Der Satz von Lagrange und endliche Körper

Kurzvortrag
Maria Gugging, 22. März 2025

1 Motivation

Teilbarkeitsaufgaben aus der Zahlentheorie, in denen eine Primzahl vorkommt, kommen in mindestens zwei Archetypen vor:

(1.) Sei p eine Primzahl, $a_1, a_2, \dots a_n \in \mathbb{Z}$, P irgendein Polynom in $a_1, \dots, a_n$, und (NB) eine Nebenbedingung. Beweise:

$$(\text{NB}) \implies p \mid P(a_1, \dots, a_n)$$

(2.) So wie in (1.), aber diesmal ist zu zeigen:

$$p \mid P(a_1, \dots, a_n) \implies c \mid Q(p),$$

wobei $c \in \mathbb{N}$ und Q ein Polynom in p ist.

Beispiel (quadratische Reziprozität): p ungerade Primzahl, $p|a^2 + 1 \implies 4|p - 1$

In diesem Vortrag finden wir eine recht allgemeine Methode, mit der man Teilbarkeiten vom Typ (2.) zeigen kann.

2 Satz von Lagrange

Definition 1 (Gruppe)**.** Eine *Gruppe* ist eine Menge G zusammen mit Funktionen $m : G \times G \to G$ (Multiplikation) und $i : G \to G$ (Inverse), sodass folgende Axiome erfüllt sind:

- Assoziativität: $m(x, m(y, z)) = m(m(x, y), z)$ für alle $x, y, z \in G$
- Neutrales Element: Es existiert ein $e \in G$ sodass für alle $x \in G$ gilt: $m(e, g) = g = m(g, e)$
- Inverse Elemente: Für alle $x \in G$ gilt $m(i(x), x) = m(x, i(x)) = e$

Oft wird ein Symbol $\bullet$ für die Multiplikation festgelegt und die Gruppe als $(G, \bullet)$ geschrieben. Man schreibt dann $x \bullet y := m(x, y)$ und $x^{-1} := i(x)$. Die Gruppenaxiome für $(G, \bullet)$ lauten dann:

- Assoziativität: $(x \bullet y) \bullet z = x \bullet (y \bullet z)$
- Neutrales Element: Es gibt ein $e \in G$ mit $e \bullet x = e = x \bullet e$
- Inverse Elemente: $x^{-1} \bullet x = x \bullet x^{-1} = e$

für alle $x, y, z \in G$. Man schreibt außerdem $x^n := m(x, m(x, \dots, m(x, x)) \dots)$, wobei x hier n-mal vorkommt, $x^{-n} := i(x^n)$, sowie $x^0 = e$ für alle $x \in G$. Damit gilt wie gewohnt $x^a \bullet x^b = x^{a+b}$ für alle $a, b \in \mathbb{Z}$ und $x \in G$.

Beispiele:

- $(\mathbb{Z}, +)$: Die Gruppenoperation ist Addition von ganzen Zahlen. Das Inverse von x ist $-x$.
- $(\mathbb{R} \setminus \{0\}, \cdot)$: Die Gruppenoperation ist Multiplikation von reellen Zahlen. Das Inverse von x ist $1/x$. Beachte, dass 0 nicht Teil dieser Gruppe sein kann, da es kein multiplikatives Inverses hat.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ mit $n \in \mathbb{N}$: Die Elemente der Gruppe sind Restklassen modulo n, die Gruppenoperation ist Addition modulo n, und das Inverse Element von x mod n ist $-x$ mod n.
- $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ mit $n \in \mathbb{N}$: Die Elemente der Gruppe sind Restklassen modulo n, die ein multiplikatives Inverses mod n haben. Die Gruppenoperation ist Multiplikation mod n.

Anmerkung: Diese Beispiele sind alle *kommutativ*, das heißt, dass $x \bullet y = y \bullet x$ für alle $x, y \in G$ gilt. Es gibt aber auch Gruppen, in denen das nicht der Fall ist. Das kleinste Beispiel ist die Gruppe S_3 der Permutationen von $\{1, 2, 3\}$. Diese Gruppe hat die gleiche Struktur wie die Gruppe der Kongruenzabbildungen eines gleichseitigen Dreiecks auf sich selbst.

Aufgabe 1. Verifiziere die Gruppenaxiome für die oben genannten Beispiele.

Aufgabe 2. Beweise, dass $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ gilt, wobei φ die Eulersche Phi-Funktion ist.

Aufgabe 3. Beweise den Satz von Euler–Fermat: Sei $n > 1$ eine natürliche Zahl und $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, dann gilt $a^{\varphi(n)} = 1$

Definition 2. Sei G eine endliche Gruppe und $x \in G$. Die *Ordnung von x in G* ist

$$\mathrm{ord}_G(x) := \min\{n \in \mathbb{N}_{\geq 1} : x^n = e\}.$$

Aufgabe 2 und 3 bedeuten dann insbesondere: Sei $n > 1$ eine natürliche Zahl und $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, dann gilt

$$\mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(a) \ \mid \ |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Der Satz von Lagrange ist eine weitreichende Verallgemeinerung davon.

