt aber: alle c_i gehören zu $\operatorname{Inv} G = K$.

Eines der η_i ist das Einselement, die entsprechende Gleichung lautet demnach

$$\sum_{j=1}^{n+1} u_j c_j = 0,$$

dabei sind die $c_j \in K$ und $0 \neq (c_1, \ldots, c_{n+1})$. Dies besagt aber, daß die Elemente $u_1, \ldots, u_{n+1}$ über K linear abhängig sind.

Es ist nun $K \subseteq L$ eine endliche Körpererweiterung, sei $m = [L : K]$. Wir wissen schon: $m \leq n$. Jedes η_i: $L \to L$ in G ist Fortsetzung der Inklusion $K \to L$. Wir brauchen den Teil (a) von folgendem Lemma, um auch $n \leq m$ zu erhalten.

Lemma: Fortsetzung von Körpermonomorphismen. *Sei η: $K \to L$ ein Körpermonomorphismus. Sei $K \subseteq K'$ eine Körpererweiterungen vom Grad n.*

(a) *Es gibt höchstens n Körpermonomorphismen η': $K' \to L$ mit $\eta'|K = \eta$.* (Man sagt, daß η' eine Fortsetzung von η auf K' ist.)

(b) *Sei $K' = \mathcal{Z}_K(f)$ für ein separables Polynom f, und $\eta(f)$ zerfalle in L in Linearfaktoren. Dann gibt es genau n Fortsetzungen von η auf K'.*

Beweis: Sei $K' = K[\alpha_1, \ldots, \alpha_t]$. Wir bilden Induktion nach t.

(a) Betrachte zuerst den Fall $t = 1$. Sei g das Minimalpolynom von $\alpha = \alpha_1$ über K. Der Grad von g sei n, also ist auch $[K' : K] = n$. Betrachte $\eta(g) \in L[T]$, dies ist ein Polynom vom Grad n über L, hat also höchstens n Nullstellen. Ist η': $K' \to L$ ein Körperisomorphismus mit $\eta'|K = \eta$, so ist $\eta'(\alpha)$ eine dieser n Nullstellen von $\eta(g)$, und η' ist durch η und $\eta'(\alpha)$ eindeutig bestimmt (denn K' hat die K-Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ also kennen wir die Bilder aller Elemente von K' unter η', wenn wir die von K unter η und $\eta'(\alpha)$ kennen — da η' multiplikativ ist, kennen wir die Bilder aller Elemente der Form $c\alpha^i$ mit $c \in K$, denn $\eta'(c\alpha^i) = \eta(c)\eta'(\alpha)^i$; da η' auch additiv ist, kennen wir auch die Bilder aller Summen derartiger Elemente).

Sei nun $t > 1$, sei $K_1 = K[\alpha_1]$ mit $[K_1 : K] = n_1 > 1$. Wie wir gezeigt haben, gibt es höchstens n_1 Körpermonomorphismen $\eta_1 \colon K_1 \to L$ mit $\eta_1 | K = \eta$. Betrachte ein derartiges η_1. Sei $m = \frac{n}{n_1}$, dies ist der Grad von K' über K_1. Nach Induktion gibt es höchstens m Fortsetzung von η_1. Insgesamt gibt es also höchstens $n_1 \cdot m = n$ Fortsetzungen von η auf K'.

(b) Wir können voraussetzen, daß die Elemente $\alpha_1, \ldots, \alpha_t$ Nullstellen des Polynoms f sind. Wieder sei g das Minimalpolynom von α_1 über K, und der Grad von g sei n_1. Das Polynom g ist ein irreduzibler Faktor von f und demnach separabel. Da g separabel über K ist, ist $\eta(g)$ separabel über $\eta(K)$. Nach Voraussetzung zerfällt $\eta(f)$ und damit $\eta(g)$ über L in Linearfaktoren: die Separabilität von g bedeutet, daß $\eta(g)$ in L genau n paarweise verschiedene Nullstellen hat. Wir erhalten also n Fortsetzungen $\eta' \colon K[\alpha_1] \to L$ von η.

Ist $t > 1$, so haben wir also n_1 Körpermonomorphismen $\eta_1 \colon K_1 \to L$ mit $\eta_1 | K = \eta$ konstruiert. Zu jedem η_1 gibt es nach Induktion $m = \frac{n}{n_1}$ Fortsetzung auf K'. Insgesamt haben wir also $n_1 \cdot m = n$ Fortsetzungen von η auf K' konstruiert. Daß es nicht mehr geben kann, wissen wir schon aus (a).

Bemerkungen. 1. Zur Formulierung des Fortsetzungslemmas: Man ist primär am Fall einer Körpererweiterung $K \subseteq L$ interessiert, wobei $\eta \colon K \to L$ die Inklusionsabbildung ist (siehe zum Beispiel das Endes des Beweises des ersten Hauptsatzes). Um alerdings den Beweis induktiv führen zu können, müssen wir die allgemeinere Situation von beliebigen Körpermonomorphismen betrachten.

2. In Anwendungsfällen betrachtet man meist separable Körpererweiterungen; nach dem Satz vom primitiven Element (der noch zu beweisen ist), werden diese Körpererweiterungen von einem Element erzeugt: Der Fall $t = 1$ reicht dann also aus.

Ist $K \subseteq L$ eine Körpererweiterung, so betrachten wir die Menge der Körperautomorphismen von L, die die Elemente von K fixieren:

$$\mathrm{Gal}(L : K) = \{\eta \in \mathrm{Aut}\, L \mid \eta(a) = a \quad \text{für alle} \quad a \in K\},$$

dies ist eine Untergruppe von $\mathrm{Aut}(L)$ (nachrechnen!). Man nennt dies die *Galois-Gruppe* der Körpererweiterung $K \subseteq L$.

Zweiter Hauptsatz. *Sei K ein Körper und $f \in K[T]$ ein separables Polynom. Sei $L = \mathcal{Z}_K(f)$ der Zerfällungskörper von f. Dann gilt*

$$\boxed{|\mathrm{Gal}(L : K)| = [L : K]}$$

.

Beweis: Sei $\eta \colon K \to L$ die Inklusionsabbildung. Nach (b) gibt es genau $[L : K]$ Fortsetzungen von η auf L, dies sind aber genau die Automorphismen von L, die K punktweise fixieren.

Wir wollen nun Körpererweiterungen die Körpererweiterungen $K \subseteq L$, die im ersten wie im zweiten Hauptsatz auftreten, charakterisieren (also solche mit

$K = \operatorname{Inv} G$ für eine endliche Gruppe von Automorphismen von L beziehungsweise solche, bei denen L der Zerfällungskörper eines separablen Polynoms ist) Es wird sich herausstellen, daß dies die "galois'schen" Körpererweiterungen sind: Dabei heißt eine endliche Körpererweiterung $K \subseteq L$ *galois'sch,* falls sie **normal** und **separabel** ist. Zur Erinnerung: Die Körpererweiterung $K \subset L$ heißt normal, wenn jedes irreduzible Polynom in $K[T]$, das in L eine Nullstelle besitzt, über L in Linearfaktoren zerfällt. Sie heißt *separabel,* wenn jedes irreduzible Polynom in $K[T]$, das in L eine Nullstelle besitzt, separabel ist (also im Zerfällungskörper paarweise verschiedene Nullstellen besitzt). Die Körpererweiterung $K \subseteq L$ ist also genau dann normal und separabel (und demnach galois'sch), wenn jedes normierte irreduzible Polynom in $K[T]$, das in L eine Nullstelle besitzt, sich über L als Produkt von Faktoren $T - \alpha_i$ mit paarweise verschiedenen $\alpha_i \in L$ schreiben läßt.

