

Körper- und Galoistheorie

Vorlesung 10

Endliche Untergruppen der Einheitsgruppe eines Körpers

Wir wollen zeigen, dass die Einheitsgruppe $\mathbb{Z}/(p)$, p Primzahl, zyklisch ist. Dafür brauchen wir einige gruppentheoretische Vorbereitungen.

LEMMA 10.1. *Sei G eine kommutative Gruppe und $x, y \in G$ Elemente der endlichen Ordnungen $n = \text{ord}(x)$ und $m = \text{ord}(y)$, wobei n und m teilerfremd seien. Dann hat xy die Ordnung nm .*

Beweis. Sei $(xy)^k = 1$. Wir haben zu zeigen, dass k ein Vielfaches von nm ist. Es ist

$$1 = (x^k y^k)^n = x^{kn} y^{kn} = y^{kn},$$

da ja n die Ordnung von x ist. Aus dieser Gleichung erhält man, dass kn ein Vielfaches der Ordnung von y , also von m sein muss. Da n und m teilerfremd sind, folgt aus Lemma 3.17, dass k ein Vielfaches von m ist. Ebenso ergibt sich, dass k ein Vielfaches von n ist, so dass k , wieder aufgrund der Teilerfremdheit, ein Vielfaches von nm sein muss. \square

DEFINITION 10.2. Der *Exponent* $\exp(G)$ einer endlichen Gruppe G ist die kleinste positive Zahl n mit der Eigenschaft, dass $x^n = 1$ ist für alle $x \in G$.

LEMMA 10.3. *Sei G eine endliche kommutative Gruppe und sei $\exp(G) = \text{ord}(G)$, wobei $\exp(G)$ den Exponenten der Gruppe bezeichnet. Dann ist G zyklisch.*

Beweis. Sei $n = \text{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

$$\exp(G) = \text{kgV}(\text{ord}(x) : x \in G).$$

Sei p_i ein Primteiler von n . Wegen $\exp(G) = \text{ord}(G)$ gibt es ein Element $x \in G$, dessen Ordnung ein Vielfaches von $p_i^{r_i}$ ist. Dann gibt es auch (in der von x erzeugten zyklischen Untergruppe) ein Element x_i der Ordnung $p_i^{r_i}$. Dann hat das Produkt $x_1 \cdots x_k \in G$ nach Lemma 10.1 die Ordnung n . \square

SATZ 10.4. *Sei $U \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K . Dann ist U zyklisch.*

Beweis. Sei $n = \text{ord}(U)$ und $e = \exp(U)$ der Exponent dieser Gruppe. Dies bedeutet, dass alle Elemente $x \in U$ eine Nullstelle des Polynoms $X^e - 1$ sind. Nach Korollar Anhang 1.5 ist die Anzahl der Nullstellen aber maximal gleich dem Grad, so dass $n = e$ folgt. Nach Lemma 10.1 ist dann U zyklisch. \square

SATZ 10.5. *Es sei K ein endlicher Körper. Dann ist die Einheitsgruppe K^\times eine zyklische Gruppe.*

Beweis. Dies folgt direkt aus Satz 10.4. □

SATZ 10.6. *Sei p eine Primzahl. Dann ist die Einheitsgruppe $(\mathbb{Z}/(p))^\times$ zyklisch der Ordnung $p - 1$. Es gibt also (sogenannte primitive) Elemente g mit der Eigenschaft, dass die Potenzen g^i , $i = 0, 1, \dots, p - 2$, alle Einheiten durchlaufen.*

Beweis. Dies folgt unmittelbar aus Satz 10.4, da $\mathbb{Z}/(p)$ ein endlicher Körper ist. □

DEFINITION 10.7. Eine Einheit $u \in (\mathbb{Z}/(n))^\times$ heißt *primitiv* (oder eine *primitive Einheit*), wenn sie die Einheitsgruppe erzeugt.

BEISPIEL 10.8. Wir betrachten die Einheitsgruppe des Restklassenkörpers $\mathbb{Z}/(23)$. Nach Satz 10.6 ist sie zyklisch und es gibt daher Erzeuger der Einheitsgruppe, also primitive Elemente. Wie kann man diese finden? Man ist hierbei prinzipiell auf Probieren angewiesen, man kann dies allerdings deutlich vereinfachen. Man weiß, dass die Einheitsgruppe 22 Elemente besitzt, als Ordnung von Elementen dieser Gruppe kommen also nur 1, 2, 11 und 22, in Frage. Es gibt genau ein Element mit der Ordnung 1, nämlich 1, und ein Element mit der Ordnung 2, nämlich $-1 = 22$. Alle anderen Elemente haben also die Ordnung 11 oder 22, und genau die letzteren sind primitiv. Der erste Kandidat ist 2. Wir müssen also

