Die einzigen Fermat'schen Primzahlen, die man kennt, sind die folgenden:

$$\begin{aligned} 2^1 + 1 &= 3, \\ 2^2 + 1 &= 5, \\ 2^4 + 1 &= 17, \\ 2^8 + 1 &= 257, \\ 2^{16} + 1 &= 65\,537. \end{aligned}$$

dagegen ist $2^{32} + 1$ keine Primzahl, denn es gilt

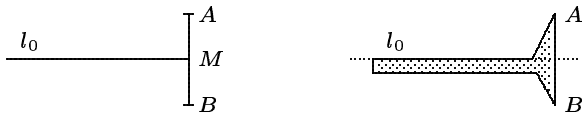
$$2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Insbesondere gilt:

(a) *Ein regelmäßiges 7-Eck ist mit Zirkel und Lineal nicht konstruierbar,* denn sonst könnte man eine primitive 7-te Einheitswurzel konstruieren. (Noch einmal explizit: Ist $\zeta = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$ und setzt man $\alpha = \zeta + \zeta^{-1}$, so ist α Nullstelle von $T^3 + T^2 - 2T - 1$ und dieses Polynom ist irreduzibel über $\mathbb{Q}$.)

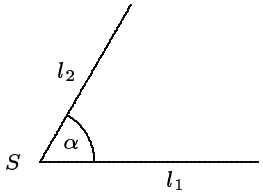
(b) *Nicht alle Winkel können mit Zirkel und Lineal gedrittelt werden,* zum Beispiel geht dies nicht für den Winkel $\alpha = 60°$. Denn ließe sich ein Winkel von $20°$ mit Zirkel und Lineal konstruieren, so hätte man auf diese Weise eine primitive 18-te Einheitswurzel konstruiert, aber $\phi(18) = 6$ ist keine Zweierpotenz. (Man kann auch folgendermaßen argumentieren: $\cos(20°) \notin \mathcal{K}$, denn allgemein gilt $\cos(3\alpha) = 4(\cos\alpha)^3 - 3\cos\alpha$, also folgt für $\alpha = 60°$ wegen $\cos(60°) = \frac{1}{2}$, daß $\cos\alpha$ Nullstelle von $4T^3 - 3T - \frac{1}{2}$ ist, und dieses Polynom ist irreduzibel über $\mathbb{Q}$.)

Drittelung eines beliebigen Winkels mit Zirkel und Lineal (und einer Klarsichtfolie): Wir wollen nun zeigen, wie man einen beliebigen Winkel "mit Zirkel und Lineal" dritteln kann: eine Konstruktion, die auf ARCHIMEDES zurückgeht. Wir zeichnen zuerst auf eine Klarsichtfolie (mit Zirkel und Lineal) eine Strecke $\overline{AB}$ der Länge 2 und dazu die Mittelsenkrechte l_0; der Schnittpunkt von l_0 mit $\overline{AB}$ sei M (also haben die Strecken $\overline{AM}$ und $\overline{MB}$ beide die Länge 1):

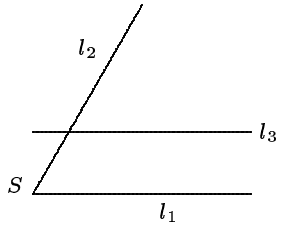


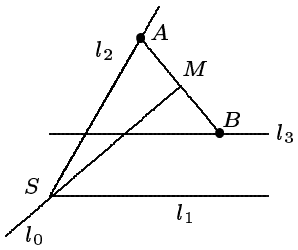
Statt mit einer Folie zu arbeiten, kann man auch aus Holz ein entsprechendes Gerät (wie rechts gezeigt) bauen: was man braucht, sind die Punkte A und B und die Gerade l_0.

Sei nun ein beliebiger Winkel α gegeben, der gedrittelt werden soll. Wir können voraussetzen, daß α ein spitzer Winkel ist (sonst hablbieren wir erst, dritteln danach und verdoppeln wieder):

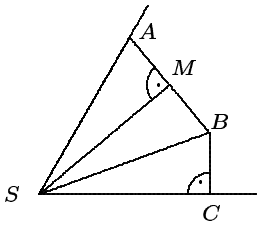


Wir zeichen (mit Zirkel und Lineal) eine Parallele l_3 zu l_1 im Abstand 1, siehe linkes Bild, und legen die Folie so auf, daß der Punkt A auf l_2, der Punkt B auf l_3 liegt und die Gerade l_0 durch den Punkt S verläuft.





Die Punkte A, M, B werden auf dem Zeichenblatt markiert (beim Arbeiten mit der Folie: die Folie durchstechen): die Geraden durch S und M und durch S und B liefern eine Dreiteilung des Winkels α. Um dies zu verfizieren, fällen wir (mit Zirkel und Lineal) das Lot von B auf die Gerade l_1, wir erhalten den Lotfußpunkt C. Offensichtlich sind die Dreiecke ASM, MSB, BSC kongruent, denn die Strecken $\overline{AM}, \overline{MB}, \overline{BC}$ haben die Länge 1:



Was lernen wir daraus? Die Konstruktion von ARCHIMEDES arbeitet zumindest vordergündig eigentlich auch nur mit Zirkel und Lineal, allerdings werden konstruierte Teilfiguren passend ineinandergeschoben — diese letzte Aktivität ("Neusis") liefert offensichtlich Punkte, die mit den Regeln (G)(K)(S) allein nicht konstruierbar sind (denn mit den Regeln (G)(K)(S) kann ja nicht jeder Winkel gedrittelt werden). Man muß also sehr genau aufpassen, wenn von Konstruktionen mit Zirkel und Lineal gesprochen wird. Schon die Erlaubnis, Punkte auf dem Lineal zu markieren (und dies ließe sich ja mit dem Zirkel durchführen!), verändert die Problemstellung. Wie immer in der Mathematik reicht es nicht, ein intuitives Verständnis zugrunde zulegen, um Aussagen zu beweisen oder zu widerlegen, man braucht klar formulierte Begriffsbildungen.

Schließlich soll angemerkt werden, daß das in den Schulen übliche Arbeiten mit dem "Geodreieck" gerade derartige Einschieb-Konstruktionen erlaubt.

6. Galois-Theorie (Nachtrag).

Das Hauptargument im Beweis des dritten Hauptsatzes, genauer: im Beweis der Implikation (4) $\Longrightarrow$ (1), sollte explizit formuliert werden: es steht im Zentrum vieler Überlegungen und ist auch für das praktische Arbeiten äußerst wichtig:

Satz. *Sei G eine endliche Gruppe von Körperautomorphismen des Körpers L, sei $K = \operatorname{Inv} G$. Sei $a \in L$. Dann hat das Minimalpolynom von a über K nur einfache Nullstellen, und diese Nullstellen bilden gerade die Bahn Ga von a unter G.*

$$Ga = \{ \text{ Nullstellen von } f \}$$

Ist $K \subseteq L$ eine normale Körpererweiterung und f das Minimalpolynom eines Elements $a \in L$ über K, so nennt man die Nullstellen von f die *zu a über K konjugierten* Elemente.

