Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 1

1 Allgemeine Hinweise

Maximale Punktzahl die man in diesem Arbeitsblatt erwerben kann sind 10 Punkte. Wenn man Aufgaben wählt, die z.B., $2+3+3+3=11$ Punkte wert sind, werden trotzdem maximal 10 Punkte angerechnet.

Lösungen werden nächste Woche (Donnerstag) sowohl elektronisch (als PDF) bereitgestellt, wie auch in der Vorlesungszeit (12:15 – 13:45) live/online von mir via Zoom erklärt.

Bei Unverständnissen, Fragen oder wenn Ihr Fehler findet, bitte an
ilia.pirashvili@math.uni-augsburg.de
wenden.

Abgabefirst ist bis einschließlich Mittwoch (29/04). Viel Glück und viel Erfolg.

2 Aufgaben

Aufgabe 1 (1 Punkt). Sei R ein Ring und $\mathbb{Z}$ das Ring der ganzen Zahlen. Zeige, dass es genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt.

Lösung. Zu zeigen, dass einen Ringhomomorphismus gibt, definiere $\kappa : \mathbb{Z} \to R$ wir folgt:

$$\kappa(n) := \begin{cases} \underbrace{1+1+\cdots+1}_{n \text{ mal}} & \text{wenn } n \geq 0 \\ \underbrace{(-1)+(-1)+\cdots+(-1)}_{-n \text{ mal}} & \text{wenn } n < 0. \end{cases}$$

Die Tatsache, dass es ein Ringhomomorphismus ist, liegt auf der Hand.

Zu sehen, dass es genau einen gibt, sei auch $\lambda : \mathbb{Z} \to R$ ein Ringhomomorphismus und sei

$$G : \{n \in \mathbb{Z} \mid \kappa(n) = \lambda(n)\}.$$

Diese Menge ist nicht leer, da $0, 1 \in G$ bei Definition von Ringhomomorphismus. Des weiteren, da Ringhomomorphismen Addition respektieren, ist G unter Addition abgeschlossen. Da nun $0, \in G$ und G unter Addition abgeschlossen ist, ist $G \subseteq \mathbb{Z}$ eine Untergruppe. Da $1 \in G$ folgt nun, dass $G = \mathbb{Z}$. □

Aufgabe 2 (5 Punkte (insgesamt)). Sei X eine Menge und $\mathfrak{P}(X)$ die Menge der Teilmengen von X.

- (2 Teilpunkte) Zeige, dass

$$A + B := A \cup B \setminus A \cap B \quad \text{und} \quad AB := A \cap B$$

eine Ringstruktur auf $\mathfrak{P}(X)$ definiert.

– Überzeugt euch, dass für ein beliebiges Element A, $2A = 0$ in diesem Ring.

- (3 Teilpunkte) Ist es möglich, mithilfe von Teilmengen einer Menge X, einen Ring der Charakteristik 3 zu definieren?

Lösung. Obwohl es möglich ist diese Aufgabe "direkt" zu lösen, ist es am geschicktesten, für beide den folgenden "Trick" zu erkennen:

Für jede Menge X gilt

$$\mathfrak{P}(X) = \mathsf{Abb}(X, \{0,1\}).$$

Diese Bijektion wird gegeben, indem wir eine Teilmenge $A \subseteq X$ zu der Abbildung $\chi_A : X \to \{0,1\}$, gegeben durch $\chi_A(A) = 1, \chi_A(X \setminus A) = 0$, senden.

Wir beobachten nun, dass die Menge der Abbildungen von X nach R, wobei R ein Ring ist, wieder ein Ring in einer natürlichen Art und Weise ist. Die Verknüpfungen werden komponentenweise definiert:

$$(f+g)(x) \coloneqq f(x) + g(x)$$

und

$$(fg)(x) \coloneqq f(x)g(x).$$

Dies stimmt für die meisten algebraischen Strukturen (abelsche Gruppen, Monoide, Module etc.,). Auch viele Eigenschaften werden übernommen, wie zum Beispiel Kommutativität, Charakter, Idempotenze u.s.w.. Jedoch nicht alle! Z.B., wenn $R = K$ ein Körper ist, sind die Abbildungen darin nur ein Ring, im allgemeinen. Hier sollte man allerdings aufpassen, dass wir alle Abbildungen nehmen. Z.B., die Menge aller Ringhomomorphismen zwischen zwei Ringen ist im allgemeinen *nicht* wieder ein Ring.