Dritter Hauptsatz. *Sei $K \subseteq L$ eine Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

(1) *$K \subseteq L$ ist eine galois'sche Körpererweiterung.*
(2) *L ist der Zerfällungskörper eines separablen Polynoms $f \in K[T]$.*
(3) *Es ist $K = \operatorname{Inv} \operatorname{Gal}(L : K)$.*
(4) *$K = \operatorname{Inv} G$ für eine endliche Gruppe G von Körperautomorphismen von L.*

Beweis: (1) $\Longrightarrow$ (2). Sei $L = K(\alpha_1, \ldots, \alpha_t)$ mit $\alpha_i \in L$. Sei f_i das Minimalpolynom von α_i über K. Sei $f = \prod_i f_i$. Dann ist f separabel (denn wegen (1) ist jedes f_i separabel). Der Körper L ist der Zerfällungskörper von f über K (denn $K \subseteq L$ ist normale Körpererweiterung).

(2) $\Longrightarrow$ (3). Sei $G = \operatorname{Gal}(L : K)$ und $K' = \operatorname{Inv} G$. Dann ist $K \subseteq \operatorname{Inv} G \subseteq L$. Der erste Hauptsatz liefert $[L : \operatorname{Inv} G] = |G|$, der zweite Hauptsatz liefert $[L : K] = |G|$. Wegen $K \subseteq \operatorname{Inv} G \subseteq L$ und $[L : K] = [L : \operatorname{Inv} G]$ folgt $K = \operatorname{Inv} G$.

(3) $\Longrightarrow$ (4): Nimm $G = \operatorname{Gal}(L : K)$.

(4) $\Longrightarrow$ (1): Sei also G eine endliche Gruppe von Körperautomorphismen von L mit $K = \operatorname{Inv} G$. Der erste Haupsatz besagt, daß $[L : K]$ eine endliche Körpererweiterung ist. Sei $g \in K[T]$ irreduzibel vom Grad t, mit einer Nullstelle $\alpha \in L$. Wir zeigen: g besitzt t paarweise verschiedene Nullstellen in L. Sei $G = \{\eta_1, \ldots, \eta_n\}$. Die Menge $\{\eta_1\alpha, \ldots, \eta_n\alpha\}$ bestehe aus genau r Elementen, etwa aus $\alpha = \alpha_1, \ldots, \alpha_r$. Aus $g(\alpha) = 0$, folgt $g(\alpha_i) = 0$ für alle i (denn ist $\alpha_i = \eta\alpha$ mit $\eta \in G$, so ist

$$g(\alpha_i) = g(\eta\alpha) = (\eta g)(\eta\alpha) = \eta(g(\alpha)) = \eta(0) = 0,$$

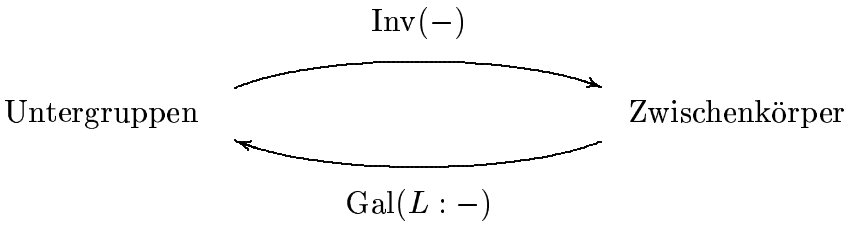
dabei gilt $g = \eta g$, denn die Koeffizienten von g liegen in $K = \operatorname{Inv} G$, und $(\eta g)(\eta\alpha) = \eta(g(\alpha))$, weil η ein Ring-Homomorphismus ist. Sei nun $h(T) = \prod_{i=1}^{r}(T - \alpha_i)$. Dies ist ein nicht-konstantes Polynom in $L[T]$, das ein Teiler von g ist. Wir zeigen, daß die Koeffizienten von h in K liegen: Sei $\eta \in G$. Unter der Anwendung von η werden die Faktoren des Produkts $\prod_{i=1}^{r}(T - \alpha_i)$ nur untereinander vertauscht, also ist $\eta h = h$. Da dies für alle $\eta \in G$ gilt, liegen die Koeffizienten von h in $\operatorname{Inv} G = K$. Da $h \in K[T]$ ein nicht-konstanter Teiler des Minimalpolynoms g ist, folgt $h = g$. Demnach zerfällt g über L in paarweise verschiedene Linearfaktoren.

Bemerkung. Die Äquivalenz dieser vier Bedingungen ist sehr wichtig. Die Implikation (2) $\Longrightarrow$ (1) besagt, daß im Zerfällungskörpers $\mathcal{Z}_K(f)$ eines separablen Polynoms **alle** Elemente über K separabel sind. Der hier notierte Beweis verwendet dabei die Gruppenoperation der Galoisgruppe!.

Die Zuordnungen $\mathrm{Inv}(-)$ und $\mathrm{Gal}(L:-)$ stellen eine Beziehung zwischen den Untergruppen der Galois-Gruppe $\mathrm{Gal}(L:K)$ und den Zwischenkörpern von $K \subseteq L$ her; diese Beziehung wollen wir genauer untersuchen. Wir betrachten also die beiden Mengen

$$\{U \mid U \text{ ist Untergruppe von } G\} \qquad \{Z \mid Z \text{ ist Zwischenkörper von } K \subseteq L\}$$

und die beiden Zuordnungen $\mathrm{Inv}(-)$ und $\mathrm{Gal}(L:-)$:



Vierter Hauptsatz. *Sei $K \subseteq L$ eine galois'sche Körpererweiterung. Ist U eine Untergruppe von* $\mathrm{Gal}(L:K)$*, so gilt*

$$\boxed{U = \mathrm{Gal}(L : \mathrm{Inv}\, U)}$$

. Für jeden Zwischenkörper Z von $K \subseteq L$ gilt

$$\boxed{Z = \mathrm{Inv}(\mathrm{Gal}(L:Z))}$$

.

Umformulierung. *Sei $K \subseteq L$ eine galois'sche Körpererweiterung. Die Zuordnungen* $\mathrm{Inv}(-)$ *und* $\mathrm{Gal}(L:-)$ *liefern eine inklusionsumkehrende Bijektion zwischen den Untergruppen von* $\mathrm{Gal}(L:K)$ *und den Zwischenkörpern von $K \subseteq L$.*

Beweis: Ist $U \subseteq \mathrm{Gal}(L:K)$ eine Untergruppe, so ist $U \subseteq \mathrm{Gal}(L : \mathrm{Inv}\, U)$. Es genügt also zu zeigen, daß diese beiden Gruppen gleiche Ordnung haben. Der erste Hauptsatz besagt $|U| = [L : \mathrm{Inv}\, U]$, und $|\,\mathrm{Gal}(L : \mathrm{Inv}\, U)| = [L : \mathrm{Inv}(\mathrm{Gal}(L : \mathrm{Inv}\, U))]$. Trivialerweise gilt: $\mathrm{Inv}\, U = \mathrm{Inv}(\mathrm{Gal}\, L : \mathrm{Inv}\, U)$, also ist $|U| = |\,\mathrm{Gal}(L : \mathrm{Inv}\, U)|$.

Sei nun Z ein Zwischenkörper von $K \subseteq L$. Mit $K \subseteq L$ ist auch $Z \subseteq L$ galois'sch. Also ist nach dem dritten Hauptsatz $Z = \mathrm{Inv}\,\mathrm{Gal}(L:Z)$.