Beweis: Sei $f \in K[T]$ irreduzibel vom Grad t, mit einer Nullstelle $a \in L$. Wir zeigen: f besitzt t paarweise verschiedene Nullstellen in L. Sei $G = \{\eta_1, \ldots, \eta_n\}$. Die Menge $\{\eta_1 a, \ldots, \eta_n a\}$ bestehe aus genau r Elementen, etwa aus $a = a_1, \ldots, a_r$ (dies ist gerade die Bahn von a unter G). Aus $f(a) = 0$, folgt $f(a_i) = 0$ für alle i (denn ist $a_i = \eta a$ mit $\eta \in G$, so ist

$$f(a_i) = f(\eta a) = (\eta f)(\eta a) = \eta(f(a)) = \eta(0) = 0,$$

dabei gilt $f = \eta f$, denn die Koeffizienten von f liegen in $K = \operatorname{Inv} G$, und $(\eta f)(\eta a) = \eta(f(a))$, weil η ein Ring-Homomorphismus ist). Wir sehen also, daß alle Elemente der Bahn Ga Nullstellen von f sind.

Sei nun $h(T) = \prod_{i=1}^{r}(T - a_i)$. Dies ist ein nicht-konstantes Polynom in $L[T]$, das ein Teiler von f 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 $\prod_{i=1}^{r}(T - a_i)$ 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 f ist, folgt $h = f$. Demnach zerfällt f über L in paarweise verschiedene Linearfaktoren und die Menge der Nullstellen von f ist die Bahn $Ga = \{a = a_1, \ldots, a_r\}$ von a unter G.)

Beweis der Implikation (4) $\Longrightarrow$ (1) des dritten Hauptsatzes: Sei also $K = \operatorname{Inv} G$ für eine endliche Gruppe G von Körperautomorphismen von L. Der erste Haupsatz besagt, daß $[L : K]$ eine endliche Körpererweiterung ist. Sei $a \in L$, sei g das Minimalpolynom von a über K. Nach dem Satz hat g nur einfache Nullstellen, ist also separabel, und alle Nullstellen liegen in L (denn die Menge der Nullstellen ist die Bahn von a in L unter G. Dies zeigt, daß die Körpererweiterung $K \subseteq$ normal und separabel ist.

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

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

.

Beweis: Sei $g \in G$. Da g ein Körperautomorphismus ist, ist mit Z auch $g(Z)$ ein Unterkörper von L und natürlich ein Zwischenkörper von $K \subseteq L$. Folgende Formel ist unmittelbar von Interesse:

$$\boxed{\operatorname{Gal}(L : g(Z)) = gUg^{-1}}$$

Um dies zu beweisen, zeigt man die Enthaltensrelation $\supseteq$, dazu nimmt man $h \in U$ und zeigt, daß der Automorphismus ghg^{-1} den Unterkörper $g(Z)$ invariant läßt:

$ghg^{-1}g(z) = gh(z) = g(z)$ für jedes $z \in Z$. Da die beiden Untergruppen gUg^{-1} und $\mathrm{Gal}(L : g(Z))$ die gleiche Ordnung haben, nämlich $|U|$, folgt die behauptete Gleichheit.

Es ist Z genau dann normal über K, wenn $g(Z) = Z$ für alle $g \in G$ gilt. Denn ist Z normal über K, und ist $a \in Z$ mit Minimalpolynom f über K, so ist $g(a)$ ebenfalls eine Nullstelle von f (Bahn = Nullstellenmenge des Minimalpolynoms), also wegen der Normailität von $K \subseteq Z$ ist $g(a) \in Z$. Ist umgekehrt $g(Z) = Z$ für alle $g \in G$, und ist $a \in Z$ mit Minimalpolynom f über K, so liegen auch die übrigen Nullstellen von f in Z, denn sie sind die Bilder von a unter G (wieder verwenden wir: Bahn = Nullstellenmenge des Minimalpolynoms).

Die Bijektion zwischen den Untergruppen U von G und den Zwischenkörpern Z von $K \subseteq L$ wird durch $\mathrm{Gal}(L : -)$ hergestellt. Also gilt: Genau dann sind die Untergruppen U und gUg^{-1} gleich, wenn die Zwischenkörper Z und $g(Z)$ gleich sind.

Zusammenfassung: Genau dann ist $U = gUg^{-1}$ für alle $g \in G$, wenn $Z = g(Z)$ für alle $g \in G$ gilt. Das erste bedeutet, daß U eine normale Untergruppe ist, das zweite, daß Z über K normal ist.

Sei nun Z normal über K. Dies bedeutet, wie wir gesehen haben, daß jeder Automorphismus $g \in G$ den Unterkörper Z in sich abbildet, also können wir die Einschränkung $g \mapsto g|Z$ betrachten, dies ist ein Gruppen-Homomorphismus

$$G = \mathrm{Gal}(L : K) \longrightarrow \mathrm{Gal}(Z : K).$$

Der Kern ist offensichtlich U (denn ist die Einschränkung von $g \in G$ die Identität, so heißt dies nichts anderes, als daß g jedes Element von Z fixiert, also zu $\mathrm{Gal}(L : Z) = U$ gehört). Also sehen wir, daß unter der Einschränkungsabbildung G/U injektiv in $\mathrm{Gal}(Z : K)$ abgebildet wird. Diese Gruppen haben aber die gleiche Ordnugn, nämlich $[Z : K]$: für $\mathrm{Gal}(Z : K)$ ist dies klar, für G/U folgt dies aus dem Gradsatz $|G/U| = |G|/|U| = [L : K]/[L : Z] = [Z : K]$.

Zusatz. *Sei $K \subseteq L$ eine Körpererweiterung und $f \in K[T]$ ein separables Polynom. Sei $L = \mathcal{Z}_K(f)$ und $L' = \mathcal{Z}_{K'}(f)$. Dann gilt:* $\mathrm{Gal}(L' : K')$ *ist isomorph zu einer Untergruppe von* $\mathrm{Gal}(L : K)$.

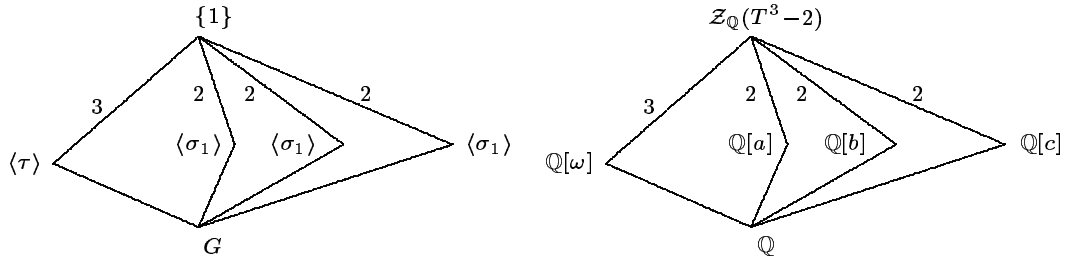
Beweis: Konstruieren wir zuerst L', so können wir L als den kleinsten Unterkörper von L', der K und alle Nullstellen von f enthält, definieren. Jedes Element der Galois-Gruppe $\mathrm{Gal}(L' : K)$ bildet offensichtlich L in sich ab, die Einschränkung $\eta \mapsto \eta|L$ liefert einen Gruppen-Homomorphismus

$$\mathrm{Gal}(L' : K') \longrightarrow \mathrm{Gal}(L : K),$$

von dem man ohne Mühe zeigt, daß er injektiv ist. Damit ist die Behauptung bewiesen.

