

## Übungsblatt 13 zur Algebra I

Abgabe bis 15. Juli 2013, 17:00 Uhr

### Aufgabe 1. Konstruierbare $n$ -Ecke

- a) Für welche  $n \in \{1, \dots, 100\}$  ist ein regelmäßiges  $n$ -Eck mit Zirkel und Lineal konstruierbar?
- b) Gib eine Konstruktionsvorschrift für das regelmäßige 15-Eck an.

### Lösung.

- a) Satz 4.30 gibt die Antwort vor: Es sind genau die  $n$ -Ecke konstruierbar, für die  $n$  von der Form  $2^r p_1 \cdots p_s$ ,  $r, s \geq 0$  sind, wobei die  $p_i$  paarweise verschiedene Fermatsche Primzahlen sind – das sind Primzahlen, die von der Form  $F_k = 2^{2^k} + 1$ ,  $k \geq 0$ , sind. Die ersten vier Fermatschen Primzahlen sind

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257.$$

(Es sind aber nicht alle  $F_k$  Primzahlen, etwa ist  $F_5$  durch 631 teilbar.)

Für  $n \leq 100$  sind nur die ersten drei Fermatschen Primzahlen relevant; es ergibt sich, dass genau folgende  $n$ -Ecke mit  $n \geq 100$  konstruierbar sind:

$$1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96.$$

Das sind insgesamt 26 Stück.

### Aufgabe 2. Fermatsche und Mersennesche Primzahlen

- a) Zeige für alle natürlichen Zahlen  $n \geq 0$ :  $F_{n+1} = 2 + F_n F_{n-1} \cdots F_0$ .
- b) Zeige, dass  $F_m$  und  $F_n$  für  $m \neq n$  teilerfremd sind. Folgere daraus, dass es unendlich viele Primzahlen gibt.
- c) Eine *Mersennesche Zahl* ist eine Zahl der Form  $M_n = 2^n - 1$ . Zeige, dass  $M_n$  höchstens dann eine Primzahl ist, wenn  $n$  eine Primzahl ist.
- d) Zeige allgemeiner, dass  $M_n$  von  $M_d$  geteilt wird, wenn  $d$  ein positiver Teiler von  $n$  ist.

### Lösung.

- a) Per Definition ist  $F_k = 2^{2^k} + 1$ . Die Konvention ist so, dass  $2^{(2^k)}$  und nicht  $(2^2)^k = 4^k$  gemeint ist. Die Behauptung zeigen wir durch einen Induktionsbeweis. Für  $n = 0$  ist die Aussage klar:

$$F_{0+1} = 5 = 2 + 3 = 2 + F_0.$$

Für den Schritt  $n \rightarrow n + 1$  rechnen wir:

$$\begin{aligned} 2 + F_{n+1} F_n F_{n-1} \cdots F_0 &= 2 + F_{n+1} \cdot (F_n F_{n-1} \cdots F_0 + 2 - 2) \\ &\stackrel{\text{IV}}{=} 2 + F_{n+1} \cdot (F_{n+1} - 2) = (F_{n+1} - 1)^2 + 1 \\ &= (2^{2^{n+1}})^2 + 1 = 2^{2^{n+2}} + 1 = F_{n+2}. \end{aligned}$$

- b) Ohne Einschränkung sei  $m > n$ . Sei  $d$  ein gemeinsamer Faktor von  $F_m$  und  $F_n$ . Aus Teilaufgabe a) kennen wir die Beziehung

$$F_m = F_{(m-1)+1} = 2 + F_{m-1} \cdots F_0.$$

Der hintere Summand ist ein Vielfaches von  $d$ , da einer der Faktoren  $F_n$  ist. Daher folgt, dass auch 2 ein Vielfaches von  $d$  ist; der Teiler  $d$  ist also  $\pm 1$  oder  $\pm 2$ . Letzteres kann aber nicht eintreten: Direkt an der Form der fermatschen Zahlen erkennt man, dass  $\pm 2$  kein Teiler von ihnen ist. Also ist  $d = \pm 1$ . Das war zu zeigen.