$$2^{11} \pmod{23}$$

ausrechnen. Es ist $2^5 = 32 = 9$ und daher ist

$$2^{11} = 9 \cdot 9 \cdot 2 = 12 \cdot 2 = 24 = 1.$$

Die Ordnung ist also 11, und die 2 ist nicht primitiv. Betrachten wir die 3. Es ist $3^3 = 27 = 4$ und daher ist

$$3^{11} = 4 \cdot 4 \cdot 4 \cdot 9 = 18 \cdot 9 = 162 = 1,$$

also wieder nicht primitiv. Der nächste Kandidat 4 muss nicht gecheckt werden, denn wegen $4 = 2^2$ ist sofort $4^{11} = 2^{22} = 1$ (diese Beobachtung gilt für alle Quadratzahlen, und zwar auch für diejenigen Zahlen, die nur modulo 23 ein Quadrat sind). Betrachten wir also 5. Es ist $5^2 = 2$. Damit ist

$$5^{11} = 2^5 \cdot 5 = 9 \cdot 5 = 45 = -1 \neq 1.$$

Daher hat 5 die Ordnung 22 und ist ein primitives Element.

Man kann diesen Sachverhalt auch so ausdrücken, dass die Abbildung

$$\mathbb{Z}/(22) \longrightarrow (\mathbb{Z}/(23))^\times, k \longmapsto 5^k,$$

einen Gruppenisomorphismus definiert. Dieser übersetzt die Addition in die Multiplikation, daher spricht man von einer *diskreten Exponentialfunktion* und nennt die Umkehrabbildung auch einen *diskreten Logarithmus*. Solche

Abbildungen spielen eine wichtige Rolle in der *Kryptologie*. Wenn man wie in diesem Beispiel einen solchen Isomorphismus gefunden hat, so kann man viele Eigenschaften der Einheitengruppe in der „einfacheren“ Gruppe entscheiden. Z.B. sind in $\mathbb{Z}/(22)$ alle ungeraden Elemente außer 11 ein Gruppenerzeuger, daher sind in der Einheitengruppe alle Elemente der Form

$$5^u, u \text{ ungerade, } u \neq 11,$$

primitiv.

Primitive Einheitswurzeln

Die Menge der n -ten Einheitswurzeln in einem Körper K bilden eine endliche Untergruppe von K^\times , die wegen Satz 10.4 zyklisch ist.

DEFINITION 10.9. Eine n -te Einheitswurzel heißt *primitiv*, wenn sie die Ordnung n besitzt.

Man beachte, dass ein Erzeuger der Gruppe der Einheitswurzeln nur dann primitiv heißt, wenn es n verschiedene Einheitswurzeln gibt. Wenn ζ eine primitive n -te Einheitswurzel ist, so sind genau die ζ^i mit $i < n$ und i teilerfremd zu n die primitiven Einheitswurzeln.¹

Endliche Körper

DEFINITION 10.10. Ein Körper heißt *endlich*, wenn er nur endlich viele Elemente besitzt.

Über die Anzahl der Elemente in einem endlichen Körper gilt folgende wichtige Bedingung.

LEMMA 10.11. *Sei K ein endlicher Körper. Dann besitzt K genau p^n Elemente, wobei p eine Primzahl ist und $n \geq 1$.*

Beweis. Der endliche Körper kann nicht Charakteristik null besitzen, und als Charakteristik eines Körpers kommt ansonsten nach Lemma 13.9 (Einführung in die Algebra (Osnabrück 2009)) nur eine Primzahl in Frage. Diese sei mit p bezeichnet. Das bedeutet, dass K den Körper $\mathbb{Z}/(p)$ enthält. Damit ist aber K ein Vektorraum über $\mathbb{Z}/(p)$, und zwar, da K endlich ist, von endlicher Dimension. Sei n die Dimension, $n \geq 1$. Dann hat man eine $\mathbb{Z}/(p)$ -Vektorraum-Isomorphie $K \cong (\mathbb{Z}/(p))^n$ und somit besitzt K gerade p^n Elemente. \square

¹Insbesondere gibt es, wenn es überhaupt primitive Einheitswurzeln gibt, genau $\varphi(n)$ primitive Einheitswurzeln, wobei $\varphi(n)$ die eulersche φ -Funktion bezeichnet. Siehe Vorlesung 19.

Die vorstehende Aussage gilt allgemeiner für endliche Ringe, die einen Körper enthalten. Es sei schon jetzt erwähnt, dass es zu jeder Potenz p^n bis auf Isomorphie genau einen Körper mit p^n Elementen gibt. Dies werden wir in der nächsten Vorlesung beweisen. Für einige Beispiele siehe auch die Aufgaben.