Beispiel. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq \mathcal{Z}_{\mathbb{Q}}(T^3 - 2) = \mathbb{Q}[\omega, a]$, dabei ist ω eine primitive dritte Einheitswurzel und $a = \sqrt[3]{2}$. Wir setzen $b = \omega a$ und $c = \omega^2 a$. Die Galois-Gruppe $G = \mathrm{Gal}(\mathcal{Z}_{\mathbb{Q}}(T^3 - 2) : \mathbb{Q})$ ist die Diedergruppe D_3 der Ordnung 6, sie enthält genau 3 Elemente $\sigma_1, \sigma_1, \sigma_3$ der Ordnung 2 und eine Untergruppe $\langle\tau\rangle$ der Ordnung 3.

Links das Untergruppen-Diagramm, rechts das der Unterkörper von $\mathbb{Q}[\omega, a]$.



Die Galois-Gruppe eines Polynoms. Ist K ein Körper und f ein separables Polynom in $K[T]$, so nennt man $G = \mathrm{Gal}(\mathcal{Z}_K(f) : K)$ die *Galois-Gruppe von f,* die Einschränkung von G auf die Nullstellen von f identifiziert G mit einer Permutationsgruppe; dies ist die klassische Sichtweise: die Galois-Gruppe des Polynoms f ist eine Untergruppe der vollen Permutationsgruppe S_N der Menge $N = N(f)$ der Nullstellen von f.

Sei also $N = N(f)$ die Menge der Nullstellen von f und S_N die Menge der Permutation der Menge N. Die Einschränkung $\eta \mapsto \eta|N$ für $\eta \in G$ liefert einen Gruppen-Homomorphismus ϵ: $G \to S_N$. (Wir wissen, daß η die Nullstellen von f permutiert, also ist $\epsilon(\eta) = \eta|N \in S_M$. Daß ϵ ein Gruppen-Homomorphismus ist, verifiziert man mühelos.) Es bleibt zu zeigen, daß ϵ injektiv ist. Sei also $\epsilon(\eta)$ das Einselement, also ist $\eta(\alpha) = \alpha$ für jede Nullstelle α von f. Nun wird aber $\mathcal{Z}_K(f)$ als Körper von den Nullstellen von f und dem Körper K erzeugt. Da $\eta(c) = c$ für $c \in K$ und $\eta(\alpha) = \alpha$ für jede Nullstelle α von f gilt, ist $\eta(x) = x$ für jedes $x \in \mathcal{Z}_K(f)$. Also ist $\eta = 1 \in G$. Dies zeigt, daß ϵ injektiv ist. Also können wir G unter ϵ mit einer Untergruppe von S_N identifizieren.

Insbesondere gilt also: *Ist f ein Polynom vom Grad n, so ist die Ordnung der Galois-Gruppe von f ein Teiler von $n!$.*

9. Reine Polynome, Radikalerweiterungen.

Sei K ein Körper. Ein Polynom der Form $T^n - c$ mit $c \in K$ heißt *reines Polynom.* Ist eine Körperweiterung $K \subseteq L$ und ein Element $a \in L$ mit $L = K[a]$ gegeben und gibt es eine natürliche Zahl n mit $a^n \in K$, so sagt man, daß man L aus K durch *Adjunktion einer n-ten Wurzel* (oder eines *Radikal vom Exponenten n*) aus K erhält und man schreibt manchmal $a = \sqrt[n]{c}$ (und $a = \sqrt{c}$ im Fall $n = 2$). (**Warnung:** diese Schreibweise suggeriert, daß a durch c und n eindeutig bestimmt sei, aber dies ist natürlich **nicht** der Fall! Wenn man $\sqrt{r}$ schreibt und r eine **positive** reelle Zahl ist, so meint man immer die **positive** Quadratwurzel von r, und die ist eindeutig bestimmt; dagegen ist schon $\sqrt{-2}$ kein eindeutig bestimmtes Element!)

Tschirnhaus-Transformation. *Sei K ein Körper und $f(T) = \sum_{i=0}^{n} a_i T^i$ ein normiertes Polynom in $K[T]$ vom Grad n. Die Charakteristik von K sei kein Teiler von n. Ersetzen wir die Variable T durch $X - \frac{a_{n-1}}{n}$, bilden wir also $g(X) = f(X - \frac{a_{n-1}}{n})$, so erhalten wir ein Polynom $g(X) = \sum_{i=0}^{n} b_i X^i$, ebenfalls normiert und vom Grad n, mit $b_{n-1} = 0$, und es gilt: Genau dann ist t Nullstelle von $f(T)$, wenn $t + \frac{a_{n-1}}{n}$ Nullstelle von $g(X)$ ist.* Die Nullstellen von g erhält man demnach durch Verschiebung der Nullstellen von f.

Zur Bestimmung der Nullstellen eines Polynoms kann man also als erstes voraussetzen, daß das Polynom normiert ist (Normieren ändert die Nullstellen nicht) und dann (bei geeigneter Charakteristik), daß der zweithöchste Koeffizient Null ist.

Polynome vom Grad 2. Wir setzen voraus, daß K ein Körper ist, dessen Charakteristik nicht 2 ist. Gegeben sei das Polynom

$$f(T) = T^2 + pT + q \quad \text{mit} \quad p, q \in K,$$

die Tschirnhaus-Transformation liefert

$$g(X) = f(X - \tfrac{p}{2}) = \big(X - \tfrac{p}{2}\big)^2 + p\big(X - \tfrac{p}{2}\big) + q = X^2 - \tfrac{1}{4}(p^2 - 4q)$$

Die Nullstellen von $g(X)$ sind $\pm\frac{1}{2}\sqrt{p^2 - 4q}$. Also sind die Nullstellen von $f(T)$ von der Form $-\frac{p}{2} \pm \frac{1}{2}\sqrt{p^2 - 4q}$, die wohlbekannte Lösungsformel für quadratische Gleichungen.