Eine unendliche Folge paarweise verschiedener Primzahlen können wir mit dieser Erkenntnis wie folgt konstruieren: Wir zerlegen sukzessive die Zahlen  $F_0, F_1, \dots$  in Primfaktoren. Diese Primfaktoren werden wegen der Teilerfremdheit alle unterschiedlich sein. Somit erhalten wir also beliebig viele paarweise verschiedene Primzahlen.

*Bemerkung:* Der Beweis stammt von Goldbach. In der Praxis ist er allerdings ein recht umständliches Verfahren zur Primzahlgenerierung, da die  $F_n$  rasant groß werden:

$$F_0 = 3$$

$$F_1 = 5$$

$$F_2 = 17$$

$$F_3 = 257$$

$$F_4 = 65537$$

$$F_5 = 4294967297 = 641 \cdot 6700417$$

$$F_6 = 18446744073709551617 = 274177 \cdot 67280421310721$$

Es ist ein offenes Forschungsproblem, ob  $F_{33}$  eine Primzahl ist.

- c) Wir zeigen: Ist  $n$  eine zusammengesetzte Zahl, so auch  $M_n$ . Sei dazu  $n = a \cdot b$  eine Zerlegung mit  $a, b \geq 2$ . Dann folgt

$$\begin{aligned} M_n &= 2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \\ &= (2^a - 1) \cdot (1 + 2^a + (2^a)^2 + \cdots + (2^a)^{b-1}). \end{aligned}$$

Da  $a, b \geq 2$ , folgt  $2^a - 1 \geq 2^2 - 1 = 3$  und (hinterer Faktor)  $\geq 1 + 2^a \geq 1 + 2^2 = 5$ , also ist diese Zerlegung von  $M_n$  eine echte und  $M_n$  somit zusammengesetzt.

- d) Gelte  $n = d \cdot \ell$ . Dann folgt völlig analog (sogar identisch!)

$$\begin{aligned} M_n &= 2^n - 1 = 2^{d\ell} - 1 = (2^d)^\ell - 1 \\ &= (2^d - 1) \cdot (1 + 2^d + (2^d)^2 + \cdots + (2^d)^{\ell-1}), \end{aligned}$$

also ist  $M_d = 2^d - 1$  ein Teiler von  $M_n$ .

### Aufgabe 3. Hauptsatz der Galoistheorie

Bestimme alle Untergruppen der galoisschen Gruppe der Nullstellen des Polynoms  $X^4 + 1$  und die zugehörigen Zwischenerweiterungen.

### Aufgabe 4. Relative galoissch Konjugierte

- a) Finde zwei algebraische Zahlen, die über  $\mathbb{Q}$  galoissch konjugiert sind, über  $\mathbb{Q}(\sqrt{3})$  aber nicht.  
b) Seien  $K$  und  $L$  Koeffizientenbereiche mit  $L \supseteq K \supseteq \mathbb{Q}$  und  $x$  eine algebraische Zahl. Zeige, dass ein galoissch Konjugiertes von  $x$  über  $L$  auch ein galoissch Konjugiertes von  $x$  über  $K$  ist.

**Lösung.**

- a) Ein Beispiel bilden die Zahlen  $\pm\sqrt{3}$ . Diese sind über  $\mathbb{Q}$  sicherlich zueinander galoissch konjugiert (ihr gemeinsames Minimalpolynom ist  $X^2 - 3$ ), aber über  $\mathbb{Q}(\sqrt{3})$  haben sie verschiedene Minimalpolynome (nämlich  $X \mp \sqrt{3}$ ).
- b) Seien  $m_K$  und  $m_L$  die Minimalpolynome von  $x$  über  $K$  bzw.  $L$ . Wenn wir  $m_K$  als Polynom über  $L$  auffassen, sagt uns der abelsche Irreduzibilitätssatz, dass  $m_L$  ein Teiler von  $m_K$  sein muss (über  $L$ ) – denn  $m_K$  und  $m_L$  haben die gemeinsame Nullstelle  $x$  und  $m_L$  ist irreduzibel über  $L$ . Folglich ist jede Nullstelle von  $m_L$ , also jedes galoissch Konjugierte von  $x$  über  $L$ , auch eine Nullstelle von  $m_K$ , also ein galoissch Konjugiertes von  $x$  über  $K$ .

