Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 12

Aufgabe 1 (3 Punkte)
Sei K ein Körper. Zeige, dass es in $K[X]$ unendlich viele Assoziiertenklassen irreduzibler Polynome gibt.

Lösung Aufgabe 1
Vorbemerkung: Wegen $K[X]^\times = K^\times$ besitzt die Assoziiertenklasse eines Polynoms ungleich 0 einen eindeutigen normierten Vertreter. Wir können also auch mit normierten irreduziblen Polynomen arbeiten, wenn man die Klassenbildung umgehen will. Wir nutzen dann, dass jedes normierte Polynom Produkt normierter irreduzibler Polynome ist...

Für den Beweis benutzen wir, dass jedes nichtkonstante Polynom Produkt von irreduziblen Polynomen ist. (Wir haben sogar Eindeutigkeit (bis auf Reihenfolge und die Multiplikation mit Einheiten) wie im ganzzahligen Fall, aber das benötigen wir hier gar nicht.)

Annahme: Gebe es nur endlich viele Klassen irreduzibler Polynome, etwa mit Vertretern $f_1, ..., f_n$. Betrachten wir $f = f_1 \cdot ... \cdot f_n + 1$, so zerfällt f in irreduzible Polynome, also gibt es mindestens ein i mit $f_i | f$, denn die f_i waren ja alle irreduziblen Polynome (bis auf Multiplikation mit Einheiten....). Aber dann teilt f_i auch die Differenz $1 = f - f_1 \cdot ... \cdot f_n$, ein Widerspruch.

Nachbemerkung: Wer das lieber konstruktiv mag, konstruiert zu jeder endlichen Menge von irreduziblen Polynomen ein weiteres, indem man diese aufmultipliziert und 1 addiert. „Jeder Primteiler“ (einen solchen gibt es) gibt dann ein neues irreduzibles Polynom.

Aufgabe 2 (4 Punkte + 1 Zusatzpunkt)
Wir schreiben das Jahr 1973. Zwischen den benachbarten Staaten Gaußland und Euklidistan herrschen Spannungen, die jederzeit in einen Krieg münden können. Jedes der Länder ist darauf bedacht, möglichst viele Informationen aus dem anderen Land zu beschaffen, Spionage und das Anwenden von Verschlüsselungsverfahren werden bereits in der Schule gelehrt.
Dem gaußischen Geheimdienst KGV liegt eine geheime Botschaft aus Euklidistan vor. Leider können sie die Nachricht nicht lesen, wenn es ihnen nicht gelingt, den geheimen Schlüssel, die Mersenne-Zahl $M := M_{131} = 2^{131} - 1$, in Primfaktoren zu zerlegen.
Leider sind die Computer im Jahre 1973 noch lange nicht weit genug entwickelt, um diese Zahl auszurechnen und einen Brute-Force-Ansatz zu versuchen, die Spionage-Abteilung funktioniert dafür ausgezeichnet. Soeben erreicht die KGV-Zentrale folgender Hinweis ihres Mannes Gegétè Primanov: „habe neue Informationen über M – Primteiler kleiner als 787“
Dies wird nicht reichen, um die Zahl komplett zu faktorisieren, ist aber ein guter Anfang. Den gaußischen Agenten gelingt es, eine Vermutung für einen Primteiler p aufzustellen. Mit geeigneter Reduktion, die sie mit Papier und Stift oder ihren veralteten Taschenrechnern (die immerhin bereits einfache Subtraktionen und Multiplikationen durchführen können) ausführen können, gelingt es ihnen, tatsächlich nachzuweisen, dass p ein Faktor von M ist.

Aus sicherer Ferne wollen wir gerne nachvollziehen, was hier passiert ist. Mache das gleiche, was auch die Agenten gemacht haben! Stelle eine Vermutung auf, was p sein könnte, und beweise, dass p tatsächlich ein Primteiler von M ist.

Einen Zusatzpunkt erhältst du, wenn du den Krieg zwischen Gaußland und Euklidistan verhinderst und für Weltfrieden sorgst.[1]

[1] Man könnte vermuten, der Übungsleiter habe einen Clown gefrühstückt. Das wird wohl so sein.

