Der Hauptsatz über endliche abelsche Gruppen

Die Punkte einer elliptischen Kurve über einem endlichen Körper k bilden eine endliche abelsche Gruppe. Wir wollen uns überlegen, daß jede solche Gruppe isomorph ist zu einem Produkt zyklischer Gruppen. Elliptische Kurven werden in der heutigen Vorlesung nicht vorkommen; erst in den nächsten werden wir sehen, inwieweit elliptische Kurven über endlichen Körpern abelsche spezielle Gruppen sind.

Erinnern wir uns zunächst an das Produkt zweier oder mehrerer Gruppen: $G_1, \ldots, G_r$ seien irgendwelche Gruppen, deren Gruppenoperation wir – wie wir es von den elliptischen Kurven gewohnt sind – additiv schreiben. Dann wird auch das kartesische Produkt $G_1 \times \cdots \times G_r$ zu einer Gruppe mit der Verknüpfung

$$(g_1, \ldots, g_r) + (h_1, \ldots, h_r) \underset{\text{def}}{=} (g_1 + h_1, \ldots, g_r + h_r)\,.$$

Das Neutralelement ist das Tupel bestehend aus den Neutralelementen der r Gruppen G_i, und auch die Inversenbildung geschieht komponentenweise.

Nun sei G eine endliche abelsche Gruppe der Ordnung n, die keine Primzahlpotenz ist. Die Primzerlegung von n sei $n = p_1^{e_1} \cdots p_r^{e_r}$ mit $r \geq 2$ verschiedenen Primzahlen $p_1, \ldots, p_r$. Wir setzen $q_i = n/p_i^{e_i}$ und

$$G_i \underset{\text{def}}{=} \left\{ g \in G \;\middle|\; p_i^{e_i} g = 0 \right\},$$

wobei 0 das Neutralelement von G bezeichnet und die Multiplikation eines Gruppenelements g mit einer natürlichen Zahl m wie wir es von elliptischen Kurven gewohnt sind die Summe aus m Summanden g. Dazu betrachten wir die Abbildung

$$\varphi\colon \begin{cases} G \to G_1 \times \cdots \times G_r \\ g \mapsto (q_1 g, \ldots, q_r g) \end{cases}.$$

Da nach LAGRANGE $ng = 0$ für alle $g \in G$, ist auch $p_i^{e_i}(qg) = 0$ für alle i. Die Abbildung ist daher wohldefiniert, und sie ist natürlich ein Homomorphismus, da die Multiplikation mit einer natürlichen Zahl in einer abelschen Gruppe verträglich ist mit der Addition. Wäre φ nicht injektiv, gäbe es daher ein $g \in G$ mit $\varphi(g) = (0, \ldots, 0)$, aber $g \neq 0$. Ist

aber $q_i g = 0$ für alle i, so ist auch $mg = 0$ für alle $m \in \mathbb{Z}$, die sich als ganzzahlige Linearkombinationen der q_i schreiben lassen. Dies gilt insbesondere für den größten gemeinsamen Teiler der q_i, der wegen der Verschiedenheit der p_i gleich eins sein muß. Also muß $g = 0$ sein und φ ist injektiv.

Da $p_i^{e_i} g = 0$ ist für alle $g \in G_i$, muß die Ordnung der Gruppe G_i eine p_i-Potenz $p_i^{f_i}$ sein. Da G_i eine Untergruppe von G ist und die Ordnung einer Untergruppe die Gruppenordnung teilt, muß dabei $f_i \leq e_i$ sein. Das kartesische Produkt der Gruppen G_i hat die Ordnung $p_1^{f_1} \cdots p_r^{f_r}$, und da φ eine injektive Abbildung von G in dieses Produkt ist, muß diese Ordnung mindestens n sein. Somit müssen alle $f_i = e_i$ sein, das Produkt der G_i hat also die gleiche Ordnung wie G, so daß die injektive Abbildung φ auch surjektiv sein muß und damit ein Isomorphismus.