Das diese Zuordnungen inklusionsumkehrend sind, ist offensichtlich: Sind $U_1 \subseteq U_2$ Untergruppen von $\mathrm{Gal}(L:K)$, so ist $\mathrm{Inv}\, U_1 \supseteq \mathrm{Inv}\, U_2$. Sind $Z_1 \subseteq Z_2$ Zwischenkörper von $K \subseteq L$, so ist $\mathrm{Gal}(L:Z_1) \supseteq \mathrm{Gal}(L:Z_2)$.

Wir wollen uns diese Bijektionen $\mathrm{Inv}(-)$ und $\mathrm{Gal}(L:-)$ noch etwas genauer ansehen. Sei $K \subseteq L$ eine beliebige (nicht notwendig galois'sche) Körpererweiterung. Ist U eine Untergruppe von $G = \mathrm{Gal}(L:K)$, so schreibe $IU = \mathrm{Inv}(U)$. Ist Z ein Zwischenkörper von $K \subseteq L$, so sei $JZ = \mathrm{Gal}(L:Z)$. Es gilt trivialerweise

(a) Sind $U_1 \subseteq U_2$ Untergruppen von G, so ist $IU_1 \supseteq IU_2$.
(a') Sind $Z_1 \subseteq Z_2$ Zwischenkörper von $K \subseteq L$, so ist $IZ_1 \supseteq IZ_2$.

(b) Ist U Untergruppe von G, so ist $U \subseteq JIU$.
(b') Ist Z Zwischenkörper von $K \subseteq L$, so ist $Z \subseteq IJZ$.

Daraus folgt nun unmittelbar:
(c) Ist U Untergruppe von G, so ist $IU = IJIU$.
(c') Ist Z Zwischenkörper von $K \subseteq L$, so ist $JZ = IJZ$.

Beweis: Wenden wir (a) auf (b) an, so erhalten wir $IU \supseteq IJIU$. Wenden wir (b) auf IU an, so erhalten wir $IU \subseteq IJIU$. Also gilt (c). Entsprechend zeigt man (c').

Aus (c) und (c') folgt nun:
(d) *Die Zuordnungen I und J liefern eine Bijektion zwischen der Menge der Untergruppen U von G mit $U = JIU$ und der Menge der Zwischenkörper Z mit $Z = IJZ$.*

Ist nun $K \subseteq L$ galois'sch, so gilt:
(e) Für jede Untergruppe U von G gilt $U = JIU$; für jeden Zwischenkörper Z gilt $Z = IJZ$.

Fünfter Hauptsatz. *Sei $K \subseteq L$ eine galois'sche Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}(L : K)$. Sei Z ein Zwischenkörper von $K \subseteq L$ mit $U = \mathrm{Gal}(L : Z)$. Genau dann ist Z normal über K, wenn U eine normale Untergruppe von G ist. In diesem Fall ist*

$$\boxed{\mathrm{Gal}(Z : K) = G/U}$$

.

Beweis:

Satz vom primitiven Element. *Ist $K \subseteq L$ eine Körpererweiterung mit nur endlich vielen Zwischenkörpern, so gibt es ein $\alpha \in L$ mit $L = K[\alpha]$.*

Beweis: Ist L ein endlicher Körper, so ist L^* eine zyklische Gruppe. Ist $\alpha \in L^*$ ein erzeugendes Element dieser Gruppe, so ist natürlich $L = K[\alpha]$. Also können wir annehmen, daß L und damit auch K unendliche Körper sind. Wir zeigen: Sind $a, b \in L$ mit $L = K[a, b]$, so gibt es $c \in L$ mit $K[a, b] = K[c]$; der Satz folgt daraus mit Induktion.

Betrachte die Unterkörper der Form $K[a+tb]$ mit $t \in K$. Da K unendlich ist, es aber nur endlich viele Zwischenkörper gibt, gibt es $t \neq t'$ mit $K[a+tb] = K[a+t'b]$. Sei $Z = K[a+tb]$. In Z liegt das Element

$$b = \frac{1}{t - t'}\left((a + tb) - (a + t'b)\right)$$

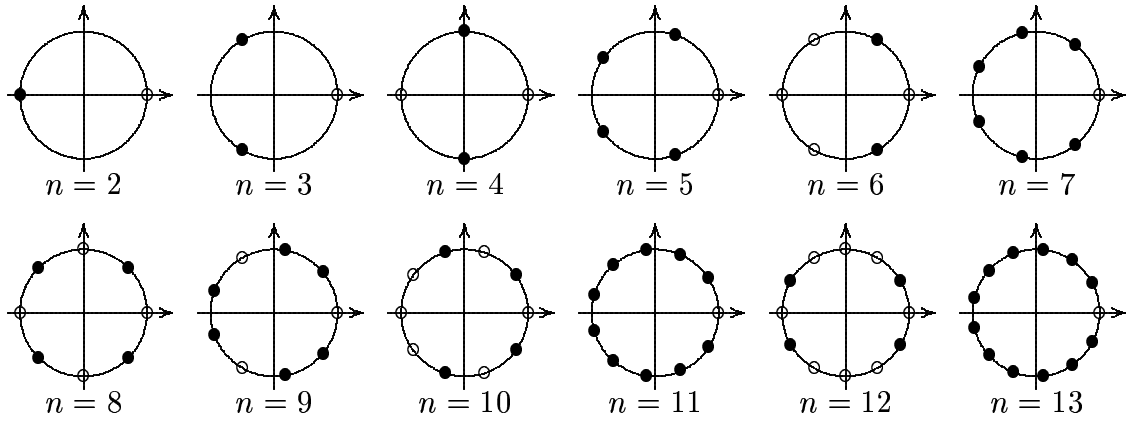
also auch das Element $a = (a + tb) - tb$. Demnach ist $Z = K[a, b]$.

Folgerung. *Ist $K \subseteq L$ eine galois'sche Körpererweiterung, so gibt es ein $\alpha \in L$ mit $L = K[\alpha]$.*

Beweis: Die Galois-Theorie liefert gerade, daß es zu $K \subseteq L$ nur endlich viele Zwischenkörper gibt.

7. Kreisteilungskörper

Einheitswurzeln. Ist K ein Körper, so nennt man die Elemente $\zeta \in K$ mit $\zeta^n = 1$ die *n-ten Einheitswurzeln;* man nennt ζ eine *primitive* n-te Einheitswurzel, falls n die kleinste natürliche Zahl mit $\zeta^n = 1$ ist (wenn also ζ als Element der multiplikative Gruppe $K^* = (K \setminus \{0\}, \cdot)$ die Ordnung n hat). Hier für $2 \leq n \leq 13$ die primitiven n-ten Einheitswurzeln in $\mathbb{C}$:



Beachte: Ist G eine endliche Untergruppe von K^*, so besteht G nur aus Einheitswurzeln!

Satz. *Sei K ein Körper, sei G eine endliche Untergruppe von K^*. Dann ist G zyklisch.*

Beweis: Da G eine endliche Gruppe ist, gibt es eine natürliche Zahl n mit $g^n = 1$ für alle $g \in G$; wir wählen n minimal. Es ist n gerade das kleinste gemeinsame Vielfache der Ordnungen der Elemente von G. Wegen $g^n = 1$ ist jedes $g \in G$ Nullstelle des Polynoms $T^n - 1 \in K[T]$. Ein Polynom n-ten Grads mit Koeffizienten in einem Körper K hat in höchstens n Nullstellen, also sehen wir $|G| \leq n$.