Polynome vom Grad 3. Sei gegeben

$$f(T) = T^3 + a_2T^2 + a_1T + a_0 \quad \text{mit} \quad a_0, a_1, a_2 \in K.$$

Ist also die Charakteristik von K nicht 3, so können wir annehmen $a_2 = 0$, also

$$f(T) = T^3 + pT + q \quad \text{mit} \quad p, q \in K.$$

Im Fall $K = \mathbb{R}$ ist die Tschirnhaus-Transformation gerade die Verschiebung der T-Achse, um den Wendepunkt bei $T = 0$ zu haben (der Wendepunkt ist die Nullstelle von $f'' = 6T + 2a_2$).

Wir nehmen zusätzlich an, daß die Charakteristik von K auch nicht 2 ist. Setze $T = X + Y$. Also

$$f(X+Y) = X^3+Y^3+3XY(X+Y)+p(X+Y)+q = X^3+Y^3+(3XY+p)(X+Y)+q.$$

Wir bestimmen die gemeinsamen Nullstellen von

$$3XY + p \quad \text{und} \quad X^3 + Y^3 + q$$

(denn ist das Paar x, y eine gemeinsame Nullstelle dieser beiden Polynome in $K[X, Y]$, so ist $x + y$ eine Nullstelle von f), oder auch von

$$X^3Y^3 + \tfrac{p^3}{27} \quad \text{und} \quad X^3 + Y^3 + q$$

Das Paar x, y sei gemeinsame Lösung dieser beiden Gleichungen. Da Summe und Produkt von x^3, y^3 bekannt sind (die Summe ist $-q$, das Produkt ist $-\frac{p^3}{27}$), sind x, y Nullstellen von

$$U^2 + qU - \tfrac{p^3}{27}.$$

also etwa

$$x^3 = -\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}, \quad y^3 = -\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}.$$

Setze

$$t = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

wobei bei der Auswahl der dritten Wurzeln berücksichtigt werden muß, daß gilt $xy = -\frac{p}{3}$. Also wähle

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

und setze

$$y = -\frac{p}{3x}.$$

Dann ist $t_1 = x + y$ eine Lösung der gegebenen kubischen Gleichung, die beiden anderen erhält man durch $t_2 = \omega x + \omega^2 y$ und $t_3 = \omega^2 x + \omega y$, hier ist ω eine primitive dritte Einheitswurzel.

Diese Lösungsformel stammt von DEL FERRO und TARTAGLIA, wurde aber zuerst von CARDANO (Ars Magna, 1545) publiziert (man sagt, er habe sie gestohlen), man nennt sie die CARDANO-Formel.

Ist $f(T) = T^3 + pT + q$, so setzt man $D(f) = -4p^3 - 27q^2$, man nennt dies die *Diskrimante* von f. Die Quadratwurzel in der Lösungsformel ist $\frac{1}{18}\sqrt{-3D(f)}$. Offensichtlich hat f genau dann zwei gleiche Nullstellen, wenn $D(f) = 0$ ist; daher der Name "Diskriminante": dieser Ausdruck $D(f)$ ist genau dann von Null verschieden, man man die Nullstellen unterscheiden kann.

Lemma. *Ist $f(T) = T^3 + pT + q$, mit $p, q \in \mathbb{R}$, so hat f genau dann drei verschiedene* **reelle** *Nullstellen, wenn $D(f) > 0$ gilt.*

Beweis: Es ist $f'(T) = 3T^2 + p$, die Nullstellen von f' sind also $a_1 = \sqrt{-\frac{p}{3}}$ und $a_2 = -\sqrt{-\frac{p}{3}}$. Dabei können wir $p < 0$ voraussetzen, denn drei reelle Nullstellen kann f nur dann besitzen, wenn f in den Extrema verschiedene Vorzeichnen annimmt, wenn also gilt

$$\begin{aligned} 0 > f(a_1)f(a_2) &= \left(\left(\sqrt{-\tfrac{p}{3}}\right)^3 + p\sqrt{-\tfrac{p}{3}} + q\right)\left(\left((-\sqrt{-\tfrac{p}{3}}\right)^3 - p\sqrt{-\tfrac{p}{3}} + q\right) \\ &= -\left(\tfrac{2p}{3}\sqrt{-\tfrac{p}{3}}\right)^2 + q^2 = -\tfrac{1}{27}\left(-4p^3 - 27q^2\right) = -\tfrac{1}{27}D(f) \end{aligned}$$

beachte dabei: $\left(\sqrt{-\frac{p}{3}}\right)^3 + p\sqrt{-\frac{p}{3}} = \frac{2p}{3}\sqrt{-\frac{p}{3}}$ und $\left(-\sqrt{-\frac{p}{3}}\right)^3 - p\sqrt{-\frac{p}{3}} = -\frac{2p}{3}\sqrt{-\frac{p}{3}}$.

Ist also $f(T) = T^3 + pT + q$, mit $p, q \in \mathbb{R}$ und $D(f) > 0$, so besitzt f genau drei reelle Nullstellen — andererseits muß man bei der Verwendung der CARDANO-Formel $\sqrt{-3D(f)}$ berechnen, also mit **komplexen** Zahlen arbeiten. Dies hat früher viele Mathematiker irritiert: um reelle Zahlen aus reellen Zahlen zu berechnen, muß man die komplexen Zahlen einführen. Man nannte dies den "casus irreducibilis".

Polynome vom Grad 4. Wieder setzen wir voraus: Die Charakteristik von K sei von 2 und 3 verschieden. Wir können wieder annehmen (Tschirnhaus): Gegeben ist

$$f(T) = T^4 + aT^2 + bT + c.$$

Wir betrachten die "kubische Resolvente"

$$g(Z) = Z^3 + 2aZ^2 + (a^2 - 4c)Z - b^2.$$

Sind u', v', w' die Nullstellen von g, so wählen wir Quadratwurzeln u, v, w von u', v', w' mit $uvw = -b$. Dann sind die vier Nullstellen von f durch

$$\frac{u+v+w}{2}, \quad \frac{u-v-w}{2}, \quad \frac{-u+v-w}{2}, \quad \frac{-u-v+w}{2}$$

gegeben. Diese Darstellung der Nullstellen eines Polynoms vierten Grads geht auf FERRARI (16.Jh) zurück.

Wir wollen noch notieren, welche Körpertürme gebraucht werden, um die Lösungen der Polynome $f \in K[T]$ zu finden; dabei ist also f ein Polynom vom Grad $n = 3$ oder 4 und die Charakteristik von K ist nicht 2 oder 3.

Fall $n = 3$**.** Gegeben ist $f(T) = T^3 + pT + q \in K[T]$. Bilde

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 = L \quad \text{mit} \quad K_i = K_{i-1}[a_i],$$
$$a_1^2 = \sqrt{D(f)}, \quad a_2^2 = -3, \quad a_3^3 = -\tfrac{q}{2} + \tfrac{1}{18}a_1a_2.$$

Beachte: K_2 entsteht aus K_1 durch Adjunktion der dritten Einheitswurzel $\omega = \frac{1}{2}(-1 + a_2)$. Daher enthält K_3 mit a_3 **alle** Wurzeln von $T^3 + \frac{q}{2} - \frac{1}{18}a_1a_2$, also auch alle Nullstellen von f.

