Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
20. Mai 2020

Algebra
Lösung Übungsblatt 5

Aufgabe 1 (2+2+4 Punkte).

a) **Vor.:** Sei D_n die Symmetriegruppe eines regelmäßigen n-Ecks (auch die Diedergruppe mit $2n$ Elementen).

Beh.: Die aufsteigende Kette von Untergruppen

$$\{id\} \subset \{\text{Drehungen eines regelmäßigen } n\text{-Ecks}\} \subset D_n$$

ist für alle n eine Subnormalteilerreihe.
Ist n prim, so ist es bereits eine Kompositionsreihe.

Bew.: Wir wissen von Blatt 3 Aufgabe 4 $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$. Bei dieser Isomorphie haben wir gesehen, dass $\{$Drehungen des regelmäßigen n-Ecks$\} \cong \mathbb{Z}_n$.
$\Rightarrow D_n/\{\text{Drehungen}\} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2/\mathbb{Z}_n \times \{0\} \cong \mathbb{Z}_2$ ist abelsch.
Außerdem $|D_n/\{\text{Drehungen}\}| = 2 \Rightarrow \{\text{Drehungen}\}$ sind Normalteiler in D_n.
Da $\{\text{Drehungen}\} \cong \mathbb{Z}_n$ ist $\{\text{Drehungen}\}/\{id\} \cong \mathbb{Z}_n$ abelsch.
$\{id\}$ ist trivialerweise normal in $\{$Drehungen$\}$.
$\Rightarrow \forall n$ ist die Kette eine Subnormalteilerkette.

Es gilt immer: $D_n/\{\text{Drehungen}\} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2/\mathbb{Z}_n \times \{0\} \cong \mathbb{Z}_2$ ist zyklisch von Primzahlordnung.
Ist n prim, so ist zusätzlich $\{\text{Drehungen}\}/\{id\} \cong \mathbb{Z}_n$ zyklisch von Primzahlordnung.
$\Rightarrow$ ist n prim, so ist die angegebene Kette eine Kompositionsreihe. $\square$.

b) **Vor.:** Sei D_n die Diedergruppe mit $2n$ Elementen.

Beh.: D_n ist auflösbar.

Bew.: Nach Definition 1.6.4 ist eine Gruppe auflösbar, wenn es eine Subnormalteilerkette aus Untergruppen gibt. Nach Teil a) ist

$$\{id\} \subset \{\text{Drehungen eines regelmäßigen } n\text{-Ecks}\} \subset D_n$$

für jedes n eine Subnormalteilerkette.
$\Rightarrow D_n$ ist auflösbar. $\square$

c) **Gesucht:** Eine Kompositionsreihe von D_{30} (mit Begründung).

Lösung: Wir wissen aus Aufgabe 4 Blatt 3: $D_{30} \cong \mathbb{Z}_{30} \rtimes \mathbb{Z}_2$. Da $\mathbb{Z}_{30}$ nicht zyklisch von Primzahlordnung ist, ist die Kette

$$\{id\} \subset K := \{\text{Drehungen eines regelmäßigen 30-Ecks}\} \cong \mathbb{Z}_{30} \subset D_{30}$$

aus Teil a) keine Kompositionsreihe. Da $D_{30}/\{\text{Drehungen}\} \cong \mathbb{Z}_2$ zyklisch ist von Primzahlordnung, müssen wir die Kette nur nach unten hin verfeinern.
Wir suchen also einen Normalteiler der Untergruppe der Drehungen (die isomorph ist zur $\mathbb{Z}_{30}$), sodass der Quotient zyklisch ist von Primzahlordnung.
Da $30 = 2 \cdot 3 \cdot 5$, ist eine mögliche Wahl die Untergruppe $U := \{id,$ Drehungen der Ordnung 15$\} \cong \mathbb{Z}_{15}$.
Damit gilt: $K/U \cong \mathbb{Z}_{30}/\mathbb{Z}_{15} \cong \mathbb{Z}_2$.
Also ist die Untergruppe U der Drehungen von Ordnung 15 ein Normalteiler in der Untergruppe der Drehungen und der Quotient ist zyklisch von Primzahlordnung.
Da $\mathbb{Z}_{15}$ noch nicht von Primzahlordnung ist, müssen wir weiter verfeiern.
Wir wählen $V = \{id, \text{Drehungen der Ordnung } 5\} \cong \mathbb{Z}_5$ als Untergruppe von U und erhalten:

Algebra
Lösung Übungsblatt 5

$U/V = \{id,$ Drehungen der Ordnung $15\}/\{id,$ Drehungen der Ordnung $5\} \cong \mathbb{Z}_3$. Zudem ist $V = V/\{id\} \cong \mathbb{Z}_5$ zyklisch von Primzahlordnung, also ist die Kette

$$\begin{aligned}\{id\} &\subset \mathbb{Z}_5 \cong \{\text{Drehungen eines regelmäßigen 30-Ecks von Ordnung } 5\} = V \\ &\subset \mathbb{Z}_{15} \cong \{\text{Drehungen eines regelmäßigen 30-Ecks von Ordnung } 15\} = U \\ &\subset \{\text{Drehungen eines regelmäßigen 30-Ecks}\} = K \cong \mathbb{Z}_{30} \subset D_{30}\end{aligned}$$

eine Kompositionsreihe von D_{30}. □

Aufgabe 2 (3+3 Punkte).

a) **Beh.:** Jeder endliche nullteilerfreie Ring ist ein Körper.

Bew.: Sei R ein endlicher nullteilerfreier Ring (nach Konvention der Vorlesung hat R eine Eins). Sei $r \in R \setminus \{0\}$ beliebig. Wir betrachten die Abbildung $\phi_r : R \to R,\ x \mapsto rx$. Da R nullteilerfrei ist gilt: falls $rx = ry \Rightarrow r(x-y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$
$\Rightarrow \phi$ ist injektiv.
Da R endlich ist, ist ϕ_r automatisch auch surjektiv, also bijektiv.
$\Rightarrow 1 \in \mathrm{im}(\phi_r) \Rightarrow \exists x \in R : \phi_r(x) = rx = 1.$
Da $r \in R \setminus \{0\}$ beliebig war, gilt insgesamt:

$$\forall r \in R \setminus \{0\} \exists x \in R : rx = 1$$

$\Rightarrow R$ ist ein Körper, da jedes Element ungleich 0 invertierbar ist. □

b) **Beh.:** Jeder endliche Ring lässt sich als Vereinigung der Menge seiner Nullteiler und der Menge seiner Einheiten schreiben.

Bew.: Sei R ein endlicher Ring. Sei $R_N := \{$Nullteiler von $R\}$, $R^\times := \{$Einheiten von $R\}$. Zu zeigen $R = R_N \cup R^\times$.
„$\supset$“ klar.
„$\subset$“ Sei $r \in R \setminus R_N$. Zu zeigen: $r \in R^\times$. Wir betrachten wie in a) die Abbildung $\phi_r : R \to R, x \mapsto rx$. Da r kein Nullteiler ist, ist ϕ_r mit dem gleichen Argument wie in a) injektiv, und da R endlich ist, auch bijektiv.
$\Rightarrow \exists x \in R : \phi_r(x) = rx = 1$
$\Rightarrow r \in R^\times$.
$\Rightarrow R = R_N \cup R^\times$. □

Aufgabe 3 (6 Punkte).
Vor.: Sei R ein Hauptidealring und $0 \neq a \in R \setminus R^\times$. Weiter sei I das von a erzeugte Hauptideal.

Beh.: Die folgenden Aussagen sind äquivalent:

1) I ist ein maximales Ideal in R.
2) I ist ein Primideal in R.
3) a ist irreduzibel.

Bew.: "a) $\Rightarrow$ b): Sei I ein maximales Ideal in R. Daraus folgt R/I ist ein Körper (algebraische Strukturen) $\Rightarrow R/I$ ist nullteilerfrei $\Rightarrow I$ ist Primideal in R .