BEISPIEL 10.12. Wir konstruieren einen Körper mit $23^2 = 529$ Elementen und knüpfen dabei an Beispiel 10.8 an. Da die $5 \in \mathbb{Z}/(23)$ primitiv ist, folgt, dass das Polynom $X^2 - 5 \in \mathbb{Z}/(23)[X]$ irreduzibel ist. Andernfalls müsste es eine Nullstelle haben und dann wäre $5 = a^2$ ein Quadrat mit $a \in \mathbb{Z}/(23)$. Doch dann wäre $5^{11} = a^{22} = 1$, was nicht der Fall ist.

Es folgt nach Satz 7.6, dass

$$K = \mathbb{Z}/(23)[X]/(X^2 - 5)$$

ein Körper ist. Dieser hat 23^2 Elemente, da man jede Restklasse auf genau eine Weise als $ax + b$ mit $a, b \in \mathbb{Z}/(23)$ schreiben kann (x bezeichne die Restklasse von X). Dieser Körper enthält $\mathbb{Z}/(23)$, und die Ordnungen dieser Elemente ändern sich nicht (und sie sind insbesondere nicht primitiv im größeren Körper).

Wir möchten eine primitive Einheit in diesem Körper finden. Die Ordnung von K^\times ist $528 = 16 \cdot 3 \cdot 11$. Wir müssen für jede dieser Primzahlpotenzen ein Element mit dieser Ordnung finden. Die 2 hat die Ordnung 11. Das Element $11 - x$ hat die Ordnung 3, es ist nämlich

$$(11-x)^3 = 121 \cdot 11 - 3 \cdot 121x + 33x^2 - x^3 = 66 - 3 \cdot 6x + 50 - 5x = 116 - 23x = 1.$$

Um ein Element der Ordnung 16 zu finden, ziehen wir sukzessive Quadratwurzeln aus -1 . Es ist

$$(3x)^2 = 9x^2 = 45 = -1.$$

Eine Quadratwurzel daraus ist $14 + 19x$, wegen

$$(14 + 19x)^2 = 196 + 361 \cdot 5 + 2 \cdot 14 \cdot 19x = 12 + 16 \cdot 5 + 5 \cdot 19x = 3x.$$

Um eine Quadratwurzel für $14 + 19x$ zu finden, setzen wir $(a+bx)^2 = 14+19x$ an, was zum Gleichungssystem $a^2 + 5b^2 = 14$ und $2ab = 19$ über $\mathbb{Z}/(23)$ führt. Es ist dann $a = 21 \cdot b^{-1}$, was zu $4b^{-2} + 5b^2 = 14$ bzw. zur *biquadratischen Gleichung*

$$5b^4 + 9b^2 + 4 = 0$$

führt. Normieren ergibt $b^4 + 11b^2 + 10 = 0$. *Quadratisches Ergänzen* führt zu

$$(b^2 + 17)^2 = 17^2 - 10 = 49.$$

Daher ist $b^2 = 13$ und somit $b = 6$ und $a = 15$, also ist $15 + 6x$ ein Element der Ordnung 16. Damit ist insgesamt

$$2(11 - x)(15 + 6x) = 2(165 - 30 + 51x) = 2(20 + 5x) = 17 + 10x$$

eine primitive Einheit nach Lemma 10.1.

SATZ 10.13. *Sei K ein endlicher Körper. Dann ist das Produkt aller von 0 verschiedener Elemente aus K gleich -1 .*

Beweis. Die Gleichung $x^2 = 1$ hat in einem Körper nur die Lösungen 1 und -1 , die allerdings gleich sein können. Das bedeutet, dass für $x \neq 1, -1$ immer $x \neq x^{-1}$ ist. Damit kann man das Produkt aller Einheiten schreiben als

$$1(-1)x_1x_1^{-1} \cdots x_kx_k^{-1}.$$

Ist $-1 \neq 1$, so ist das Produkt -1 . Ist hingegen $-1 = 1$, so fehlt in dem Produkt der zweite Faktor und das Produkt ist $1 = -1$. \square

Die folgende Aussage heißt *Satz von Wilson*.

KOROLLAR 10.14. *Sei p eine Primzahl. Dann ist*

$$(p-1)! = -1 \pmod{p}.$$

Beweis. Dies folgt unmittelbar aus Satz 10.13, da ja die Fakultät durch alle Zahlen zwischen 1 und $p-1$ läuft, also durch alle Einheiten im Restklassenkörper $\mathbb{Z}/(p)$. \square