Lösung Aufgabe 2
Für einen Primteiler p von n gilt $p|2^{131}-1$, also ist $2^{131} \equiv 1$ modulo p. Die multiplikative Ordnung von 2 in $\mathbb{Z}/p\mathbb{Z}$ ist also ein Teiler von 131. Da 131 prim und die Ordnung mindestens 2 ist (sonst wäre ja $2 = 1$, was nur im Nullring gilt), ist die Ordnung 131.
Mit dem Satz von Lagrange gilt aber weiterhin, dass ord(2) die Gruppenordnung $\#(\mathbb{Z}/p\mathbb{Z}^\times) = p-1$ teilt.
p ist also eine Primzahl < 878, so dass $p-1$ ein Vielfaches von 131 ist. Letztere Bedingung gibt $p \in \{1, 132, 263, 394, 525, 656\}$, aber nur 263 ist prim. Unsere Vermutung ist also $p = 263$ als Primteiler von M.

Wir berechnen $2^{131} = 2 \cdot 2^2 \cdot 2^{128}$ modulo 263. Dafür berechnen wir $2^{\text{Zweierpotenz}}$ durch iteriertes Quadrieren. Dazu müssen wir nur Multiplikationen kleiner 263^2 und Subtraktionen durchführen, was unser Taschenrechner kann (und was jeder Schüler mit Papier und Stift können sollte!).

2
$2^2 \equiv 4$
$2^4 \equiv 16$
$2^8 = 256 \equiv -7$
$2^{16} \equiv (-7)^2 \equiv 49$
$2^{32} \equiv 49^2 \equiv 2401 \equiv 34$
$2^{64} \equiv 34^2 \equiv 1156 \equiv 104$
$2^{128} \equiv 104^2 \equiv 10816 \equiv 33$

Also ist $2^{131} \equiv 2 \cdot 4 \cdot 33 \equiv 264 \equiv 1$ modulo 263, womit die Behauptung gezeigt wäre.

Aufgabe 3 (4 Punkte) (*Dies ist wieder einmal eine alte Klausuraufgabe – zumindest fast.*)
Es sei $a \in \mathbb{Z}$ beliebig.

a) Zeige, dass es unendlich viele Primzahlen p gibt, sodass die Restklasse von a in $\mathbb{F}_p$ eine dritte Potenz ist.
Hinweis: Betrachte natürliche Zahlen der Form $x^3 - a$.

b) Finde für $a = 5$ zwei verschiedene Primzahlen > 25, die die Bedingung aus a) erfüllen.

Lösung Aufgabe 3

a) Ohne Einschränkung ist $a \neq 0$, sonst erfüllt jede Primzahl die Bedingung, denn $0^3 = 0$.
Zu $N \in \mathbb{N}$ betrachten wir $x = N! \cdot |a|$. Dann ist $x^3 - a = (N!^3|a|^3) \pm |a| = (N!^3|a|^2 \pm 1) \cdot |a|$, je nach Vorzeichen von a.
Für jeden Primteiler p von $N!^3|a|^2 \pm 1$ ist $x^3 - a \equiv 0$ modulo p, also $a \equiv x^3$ eine dritte Potenz.
Hätte $N!^3|a|^2 \pm 1$ einen Teiler $p \leq N$, so wäre (mit dem Standardargument, das wir in Aufgabe 1 noch einmal wiederholt haben) p auch ein Teiler von 1 WIDERSPRUCH.
Also hat $N!^3|a|^2 \pm 1$ nur und damit mindestens einen Primteiler größer N und da N beliebig groß gewählt werden kann, gibt es beliebig große Primzahlen, die die Bedingung erfüllen.

b) Die Theorie schlägt vor, $N = 25$ zu setzen, also Primteiler von $25!^3 \cdot 5^2 - 1$ zu berechnen. In der Praxis probieren wir verschiedene x durch. Die Chance, Erfolg zu haben, ist gut, schließlich reicht es ja, einen Primteiler > 25 zu finden, nicht alle Primteiler müssen > 25 sein.
Für $x = 6$ ist $x^3 - a = 216 - 5 = 211$ bereits prim, für $x = 9$ ist $x^3 - a = 729 - 5 = 724 = 2 \cdot 2 \cdot 181$.
Passende Primzahlen sind also 181 und 211.