**Aufgabe 5. Relative Galoisgruppen**

- a) Finde ein normiertes separables Polynom mit rationalen Koeffizienten, sodass die galoissche Gruppe seiner Nullstellen über  $\mathbb{Q}$  gleich der über  $\mathbb{Q}(\sqrt[3]{5})$  ist.
- b) Sei  $f \in K[X]$  ein normiertes separables Polynom und  $x_1, \dots, x_n$  seine Nullstellen. Sei  $y \in K(x_1, \dots, x_n)$ . Zeige:

$$\text{Gal}_{K(y)}(x_1, \dots, x_n) = \{\sigma \in \text{Gal}_K(x_1, \dots, x_n) \mid \sigma \cdot y = y\}.$$

**Lösung.**

- a) Ein Beispiel ist das Polynom  $X - 1$ .

**Aufgabe 6. Zentrum einer Galoisgruppe**

Sei  $p$  eine Primzahl und  $x$  eine algebraische Zahl vom Grad  $p^n$ . Seien alle galoissch Konjugierten  $x_1 = x, x_2, \dots, x_{p^n}$  von  $x$  in  $x$  rational.

- a) Zeige, dass das Zentrum der galoisschen Gruppe der  $x_1, \dots, x_{p^n}$  ein Element  $\sigma$  der Ordnung  $p$  enthält.
- b) Sei  $\sigma$  eine Permutation wie in a) und  $y$  ein primitives Element zu den Zahlen  $e_i(x_1, \sigma \cdot x_1, \dots, \sigma^{p-1} \cdot x_1)$ ,  $i = 1, \dots, p$ . Zeige, dass  $y$  vom Grad  $p^{n-1}$  ist.

**Lösung.**

- a) Die Anzahl der Elemente der Galoisgruppe ist eine  $p$ -Potenz:

$$|\text{Gal}_{\mathbb{Q}}(x_1, \dots, x_{p^n})| = [\mathbb{Q}(x_1, \dots, x_{p^n}) : \mathbb{Q}] = [\mathbb{Q}(x) : \mathbb{Q}] = p^n.$$

Nach Proposition 4.24 gibt es daher ein Element der Ordnung  $p$  im Zentrum.

- b) *Schritt 1:* Wir sollten uns zunächst ein wenig Übersicht verschaffen. Da die Ordnung der Permutation  $\sigma$  die Primzahl  $p$  ist, zerfällt  $\sigma$  in lauter disjunkte  $p$ -Zykel. Da  $\sigma$  keine Nullstelle  $x_i$  festhalten darf (denn  $x_i$  ist nach Proposition 4.4 wie  $x_1$  ein primitives Element – würde  $\sigma$  daher  $x_i$  festhalten, so würde  $\sigma$  alle Nullstellen festhalten und wäre somit die Identitätspermutation), kommt sogar *jede* Zahl aus  $\{1, \dots, p^n\}$  in einem dieser Zykel vor.

Die Nullstellen  $x_1, \dots, x_{p^n}$  zerfallen also in  $p^{n-1}$  Blöcke von je  $p$  Zahlen, die von  $\sigma$  jeweils nur unter sich abgebildet werden. Einer dieser Blöcke ist

$$x_1, \sigma \cdot x_1, \dots, \sigma^{p-1} \cdot x_1. \quad (\star)$$

Die anderen Blöcke erhält man, wenn man statt mit  $x_1$  mit einer anderen Nullstelle  $x_i$  beginnt (einer, die nicht in diesem Block auftritt).