Betrachte die Primfaktorzerlegung $n = p_1^{e_1} \cdots p_t^{e_t}$ von n mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$. Zu $1 \leq i \leq t$ muß es ein Element $h_i \in G$ geben, dessen Odnung durch $p_i^{e_i}$ teilbar ist (sonst wäre n nicht das kleinste gemeinsame Vielfache der Ordnungen der Elemente von G). Ist $p_i^{e_i} m_i$ die Ordnung von h_i, so hat $g_i = h_i^{m_i}$ die Ordnung $p_i^{e_i}$. Die Ordnung von $h = h_1 \cdots h_t$ ist dann gerade n.

Korollar. *Sei q eine Primzahlpotenz. Dann ist $\mathbb{F}_q^*$ eine zyklische Gruppe, also*

$$\boxed{\mathbb{F}_q^* \simeq C_{q-1}}$$

Insbesondere ist also für jede Primzahl p die Gruppe $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ zyklisch. Ein erzeugendes Element dieser Gruppe $\mathbb{F}_p^*$ nennt man *Primitivzahl modulo p*, dies ist also eine Zahl a mit $1 \leq a < p$, so daß die Potenzen $a, a^2, a^3, \ldots, a^{p-1}$ paarweise verschieden sind. Der Beweis des Satzes war ganz einfach, aber in Anwendungen ist es gar nicht immer einfach, für eine vorgegebene endliche Untergruppe von K^*, wie hier für $\mathbb{F}_p^*$ ein erzeugendes Element zu finden. In Zahlentheorie-Lehrbüchern gibt es dazu Listen!

Hier eine kleine Aufstellung:

Primzahl p	2	3	5	7	11	13	17	19	23	31	37
Primitivzahl a	1	2	3	3	2	2	3	2	5	3	2

Die Existenz primitiver n-ter Einheitswurzeln. Sei K ein Körper. Da $X^n - 1$ höchstens n verschiedene Nullstellen in K haben kann, gibt es höchstens n verschiedene n-te Einheitswurzeln. Diese bilden offensichtlich eine Untergruppe von K^*, und dies ist (nach obigem Satz) eine zyklische Gruppe. Gibt es eine primitive n-te Einheitswurzel in K, so gibt es genau n n-te Einheitswurzeln und genau $\phi(n)$ primitive n-te Einheitswurzeln.

Die Kreisteilungspolynome. Sei nun $K = \mathbb{C}$. In $\mathbb{C}$ gibt es zu jedem $n \in \mathbb{N}_1$ eine primitive n-te Einheitswurzel, nämlich $e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Sei E_n die Menge der n-ten Einheitswurzeln in $\mathbb{C}$, und F_n die Teilmenge der primitiven n-ten Einheitswurzeln. Dann ist E_n offensichtlich die disjunkte Vereinigung der Mengen F_d mit $d|n$. Das *n-te Kreisteilungspolynom* Φ_n ist definiert durch

$$\Phi_n(T) := \prod_{\zeta \in F_n} (T - \zeta).$$

Da E_n die disjunkte Vereinigung der Mengen F_d mit $d|n$ ist, und E_d die Menge der Nullstellen von $T^n - 1$ ist, folgt

$$T^n - 1 = \prod_{\zeta \in E_n} (T - \zeta) = \prod_{d|n} \Phi_d(T),$$

also ist

$$\Phi_n(T) = \frac{T^n - 1}{\prod_{d|n, d \neq n} \Phi_d(T)},$$

dies liefert also eine induktive Definition von Φ_n. Es gilt: $\Phi_d(T)$ *ist ein normiertes Polynom in* $\mathbb{Z}[T]$. (Setzt man $g(T) = \prod_{d|n, d\neq n} \Phi_d(T)$, so ist $T^n - 1 = \Phi_d(T) \cdot g(T)$ Nach Induktion ist $g(T)$ normiertes Polynom mit ganzzahligen Koeffizienten. Da auch $T^n - 1$ normiertes Polynom mit ganzzahligen Koeffizienten ist, folgt aus dem Gauß-Lemma, daß $\Phi_d(T)$ ebenfalls normiert mit ganzzahligen Koeffizienten ist.

Offensichtlich ist der Grad von Φ_n gerade $\phi(n)$. Ist p eine Primzahl, so ist $\Phi_p = \sum_{i=0}^{p-1} T^i$. denn $F_n = E_n \setminus \{1\}$, also ist $\Phi_p = \frac{T^p - 1}{T - 1}$.

Satz von Gauß. *Die Kreisteilungspolynome Φ_n sind über $\mathbb{Q}$ irreduzibel.*

Beweis: Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$, sei f das Minimalpolynom von ζ über $\mathbb{Q}$. Wir wollen zeigen: $f = \Phi_n$. Dazu genügt es zu zeigen: Ist p eine Primzahl, die n nicht teilt, so ist auch ζ^p eine Nullstelle von f. (Denn induktiv erhalten wir durch Potenzieren mit geeigneten Primzahlen p, die n nicht teilen, alle primitiven n-ten Einheitswurzeln. Sind aber alle primitiven n-ten Einheitswurzeln Nullstellen von f, so ist der Grad von f mindestens $\phi(n)$. Andererseits ist f ein Teiler von Φ_n.)

Sei also p eine Primzahl, die kein Teiler von n ist. Wir nehmen an, daß ζ^p keine Nullstelle von f ist und wollen dies zum Widerspruch führen. Sei g das Minimalpolynom von ζ^p über $\mathbb{Q}$. Da auch ζ^p eine primitive n-te Einheitswurzel ist, ist auch g ein Teiler

von Φ_n. Wegen $f \neq g$ ist fg ein Teiler von Φ_n. Es gibt also $h \in \mathbb{Q}[T]$ mit $T^n - 1 = fgh$. Da $f, g, T^n - 1$ normierte Polynome sind und $fgh = T^n - 1$ Koeffizienten in $\mathbb{Z}$ hat, sind auch die Polynome $f, g, h \in \mathbb{Z}[T]$ (Gauß-Lemma).

Da ζ eine Nullstelle von $g(T^p)$ ist, ist f ein Teiler von $g(T^p)$, etwa $g(T^p) = f(T)q(T)$, mit $q \in \mathbb{Q}[T]$. Wieder verwenden wir das Gauß-Lemma: es zeigt, daß die Koeffizienten von q in $\mathbb{Z}$ liegen.

Da alle unsere Polynome $f, g, h, q, T^n - 1$ Koeffizienten in $\mathbb{Z}$ haben, können wir modulo p rechnen, wir bezeichnen die entsprechenden Polynome in $\mathbb{F}_p$ mit $\overline{f}, \overline{q}, \ldots$. Sei u ein (normierter) irreduzibler Faktor von $\overline{f}$. Es ist $\overline{g}(T^p) = \overline{g}(T)^p$, denn wir sind nun in Charakteristik p. Da u ein irreduzibler Teiler von $\overline{f}$ und $\overline{f}$ ein Teiler von $\overline{g}(T^p) = \overline{g}^p$ ist, ist u ein Teiler von $\overline{g}$. Also ist u^2 ein Teiler von $\overline{f}\,\overline{g}\,\overline{h} = T^n - \overline{1}$, und demnach ist u ein Teiler der Ableitung von $T^n - \overline{1}$. Die Ableitung von $T^n - \overline{1}$ ist aber $\overline{n}T^{n-1}$. Da p kein Teiler von n ist, ist $\overline{n}T^{n-1} \neq 0$ und das einzige (normierte) irreduzible Polynom, das $\overline{n}T^{n-1}$ teilt, ist $u = X$. Aber $u = X$ ist kein Teiler von $X^n - 1$. Dieser Widerspruch bedeutet, daß unsere Annahme falsch war: Demnach muß ζ^p Nullstelle von f sein.