Wir definieren die (einzige) Ringstruktur (Körperstruktur) auf $\{0,1\}$, nämlich $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

1. Den ersten Teil beweisen wir indem wir zeigen, dass die natürliche Ringstruktur auf

   $$\mathsf{Abb}(X, \mathbb{F}_2),$$

   mit der Struktur in der Aufgabe übereinstimmt. Sein $A, B \subseteq X$. Wir haben $\chi_A(x) = 1 \Leftrightarrow x \in A$ und $\chi_A(x) = 0 \Leftrightarrow x \in X \setminus A$. Gleichwie für B.

   ▷ Addition: Wir wollen zeigen, dass $(\chi_A + \chi_B)(x) = 1$ genau dann wenn

   $$x \in A + B = A \cup B \setminus A \cap B.$$

   Wenn wir "genau dann" zeigen, haben wir auch gezeigt, dass $(\chi_A + \chi_B)(x) = 0$ genau dann wenn $x \in X \setminus (A + B)$.
   In $\mathbb{F}_2$ ist $1 = 1 + 0$ oder $0 + 1$. Daher, ist

   $$(\chi_A + \chi_B)(x) = (\chi_A)(x) + \chi_B(x) = 1$$

   genau dann wenn

   $$\{\chi_A(x) = 1 \text{ und } \chi_B(x) = 0\} \text{ oder } \{\chi_A(x) = 0 \text{ und } \chi_B(x) = 1\}.$$

   Übersetzt heißt es

   $$\begin{aligned} x &\in (A \cap (X \setminus B)) \cup (B \cap (X \setminus A)) \\ &= (A \cup B) \cap [A \cup (X \setminus A)] \cap [(X \setminus B) \cup B] \cap [(X \setminus B) \cup (X \setminus A)] \\ &= (A \cup B) \cap X \cap X \cap [X \setminus (A \cap B)] \\ &= (A \cup B) \cap [X \setminus (A \cap B)] \\ &= (A \cup B) \setminus (A \cap B), \end{aligned}$$

   was genau die obige Definition der Addition ist.

▷ Multiplikation: Dies ist einfacher. $(\chi_A\chi_B)(x) = (\chi_A)(\chi_B)(x) = 1$, genau dann wenn $\chi_A(x) = 1$ und $\chi_B(x) = 1$. Das heißt, genau dann wenn

$$x \in A \cap B,$$

was wir auch wollen.

2. Nach unserer Diskussion ist es klar, dass wir für Charakteristik 3 einen Ring mit $\mathsf{Char}(3)$ nehmen müssen. Das einfachste solche ist $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$. Daher betrachten wir

$$\mathfrak{P}_3 \coloneqq \mathsf{Abb}(X, \mathbb{F}_3).$$

Wir können uns Objekte von $\mathfrak{P}_3$ als Paare von Teilmengen von X vorstellen, deren Schnitte leer sind. Also

$$\mathfrak{P}_3 \simeq \{A, B \subseteq X \mid A \cap B = \varnothing\} \text{ oder } \{(A, B) \subseteq X \times X \mid A \cap B = \varnothing\}.$$

Diese Äquivalenz wir gegeben, indem wir $A \subseteq X$ auf $1 \in \mathbb{F}_3$, $B \subseteq X$ auf $2 \in \mathbb{F}_3$ und $X \setminus (A \cup B)$ auf $0 \in \mathbb{F}_3$ senden. Also

$$(A, B) \mapsto \chi_{A,B} : X \to \mathbb{F}_3, \quad \text{gegeben durch } \chi_{A,B}(A) = 1, \chi_{A,B}(B) = 2 \text{ und } \chi_{A,B}(X \setminus (A \cup B)) = 0.$$

Um jetzt $(A, B) + (c, D)$ zu definieren, müssen wir verstehen, was $(\chi_{A,B} + \chi_{C,D})(x)$ ist und es Mengentheoretisch interpretieren. Nachdem man alles entziffert hat, erhält man

$$(A, B) + (C, D) = (E, F)$$

und

$$(A, B)(C, D) = (G, H),$$

wobei

$$E = (A \cap ((X \setminus C) \setminus D)) \cup (((X \setminus A) \setminus B) \cap C) \cup (B \cap D),$$
$$F = (A \cap C) \cup (B \cap ((X \setminus C) \setminus D)) \cup (((X \setminus A) \setminus B) \cap D),$$
$$G = (A \cap C) \cup (B \cap D)$$

und

$$H = (A \cap D) \cup (B \cap C)$$

□

Aufgabe 3 (2 Punkt (insgesamt)). Sei $f : R \to S$ ein Ringhomomorphismus und $I \subseteq S$ ein Ideal.