Fall $n = 4$**.** Gegeben sei $f(T) = T^4 + aT^2 + bT + c \in K[T]$. Bilde

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq K_4 \subseteq K_5 = L,$$

dabei ist $K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3$ der im Fall $n = 3$ angegebene Körperturm der kubischen Resolventen; und es ist (mit den oben verwendeten Bezeichnungen):

$$K_4 = K_3[u], \quad K_5 = K_4[v] \quad \text{mit} \quad u^2 = u', \ v^2 = v',$$

Eine Körpererweiterung $K \subseteq L$ heißt *Radikal-Erweiterung,* wenn es einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

und für $1 \leq i \leq n$ jeweils ein Element $a_i \in K_i$ und eine natürliche Zahl n_i gibt mit $a_i^{n_i} \in K_{i-1}$, wenn also jedes K_i aus K_{i-1} durch Adjunktion einer n_i-ten Wurzel hervorgeht (dabei kann man offensichtlich immer annehmen, daß die Zahlen n_i Primzahlen sind: ist nämlich $L = K[a]$ und $a^{nn'} \in K$ mit natürlichen Zahlen n, n', so kann man $K' = K[b]$ mit $b = a^n$ bilden und erhält einen Körperturm $K \subseteq K' \subseteq L$ mit $K' = K[b], L = K'[a]$ und $b^{n'} \in K, \ a^n \in K'$).

Ist $f \in K[X]$ ein Polynom, so sagt man, *die Gleichung* $f = 0$ *ist durch Radikale auflösbar,* wenn es eine Radikalerweiterung $K \subseteq L$ gibt mit $\mathcal{Z}_K(f) \subseteq L$.

Wir haben gesehen, daß sich, falls die Charakteristik des Grundkörpers nicht 2 oder 3 ist, die Gleichung $f = 0$ für jedes Polynom f vom Grad höchstens 4 durch Radikale auflösbar ist.

Bemerkung: Ist $K \subseteq L$ eine Radikalerweiterung und $K \subseteq \mathcal{Z}_K(f) \subseteq L$, so braucht $K \subseteq \mathcal{Z}_K(f)$ selbst keine Radikalerweiterung zu sein. Hier ein Beispiel: Sei $K = \mathbb{Q}$, und $f = X^3 + X^2 - 2X - 1$, dies ist das Minimalpolynom von $\zeta + \zeta^{-1}$ über $\mathbb{Q}$, wobei ζ eine primitive 7-te Einheitswurzel ist. Der Zerfällungskörper $K' = \mathcal{Z}_K(f) = \mathbb{Q}[\zeta + \zeta^{-1}]$ ist galois'sch über $\mathbb{Q}$ mit Galois-Gruppe C_3, aber es gibt kein Element $a \in K' \setminus \mathbb{Q}$ mit $a^n \in \mathbb{Q}$ für ein $n \in \mathbb{N}_1$. Andererseits ist $K' \subset \mathbb{Q}[\zeta]$ und $K \subset \mathbb{Q}[\zeta]$ ist eine Radikalerweiterung.

Zuerst zeigen wir, wie man in einer Körpererweiterung Elemente konstruieren kann, deren Minimalpolynome reine Polynome sind.

Proposition 1. *Sei $K \subseteq L$ eine Körpererweiterung vom Grad n und K enthalte eine primitive n-te Einheitswurzel. Ist $K \subseteq L$ eine galois'sche Körpererweiterung mit zyklischer Galois-Gruppe, so gibt es $a \in L$ mit $L = K[a]$ und $a^n \in K$.*

Zum Beweis brauchen wir folgendes Lemma:

Lemma (Dedekind). *Sei H eine Halbgruppe, sei L ein Körper. Gegeben seien paarweise verschiedene Halbgruppen-Homomorphismen $\sigma_1, \ldots, \sigma_n \colon H \to L^*$. Dann sind die Elemente $\sigma_1, \ldots, \sigma_n$ im L-Vektorraum* $\mathrm{Abb}(H, L)$ *linear unabhängig* (das heißt: Sind $\lambda_1, \ldots, \lambda_n \in L$ mit $\sum \lambda_i \sigma_i = 0$, so sind alle $\lambda_i = 0$.)

Beweis: Induktion nach n. Ist $n = 1$, so ist also $\sigma_1 \colon H \to L^*$ gegeben. Diese Abbildung ist nicht Null, denn das Bild von σ_1 liegt ja in $L^* = L \setminus \{0\}$.

Nehmen wir nun an, die Behauptung ist richtig für $n - 1$. Seien $\lambda_i \in L$ gegeben mit

$$(*) \qquad \sum\nolimits_{i=1}^{n} \lambda_i \sigma_i = 0.$$

Da $\sigma_1 \neq \sigma_n$, gibt es $h \in H$ mit $\sigma_1(h) \neq \sigma_n(h)$. Wenden wir $(*)$ auf xh für ein $x \in H$ an, so erhalten wir

$$0 = \sum\nolimits_{i=1}^{n} \lambda_i \sigma_i(xh) = \sum\nolimits_{i=1}^{n} \lambda_i \sigma_i(x) \sigma_i(h),$$

Wenden wir $(*)$ auf x an und multiplizieren wir dies mit $\sigma_n(h)$, so erhalten wir

$$0 = \sum\nolimits_{i=1}^{n} \lambda_i \sigma_i(x) \sigma_n(h).$$

Subtraktion liefert:

$$0 = \sum\nolimits_{i=1}^{n} \lambda_i \sigma_i(x) \big(\sigma_i(h) - \sigma_n(h)\big) = \sum\nolimits_{i=1}^{n-1} \lambda_i \sigma_i(x) \big(\sigma_i(h) - \sigma_n(h)\big).$$

also ist $\sum_{i=1}^{n-1} \lambda_i' \sigma_i = 0$ mit $\lambda_i' = \lambda_i \big(\sigma_i(h) - \sigma_n(h)\big)$. Nach Induktion ist also $\lambda_i' = 0$ für $1 \leq i < n$. Für $i = 1$ schließen wir aus $0 = \lambda_1' = \lambda_1 \big(\sigma_i(h) - \sigma_n(h)\big)$ wegen $\sigma_1(h) \neq \sigma_n(h)$, daß gilt $\lambda_1 = 0$. Aber nun können wir in $(*)$ den ersten Summanden weglassen und erhalten wieder mit Induktion, daß gilt $\lambda_2 = \cdots = \lambda_n = 0$.