Umformulierung. *Sei $n \in \mathbb{N}_1$ und ζ eine primitive n-te Einheitswurzel. Dann ist* $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(n)$.

Beweis: Setzen wir voraus, daß Φ_n irreduzibel ist, so ist Φ_n das Minimalpolynom von ζ und der Grad von Φ_n ist $\phi(n)$. Der Grad der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\zeta]$ ist aber der Grad des Minimalpolynoms von ζ.

Wir wollen aber auch zeigen, daß aus $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(n)$ folgt, daß Φ_n irreduzibel ist: Der Grad der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\zeta]$ ist der Grad des Minimalpolynoms f von ζ. Es ist f ein Faktor von Φ_n. Nach Voraussetzung hat f den Grad $\phi(n)$. Da auch Φ_n den Grad $\phi(n)$ hat, folgt $f = \Phi_n$ und demnach ist Φ_n irreduzibel.

Es sei ζ eine primitive n-Einheitswurzel und a eine natürliche Zahl mit $(a, n) = 1$. Dann ist auch ζ^a eine primitive n-te Einheitswurzel. Da Φ_n irreduzibel ist, ist Φ_n das Minimalpolynom aller seiner Nullstellen in $\mathbb{C}$. Es ist eine Nullstelle gegeben, nämlich ζ, die übrigen sind von der Form ζ^a (für ein a mit $1 \leq a \leq n$ und $(a, n) = 1$). Alle diese Potenzen von ζ liegen in $\mathbb{Q}[\zeta]$, also gilt: Φ_n *zerfällt über* $\mathbb{Q}[\zeta]$ *in Linearfaktoren.* Und wir sehen: Die Zuordnung $\zeta \mapsto \zeta^a$ liefert einen eindeutig bestimmten Automorphismus von $\mathbb{Q}[\zeta]$, der mit g_a bezeichnet werden soll. (Im allgemeinen gilt: Ist eine primitive Körpererweiterung $K[\alpha]$ eines Körpers K gegeben, ist f das Minimalpolynom von α über K, und ist β eine weitere Nullstelle von f in $K[\alpha]$ so erhält man durch $\alpha \mapsto \beta$ und $c \mapsto c$ für $c \in K$ einen **eindeutig bestimmten** Automorphismus von $K[\alpha]$; da jeder Automorphismus eines Körpers den Primkörper elementweise fixiert und $\mathbb{Q}$ der Primkörper von $\mathbb{Q}[\alpha]$ ist, brauchen wir die Bedingung $c \mapsto c$ für alle $c \in \mathbb{Q}$ nicht notieren: sie ist automatisch erfüllt.)

Dieser Automorphismus g_a von $\mathbb{Q}[\zeta]$ hat die folgende Eigenschaft: jede n-te Einheitswurzel ζ' wird in die a-te Potenz gehoben: $g_a(\zeta') = (\zeta')^a$. (Denn $\zeta' = \zeta^m$ für eine natürliche Zahl m, also

$$g_a(\zeta') = g_a(\zeta^m) = (g_a(\zeta))^m = (\zeta^a)^m = \zeta^{am} = (\zeta^m)^a = (\zeta')^a,$$

dabei ist das einzig interessante Gleichheitszeichen das zweite: hier verwenden wir, daß g_a multiplikativ ist.) Wir erhalten durch $a \mapsto g_a$ eine Bijektion zwischen den zu n teilerfremden Zahlen zwischen 1 und n und den Automorphismen von $\mathbb{Q}[\zeta]$.

Wir zeigen noch, daß für zwei zu n teilerfremde Zahlen a, a' gilt: $g_a g_{a'} = g_{aa'}$. Zum Beweis genügt es, beide Seiten auf ζ auszuwerten:

$$g_a g_{a'}(\zeta) = g_a(\zeta^{a'}) = \zeta^{a'a} = g_{aa'}(\zeta).$$

Wir sehen also, daß die Hintereinanderschaltung der Automorphismen der Multiplikation in $\mathbb{Z}/n\mathbb{Z}$ entspricht. Insgesamt haben wir gezeigt:

Korollar. *Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann ist $\mathbb{Q} \subseteq \mathbb{Q}[\zeta]$ eine galois'sche Körpererweiterung vom Grad $\phi(n)$ mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^*$;* dabei wird jedem $a \in \mathbb{Z}$ mit $1 \leq a \leq n$ und $(a, n) = 1$ der Automorphismus $\zeta \mapsto \zeta^a$ zugeordnet:

$$\boxed{\mathrm{Gal}(\mathbb{Q}[\zeta] : \mathbb{Q}]) \;\simeq\; (\mathbb{Z}/n\mathbb{Z})^*}$$

Beispiel: Sei $n = 12$. Es ist $\phi(12) = 4$. Ist ζ eine primitive 12-te Einheitswurzel in $\mathbb{C}$, so ist $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 4$, also hat $G = \mathrm{Gal}(\mathbb{Q}[\zeta] : \mathbb{Q}])$ die Ordnun g 4. Wie sehen diese vier Automorphismen aus? Es sind dies gerade die Automorphismus g_a von $\mathbb{Q}[\zeta]$ mit $g_a(\zeta) = \zeta^a$ und $a = 1, 5, 7, 11$ (denn $\{1, 5, 7, 11\}$ ist die Menge der zu 12 teilerfremden Zahlen zwischen 1 und 12). Es ist

$$\begin{aligned} 5^2 &= 25 \equiv 1 \mod 12, \\ 7^2 &= 49 \equiv 1 \mod 12, \\ 11^2 &= 121 \equiv 1 \mod 12, \end{aligned}$$

und demnach also $g_5^2 = g_{5^2} = g_1$ usw. Also haben die Automorphismen g_5, g_7, g_{11} die Ordnung 2 und demnach ist G die Klein'sche Vierergruppe.

Bemerkung. Eine ganz wichtige Einsicht ist zu betonen: *Die Galoisgruppe von* $\mathrm{Gal}(\mathbb{Q}[\zeta) : \mathbb{Q})$ *ist abelsch.* Es gilt der **Satz von Kronecker-Weber:** *Ist $\mathbb{Q} \subset K$ eine galois'sche Körpererweiterung mit abelscher Galois-Gruppe, so ist K Unterkörper eines Kreisteilungskörpers.* (Das ist aber nicht einfach zu zeigen!)

Insbesondere schauen wir uns den Fall einer Primzahl $n = p$ an:

Satz. *Ist p eine Primzahl und ζ eine primitive p-te Einheitswurzel in $\mathbb{C}$, so gilt:*

$$\boxed{\mathrm{Gal}(\mathbb{Q}[\zeta] : \mathbb{Q}]) \;\simeq\; C_{p-1}}$$

Beweis: Dies folgt aus dem letzten Korollar und der Tatsache, daß die multiplikative Gruppe $\mathbb{F}_p^*$ zyklisch ist.

