WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

4. November 2020

6. Übungsblatt Algebra

Aufgabe 1: *(10 Punkte)*

Wir betrachten $R = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$.

a) Zeigen Sie, daß R bezüglich der Addition und Multiplikation komplexer Zahlen ein kommutativer Ring ist!

Lösung: R ist eine Teilmenge des Körpers der komplexen Zahlen, die sowohl die Null als auch die Eins enthält. Außerdem haben für $a, b, c, d \in \mathbb{Z}$ auch

$$(a + ib) + (c + id) = (a + c) + i(b + d) \quad \text{und} \quad (a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

ganzzahlige Real- und Imaginärteile, so daß Summen und Produkte von Elementen aus R wieder in R liegen. Die Kommutativ-, Assoziativ- und Distributivgesetze gelten in $\mathbb{C}$, also erst recht in der Teilmenge R. Somit ist R ein kommutativer Ring.

b) Ist R ein Integritätsbereich?

Lösung: Natürlich, denn als Teilmenge eines Körpers kann R keine Nullteiler enthalten.

c) Zeigen Sie, daß jede Einheit in R den Betrag eins hat, und bestimmen Sie die Menge aller Einheiten!

Lösung: Für $z = a + ib \in R$ ist

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}\,.$$

Für eine Einheit $z \in R^\times$ muß $a^2 + b^2$ also sowohl a als auch b teilen. Für $|a| > 1$ ist $a^2 + b^2 > |a|$, kann also kein Teiler von a sein. Genauso kann $a^2 + b^2$ im Falle $|b| > 1$ kein Teiler von b sein. Somit sind $|a|$ und $|b|$ beide höchstens eins, und mindestens einer der beiden Beträge muß eins sein, da Null keine Einheit ist. Also ist $a^2 + b^2$ ein Teiler von ± 1 und als Summe zweier Quadrate nicht negativ, d.h. $|z|^2 = a^2 + b^2 = 1$. Damit ist auch $|z| = 1$.

Für eine ganzzahlige Lösung der Gleichung $a^2 + b^2 = 1$ muß a oder b verschwinden, und die jeweils andere Zahl ist ± 1. Die Einheitengruppe besteht also aus den vier Elementen ± 1 und $\pm i$.

d) Ist $R^\times$ eine zyklische Gruppe?

Lösung: Ja, denn ihre sämtlichen Elemente sind $i, i^2 = -1, i^3 = -i$ und $i^4 = 1$.

e) Welche der folgenden Teilmengen von R ist ein Ideal? Beweisen Sie entweder, daß es sich um ein Ideal handelt, oder zeigen Sie mit einem Gegenbeispiel, daß eine der Forderungen an ein Ideal verletzt ist!

$I_1 = \{a + bi \in R \mid a \equiv 0 \bmod 2\}$, $I_2 = \{a + bi \in R \mid b \equiv 0 \bmod 2\}$,
$I_3 = \{a + bi \in R \mid a \equiv b \equiv 0 \bmod 2\}$, $I_4 = \{a + bi \in R \mid a^2 + b^2 \equiv 0 \bmod 2\}$,
$I_5 = \{a + bi \in R \mid b = 0\}$, $I_6 = \{a + bi \in R \mid a + b = 0\}$

Lösung: I_1 ist kein Ideal, denn zwar liegt $2+i$ in I_1, nicht aber $(1+i)(2+i) = 1+3i$.
Auch I_2 ist kein Ideal, denn zwar liegt $1+2i$ in I_1, nicht aber $(1+i)(1+2i) = -1+3i$.
I_3 besteht genau aus den Elementen $z = a+ib$ von R, für die es Elemente $w = c+id \in R$ gibt, für die $z = 2w$ ist. Somit ist I_3 das von der Zwei erzeugte Hauptideal von R.
a^2+b^2 ist genau dann gerade, wenn entweder a^2 und b^2 beide gerade oder beide ungerade sind. Das ist natürlich äquivalent dazu, daß a und b entweder beide gerade oder beide ungerade sind, d.h.