"b) $\Rightarrow$ c): Sei $I = \langle a \rangle$ ein Primideal in R. z.Z. a ist irreduzibel, d.h. für $x, y \in R$ mit $a = xy$ folgt $x \in R^\times$ oder $y \in R^\times$.
Da I prim ist, gilt für $x, y \in R$ mit $xy \in I$, dass $x \in I$ oder $y \in I$. Daraus folgt: Sind $x, y \in R$ bel. mit $xy = a \in \langle a \rangle$,

Algebra
Lösung Übungsblatt 5

---

dann muss $a|x$ oder $a|y$.
Ohne Einschränkung gilt $a|x$. $\Rightarrow \exists z \in R : x = az$
$\Rightarrow\ a = xy = azy \Rightarrow a(1 - zy) = 0$
Da R als Hauptidealring nullteilerfrei ist, muss also $1 = zy$, d.h. y eine Einheit sein.
$\Rightarrow a$ ist irreduzibel.

„c) $\Rightarrow$ a)“: Sei $J = \langle b \rangle \subsetneq R$ ein Ideal in R mit $\langle a \rangle = I \subset J = \langle b \rangle \subsetneq R$. Dann $\exists c \in R$ mit $a = bc$.
Da a irreduzibel, gilt $b \in R^\times$ oder $c \in R^\times$. Da $J \neq R$ ist $b \notin R^\times$.
$\Rightarrow c \in R^\times$
$\Rightarrow I = J$
$\Rightarrow I$ ist maximal. $\square$

Aufgabe 4 (3+4 Punkte).
Vor.: Sei $R = \mathbb{Z}[i]$.

a) **Beh.:** Der Chinesische Restsatz liefert einen Isomorphismus $\phi : R/(7 - 11i) \to R/(3 + 5i) \times R/(1 + 2i)$.

   Bew.: Nach dem Chinesischen Restsatz gilt, falls $I_1 := \langle 3 + 5i \rangle$, $I_2 = \langle 1 + 2i \rangle$ coprim sind, ist die Abbildung $\psi : R \to R/I_1 \times R/I_2$ surjektiv mit Kern $\ker(\psi) = I_1 \cap I_2$.
   Nachdem Homorphiesatzt ist dann $\overline{\psi} : R/I_1 \cap I_2 \to R/I_1 \times R/I_2$ ein Isomorphismus.
   z.z.: I_1, I_2 coprim und $I_1 \cap I_2 = (7 - 11i)$.
   I_1 und I_2 sind coprim $\Leftrightarrow I_1 + I_2 = R$
   „$\subset$“klar.
   „$\supset$ “Da $R = \mathbb{Z}[i]$ euklidisch, $\exists r, s \in R : r(3+5i) + s(1+2i) = \mathrm{ggT}(3+5i, 1+2i)$. Da $3+5i-3(1+2i) = -i$ eine Einheit in R ist, ist $I_1 + I_2 = R$.
   Nach dem Chinesischen Restsatz gilt außerdem, falls I_1, I_2 coprim, gilt $I_1 I_2 = I_1 \cap I_2$.
   Damit gilt: $I_1 \cap I_2 = I_1 I_2 = \langle (3 + 5i)(1 + 2i) \rangle = (7 - 11i)$. $\square$

b) **Gesucht:** Das Urbild $x \in R/(7 - 11i)$ von $(\overline{1 + i}, \overline{2 + i}) \in R/(3 + 5i) \times R/(1 + 2i)$ unter ϕ.

   Lösung: Suche $x \in R/(7 - 11i)$ mit $x = 1 + i \mod 3 + 5i$ und $x = 2 + i \mod 1 + 2i$.
   Die Existenz von x ist gesichert, durch Aufgabenteil a).
   Berechne mit dem euklidischen Algorithmus: $\mathrm{ggT}(3 + 5i, 1 + 2i) = 3(1 + 2i) - (3 + 5i) = i$.
   $\Rightarrow 1 = i(3 + 5i) - 3i(1 + 2i)$.
   $\Rightarrow x = (1 + i)(-3i)(1 + 2i) + (2 + i)i(3 + 5i) = -4 + 4i \in R/(7 - 11i)$

Zusatzaufgabe 5 (3+3 Zusatzpunkte).

a) **Vor.:** Sei $R = \mathbb{Z}[X]$.