Da wir die Untergruppen einer zyklischen Gruppe mühelos überblicken, können wir auf diese Weise alle Unterkörper von dieser Kreisteilungskörper $\mathbb{Q}[\zeta]$ bestimmen! Wir verwenden dazu die folgende Indizierung der primitiven p-ten Einheitswurzeln:

- Wähle eine beliebige primitive p-te Einheitswurzel ζ_0
- Wähle eine Primitivzahl a modulo p

- Setze nun

$$\boxed{\zeta_i = (\zeta_0)^{a^i}.}$$

Weil a eine Primitivzahl modulo p ist, sind die Restklassen von

$$1 = a^0, a^1, a^2, \ldots a^{p-2}$$

modulo n paarweise verschieden: dies ist also eine Liste der Restklassen $\overline{1}, \overline{2}, \ldots, \overline{p-1}$, also ist

$$\zeta_0, \zeta_1, \ldots, \zeta_{p-2}$$

eine vollständige Liste der primitiven p-ten Einheitswurzeln.

Da a eine Primitivzahl modulo p ist, erzeugt $g = g_a$ die Galois-Gruppe $G = \mathrm{Gal}(\mathbb{Q}[\zeta] : \mathbb{Q}])$. Um zu wissen, wie G auf der Menge der primitiven p-ten Einheitswurzeln operiert, reicht es zu wissen, wie g auf dieser Menge operiert. Nach unserer Indizierung gilt:

$$\boxed{g(\zeta_i) = \zeta_{i+1} \quad \text{für} \quad 0 \leq i \leq p-1}$$

(dabei sei wie üblich $\zeta_{p-1} = \zeta_0$ gesetzt): *Es ist also g auf der Menge $\{\zeta_0, \zeta_1, \ldots, \zeta_{p-2}\}$ eine zyklische Permutation!.*

- Ist m ein Teiler von $p-1$, so erzeugt g^m eine (= die) Untergruppe von G der Ordnung $\frac{p-1}{m}$. Wie sieht $\mathrm{Inv}(g^m)$ aus?

Natürlich ist

$$\eta_i(d) = \sum\nolimits_{j=0}^{d-1} \zeta_{i+jm} = \zeta_i + \zeta_{i+m} + \zeta_{i+(d-1)m}$$

unter g^m invariant! Man nenn diese Elemente die *d-gliedrigen Gauß'schen Perioden.* Es gibt genau m verschiedene d-gliedrige Gauß'sche Perioden, nämlich $\eta_0(d), \eta_1(d), \ldots, \eta_{m-1}(d)$.

Satz. *Sei $p - 1 = md$. Dann ist*

$$\boxed{\mathrm{Inv}(g^m) = \mathbb{Q}[\eta_0(d)]}$$

und dieser Körper hat als $\mathbb{Q}$-Basis die Menge der d-gliedrigen Gauß'schen Perioden, insbesondere ist $[\mathrm{Inv}(g^m) : \mathbb{Q}] = m$. Wegen

$$\boxed{g(\eta_i(d)) = \eta_{i+1}(d) \quad \text{für} \quad 0 \leq i \leq p-1}$$

liefert g einen Automorphismus der Ordnung m von $\mathrm{Inv}(g^m)$, insbesondere ist also $\mathbb{Q} \subseteq \mathrm{Inv}(g^m)$ wieder galois'sch (und wieder mit zyklischer Galois-Gruppe).

Beweis: Die d-gliedrigen Gauß'schen Perioden $\eta_0(d), \eta_1(d), \ldots, \eta_{m-1}(d)$ sind offensichtlich linear unabhängig über $\mathbb{Q}$ und gehören zu $\mathrm{Inv}(g^m)$. Die Galois-Theorie besagt:

$$[\mathbb{Q}[\zeta] : \mathrm{Inv}(g^m)] = |\langle g^m \rangle| = d,$$

also ist

$$[\mathrm{Inv}(g^m) : \mathbb{Q}] = \tfrac{p-1}{d} = m$$

und demnach sind die d-gliedrigen Gauß'schen Perioden auch ein Erzeugendensystem von $\mathrm{Inv}(g^m)$.

Insbesondere wissen wir, daß $\mathbb{Q}[\eta_0(d)]$ ein Unterkörper von $\mathrm{Inv}(g^m)$ ist. Wäre dies eine echte Inklusion, so wäre $\mathbb{Q}[\eta_0(d)] = \mathrm{Inv}(g^{m'})$, wobei m' ein echter Teiler von m wäre (wieder verwenden wir die Galois-Theorie und das Wissen über die Untergruppen zyklischer Gruppen). Aber $\eta_0(d)$ ist unter $g^{m'}$ nicht invariant, denn $g^{m'}(\zeta_0 + \zeta_m + \cdots + \zeta_{(d-1)m}) = \zeta_{m'} + \ldots$ und dieser Summand ζ'_m taucht in $\eta_0(d)$ nicht auf!

$$\begin{array}{rcl} \mathbb{Q}[\zeta] & \Big| & \langle g^{p-1}\rangle = \{1\} \\ & \Big| d & \\ \mathbb{Q}[\eta_0(d), \ldots, \eta_{m-1}(d)] & + & \langle g^m\rangle \\ & \Big| & \\ \mathbb{Q}[\eta_0(d)] & + & \langle g^{m'}\rangle \\ & \Big| & \\ \mathbb{Q} & \Big| & \langle g\rangle \end{array}$$

Beispiel: $p = 5$. Sei ζ_0 primitive 5-te Einheitswurzel, es ist $a = 2$ Primitivzahl modulo 5, also indizieren wir die primitiven 5-ten Einheitswurzeln wie folgt:

$$\zeta_0, \quad \zeta_1 = \zeta^2, \quad \zeta_2 = \zeta^4, \quad \zeta_3 = \zeta^8 = \zeta^3.$$

Es gibt genau einen echten Zwischenkörper $\mathbb{Q} \subset L \subset \mathbb{Q}[\zeta_0]$, nämlich $L = \mathbb{Q}[\zeta_0 + \zeta_2] = \mathbb{Q}[\zeta_0 + \zeta_0^4]$.

$$\begin{array}{rcl} \mathbb{Q}[\zeta] & \Big| & \langle g^4\rangle = \{1\} \\ & \Big| 2 & \\ \mathbb{Q}[\eta_0(2)] & + & \langle g^2\rangle \\ & \Big| 2 & \\ \mathbb{Q} & \Big| & \langle g\rangle \end{array}$$

Den Körper $\mathbb{Q}[\eta_0(2)]$ kann man auch anders beschreiben. Das Minimalpolynom f von $z = \zeta_0 + \zeta_2$ hat den Grad 2 und als zweite Nullstelle $\zeta_1 + \zeta_3$ (denn g vertauscht diese beiden Elemente). Also

$$f(T) = (T - (\zeta_0 + \zeta_2))(T - (\zeta_1 + \zeta_3)) = T - aT + b,$$

für geeignete $a, b \in \mathbb{Q}$. Es ist $a = \zeta_0 + \zeta_1 + \zeta_2 + \zeta_3 = -1$, denn die Summe der primitiven p-ten Einheitswurzeln, p Primzahl, ist immer -1, da die Summe aller n-ten Einheitswurzeln für jedes $n > 1$ Null ist: dies sieht man an der Faktorisierung $T^n - 1 = (T-1)(T^{n-1} + T^{n-2} + \cdots + T + 1)$. Es ist $b = (\zeta_0 + \zeta_2)(\zeta_1 + \zeta_3) = (\zeta + \zeta^4)(\zeta^2 + \zeta^3) = a$, also ist

$$f(T) = T^2 + T - 1$$

und die Nullstellen dieses Polynoms sind bekanntlich $-\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1}{2}(-1 \pm \sqrt{5})$. Es folgt: $\mathbb{Q}[\eta_0(2)] = \mathbb{Q}[\sqrt{5}]$.