$$I_4 = \{a+ib \in R \mid a \equiv b \bmod 2\}.$$

Sind $a+ib$ und $c+id$ zwei Elemente von I_4, so ist $a \equiv b \bmod 2$ und $c \equiv d \bmod 2$, also auch $a+c \equiv b+d \bmod 2$, so daß auch die Summe $(a+c)+i(b+d)$ in I_4 liegt. Für $a+ib \in I_4$ und $c+id \in R$ ist $(c+id)(a+ib) = (ac-bd)+i(ad+bc)$. Falls a und b beide gerade sind, sind auch $ac-bd$ und $ad+bc$ beide gerade. Sind beide ungerade, so sind $ac-bd$ und $ad+bc$ beide gerade, falls $c \equiv d \bmod 2$, und beide ungerade sonst. Damit liegt das Produkt in I_4. Schließlich ist I_4 nicht leer, da die Null offensichtlich in I_4 liegt. I_4 erfüllt also alle Forderungen an ein Ideal und ist somit eines.
$I_5 = \mathbb{Z}$ ist offensichtlich kein Ideal: $1 \in I_5$, aber $i \cdot 1 = i \notin I_5$.
Auch I_6 ist kein Ideal, denn $1-i \in I_6$, aber $(1+i)(1-i) = 2 \notin I_6$.

f) Welche der Ideale unter diesen Mengen sind Hauptideale?

Lösung: I_3 ist, wie wir gesehen haben, das von der Zwei erzeugte Hauptideal.
Das zweite Ideal unter den sechs Teilmengen ist I_4. Falls es ein Hauptideal ist, muß das erzeugende Element eines von minimalem Betrag sein, den jedes Vielfache (außer der Null) hat mindestens den gleichen Betrag. Die Elemente ungleich Null von kleinstem Betrag sind $\pm 1 \pm i$, und sie sind alle konjugiert zueinander: $i(1+i) = -1+i$, $-(1+i) = -1-i$ und $(-i)(1+i) = 1-i$. Wenn I_4 Hauptideal ist, wird es also von jedem dieser vier Elemente erzeugt. Betrachten wir $1+i$. Für $a+ib \in I_4$ ist

$$\frac{a+ib}{1+i} = \frac{(a+ib)(1-i)}{(1+i)(1-i)} = \frac{(a+b)+i(b-a)}{2}.$$

Da $a \equiv b \bmod 2$, sind sowohl $a+b$ als auch $b-a$ durch zwei teilbar, so daß der Quotient in R liegt. Also ist jedes Element von I_4 ein Vielfaches von $1+i$, und I_4 ist das von $1+i$ erzeugte Hauptideal.

Aufgabe 2: *(4 Punkte)*
Nun sei $R = \mathbb{Z}/10$.

a) Bestimmen Sie alle Nullstellen in R der Polynome $f = 2X+5$ und $g = 5X+2$ aus R[X]!

Lösung: Für jede ganze Zahl x ist $f(x) = 2x+5$ ungerade, kann also nicht kongruent Null modulo zehn sein. Für gerade $x \in \mathbb{Z}$ ist $g(x) \equiv 2 \bmod 10$, für ungerade x ist $g(x)$ kongruent zu 7 modulo 10. Somit hat weder f noch g eine Nullstelle in $\mathbb{Z}/10$.

b) Berechnen Sie das Produkt $fg \in R[X]$ und dessen Nullstellen!

Lösung: In $\mathbb{Z}[X]$ ist $(2X+5)(5X+2) = 10X^2+9X+10$; in R[X] ist daher $fg = 9X = -X$. Dieses Polynom hat die Null als einzige Nullstelle.

c) Bestimmen Sie auch für $p = 3X+5$ und $q = 7X+2$ aus R[X] alle Nullstellen von p, q und pq in R!

Lösung: $3 \cdot 7 = 21 \equiv 1 \bmod 10$; daher sind 3 und 7 zueinander invers in $\mathbb{Z}/10$. Die Gleichung $3x+5 = 0$ ist also in $\mathbb{Z}/10$ äquivalent zu $7 \cdot 3x + 7 \cdot 5 = x+5 = 0$, so daß $x = 5$ die einzige Lösung ist. Entsprechend ist $7x+2 = 0$ äquivalent zu $3 \cdot 7x + 3 \cdot 2 = x+6 = 0$; hier ist $x = 4$ die einige Lösung.