- (1 Teilpunkt) Beweis, dass das Uhrbild $f^{-1}(I) \subseteq R$ von I ein Ideal von R ist.
- (1 Teilpunkt) Sein $I = \mathfrak{p}$ zusätzlich prim. Zeige, dass $f^{-1}(\mathfrak{p})$ auch prim ist.

Lösung. Teil 1.

- $0 \in I, f(0) = 0 \Rightarrow 0 \in f^{-1}(I)$
- Sein $a, b \in f^{-1}(I)$. Dann ist
$$f(a + b) = f(a) + f(b) \in I,$$
also $a + b \inf^{-1}(I)$.
- Sei $a \in f^{-1}(I)$ und $r \in R$. Daher ist
$$f(ra) = f(r)f(a) \in I,$$
da $f(r) \in S$ und $I \subseteq S$ ein Ideal ist. Also ist $ra \in f^{-1}(I)$.

Für den zweiten Teil sei $ab \in f^{-1}(\mathfrak{p})$. Daher

$$f(ab) = f(a)f(b) \in \mathfrak{p} \Rightarrow f(a) \in \mathfrak{p} \text{ oder } f(b) \in \mathfrak{p}.$$

Im ersten Fall ist $a \in f^{-1}(\mathfrak{p})$, im zweiten ist $b \in f^{-1}(\mathfrak{p})$. □

Aufgabe 4 (1 Punkt). Sei $f : R \to S$ ein surjektiver Ringhomomorphismus und $I \subseteq R$ ein Ideal. Beweise, dass $f(I) \subseteq S$ ein Ideal von S ist.

Lösung. Sein $a, b \in f(I)$ und $s \in S$. i.e., $\exists a', b' \in I$, so dass $f(a') = a$, $f(b') = b$ und da f surjektiv ist, $\exists r \in R$, so dass $f(r) = s$.

- $0 \in I, f(0) = 0 \Rightarrow 0 \in f(I)$.
- $f(a' + b') = f(a') + f(b') = a + b$. Da $a', b' \in I \Rightarrow a' + b' \in I \Rightarrow a + b \in f(I)$.
- $f(ra') = f(r)f(a') = sa$. Da $ra' \in I \Rightarrow sa \in f(I)$.

□

Aufgabe 5 (1 Punkt). Sei $u \in R$ eine Einheit von R und $I \subseteq R$ ein Ideal. Zeige, dass

$$I = (u)I.$$

Lösung. Wie schon in Korollar 1.1.13 gezeigt ist $(u) = (1)$. Wir haben $(1)(I) = (xy \mid x \in (1), y \in I)$. Da $1 \in (1)$ folgt direkt, dass $(1y \mid y \in I) \subseteq (1)(I)$. Auf der anderen Seite ist $IJ \subseteq I$ für alle Ideale I, J, in jedem beliebigen Ring, wegen dem dritten Axiom der Ideale. □

Aufgabe 6 (2 Punkte). Beweise direkt, dass $\mathbb{Z}$ ein Hauptidealring ist.

Lösung. Dies wird genau wie Proposition 1.1.26 beweisen. - Dieser Beweis gilt für alle euklidische Ringe. Wie nehmen einen Ideal $1 \neq I \neq (0)$ und $0 \neq n \in I$ mit dem kleinstmöglichem Betrag. Wir wollen beweisen, dass jedes $m \in I$ ein vielfaches von n ist. In anderen Worten, dass $I = (n)$.

Der euklidische Algorithmus besagt, dass es ganze Zahlen $a, b \in \mathbb{Z}$ gibt, so dass

$$m = an + b,$$

mit $|b| < |n|$. Es folgt

$$b = m + an.$$

Da $m \in I, n \in I$, folgt $b \in I$. Da bei Annahme n den kleinstmöglichen, streng positiven Betrag hatte, muss $b = 0$ sein. Also, $m = an$, was unseren Beweis abschließt. □

Aufgabe 7 (2 Punkte). Sei $p \in \mathbb{Z}$ eine Primzahl. Zeige, dass das Ideal

$$(p, x) \subseteq \mathbb{Z}[X]$$

kein Hauptideal ist.

Lösung. Man brauch hier eigentlich nicht, dass p eine Primzahl ist, nur dass $p \geq 2$.

Angenommen, $(p, x) = (f)$, für irgendein $f(x) \in \mathbb{Z}[X]$. Das heißt, es gibt $g(x), h(x) \in \mathbb{Z}[X]$, mit $p = g(x)f(x)$ und $x = h(x)f(x)$.