Wir wollen noch kurz untersuchen, was mit einem solchen Block passiert, wenn man eine beliebige Symmetrie  $\tau$  der Galoisgruppe auf ihn anwendet: Da  $\sigma$  (und somit auch  $\sigma^j$ ) im Zentrum liegt (hier geht diese Eigenschaft das erste Mal ein), gilt

$$\tau \cdot (\sigma^j \cdot x_i) = \sigma^j \cdot (\tau \cdot x_i).$$

Die Wirkung von  $\tau$  vertauscht also die Blöcke untereinander.

*Schritt 2:* Da  $y$  ein primitives Element von  $\mathbb{Q}(e_1(\star), \dots, e_p(\star))$  ist, gibt es ein Polynom  $r \in \mathbb{Q}[E_1, \dots, E_p]$  mit  $y = r(e_1(\star), \dots, e_p(\star))$ . Ferner können wir ein symmetrisches Polynom  $s \in \mathbb{Q}[Y_1, \dots, Y_p]$  mit  $y = s(x_1, \sigma \cdot x_1, \dots, \sigma^{p-1} \cdot x_1)$  finden. Da  $s$  symmetrisch ist, ergibt es Sinn, das Polynom

$$g(X) := \prod (X - s(b_1, \dots, b_p))$$

zu definieren, wobei das Produkt über jeden Block  $(b_1, \dots, b_p)$  genau einmal gehen soll. Dieses Polynom ist normiert, hat  $y$  als Nullstelle und hat rationale Koeffizienten – denn diese sind unter der Wirkung der Galoisgruppe invariant: Sei  $\tau \in \text{Gal}_{\mathbb{Q}}(x_1, \dots, x_{p^n})$  beliebig. Dann gilt

$$\tau \cdot g(X) = \prod (X - s(\tau \cdot b_1, \dots, \tau \cdot b_p)) = \prod (X - s(b_1, \dots, b_p)) = g(X),$$

denn wie wir oben schon gesehen haben, führt  $\tau$  nur zu einer Vertauschung der Blöcke. Der Grad von  $y$  über  $\mathbb{Q}$  ist also höchstens gleich dem Grad von  $g$ , und dieser ist  $p^{n-1}$ .

*Schritt 3:* Das Polynom

$$h(X) := \prod_{j=0}^{p-1} (X - \sigma^j \cdot x_1)$$

ist normiert, hat  $x_1$  als Nullstelle und hat Koeffizienten aus  $\mathbb{Q}(y)$ : Denn diese sind bis auf Vorzeichen durch die elementarsymmetrischen Funktionen in den  $\sigma^j \cdot x_1$ ,  $j = 0, \dots, p-1$  gegeben – und diese sind nach Voraussetzung rational in  $y$ . Folglich ist der Grad von  $x_1$  über  $y$  höchstens  $p$ . Somit folgt

$$[\mathbb{Q}(y) : \mathbb{Q}] = \frac{[\mathbb{Q}(x_1) : \mathbb{Q}]}{[\mathbb{Q}(x_1) : \mathbb{Q}(y)]} \geq \frac{p^n}{p} = p^{n-1}.$$

Das zeigt die Behauptung.

*Bemerkung:* Mit dem Hauptsatz der Galoistheorie kann man einen drastisch kürzeren Beweis angeben. Vielleicht enthält er aber einen Fehler, da die Voraussetzung, dass  $\sigma$  im Zentrum liegt, nicht eingeht! Nach Proposition 5.9 ist  $\mathbb{Q}(y)$  gerade der Fixkörper der Untergruppe  $U := \{\sigma^0, \dots, \sigma^{p-1}\} \subseteq \text{Gal} =: G$ . Daher folgt

$$[\mathbb{Q}(y) : \mathbb{Q}] = [G : U] = p^n / p = p^{n-1}.$$