Beweis der Proposition. Es ist $G = \mathrm{Gal}(L : K)$ nach Voraussetzung eine zyklische Gruppe, sei σ ein erzeugendes Element. Die Automorphismen $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ sind paarweise verschieden, also nach dem Dedekind-Lemma linear unabhängig. Also ist $\sum_{i=0}^{n-1} \zeta^i \sigma^i \neq 0$ und demnach gibt es $b \in L$ mit $\sum_{i=0}^{n-1} \zeta^i \sigma^i(b) \neq 0$. Man nennt

$$a = \sum\nolimits_{i=0}^{n-1} \zeta^i \sigma^i(b)$$

eine **Lagrange'sche Resolvente.** Es ist $\sigma(a) = \zeta^{-1} a$, denn

$$\sigma(a) = \sigma\left(\sum\nolimits_{i=0}^{n-1} \zeta^i \sigma^i(b)\right) = \sum\nolimits_{i=0}^{n-1} \zeta^i \sigma^{i+1}(b) = \zeta^{-1} \sum\nolimits_{i=0}^{n-1} \zeta^{i+1} \sigma^{i+1}(b) = \zeta^{-1} a,$$

dabei haben wir beim zweiten Gleichheitszeichen $\sigma(\zeta) = \zeta$ und beim letzten Gleichheitszeichen $\zeta^n \sigma^n = \zeta^0 \sigma^0$ verwandt. Daraus folgt:

$$\sigma(a^n) = (\sigma(a))^n = (\zeta^{-1} a)^n = a^n,$$

demnach liegt also $a^n \in \mathrm{Inv}\, G = K$. Und es folgt auch

$$\sigma^j(a) = \zeta^{-j} a \quad \text{für jedes} \quad j \in \mathbb{N}.$$

Wegen $a \neq 0$ folgt aus $\sigma^j(a) = a$, daß gilt $\zeta^{-j} = 1$, also daß n ein Teiler von j ist. Dies impliziert $K[a] = L$, denn wäre $K[a]$ ein echter Unterkörper von L, so wäre $K[a] = \mathrm{Inv}\, U$ für eine Untergruppe $U \neq \{1\}$ von G, also $\sigma^j(a) = a$ für ein j mit $1 \leq j < n$.

Prposition 2. *Sei $K \subseteq L$ eine Körpererweiterung und K enthalte eine primitive n-te Einheitswurzel. Ist $L = K[a]$ mit $a \in L$ and $a^n \in K$, so ist $K \subseteq L$ eine galois'sche Körpererweiterung mit zyklischer Galois-Gruppe und $[L : K]$ ist ein Teiler von n.*

Beweis: Sei ζ eine primitive n-te Einheitswurzel. Wir können $a \neq 0$ annehmen. Sei $c = a^n$, nach Voraussetzung liegt $c \in K$. Die Elemente $\zeta^i a$ mit $0 \leq i < n$ sind paarweise verschieden und es sind Nullstellen von $T^n - c$, also ist $T^n - c = \prod_{i=0}^{n-1} (T - \zeta^i a)$. Das Minimalpolynom g von a über K ist ein Teiler von $T^n - c$, hat also, wie T^n paarweise verschiedene Nullstellen und alle Nullstellen liegen in L. Dies zeigt, daß L der Zerfällungskörper des separablen Polynoms g ist, also ist $K \subseteq L$ galois'sche Erweiterung. Sei $G = \mathrm{Gal}(L : K)$. Ist $\eta \in G$, so ist $\eta(a)$ eine Nullstelle von g, also von $T^n - c$ und demnach $\eta(a) = \zeta^{i(\eta)} a$ für ein $i(\eta) \in \mathbb{Z}/n\mathbb{Z}$. Die Zuordnung $i\colon G \to (\mathbb{Z}/n\mathbb{Z}, +) = C_n$ ist ein Gruppen-Homomorphismus, denn sind $\eta, \eta' \in G$, so ist

$$\eta\eta'(a) = \eta(\zeta^{i(\eta)} a = \zeta^{i(\eta')} \eta(a) = \zeta^{i(\eta')} \zeta^{i(\eta)} a = \zeta^{i(\eta)+i(\eta')} a.$$

Die Zuordnung ist injektiv, denn ist $i(\eta) = \overline{0}$, also $\eta(a) = a$, so ist η die Identität, da L von a über K erzeugt wird. Als Untergruppe von C_n ist G zyklisch und die Ordnung von G ist ein Teiler von n. Die Ordnung von G ist aber gleich $[L : K]$.

Korollar. *Sei $K \subseteq L$ eine Körpererweiterung mit Primzahlgrad p und K enthalte eine primitive p-te Einheitswurzel. Dann sind äquivalent:*
(i) *Es ist $L = K[a]$ mit $a \in L$ and $a^p \in K$.*

(ii) *$K \subseteq L$ ist galois'sch.*

Die Implikation (i) $\Longrightarrow$ (ii) folgt direkt aus der Proposition 2, die Implikation (ii) $\Longrightarrow$ (i) aus der Proposition 1.

Satz. *Sei K eine Körper der Charakteristik 0. Sei $f \in K[X]$ ein Polynom vom Grad n. Die folgenden Aussagen sind äquivalent:*

(i) $\mathrm{Gal}(\mathcal{Z}_K(f) : K)$ *ist auflösbar.*

(ii) *Die Gleichung $f = 0$ ist durch Radikale auflösbar.*

(iii) *Es gibt eine schöne Radikalerweiterung $K \subseteq L$, die galois'sch ist, sodaß $\mathcal{Z}_K(f)$ in L enthalten ist.*

Dabei nennen wir eine Körpererweiterung $K \subseteq L$ eine *schöne Radikalerweiterung,* wenn es einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

gibt, sodaß für jedes $1 \leq i \leq n$ die Körpererweiterung $K_{i-1} \subseteq K_i$ galois'sch mit Primzahlgrad $p_i = [K_i : K_{i-1}]$ ist und K_{i-1} eine primitive p_i-te Einheitswurzel enthält (insbesondere entsteht dann K_i aus K_{i-1} durch Adjunktion einer p_i-ten Wurzel).

Vorbemerkung: *Eine schöne Radikalerweiterung $K \subseteq L$ läßt sich zu einer schönen Radikalerweiterung $K \subseteq L \subseteq L'$ fortsetzen, so daß $K \subseteq L'$ galois'sch ist.*

Beweis der Vorbemerkung. Sei gegeben ein Körperturm

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L,$$

sei $[K_i : K_{i-1}] = p_i$ Primzahl, sei $a_i \in K_i$ mit $K_i = K_{i-1}[a_i] = K_i$ und $a_i^{p_i} \in K_{i-1}$, und $K_i i - 1$ enthalte eine primitive p_i-te Einheitswurzel. Seien a_{ij} die zu a_i über K konjugierten Elemente in K_i, mit $1 \leq j \leq t_i$ und $a_{i1} = a_i$. Wir adjungierten sukzessive die Elemente a_{ij}, in folgender Reihenfolge:

$$a_{11}, a_{12}, \ldots, a_{1t_1},\ a_{21}, a_{22}, \ldots, a_{2t_2},\ \ldots\ldots\ ,\ a_{m1}, a_{m2}, \ldots, a_{mt_m}.$$

Bezeichnen wir mit E_r den Körper, den wir erhalten, wenn wir zu K alle Elemente a_{ij} mit $1 \leq i \leq r$ adjungieren. Nach Konstruktion ist jedes E_i über K normal. Da a_{ij} zu a_i konjugiert ist, ist $a_{ij}^{p_i}$ zu $a_i^{p_i} \in K_i \subseteq E_{i-1}$ konjugiert, gehört also zu E_{i-1}. Da jedes K_{i-1} eine primitive p_i-te Einheitswurzel enthält, so enthält E_{i-1} eine primitive p_i-te Einheitswurzel.