Aus $p = g(x)f(x)$ folgt, dass $\mathsf{grad}(f) = 0$ und daher, $f(x) = a$, mit $a\mathbb{Z}$. Aus $x = h(x)f(x)$ und $\mathsf{grad}(f) = 0$ folgt, dass $\mathsf{grad}(h) = 1$, also $h(x) = h_0 + h_1 x$. Wir haben $x = (h_0 + h_1 x)a = h_0 a + h_1 ax$, woraus folgt, dass $h_0 = 0$ und $h_1 a = 1$. Da dies in $\mathbb{Z}$ ist, haben wir $a = f(x) = \pm 1$.

Die einzige Möglichkeit ist also, dass $(p, x) = (1)$. Dies ist jedoch nicht möglich, da $1 \notin (p, x)$. Um dies zu sehen, sein

$$u(x) = u_0 + \cdots + u_l x^l$$

und

$$v(x) = v_0 + \cdots + v_k x^k,$$

so dass

$$1 = u(x)p + v(x)x.$$

Das freie Term der rechten Seite ist $u_0 p$ was nicht ± 1 sein kann, wenn $p \geq 2$ ist. □

Aufgabe 8 (2 Punkte). Bestimme, ob das Ideal $(X^2+9X+18, X^3+9X^2-54) \subseteq \mathbb{Z}[X]$ ein Hauptideal ist.

Lösung. Wir fangen an, indem wir den größten gemeinsamen Teiler dieser beiden Polynome bestimmen. In diesem Fall ist es recht einfach, da wir für quadratische Polynome ein einfaches Formel haben. Es ist nicht schwer zu sehen, dass

$$x^2 + 9x + 18 = (x+3)(x+6)$$

und

$$x^3 + 9x^2 - 54 = (x+3)(x^2+6x-18).$$

Die Wurzeln von $(x^2+6x-18)$ sind $-3 \pm \sqrt{3}$, welche natürlich nicht mehr in $\mathbb{Z}$ liegen. Daher ist die Frage

$$(x^2+9x+18, x^3+9x^2-54) = (x+3)?$$

Dafür müsste es $f(x), g(x) \in \mathbb{Z}[X]$ geben, mit

$$x+3 = (x^2+9x+18)f(x) + (x^3+9x^2-54)g(x).$$

Sein f_0 und g_0 die freien Terme von $f(x)$ und $g(x)$. Dann müsste

$$3 = 18f_0 + 54g_0$$

gelten. Da $18|54$, ist dies in $\mathbb{Z}$ nicht möglich. Daher ist $(x^2+9x+18, x^3+9x^2-54)$ kein Hauptideal in $\mathbb{Z}[X]$. □

Aufgabe 9 (1 Punkt). Beweise, dass ein Ring R genau dann ein Integritätsbereich ist, wenn $\{0\} = (0) \subseteq R$ ein Primideal ist.

Lösung. Da $(0) = \{0\}$ in jedem Ring, ist $ab \in (0) \Leftrightarrow ab = 0$. Aus R Integritätsbereich folgt $a = 0$ oder $b = 0$, daher $a \in (0)$ oder $b \in (0)$, was prim impliziert. Auf der anderen Seite, wenn (0) prim ist, folgt aus $ab = 0$ $a = 0$ oder $b = 0$, also $R =$ Integritätsbereich. □

Aufgabe 10 (2 Punkte). Sei $I \subseteq R$ ein Ideal eines Ringes R. Zeige, dass R/I wirklich ein Ring ist. Das heißt, dass Assoziativität, Distributivität, Wohldefiniertheit etc. erfüllt sind.

Lösung. Es reicht aus zu zeigen, dass die Äquivalenzrelation auf R, die durch R/I definiert wird, eine Kongruenzrelation ist. Das heißt, dass es die Verknüpfungen von R respektiert. Wenn wir dies gezeigt haben, wir aus allgemeinen Fakten aus Algebra folgen, dass R/I auch ein Ring ist.

Sei $a \sim b$ und $c \sim d$. Das heißt, es gibt $x, y \in I$, so dass $a = b + x$ und $c = d + y$. Dann gilt

$$a + c = (b + x) + (d + y) = (b + d) + (x + y)$$

und

$$ac = (b + x)(d + y) = bd + by + dx + xy.$$

Da $x + y \in$ und $by + dx + xy \in I$, haben wir gezeigt, dass $a + c \sim b + c$ und $ac \sim bd$. Daher ist es eine Kongruenzrelation.