   Gesucht: Ein Ideal $I = \langle f_1, ..., f_n \rangle \subset R, n \geq 2$, das kein Hauptideal ist und berechnen Sie für die Erzeuger f_i des Ideals ggT und kgV (falls existent).

   Lösung: Setze $I = \langle 3, X \rangle$. Nach Definition ist I ein Ideal in R. Aber I ist kein Hauptideal, da sonst ein $r \in \mathbb{Z}[X]$ existieren müsste, sodass $I = \langle r \rangle$, also $3 = ar$ und $X = br$ für passende $a, b \in \mathbb{Z}[X]$. Da $R/\langle 3 \rangle = \mathbb{Z}_3[X]$ ein Integritätsring ist und $R/\langle X \rangle = \mathbb{Z}$ ebenfalls ein Integritätsring ist, sind 3 und X nach Aufgabe 3 irreduzible Elemente. Da $I \neq R$ ist r keine Einheit, also folgt $a, b \in \mathbb{Z}[X]^\times = \{\pm 1\}$ und somit ein Widerspruch (da $r = 3 \neq \pm X = r$).
   Da $\mathbb{Z}[X]$ ein faktorieller Ring ist, sind Existenz von ggT und kgV gesichert.
   Es ist $\mathrm{ggT}(3, X) = \pm 1$, nach obigem Argument, da für $d \in \mathrm{ggT}(3, X)$ gelten muss: $3 = ad$ und $X = bd$ für passende $a, b \in R$. Zudem teilt ± 1 jedes Element in R und erfüllt damit insbesondere die Eigenschaften des ggT von 3 und X.
   Da in einem faktoriellen Ring gilt: $ab = \mathrm{kgV}(a, b)\mathrm{ggT}(a, b)$ (algebraische Strukturen), folgt: $\mathrm{kgV}(3, X) = 3X$.

Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
20. Mai 2020

Algebra
Lösung Übungsblatt 5

---

b) **Vor.:** Sei $R = \mathbb{R}[X, Y]$.

Gesucht: Ein Ideal $I = \langle f_1, ..., f_n \rangle \subset R, n \geq 2$, das kein Hauptideal ist und berechnen Sie für die Erzeuger f_i des Ideals ggT und kgV (falls existent).

Lösung: Wähle $I = \langle X, Y \rangle$. Nach Definition ist I ein Ideal in R, aber es ist kein Hauptideal, denn: Wäre I ein Hauptideal so gäbe es ein $r \in \mathbb{R}[X, Y]$ sodass $\langle r \rangle = \langle X, Y \rangle$, d.h. es gibt passende $a, b \in R$, sodass $X = ar$ und $Y = br$.
Analog zu Teil a) können wir argumentieren, dass X und Y irreduzibel sind ($R/\langle X \rangle \cong \mathbb{R}[Y]$, $R/\langle Y \rangle \cong \mathbb{R}[X]$ sind Integritätsringe, also sind $\langle X \rangle, \langle Y \rangle$ Primideale).
Damit folgt, da $I \neq R$, dass $a, b \in \mathbb{R}[X, Y]^\times = \mathbb{R}^\times$. Widerspruch, da $X \neq aY \; \forall a \in \mathbb{R} \setminus \{0\}$.
Mit dieser Argumentation folgt (wie bei a)) bereits, dass ggT$(X, Y) \in \mathbb{R}^\times$. Da nun für den ggT von X und Y nun noch zusätzlich gelten muss, dass er von allen gemeinsamen Teilern von X und Y (und die gemeinsamen Teiler sind die Einheiten von R) geteilt wird
$\Rightarrow$ bis auf Einheiten ist ggT$(X, Y) = 1$.
Wie in Teil a) können wir argumentieren, dass kgV$(X, Y) = XY$, da $\mathbb{R}[X, Y]$ faktoriell ist und hier gilt: $XY =$ kgV(X, Y)ggT(X, Y).