Nachtrag: Eine alternative Lösung zu a), mit der Aufgabenteil b) mehr Spaß macht, findet man unter `http://www.math.kit.edu/iag3/lehre/einfalgzahl2011s/media/loesungeazf12.pdf`.

In der Vorlesung waren arithmetische Funktionen ein Thema. Zu diesen findet man auf dieser Seite gar keine Aufgabe. Der schlaue Student schließt messerscharf, dass es eine Rückseite geben muss. Tatsächlich, dreh das Blatt doch einmal um.[2]

[2] Ja, hat er...

Aufgabe 4 (5 Punkte)
Sei $\mathcal{A}$ der Ring der arithmetischen Funktionen. Die eulersche φ-Funktion φ, die konstante Funktion $\eta \equiv 1$ und die kanonische Einbettung $\mathrm{Id}_{\mathbb{N}}$ sind Elemente aus $\mathcal{A}$. Zeige:

a) Die Menge aller multiplikativen arithmetischen Funktionen ist eine Untergruppe von $\mathcal{A}^\times$.

b) Es ist $\mathrm{Id}_{\mathbb{N}} = \eta * \varphi$.

(*Hinweis:* Es ist in a) relativ einfach zu zeigen, dass ein Untermonoid vorliegt. Um zu zeigen, dass die Inverse β einer arithmetischen multiplikativen Funktion (die Inverse existiert, nicht wahr?) selbst multiplikativ ist, könnte folgender Ansatz helfen: Es reicht zu zeigen (wieso?), dass $\beta(p^e \cdot m) = \beta(p^e) \cdot \beta(m)$ für alle $p \in \mathbb{P}$, $e \in \mathbb{N}_0$ und für alle zu p teilerfremden $m \in \mathbb{N}$ gilt. Diese Aussage kann etwa mit doppelter Induktion nach e und m bewiesen werden.
In b) genügt es, die Monoid-Eigenschaft aus a) zu kennen. Wieso reicht es, die Aussage für Primpotenzen zu beweisen?)

Lösung Aufgabe 4

a) In der Vorlesung haben wir gesehen, dass $\psi \in \mathcal{A}^\times$, wenn $\psi(1) \neq 0$. Bei multiplikativen arihtmetischen ist $\psi(1) = 1$, also existiert ψ^{-1}. Dies zeigt, dass eine Teilmenge von $\mathcal{A}^\times$ vorliegt.

nicht leer:
Es gibt multiplikative arithmetische Funktionen, wir haben doch schon Beispiele dafür gesehen: Die eulersche φ-Funktion, die konstante Funktion $\eta = (111...)$, das Einselement $(1000...)$ (Kronecker-Delta $\delta_{1,*}$) sind multiplikativ.

Abgeschlossenheit unter $*$:
Seien ξ, ψ multiplikativ, insbesondere also $\xi(1) = \psi(1) = 1$. Dann ist $(\xi * \psi)(1) = \xi(1)\psi(1) = 1$ und es reicht zu zeigen, dass $(\xi * \psi)(m \cdot n) \overset{(!)}{=} (\xi * \psi)(m) \cdot (\xi * \psi)(n)$ für teilerfremde m, n ist.
Dazu benutzen wir folgende **Aussage**: Sind m, n teilerfremde natürliche Zahlen, so finden wir die Teiler von $m \cdot n$ eineindeutig als Produkte $d \cdot e$ mit $d|m, e|n$, was man etwa direkt an der Zerlegung von m, n in Primzahlpotenzen mit paarweise verschiedenen Primzahlen sieht.
Damit gilt für multiplikative ψ, ξ und m, n teilerfremd:
$(\xi * \psi)(m \cdot n) = \sum\limits_{f|mn} \xi(f)\psi(\frac{mn}{f}) = \sum\limits_{d|m, e|n} \xi(de)\psi(\frac{mn}{de}) \overset{!}{=} \sum\limits_{d|m} \sum\limits_{e|n} \xi(d)\xi(e)\psi(\frac{m}{d})\psi(\frac{n}{e}) =$
$= \left(\sum\limits_{d|m} \xi(d)\psi(\frac{m}{d}) \right) \left(\sum\limits_{e|n} \xi(e)\psi(\frac{n}{e}) \right) = (\xi * \psi)(m) \cdot (\xi * \psi)(n).$
An der Stelle ! benutzen wir dabei, dass Teiler teilerfremder Zahlen auch teilerfremd sind, wir also die Multiplikativität von ξ, ψ anwenden können.