Zur nähren Erklärung unseres obigen Arguments: Sei

$$f : X \to Y$$

eine surjektive Abbildung und $\star : X \times X \to X$ eine Verknüpfung die irgendwelche Gleichungen erfühlt. Wenn f folgenden Eigenschaft erfüllt: für all $a, b, c, d \in X$ mit

$$f(a) = f(c) \quad \text{und} \quad f(b) = f(d)$$

folgt

$$a \star b = c \star d,$$

dann definiert

$$x \overline{\star} y := f(a \star b),$$

wobei $x, y \in Y$ und $a, b \in X$ mit $f(a) = x, f(b) = y$, eine Verknüpfung auf Y, die alle algebraischen Gleichungen (z.B., Kommutativität, Assoziativität, Torsion etc.,) erfüllt, die $\star$ in X erfüllte.

Dies gilt auch mit mehreren Verknüpfungen und Gleichungen wie Distributivität werden auch erfüllt. □

Aufgabe 11 (1 Punkt). Sei $f : R \to S$ ein Ringhomomorphismus. Zeige, dass $\mathsf{Ker}(f) \subseteq R$ ein Ideal von R ist.

Lösung. Dies folgt aus Aufgabe 4, Teil 1 und der Tatsache, dass $(0) = \{0\}$ in jedem Ring ein Ideal ist. □

Aufgabe 12 (2 Punkt). Sein A, B abelsche Gruppen und $f : A \to B$ ein Gruppenhomomorphismus. Der sogenannte *erste Isomorphiesatz* besagt, dass die Abbildung

$$A/\mathsf{Ker}(f) \to \mathsf{Bild}(f),$$

gegeben durch $[a] \mapsto f(a)$, ein (wohldefiniertes) Gruppenisomorphismus ist. Sein, des weiteren, A und B mit Ringstrukturen versehen und sei $f : A \to B$ zusätzlich ein Ringhomomorphismus. Unter Annahme des ersten Isomorphiesatzes für Gruppen, zeige, dass das kanonische Isomorphismsus

$$R/\mathsf{Ker}(f) \simeq \mathsf{Bild}(f)$$

ein Ringhomomorphismus ist.

In anderen Worten, beweise den ersten Isomorphiesatz für Ringe, wenn man es für Gruppen schon kennt.

Lösung. Unter Annahme, dass $[a] \mapsto f(a)$ ein Gruppenisomorphismus ist, bleibt zu zeige, dass dies auch ein Monoidhomomorphismus ist, damit wir sehen, dass es eine Isomorphie von Ringen ist.

Dazu sehen wir, dass $[1] \mapsto 1$, denn $f(1) = 1$ und $[a + b] \mapsto f(a + b) = f(a) + f(b)$. □

Aufgabe 13 (2 Punkt). Sei R ein Ring und $I \subseteq J \subseteq R$ Ideale von R. Zeige, dass

$$R/J = (R/I)/(J/I).$$

Lösung. Dies ist ein Korollar der obigen Aufgabe. Da $I \subseteq J$ gegeben ist, gibt es ein surjektives Ringhomomorphismus

$$R/I \xrightarrow{\varphi} R/J.$$

Der Kernel dieser Abbildung ist $\mathsf{Ker}(\varphi) = J/I$. Der erste Isomorphiesatz (vorige Aufgabe) besagt nun, dass

$$(R/I)/(J/I) \simeq \mathsf{Im}(\varphi) = R/J$$

gilt. □

Aufgabe 14 (1 Punkt). Zeige, dass ein Ringhomomorphismus $f : R \to S$ genau dann injektiv ist, wenn der Kern $\mathsf{Ker}(f) = (0) = \{0\}$ trivial ist.

Lösung. Sei f injektiv und $a \in \mathsf{Ker}(f)$. Daher, $f(a) = 0 = f(0)$. Injektivität besagt nun $a = 0$. Auf der anderen Seite sie der Kern trivial und gelte $f(a) = f(b)$. Es folgt $f(a-b) = f(a) - f(b) = 0$, also $a - b \in \mathsf{Ker}(f)$, woraus $a - b = 0$ und daher $a = b$ folgt. □

Aufgabe 15 (1 Punkt). Sei K ein Körper und $R \neq \{0\}$ nicht das Nullring. Beweise, dass ein Ringhomomorphismus $f : K \to R$ immer injektiv ist.

Lösung. Wir wissen, dass das Kern $\mathsf{Ker}(f) \subseteq K$ ein Ideal ist. Da K ein Körper ist, muss $\mathsf{Ker}(f) = (0)$ oder $\mathsf{Ker}(f) = (1) = K$ sein. Im ersten Fall ist f injektiv. Im zweiten Fall muss ganz K auf das Null von R abbilden. Daher, 1_K muss auf 0_R gehen. Dies jedoch passiert genau dann, wenn $1_R = 0_R$, da die Einheit auf die Einheit abbilden muss. □