Damit wissen wir, daß sich jede endliche abelsche Gruppe als Produkt abelscher Gruppen von Primzahlpotenzordnung schreiben läßt, und es reicht, wenn wir diese Gruppen weiter untersuchen.

Eine Gruppe von Primzahlordnung p muß offensichtlich zyklisch sein, denn die Ordnung eines jeden Elements muß ein Teiler von p sein, und da nur das Neutralelement die Ordnung eins hat, haben alle anderen Elemente Ordnung p, erzeugen also die Gruppe.

Wenn die Ordnung der Gruppe eine höhere Potenz von p ist, muß die Gruppe nicht mehr zyklisch sein: Beispielsweise kann $\mathbb{Z}/p \times \mathbb{Z}/p$ nicht zyklisch sein, da $p(g, h) = (pg, ph) = (0, 0)$ für alle $(g, h) \in \mathbb{Z}/p \times \mathbb{Z}/p$, so daß es kein Element der Ordnung p^2 geben kann. Die Strategie zur weiteren Zerlegung einer nichtzyklischen abelschen Gruppe G von Primzahlpotenzordnung besteht darin, daß wir Elemente maximaler Ordnung suchen und die davon erzeugte Untergruppe abspalten. Dies ist möglich nach dem folgenden

Lemma: G sei eine abelsche Gruppe von p-Potenzordnung, $g \in G$ sei ein Element maximaler Ordnung und $Z \leq G$ die von g erzeugte zyklische Untergruppe. Dann gibt es eine Untergruppe $H \leq G$, so daß $G \cong Z \times H$ ist.

Beweis: Falls G zyklisch ist, muß $Z = G$ sein, und wir nehmen für H die Gruppe, die nur das Neutralelement enthält. Andernfalls sei wieder p^n die Gruppenordnung von G, und wir beweisen das Lemma durch Induktion nach n.

Im Falle $n = 1$ ist G zyklisch, so daß es nichts mehr zu zeigen gibt. Andernfalls sei $g \in G$ ein Element maximaler Ordnung. Wenn G nicht zyklisch ist, gibt es Elemente, die keine Vielfache von g sind. Auch die Ordnungen dieser Elemente müssen Potenzen von p sein; indem wir ein geeignetes Vielfaches nehmen, bekommen wir ein Element a der Ordnung p, das nicht in der von g erzeugten Untergruppe Z liegt. Die von a erzeugte zyklische Gruppe sei P. Wir betrachten die Gruppe aller Restklassen modulo P, d.h. die Faktorgruppe G/P. Da a nicht in Z liegt, kann keine Restklasse mehr als ein Element von Z enthalten. Die kanonische Abbildung $\pi\colon G \to G/P$, die jedem Element seine Restklasse modulo P zuordnet, ist also auf Z injektiv. Somit ist die Ordnung von $\pi(g)$ in G/P gleich der Ordnung von g in G und damit maximal in G/P.

Nach Induktionsannahme gibt es daher eine Untergruppe $\overline{H}$ von G/P, so daß G/P isomorph ist zu $\pi(Z)\times\overline{H}$. Wir betrachten das Urbild $H \leq G$ von $\overline{H} \leq G/P$ unter π und die Abbildung

$$\varphi\colon \begin{cases} Z \times H \to G \\ \quad (z,h) \mapsto z + h \end{cases} .$$

Sie ist injektiv, denn ist $\varphi(z_1, h_1) = \varphi(z_2, h_2)$, so ist $z_1 + h_1 = z_2 + h_2$, also liegt $z_1 - z_2 = h_2 - h_1$ sowohl in Z als auch in H. Das Bild unter π liegt somit sowohl in $\varphi(Z)$ als auch in $\varphi(H) = \overline{H}$, und diese beiden Untergruppen von G/P haben nur das Neutralelement gemeinsam, da G/P isomorph zum Produkt dieser Gruppen ist. Damit muß $z_1 - z_2 \in Z$ auch in P liegen, und nach Konstruktion von a enthält Z außer dem Neutralelement kein Vielfaches von a. Somit ist $z_1 - z_2 = h_1 - h_2 = 0$, also $(z_1, h_1) = (z_2, h_2)$.