Das Minimalpolynom g von ζ_0 über $\mathbb{Q}[\sqrt{5}]$ ist

$$h(T) = T^2 - zT + 1 \quad \text{mit} \quad z = \zeta_0 + \zeta_2,$$

denn $h(T) = (T-\zeta_0)(T-\zeta_2)$, da g die Elemente ζ_0, ζ_2 vertauscht und $\mathbb{Q}[\sqrt{5}]$ fixiert. Also $h(T) == T^2 - (\zeta_0+\zeta_2)T + \zeta_0\zeta_2$ und $\zeta_0\zeta_2 = 1$.

Bemerkung 1. *Sei ζ eine primitive p-te Einheitswurzel in $\mathbb{C}$, sei $p-1 = dm$. Die Menge der d-gliedrigen Gauß'schen Perioden im Kreisteilungskörper $\mathbb{Q}[\zeta]$ hängt weder von der Auswahl von ζ noch der Primitivzahl a modulo p ab.* Beweis: Eine andere primitive p-te Einheitswurzel ist von der Form $\zeta' = \zeta^{a^r}$ für ein r und eine d-gliedrige Periode gebildet ausgehend von ζ' ist

$$\sum_{j=0}^{d-1} (\zeta')^{a^{i+jm}} = \sum_{j=0}^{d-1} (\zeta^{a^r})^{a^{i+jm}} = \sum_{j=0}^{d-1} (\zeta^{a^{r+i+jm}} = \eta_{r+i}(d).$$

Eine anderer Primitivzahl modulo p ist modulo p kongruent zu einem a^s mit $(s, p-1) = 1$. Eine d-gliedrige Periode gebildet bezüglich a^s ist

$$\sum_{j=0}^{d-1} \zeta^{(a^s)^{i+jm}} = \sum_{j=0}^{d-1} \zeta^{a^{si+(sj)m}} = \eta_{si}(d),$$

dabei verwenden wir folgendes: duchläuft j die Menge $\{0, 1, \ldots, d-1\}$, so durchläuft sj ebenfalls alle Restklassen modulo m, denn $(s, p-1) = 1$.

Bemerkung 2. Sei $p \geq 3$ Primzahl, seien η_0 und η_1 die beiden $\frac{p-1}{2}$-gliedrigen Perioden im p-ten Kreisteilungskörper. Dann ist

$$\eta_0\eta_1 = \begin{cases} \frac{1-p}{4} & \text{falls} \quad p \equiv 1 \mod 4, \\ \frac{1+p}{4} & \text{falls} \quad p \equiv 3 \mod 4, \end{cases}$$

dies rechnet man recht einfach nach. Nun sind aber η_0, η_1 die Nullstellen des Polynoms $(T-\eta_0)(T-\eta_1) = T^2 + T + \eta_0\eta_1$, denn $\eta_0 + \eta_1 = -1$. Also gilt:

$$\eta_0, \eta_1 = -\frac{1}{2} \pm \sqrt{(-1)^{\frac{p-1}{2}} p}$$

Daraus folgt: *Ist K ein quadratischer Zahlkörper (also ein Körper mit $[K : \mathbb{Q}] = 2$) dann liegt K in einem geeigneten Kreisteilunskörper.* (Dies also ein Spezialfall des Satzes von Kronecker-Weber). Beweis: Es ist $K = \mathbb{Q}[\sqrt{c}]$ dabei ist $c \neq 1$ eine quadratfreie ganze Zahl, also $a = -1$ oder $a = \pm p_1 \cdots p_t$ mit Primzahlen $p_1 < p_2 < \cdots < p_t$ und $t \geq 1$. Dann ist K im n-ten Kreisteilungskörper mit $n = 4p_1 \cdots p_t$ enthalten (denn $\mathbb{Q}[\sqrt{-1}]$ ist der 4-te Kreisteilungkörper, also enthält der $4p$-te Kreisteilungskörper sowohl $\sqrt{p}$ als auch $\sqrt{-p}$).

8. Konstruktionen mit Zirkel und Lineal.

Vorbemerkung: Körpererweiterungen vom Grad 2. *Ist $K \subset L$ eine Körpererweiterung vom Grad 2, und ist K kein Körper der Charakteristik 2, so gibt es $a \in L \setminus K$ mit $a^2 \in K$.*

Beweis: Sei $b \in L \setminus K$. Das Minimalpolynom f von b über K hat den Grad 2, ist also von der Form $f(T) = T^2 + cT + d$ mit $c, d \in K$. Wegen der Voraussetzung, daß die Charakteristik von K von 2 verschieden ist, können wir das Element $a = b + \frac{1}{2}c$ bilden, es gehört ebenfalls zu $K \setminus L$ und es ist $a^2 = (b + \frac{1}{2}c)^2 = b^2 + bc + \frac{1}{4}c^2 = -d + \frac{1}{4}c^2 \in K$ (wir verwenden hier $0 = f(b) = b^2 + bc + d$).

Gegeben sei die euklid'sche Ebene $\mathbb{R}^2$ (die wir mit der Menge $\mathbb{C}$ der komplexen Zahlen identifizieren wollen. Induktion definieren wir die Menge $\mathcal{K}$ der Punkte in der Ebene, die ausgehend von $0 = [0\ 0]$ und $1 = [1\ 0]$ mit Zirkel und Lineal konstruiert werden können. Dabei konstruieren wir neue Punkte induktiv wie folgt:

(G) Sind zwei Punkte $a \neq b$ schon konstruiert, so zeichne man die Gerade durch a und b (Verwendung des Lineals).

(K) Sind drei Punkte a, b, c mit $b \neq c$ schon konstruiert, so zeichne man den Kreis mit Radius $||b - c||$ um den Punkt a (Verwendung des Zirkels: Man greift den Abstand von b und c ab, und schlägt um a den Kreis mit diesem Radius).

(S) Schnittpunkte von Geraden mit Geraden, von Geraden und Kreisen und von Kreisen mit Kreisen, die nach (G) und (K) konstruiert wurden, sind neu konstruierte Punkte. Die Menge $\mathcal{K}$ besteht also aus all den Punkten der Ebene, die durch endlich viele Konstruktionsschritte erhalten werden.

Satz 1. *Sei $a \in \mathbb{C}$. Genau dann gehört a zu $\mathcal{K}$, wenn es einen Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$ mit $[K_i : K_{i-1}] = 2$ für alle $1 \leq i \leq n$ und $a \in K_n$ gibt.*

Beweis: langwierig, aber einfach. Verwendet wird fast die ganze Mittelstufengeometrie: Strahlensätze und Höhensatz, aber auch die algebraische Beschreibung von Geraden und Kreisen in der Ebene.

Satz 2. *Sei $a \in \mathbb{C}$ mit Minimalpolynom f über $\mathbb{Q}$. Genau dann gehört a zu $\mathcal{K}$, wenn $[\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q}]$ eine Zweierpotenz ist.*

Beweis: Die Körpererweiterung $\mathbb{Q} \subseteq \mathcal{Z}_{\mathbb{Q}}(f)$ ist galois'sch. Es ist $[\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q}]$ die Ordnung der Galois-Gruppe $G = \mathrm{Gal}(\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q})$. Ist aber $|G| = 2^n$, so besitzt G als 2-Gruppe eine Kette von Untergruppen

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

mit $[G_i : G_{i+1}] = 2$. Die Galois-Korrespondenz liefert entsprechend Zwischenkörper

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = \mathcal{Z}_{\mathbb{Q}}(f)$$

mit $[K_i : K_{i-1}] = 2$ für alle $1 \leq i \leq n$.