Abgeschlossenheit unter Inversion:
Sei nun ψ multiplikativ und $\xi := \psi^{-1}$ ihre Inverse. Wir müssen zeigen, dass ξ multiplikativ ist.
Es ist $\xi(1) = \xi(1)\psi(1) = (\xi * \psi)(1) = 1$ (denn $\xi * \psi$ ist das Einselement $(1000...)$).
Es verbleibt zu zeigen, dass $\xi(mn) \overset{(!)}{=} \xi(m)\xi(n)$ für teilerfremde m, n ist.

Behauptung: Es reicht, zu zeigen, dass wir Primpotenzen abspalten können, also

$$\xi(p^e \cdot m) \overset{(!)}{=} \xi(p^e)\xi(m) \text{ für } p \nmid m, m \in \mathbb{N}, e \in \mathbb{N}_0.$$

Beweis der Behauptung: Unter dieser Voraussetzung können wir dann beliebige teilerfremde Produkte zerlegen. Beliebige n zerlegen wir dafür in Primpotenzen $n = p_1^{e_1} \cdot ... \cdot p_r^{e_r}$ (mit p_i paarweise verschiedene Primzahlen, die nicht in der Primzerlegung von m vorkommen, e_r in $\mathbb{N}$, $r \in \mathbb{N}_0$), die wir mit der Voraussetzung einzeln abspalten können. Anschließend können wir sie dann einzeln wieder anfügen. Formal liest sich das etwa so:
$\xi(m \cdot n) = \xi(m \cdot \prod\limits_{i=1}^{r} p_i^{e_i}) = \xi(m \cdot \prod\limits_{i=2}^{r} p_i^{e_i}) \cdot \xi(p_1^{e_1}) = \xi(m \cdot \prod\limits_{i=3}^{r} p_i^{e_i}) \cdot \xi(p_2^{e_2}) \cdot \xi(p_1^{e_1}) = ... = \xi(m) \cdot \prod\limits_{i=1}^{r} \xi(p_i^{e_i}) =$
....
Aber dies gilt doch für alle m und für $m = 1$ (mit $\xi(m) = 1$) lesen wir gerade $\xi(n) = \prod\limits_{i=1}^{r} \xi(p_i^{e_i})$, womit der letzte Term also
$... = \xi(m)\xi(n)$ ist. (Wer den Trick mit $m = 1$ nicht mag, macht halt genau das gleiche wie vorher

und zieht die Potenzen Stück für Stück wieder zusammen.)

Die Bedingung $\xi(p^e \cdot m) = \xi(p^e)\xi(m)$ zeigen wir per Induktion nach $m \cdot e$. Sie ist offensichtlich richtig für $m \cdot e = 0$ (dann ist $e = 0$, also $p^e = 1$) und $m \cdot e = 1$ (dann ist $m = 1$), denn den Faktor 1 können wir wegen $\xi(1) = 1$ abspalten.
Sei die Aussage richtig für alle e', m' mit $e'm' < em (\geq 2)$. Für die nachfolgenden Rechnungen benutzen wir die Induktionsvoraussetzung (markiert mit $(*)$), dass $(\psi * \xi)(n) = 0$ für $n > 1$ ist und dass die Teiler von mp^e nach obiger Aussage genau die Zahlen dp^k mit $d|m$, $0 \leq k \leq m$ sind.