Bevor wir mit dem Beweis der Implikation (i) $\Longrightarrow$ (iii) beginnen, betrachten wir den folgenden Spezialfall:

Lemma. *Sei K ein Körper der Charakteristik 0, sei $f \in K[X]$ ein Polynom vom Grad n. Für jede Primzahl $p \leq n$ enthalte K eine primitive n-te Einheitswurzel. Ist $\mathrm{Gal}(\mathcal{Z}_K(f) : K)$ auflösbar, so ist $K \subseteq \mathcal{Z}_K(f)$ eine schöne Radikalerweiterung.*

Beweis: Sei

$$\mathrm{Gal}(\mathcal{Z}_K(f) : K) = G = G_0 \supset G_1 \supset \cdots \supset G_t = \{1\}$$

eine Kette von Untergruppen, dabei sei G_i Normalteiler von G_{i-1} mit Primzahlindex $[G_{i-1} : G_i] = q_i$. Da die Ordnung von G ein Teiler von $n!$ ist, sind auch die q_i Teiler von $n!$ und demnach gilt $q_i \leq n$.

Betrachte nun die zugehörigen Unterkörper $K_i = \operatorname{Inv} G_i$, also

$$K = K_0 \subset K_1 \subset \cdots \subset K_t = \mathcal{Z}_K(f)$$

Weil G_i Normalteiler von G_{i-1} mit Index q_i ist, ist $K_{i-1} \subset K_i$ galois'sch und die entsprechende Galois-Gruppe hat Primzahlordnung, insbesondere ist sie zyklisch. Da K_{i-1} eine primitive q_i-te Einheitswurzel enthält, gibt es nach der Proposition $a_i \in K_i$ mit $K_i = K_{i-1}[a_i]$ und $a_i^n \in K_i$. Dies liefert die Behauptung.

Beweis der Implikation (i) $\Longrightarrow$ (iii). Seien $2 = p_1 < p_2 < \cdots < p_s$ die Primpzahlen $p_i \leq n$. Sei ζ_i eine primitive p_i-te Einheitswurzel, sei $Z_i = K[\zeta_1, \ldots, \zeta_i]$. Wir haben also $Z_i = Z_{i-1}[\zeta_i]$ und $\zeta_i^{p_i} = 1 \in Z_{i-1}$. Da $\mathbb{Q} \subseteq \mathbb{Q}[\zeta_i]$ galois'sch mit zyklischer Galois-Gruppe C_{p_i-1} ist, ist $Z_{i-1} \subseteq Z_{i-1}[\zeta_i]$ ebenfalls galois'sch mit zyklischer Galoisgruppe G_i, und die Ordnung von G_i ist ein Teiler von $p_i - 1$. Insgesamt sehen wir: Wir haben einen Körperturm

$$K = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_s \subseteq Z_{s+1} = \mathcal{Z}_{Z_s}(f),$$

wobei alle Erweiterungen $Z_{i-1} \subseteq Z_i$ für $1 \leq i \leq s+1$ galois'sch mit auflösbarer Galois-Gruppe G_i sind, und Z_{i-1} für jeden Primteiler p_i von $|G_i|$ eine primitive p_i-te Einheitswurzel enthält. Für $1 \leq i \leq s$ haben wir dies gerade notiert, die auftretenden Galois-Gruppen sind sogar zyklisch; für $i = s+1$ sei auf den Zusatz zu §6 verwiesen: dort steht, daß die Galois-Gruppe $\operatorname{Gal}(\mathcal{Z}_{Z_s}(f) : Z_s)$ zu einer Untergruppe von $\operatorname{Gal}(\mathcal{Z}_K(f) : K)$ isomorph ist, und demnach ist sie ebenfalls auflösbar.

Wir wenden nun das Lemma auf diese Körpererweiterungen $Z_{i-1} \subseteq Z_i$ und sehen, daß dies eine schöne schöne Radikalerweiterung ist. Dann ist auch die gesamte Erweiterung eine schöne Radikalerweiterung und die Vorbemerkung besagt, daß wir dies zu einer schönen Radikalerweiterung $K \subseteq L$ mit $\mathcal{Z}_{Z_s}(f) \subseteq L$ fortsetzen können. Dies liefert die Behauptung, denn $\mathcal{Z}_K(f) \subseteq \mathcal{Z}_{Z_s}(f)$.

Die Implikation (iii) $\Longrightarrow$ (ii) ist trivial.

Auch die Implikation (iii) $\Longrightarrow$ (i) ist leicht zu sehen: Sei $K \subseteq L$ eine galois'sche Erweiterung, die eine schöne Radikalerweiterung ist. Dann ist die Galois-Gruppe $G = \operatorname{Gal}(L : K)$ auflösbar, denn es gibt einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

gibt, sodaß für jedes $1 \leq i \leq n$ die Körpererweiterung $K_{i-1} \subseteq K_i$ galois'sch mit Primzahlgrad $p_i = [K_i : K_{i-1}]$ ist, also erhalten wir unter $\operatorname{Gal}(L : -)$ Untergruppen $G_i = \operatorname{Gal}(L : K_i)$

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

und jedes G_i ist Normalteiler in G_{i-1} mit Primzahlindex p_i. Dies zeigt, daß G auflösbar ist.

Es bleibt zu zeigen: (ii) $\Longrightarrow$ (iii). Sei also die Gleichung $f = 0$ durch Radikale auflösbar, es gibt also einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = L,$$

Primzahlen p_i und Elemente $a_i \in K_i$ mit $K_i = K_{i-1}[a_i] = K_i$ und $a_i^{p_i} \in K_{i-1}$, sodaß der Zerfällungskörper $\mathcal{Z}_K(f)$ in L enthalten ist.

Sei m das kleinste gemeinschaftliche Vielfache der Primzahlen p_i mit $1 \leq i \leq m$. Wir wenden die Implikation (i) $\Longrightarrow$ (iii) auf das Kreisteilungspolynom Φ_m an, denn die Galois-Gruppe $\mathrm{Gal}(\mathbb{Q}[\Phi_m] : \mathbb{Q}]$ ist abelsch, also ist auch die Untergruppe $\mathrm{Gal}(K[\Phi_m] : K]$ abelsch. Wir erhalten eine schöne Radikalerweiterung $K \subseteq L'$ mit $\mathcal{Z}_K(\Phi_m) \subseteq L'$. Adjungieren wir nun zu L' sukzessive die Elemente $a_1, \ldots, a_s$, so ist $L' \subseteq L'[a_1, \ldots, a_s] = L''$ ebenfalls eine schöne Radikalerweiterung. Nach der Vorbemerkung können wir schließlich die schöne Radikalerweiterung $K \subseteq L' \subseteq L''$ zu einer schönen Radikalerweiterung $K \subseteq L' \subseteq L'' \subseteq L$ mit $K \subseteq L$ galois'sch fortsetzen.