Satz 1 (Lagrange)**.** *Sei G eine endliche Gruppe und $x \in G$. Dann gilt $\mathrm{ord}_G(x) \mid |G|$.*

Anmerkung: Tatsächlich ist der Satz von Lagrange etwas allgemeiner und besagt, dass $|H| \mid |G|$ für jede Untergruppe H von G gilt. Eine Teilmenge H von G heißt *Untergruppe*, falls für alle $x, y \in H$ die Elemente $x \bullet y$ und x^{-1} ebenfalls in H liegen. Satz 1 folgt dann daraus, dass die Menge

$$\langle x \rangle := \{x^n : n \in \mathbb{Z}\} \subseteq G$$

eine Teilgruppe von G bildet und $|\langle x \rangle| = \mathrm{ord}_G(x)$ gilt.

3 Endliche Körper

Definition 3. Ein *Körper* ist eine Menge K mit:

- einer kommutativen Gruppe $(K, +)$ mit neutralem Element 0 (additive Gruppe)
- einer kommutativen Gruppe $(K \setminus \{0\}, \cdot)$ mit neutralem Element 1 (multiplikative Gruppe),

sodass das Distributivgesetz gilt: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ für alle $a, b, c \in K$.

Beispiele:

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $\mathbb{Q}[i] := \{a + bi : a, b \in \mathbb{Q}\}$ mit $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} \in \mathbb{Q}[i]$
- $\mathbb{F}_p$, der Körper mit p Elementen, dessen Elemente die Restklassen modulo der Primzahl p sind.

Anmerkung: Hier benötigen wir, dass p eine Primzahl ist, da sonst nicht jede Restklasse außer 0 ein multiplikatives Inverses hat!

Aufgabe 4. Sei $\mathbb{F}_p[i] := \{a + bi : a, b \in \mathbb{F}_p\}$, wobei i die imaginäre Einheit mit $i^2 = -1$ ist und p eine Primzahl. Analog zu den komplexen Zahlen statten wir $\mathbb{F}_p[i]$ mit Addition und Multiplikation aus. Bestimme alle Primzahlen p, für die $\mathbb{F}_p[i]$ ein Körper ist.

Satz 2 (Klassifikation endlicher Körper)**.**

(i) Sei K ein endlicher Körper. Dann gibt es eine Primzahl p und $e \in \mathbb{N}_{\geq 1}$, sodass $|K| = p^e$ gilt. p heißt dann die Charakteristik von K.

(ii) Für jede Primzahl p und jedes $e \in \mathbb{N}_{\geq 1}$ gibt es einen Körper K mit $|K| = p^e$. Alle Körper dieser Ordnung sind "strukturell ident" bis auf Umbenennung der Elemente[1]*. Wir schreiben $\mathbb{F}_{p^e}$ für diesen Körper.*

(iii) Es gilt[2] *$\mathbb{F}_{p^e} \subseteq \mathbb{F}_{p^f}$ dann und nur dann, wenn $e \mid f$.*

Satz 3. *(Körpererweiterungen)*

(i) Sei K ein Körper und $P \in K[X]$ ein irreduzibles Polynom mit Koeffizienten in K. Dann gibt es einen Körper L, der K enthält[3] *und ein $a \in L$ hat, sodass $P(a) = 0$.*

(ii) Wenn $K = \mathbb{F}_p$ ist, dann können wir für L den Körper $\mathbb{F}_{p^e}$ mit $e = deg(P)$ verwenden.

Aufgabe 5. Zeige im Kontext von Satz 3 (ii): Wenn wir im Körper L ein Element mit multiplikativer Ordnung d finden, dann gilt $d \,|\, p^e - 1$.

Hinweis: Satz von Lagrange.

Aufgabe 6. Sei p eine ungerade Primzahl. Beweise mit dem Satz von Lagrange: Wenn es $a \in \mathbb{Z}$ gibt mit $p \mid a^2 + 1$, dann gilt $4 \mid p - 1$.

Aufgabe 7 (Brasilianische Mathematik Olympiade 2017, Aufgabe 6)**.** Sei a eine positive ganze Zahl und $p \neq 3$ ein Primteiler von $a^3 - 3a + 1$. Beweise, dass $p \equiv \pm 1 \bmod 9$ ist.

Hinweis: Aufgabe 5 und $a = t + \frac{1}{t}$.

[1] Zwei Körper K und L sind *"strukturell ident"* oder *isomorph*, wenn es eine Bijektion $f : K \to L$ gibt, sodass $f(1) = 1$, $f(a + b) = f(a) + f(b)$ und $f(a \cdot b) = f(a) \cdot f(b)$ für alle $a, b \in K$ gilt. Ein solches f heißt dann *(Körper-)Isomorphismus*. Beispiel/Aufgabe: Der einzige Körper-Isomorphismus $\mathbb{Q} \to \mathbb{Q}$ ist $x \mapsto x$. Andererseits ist $\mathbb{Q}[i] \to \mathbb{Q}[i]$, $i \mapsto -i$ ein nicht-trivialer Körper-Isomorphismus.

[2] Für Körper K und L bedeutet $K \subseteq L$, dass $(K, +)$ eine Untergruppe von $(L, +)$ ist und $(K \setminus \{0\}, \cdot)$ eine Untergruppe von $(L \setminus \{0\}, \cdot)$ ist. Anders gesagt: K ist eine Teilmenge von L, die Null- und Einselemente von K und L sind jeweils gleich, und Multiplikation, Addition, und das Nehmen von additiven bzw. multiplikativen Inversen von Elementen in K ergibt wiederum Elemente in K. Das bekannteste Beispiel ist $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

[3] siehe vorige Fußnote.