Wegen $G/P \cong Z \times \overline{H}$ ist die Ordnung von $\overline{H}$ gleich der von G/P dividiert durch die Ordnung von a. Die Ordnung von G ist gleich der von G/P mal p und die von H ist gleich der von $\overline{H}$ mal p, also ist

die Ordnung von G das Produkt der Ordnungen von Z und von H. Damit ist der injektive Homomorphismus φ auch surjektiv, also ein Isomorphismus, was die Behauptung beweist. ∎

Induktiv folgt

Satz: Jede abelsche Gruppe G von p-Potenzordnung ist isomorph zum Produkt zyklischer Gruppen $G_1, \ldots, G_r$ mit Ordnungen p^{e_i}, wobei

$$e_1 \geq \cdots \geq e_r$$

ist. Das Tupel $(e_1, \ldots, e_r)$ ist durch G eindeutig bestimmt.

Beweis: Für eine zyklische Gruppe G können wir einfach $G = G_1$ setzen, und das ist auch die einzige Möglichkeit: Wäre nämlich die zyklische Gruppe der Ordnung p^e isomorph zum Produkt zyklischer Gruppen der Ordnungen p^{e_i} mit $e_i < e$, so wäre die Ordnung eines jeden Elements ein Teiler von $p^{e'}$, wobei e' das Maximum der e_i bezeichnet und echt kleiner als e wäre. Das ist in einer zyklischen Gruppe der Ordnung p^e natürlich nicht möglich.

Allgemein sei $\#G = p^n$. Für $n = 1$ ist die Gruppe zyklisch und der Satz somit richtig. Für $n \geq 2$ und eine nichtzyklische Gruppe G betrachten wir ein Element g maximaler Ordnung. Nach dem gerade bewiesenen Lemma ist G isomorph zum Produkt der von g erzeugten zyklischen Untergruppe Z mit einer weiteren Untergruppe H, deren Ordnung kleiner als p^n sein muß. Somit läßt sich H nach Induktionsannahme schreiben als

$$H \cong G_2 \times \cdots \times G_r \qquad \text{mit} \qquad \#G_2 \geq \cdots \geq \#G_r\,.$$

Da Z von einem Element maximaler Ordnung erzeugt wird, kann G_2 nicht größer sein als Z; mit $G_1 = Z$ ist also

$$G \cong G_1 \times \cdots \times G_r \qquad \text{mit} \qquad \#G_1 \geq \cdots \geq \#G_r\,.$$

Bleibt noch zu zeigen, daß die Ordnungen der G_i durch G eindeutig bestimmt sind. Für zyklische Gruppen G haben wir das bereits gezeigt; für nichtzyklische arbeiten wir wieder mit Induktion: g_i sei ein erzeugendes

Element von G_i; seine Ordnung p^{e_i} sei echt größer p für $i = 1, \ldots, s$. Dann ist

$$G' = \{\, pg \mid g \in G \} \cong G'_1 \times \cdots \times G'_s \,,$$

wobei G'_i die von pg_i erzeugte zyklische Gruppe bezeichnet. Deren Ordnung ist p^{e_i-1}, und nach Induktionsannahme ist die Folge der Zahlen $e_1 - 1, \ldots, e_s - 1$ durch G' und damit auch durch G eindeutig bestimmt. Die Anzahl $r - s$ der verbleibenden Faktoren der Ordnung p in der Zerlegung von G ist dann durch die Gruppenordnung von G und die restlichen e_i eindeutig bestimmt.