(Damit man beim Lesen nicht den roten Faden verliert, sollte man sich klar machen, was hier geschieht. Auf die meisten $\xi(x...)$ können wir die Induktionsvoraussetzung anwenden. Dazu zerlegen wir die Summen und betrachten diejenigen Werte, für die das nicht geht, einzeln. So zum Beispiel spalten wir den Summanden für den Teiler $d = 1$ von m als erstes ab. Die Reste können wir geeignet verrechnen.)

$$0 \overset{p^e m > 1}{=} (\psi * \xi)(p^e m) = \sum_{d|m} \sum_{k=0}^{e} \psi(dp^k)\xi(\tfrac{m}{d}p^{e-k}) = \sum_{d|m, d\neq 1} \sum_{k=0}^{e} \psi(dp^k)\xi(\tfrac{m}{d}p^{e-k}) + \sum_{k=0}^{e} \psi(p^k)\xi(mp^{e-k})$$
$$\overset{(*)}{=} \sum_{d|m, d\neq 1} \sum_{k=0}^{e} \psi(d)\psi(p^k)\xi(\tfrac{m}{d})\xi(p^{e-k}) + \sum_{k=0}^{e} \psi(p^k)\xi(mp^{e-k}) = ...$$

(**Nebenrechnung 1:** Es ist

$$\sum_{d|m, d\neq 1} \sum_{k=0}^{e} \psi(d)\psi(p^k)\xi(\tfrac{m}{d}))\xi(p^{e-k}) = \left(\sum_{d|m, d\neq 1} \psi(d)\xi(\tfrac{m}{d})\right) \cdot \left(\sum_{k=0}^{e} \psi(p^k)\xi(p^{e-k})\right)$$
$$= \left(\sum_{d|m, d\neq 1} \psi(d)\xi(\tfrac{m}{d})\right) \cdot (\psi * \xi)(p^e) \overset{p^e \geq 1}{=} \left(\sum_{d|m, d\neq 1} \psi(d)\xi(\tfrac{m}{d}\right) \cdot 0 = 0.$$

Damit vereinfacht sich der Term oben stark:)

$$0 = ... = \sum_{k=0}^{e} \psi(p^k)\xi(mp^{e-k}) = \sum_{k=0} \psi(p^k)\xi(mp^{e-k}) + \sum_{k=1}^{e} \psi(p^k)\xi(mp^{e-k})$$
$$\overset{(*)}{=} \xi(mp^e) + \sum_{k=1}^{e} \psi(p^k)\xi(m)\xi(p^{e-k}) = ...$$

(**Nebenrechnung 2:** Dabei ist

$$\sum_{k=1}^{e} \psi(p^k)\xi(m)\xi(p^{e-k}) = \xi(m) \cdot \left(\sum_{k=1}^{e} \psi(p^k)\xi(p^{e-k})\right) = \xi(m) \cdot \left(\sum_{k=1}^{e} \psi(p^k)\xi(p^{e-k}) + \psi(1)\xi(p^e) - \psi(1)\xi(p^e)\right)$$
$$= \xi(m) \cdot \left(\sum_{k=0}^{e} \psi(p^k)\xi(p^{e-k}) - \xi(p^e)\right) = \xi(m) \cdot ((\xi * \psi)(p^e) - \xi(p^e)) \overset{p^e \geq 1}{=} -\xi(m)\xi(p^e)$$

und damit vereinfachen wir zu)

$0 = ... = \xi(mp^e) - \xi(m)\xi(p^e)$ und genau das war zu zeigen. Uff!

b) Die beteiligten Funktionen sind (offensichtlich) multiplikativ, also wegen a) auch das Produkt $\eta * \varphi$. Für eine Primpotenz p^r gilt:
$(\eta * \varphi)(p^r) = (\varphi * \eta)(p^r) = \sum_{i=0}^{r} \varphi(p^i) \cdot \eta(p^{r-i}) = \sum_{i=1}^{r} \varphi(p^i) + \varphi(1) = \sum_{i=1}^{r} (p^i - p^{i-1}) + 1 = p^r - 1 + 1 = p^r.$
Die Funktionen $\eta * \varphi$ und $\mathrm{Id}_{\mathbb{N}}$ stimmen also auf Primpotenzen überein. Da jedes n als Produkt paarweise teilerfremder Primpotenzen dargestellt werden kann, folgt die Gleichheit der Funktionen wegen der Multiplikativität auf ganz $\mathbb{N}$.
(**Nachtrag:** Die bekannte zugehörige Formel besagt gerade $n = \sum_{d|n} \varphi(d)$, jede Zahl ist die Summe der eulerschen φ-Funktionswerte ihrer Teiler.)