Beispiele von Polynomen f, die nicht durch Radikale auflösbar sind. Für jede Primzahl $p \geq 5$ konstruieren wir Polynome $f \in \mathbb{Q}[T]$ vom Grad p, mit $\mathrm{Gal}(\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q}) = S_p$. Da wir wissen, daß die Gruppen S_n für $n \geq 5$ nicht auflösbar ist, folgt, daß f nicht durch Radikale auflösbar ist.

Satz. *Sei p Primzahl, sei $f \in \mathbb{Q}[T]$ irreduzibel vom Grad p. Besitzt f genau zwei nicht-reelle Nullstellen, so ist* $\mathrm{Gal}(\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q}) = S_p$.

Beweis: Seien $a_1, \ldots, a_p$ die Nullstellen von f im Zerfällungskörper $L = \mathcal{Z}_{\mathbb{Q}}(f) \subset \mathbb{C}$; wie betrachten $G = \mathrm{Gal}(\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q})$ als Permutationsgruppe auf der Menge $\{a_1, \ldots, a_p\}$. Da f ein Polynom mit reellen Koeffizienten ist, bildet die komplexe Konjugation (das heißt die Abbildung η: $\mathbb{C} \to \mathbb{C}$ mit $\eta(a + bi) = a - bi$ für $a, b \in \mathbb{R}$) den Körper L in sich ab; die Einschränkung von η auf L (die wir wieder mit η bezeichnen) gehört zu G. Es ist $\eta(a_i) = a_i$ genau dann, wenn gilt $a_i \in \mathbb{R}$. Nach Voraussetzung ist also η eine Transposition. Andererseits ist $\mathbb{Q}[a_1]$ ein Unterkörper von L und $[\mathbb{Q}[a_1] : \mathbb{Q}] = p$, denn f ist das Minimalpolynom von a_1. Der Gradsatz zeigt, daß p ein Teiler von $[\mathcal{Z}_{\mathbb{Q}}(f) : \mathbb{Q}] = |G|$ ist. Die Behauptung folgt nun aus folgendem Lemma:

Lemma. *Sei p eine Primzahl und G eine Untergruppe der S_p. Enthält G mindestens eine Transposition und ist p ein Teiler von $|G|$, so ist $G = S_p$.*

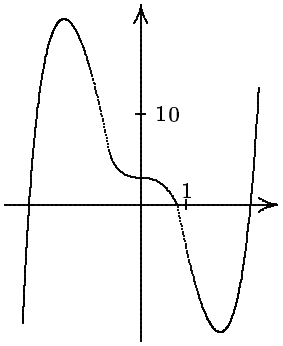
Beweis: Nach dem Satz von Cauchy enthält G ein Element g der Ordnung p, die muß ein Zykel der Länge p sein, wir können annehmen $g = (1\,2\,\ldots\,p)$. Die Gruppe G enthält auch eine Transposition, sagen wir $\tau = (i\,j)$ mit $i \neq j$. Wir können annehmen $i = 1$, also $2 \leq j \leq p$. Mit g hat auch g^{j-1} die Ordnung p (hier verwenden wir, daß p eine Primzahl ist) und $g^j = (1, j, \ldots)$. Also können wir annehmen $i = 1$, $j = 2$. Die Zykel $g = (1\,2\,\ldots\,n)$ und $\tau = (1\,2)$ erzeugen aber die S_n, für jedes n.

Beispiel für $p = 5$.

$$f(T) = T^5 - 6T^3 + 3$$

Das Polynom f ist irreduzibel (verwende das Eisenstein-Kriterium, siehe Übungsaufgabe 46). Um zu sehen, daß f genau drei reelle Nullstellen hat, verwende Kurvendiskussion:

es ist $f' = (5T^2 - 18)T^2$, also hat der Graph von f die folgende Form



Beispiele für beliebiges $p \geq 5$.

- Wähle ganze Zahlen $n_1 < n_2 < \cdots < n_{p-2}$
- Wähle eine ganze Zahl $m > \sum_{i=1}^{p-2} n_i^2$.

Betrachte das Polynom

$$f(T) = (T^2 + 2m)(T - 2n_1)\cdots(T - 2n_{p-2}) - 2$$

Das Polynom $f \in \mathbb{Q}[T]$ ist irreduzibel nach dem Eisenstein-Kriterium: der höchste Koeffizient ist 1, alle anderen Koeffizienten sind durch 2 teilbar, der konstante Koeffizient ist $-2 + 2^{p-1}m\prod n_i$, also nicht durch 4 teilbar.

Das Polynom f hat mindestens $p-2$ reelle Nullstellen, denn

$$f(2n_i) = -2 \quad \text{für} \quad 1 \leq i \leq p-2$$
$$f(2n_{2j-1} + 1) \geq 1 \quad \text{für} \quad 1 \leq j \leq \tfrac{p-3}{2}$$

(ist $a = 2n_{2j-1} + 1$, so ist $a^2 + 2m \geq 3$ und $|a - 2n_i| \geq 1$, und die Anzahl der negativen Faktoren ist gerade). Also gibt es mindestens $p-3$ reelle Nullstellen, und zwar je eine in den Intervallen

$$(2n_1, 2n_2), \ldots, (2n_{p-3}, 2n_{p-2}).$$

Da $f(2n_{p-2}) = -2$ und $\lim_{x\to\infty} f(x) = +\infty$, gibt es eine weitere reelle Nullstelle im Intervall $(2n_{p-2}, \infty)$.

Das Polynom f hat mindestens zwei nicht-reelle Nullstellen. Seien $a_1, \ldots, a_p$ die Nullstellen von f. Koeffizientenvergleich von $f(T) = \prod(T - a_i)$ zeigt: der zweithöchste Koeffizient von $f(T)$ ist

$$-\sum_{i=1}^{p-2} 2n_i = -\sum_{s=1}^{p} a_s.$$

Der dritthöchste Koeffizient ist

$$\sum_{i<j} 2n_i 2n_j + 2m = \sum_{s<t} a_s a_t.$$

Also gilt

$$\begin{aligned}\sum_s a_s^2 &= (\sum_s a_s)^2 - 2\sum_{s<t} a_s a_t \\ &= (\sum_i 2n_i)^2 - 2\sum_{i<j} 2n_i 2n_j - 2\cdot 2m \\ &= 4(\sum_i n_i^2 - m) < 0.\end{aligned}$$

Eine Summe von Quadraten reeller Zahlen kann nicht negativ sein, also gibt es mindestens eine nicht-reelle Nullstelle, und dann sogar mindestens zwei.