Umgekehrt sei ein Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$ mit $[K_i : K_{i-1}] = 2$ für alle $1 \leq i \leq n$ und $a \in K_n$ gegeben. Es gibt Elemente $a_i \in K_i$ mit $K_i = K_{i-1}[a_i]$ und $a_i^2 \in K_{i-1}$. Sei g_i das Minimalpolynom von a_i über $\mathbb{Q}$, und $E_i = \mathcal{Z}(g_1 \cdots g_i) \subseteq \mathbb{C}$. Da wir alle E_i als Unterkörper von $\mathbb{C}$ interpretieren, sieht man unmittelbar, daß sowohl K_i als auch E_{i-1} Unterkörper von E_i sind. Mit Induktion zeigen wir, daß $[E_i : \mathbb{Q}]$ eine Zweierpotenz ist. Für $i = 0$ ist nichts zu zeigen. Sei schon gezeigt, daß

$[E_{i-1} : \mathbb{Q}]$ eine Zweierpotenz ist, für ein $1 \leq i \leq n$. Seien $b_1, \ldots, b_t$ die Nullstellen von g_i in E_i, dabei können wir voraussetzen, daß $b_1 = a_i$ gilt. Es entsteht also E_i aus E_{i-1} durch Adjunktion der Elemente $b_1, \ldots, b_t$. Die Galois-Gruppe operiert transitiv auf den Elementen $b_1, \ldots, b_t$, es gibt also zu b_j einen Automorphismus η von E_i mit $\eta(b_1) = b_j$. Da $\mathbb{Q} \subseteq E_{i-1}$ eine normale Körpererweiterung ist, wird E_{i-1} vom der Automorphismus η in sich abgebildet. Nun ist aber $b_1^2 = a_i^2 \in E_{i-1}$, also ist auch $b_j^2 = \eta(b_1)^2 = \eta(b_1^2)$ in E_{i-1}. Demnach enthält E_{i-1} die Elemente $b_1^2, \ldots, b_t^2$. Betrachten wir den Körperturm

$$E_{i-1} \subseteq E_{i-1}[b_1] \subseteq E_{i-1}[b_1, b_2] \subseteq \cdots \subseteq E_{i-1}[b_1, \ldots, b_t] = E_i,$$

so haben alle diese Körpererweiterungen den Grad 1 oder 2. Insgesamt sehen wir, daß $[E_i : E_{i-1}]$ eine Zweierpotenz ist. Da nach Induktion $[E_{i-1} : \mathbb{Q}]$ eine Zweierpotenz ist, folgt die Behauptung.

Nun ist $\mathcal{Z}_{\mathbb{Q}}(f)$ ein Unterkörper von E_n. Da $[E_n : \mathbb{Q}]$ eine Zweierpotenz ist, ist auch $[\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q}]$ eine Zweierpotenz.

Warnung: Es gibt viele algebraische Elemente in $\mathbb{C}$, die nicht zu $\mathcal{K}$ gehören, deren Minimalpolynome aber als Grad Zweierpotenzen haben. Nimm etwa die Nullstellen eines irreduziblen Polynoms vom Grad 4 über $\mathbb{Q}$, dessen Galois-Gruppe die A_4 oder die S_4 ist.

Das Deli'sche Problem: Verdopplung eines Würfels. Ist ein Würfel mit Kantenlänge a gegeben, so hat der Würfel mit doppeltem Rauminhalt die Kantenlänge $\sqrt[3]{2}a$. Es fragt sich also: Ist $\sqrt[3]{2}$ mit Zirkel und Lineal konstruierbar? Nein, denn das Minimalpolynom von $\sqrt[3]{2}$ ist $T^3 - 2$, und dieses Polynom ist irreduzibel über $\mathbb{Q}$.

Quadratur des Kreises. *Die Zahl π kann nicht mit Zirkel und Lineal konstruiert werden*, denn sie ist nicht einmal algebraisch (Beweis: siehe zum Beispiel Jacobson, Basic Algebra I). Es ist daher unmöglich, ein Quadrat mit Zirkel und Lineal zu konstruieren, dessen Flächeninhalt gleich des Einheitskreises ist (der Flächenhalt des Kreises mit Radius r ist πr^2, der des Einheitskreises also π; gesucht wäre also ein Quadrat mit Kantenlänge $\sqrt{\pi}$).

Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal. Diese Aufgabe entspricht gerade der Aufgabe, eine primitive n-te Einheitswurzel mit Zirkel und Lineal zu konstruieren.

Satz. *Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Genau dann ist ζ mit Zirkel und Lineal konstruierbar, wenn gilt:*

$$n = 2^e p_1 \cdots p_t \quad \text{mit Fermat'schen Primzahlen} \quad p_1 < p_2 < \cdots < p_t.$$

Dabei heißt eine Primzahl p eine *Fermat'schen Primzahl,* wenn $p-1$ eine Zweierpotenz ist.

Beweis: Ist ζ in $\mathcal{K}$, so muß der Grad $\phi(n)$ des Minimalpolynoms von ζ auf jeden Fall eine Zweierpotenz sein. Dies zeigt, daß n die angegebene Form haben muß. Umgekehrt sei nun $n = 2^e p_1 \cdots p_t$ mit Fermat'schen Primzahlen $p_1 < p_2 < \cdots < p_t$. Es ist dann $\phi(n)$ eine Zweierpotenz. Da $\mathbb{Q} \subseteq \mathbb{Q}[\zeta]$ eine galois'sche Erweiterung mit Index ϕ ist, ist $\zeta \in \mathbb{K}$.

Um also eine primitive n-te Einheitswurzel (oder eben ein regelmäßiges n-Eck) zu konstruieren, geht man wie folgt vor: Sind m_1, m_2 teilerfremde Zahlen mit $n = m_1 m_2$, und hat man eine primitive m_1-te und eine primitive m_2-te Einheitswurzel konstruiert, so kann man mit Hilfe der Bézout'schen Gleichung sofort eine primitive n-te Einheitswurzel konstruieren. Also reicht es, den Fall einer Primzahlpotenz zu betrachten. Ist n eine Zweierpotenz, so muß man iterativ Winkel halbieren, dies geht unproblematisch mit Zirkel unde Lineal. Ist $n = p = 2^s + 1$ eine Fermat'sche Primzahl, und ζ eine primitive n-te Einheitswurzel, so ist $G = \mathrm{Gal}(\mathbb{Q}[\zeta] : \mathbb{Q})$ eine zyklische 2-Gruppe: sie besitzt eine (und nur eine) Kette von Untergruppen

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_s = G$$

mit $[G_i : G_{i+1}] = 2$. Die Galois-Korrespondenz liefert entsprechend Zwischenkörper

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_s = \mathbb{Q}[\zeta]$$

mit $[K_i : K_{i-1}] = 2$ für alle $1 \leq i \leq s$. Der Körper K_i wird von den 2^{s-i}-gliedrigen Gauß'schen Perioden erzeugt.

Zusatz. *Ist $s \in \mathbb{N}$ und ist $2^s + 1$ eine Primzahl, so ist s eine Zweierpotenz.* Fermat'sche Primzahlen sind also von der Form $2^{2^s} + 1$.

Beweis: Seien s, t natürliche Zahlen und $t > 1$ ungerade. Dann ist $2^{st} + 1$ keine Primzahl, denn es gilt

$$2^{st} + 1 = (2^s + 1)(2^{s(t-1)} - 2^{(s(t-2)} + \cdots - 2^s + 1).$$