In $\mathbb{Z}[X]$ ist $(3X+5)(7X+2) = 21X^2+41X+10$, d.h. $pq = X^2+X$ in $R[X]$. Natürlich hat pq die Nullstellen 5 und 4 von p und q als Nullstellen, außerdem offensichtlich auch 0 und -1. Mehr als vier Nullstellen kann es nicht geben, denn sowohl modulo zwei als auch modulo fünf kann eine quadratische Gleichung nicht mehr als zwei Lösungen haben, und die Lösungen modulo zehn lassen sich nach dem chinesischen Restesatz durch Kombination der Lösungen aus den Körpern $\mathbb{F}_2$ und $\mathbb{F}_5$ bestimmen.

Aufgabe 3: *(6 Punkte)*

a) $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ sei ein primitives Polynom und p sei eine Primzahl, die alle a_i außer a_n teilt und deren Quadrat kein Teiler von a_0 ist. (Ein solches Polynom heißt p-EISENSTEINsch.) Zeigen Sie, daß f irreduzibel ist!
Hinweis: Sie können ähnlich vorgehen wie beim Beweis, daß das Produkt zweier primitiver Polynome wieder primitiv ist.

Lösung: Wäre f reduzibel, gäbe es Polynome g, h positiven Grades mit $f = gh$. Wegen der Primitivität von f könnten auch g und h als primitive Polynome gewählt werden. Sei

$$g = b_dX^d + \cdots + b_1X + b_0 \quad \text{und} \quad h = c_eX^e + \cdots + c_1X + c_0\,.$$

Dann ist $a_0 = b_0c_0$ durch p teilbar, nicht aber durch p^2. Somit ist entweder b_0 oder c_0 durch p teilbar, nicht aber beide. Da es auf die Reihenfolge der Faktoren nicht ankommt, können wir annehmen, daß b_0 durch p teilbar ist, c_0 aber nicht.
Da $a_n = b_dc_e$ nicht durch p teilbar ist, kann auch weder b_d noch c_e durch p teilbar sein. Es gibt daher einen Index $1 \le \mu < d$ derart, daß b_i für alle $i < \mu$ durch p teilbar ist, nicht aber b_μ. Dann sind in der Summe

$$a_\mu = \sum_{i=0}^{\mu} b_ic_{\mu-i}$$

alle Summanden mit $i < \mu$ durch p teilbar, da b_i ein Vielfaches von p ist. Für $i = 0$ ist aber weder b_μ noch c_0 ein Vielfaches von p, so daß die gesamte Summe nicht durch p teilbar ist. Dies widerspricht der Voraussetzung, daß alle a_i mit $i < n$ durch p teilbar sind. Damit kann f nicht reduzibel sein, und die Behauptung ist bewiesen.

b) Zeigen Sie: Ein Polynom $f = f(X) \in R[X]$ über einem Integritätsbereich R ist genau dann irreduzibel, wenn das Polynom $f(X+1)$ irreduzibel ist.

Lösung: Ist $f(X+1) = gh$ mit $g, h \in \mathbb{Z}[X]$, so ist $f = f(X) = g(X-1)h(X-1)$; aus der Reduzibilität von $f(X+1)$ folgt also die von f, denn $g(X-1)$ und $h(X-1)$ haben natürlich die gleichen Grade wie g und h. Ist umgekehrt $f = gh$ reduzibel, so auch $f(X+1)$, denn $f(X+1) = g(X+1)h(X+1)$.

c) Schreiben Sie $f = \dfrac{X^p-1}{X-1}$ als Polynom, und folgern Sie aus *a)* und *b)*, daß dieses für prime p irreduzibel ist!

Lösung: Nach der Summenformel für endliche geometrische Reihen ist

$$f = \frac{X^p-1}{X-1} = \sum_{i=0}^{p} X^{p-1} \quad \text{und} \quad f(X+1) = \frac{(X+1)^p-1}{(X+1)-1} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}\,.$$

Der führende Koeffizient von $f(X+1)$ ist $\binom{p}{p} = 1$, alle anderen Koeffizienten $\binom{p}{i}$ sind durch p teilbar. Der konstante Koeffizient $\binom{p}{1} = p$ ist nicht durch p^2 teilbar. Damit ist $f(X+1)$ p-EISENSTEINsch, also irreduzibel. Nach *b)* ist dann auch f irreduzibel.