∎

Da wir uns bereits zu Beginn dieses Abschnitts überlegt haben, daß jede endliche abelsche Gruppe isomorph ist zum Produkt abelscher Gruppen von Primzahlpotenzordnung, folgt nun sofort die erste Version des Hauptsatzes über die Struktur endlicher abelscher Gruppen:

Satz: Jede endliche abelsche Gruppe ist isomorph zum Produkt zyklischer Gruppen von Primzahlpotenzordnung. Die Gruppenordnungen der Faktoren sind dabei durch die Gruppe eindeutig festgelegt.

∎

Für die Anwendung auf elliptische Kurven ist eine zweite Version nützlicher: Nach dem chinesischen Restesatz ist das Produkt zweier zyklischer Gruppen mit teilerfremden Ordnungen r und s isomorph zur zyklischen Gruppe der Ordnung rs. Ist daher G eine abelsche Gruppe der Ordnung $n = p_1^{e_1} \cdots p_r^{e_r}$, so können wir G zunächst nach obigem Satz schreiben als Produkt zyklischer Gruppen, deren Ordnungen Potenzen der p_i sind. In einem nächsten Schritt wählen wir für jede Primzahl p_i unter den Faktoren von p_i-Potenzordnung einen maximalen aus. Das Produkt dieser Faktoren ist nach dem chinesischen Restesatz isomorph zu einer zyklischen Gruppe, deren Ordnung n_1 das Produkt der Ordnungen der Faktoren ist. Das Produkt der restlichen Faktoren ist eine Gruppe der Ordnung n/n_1. Mit diesem Produkt verfahren wir genauso, d.h. wir wählen für jede Primzahl p_i, für die es noch einen Faktor gibt, einen maximalen und bilden das Produkt dieser Faktoren. Wieder zeigt uns der chinesische Restesatz, daß dies eine zyklische Gruppe ist, und nach Konstruktion ist ihre Ordnung n_2 ein Teiler von n_1. Induktiv

erhalten wir die zweite Version des Hauptsatzes über die Struktur endlicher abelscher Gruppen:

Satz: Jede endliche abelsche Gruppe ist isomorph zum einem Produkt

$$\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s \qquad \text{mit} \qquad n_s|n_{s-1}|\cdots|n_2|n_1\,.$$

Die n_i sind dabei durch die Gruppe eindeutig festgelegt. ∎

Als Anwendungsbeispiel wollen wir sämtliche abelsche Gruppen der Ordnung 100 bestimmen. Da $100 = 2^2 \cdot 5^2$ ist, ist jede abelsche Gruppe der Ordnung 100 zunächst einmal isomorph zum Produkt einer Gruppe der Ordnung vier mit einer Gruppe der Ordnung 25. Der Faktor der Ordnung vier ist entweder zyklisch oder das Produkt zweier zyklischer Gruppen der Ordnung zwei; entsprechend der Faktor der Ordnung 25. Somit ist die Gruppe isomorph zu einer der vier Gruppen $G_1 = \mathbb{Z}/4 \times \mathbb{Z}/25$, $G_2 = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/25$, $G_3 = \mathbb{Z}/4 \times \mathbb{Z}/5 \times \mathbb{Z}/5$ und $G_4 = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/5 \times \mathbb{Z}/5$.

Nach dem chinesischen Restesatz ist $G_1 \cong \mathbb{Z}/100$. Bei G_2 wählen wir im ersten Schritt einen der Faktoren $\mathbb{Z}/2$ aus und kombinieren ihn mit $\mathbb{Z}/25$; wir erhalten $G_2 \cong \mathbb{Z}/50 \times \mathbb{Z}/2$. Bei G_3 müssen wir entsprechend einen der Faktoren $\mathbb{Z}/5$ auswählen und erhalten $G_3 \cong \mathbb{Z}/20 \times \mathbb{Z}/5$. Bei G_4 schließlich müssen wir im ersten Schritt einer der beiden Faktoren $\mathbb{Z}/2$ und einen der beiden Faktoren $\mathbb{Z}/5$ auswählen; übrig bleiben die beiden restlichen, so daß $G_4 \cong \mathbb{Z}/10 \times \mathbb{Z}/10$ ist.