Universität Konstanz Dr. Andrew Dolphin
Fachbereich Mathematik und Statistik Prof. Dr. Markus Schweighofer
Wintersemester 2010/2011

Übungsblatt 8 zur Einführung in die Algebra: Solutions

Aufgabe 1.

(a) Zeige, dass $4X^3 - 15X^2 + 60X + 180 \in \mathbb{Q}[X]$ irreduzibel ist.

(b) Zeige, dass $X^3 + 3X^2 + 5X + 5 \in \mathbb{Q}[X]$ irreduzibel ist.

(c) Zeige, dass $X^4 + 2X^2 + 4 \in \mathbb{Q}[X]$ irreduzibel ist.

Solution

(a) This is irreducible in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ by Eisenstein's Criterion. It is a primitive polynomial in $\mathbb{Z}[X]$, and we apply the Criterion with the prime p taken to be 5: for 5 does not divide the leading coefficient but it divides all the others, and its square, 25, does not divide 180.

(b)Call the polynomial f. Eisenstein's Criterion does not apply since there is no suitable prime. Substituting $X - 1$ for X gives the polynomial $X^3 + 2X + 2$ to which Eisenstein does apply, with $p = 2$. We deduce that $f(X - 1)$ is irreducible in $\mathbb{Q}[X]$. Applying the automorphism of $\mathbb{Q}[X]$ sending X to$X + 1$ it follows that $f = f(X + 1 - 1)$ is irreducible in $\mathbb{Q}[X]$.

(c) For any rational number a/b, we have

$$(a/b)^4 + 2(a/b)^2 + 4 \geqslant 0 + 2 \cdot 0 + 4 = 4 > 0$$

so f has no rational roots, and hence no linear factors in $\mathbb{Q}[X]$. Since it is of degree 4, the lack of roots also implies that it has no cubic factors either, since if $p = qr$ for some q,$r \in \mathbb{Q}[X]$, and $\deg(q) = 3$, then $\deg(r) = \deg(p) - \deg(r) = 4 - 3 = 1$. But r cannot have degree 1, as f has no linear factors, and hence q has no factors of degree 3.

It remains to show that the polynomial has no quadratic factors. Assume to the contrary that p has quadratic factors g,$h \in \mathbb{Q}[X]$ such that $p = gh$. Without loss of generality we assume that g is primitive in $\mathbb{Z}[X]$. Then Gauss' Lemma implies that we also have $h \in \mathbb{Z}[X]$. So $q = aX^2 + bX + c$ and $r = dX^2 + eX + f$ where $a, b, c, d, e, f \in \mathbb{Z}$.

If we multiply q, r , we can collect like terms to obtain

$$p = qr = adX^4 + (ae + bd)X^3 + (af + be + cd)X^2 + (bf + ce)X + cf.$$

Two polynomials are equal if and only if their coefficients are equal, so

$$\begin{aligned} 1 &= ad \\ 0 &= ae + bd \\ 2 &= af + be + cd \\ 0 &= bf + ce \\ 4 &= cf. \end{aligned}$$

Since a, d are integers and $ad = 1$, we may assume that $a = d = 1$. The system now becomes

$$\begin{aligned} 0 &= e + b \\ 2 &= f + be + c \\ 0 &= bf + ce \\ 4 &= cf. \end{aligned}$$

Observe that $b = -e$, so we have

$$\begin{aligned} 2 &= f - b^2 + c && (1) \\ 0 &= bf - bc && (2) \\ 4 &= cf. && (3) \end{aligned}$$

From equation (2), we know that $b = 0$ or $f = c$. We consider two cases

Case 1: If $f = c$, equation (3) tells us that $c = \pm 2$. Substituting this into equation (1) we see that $b^2 = 2$ or $b^2 = -4$, neither of which has an integer solution. Since b must be an integer, $f \neq c$.

Case 2: If $b = 0$, equation (1) tells us that $f + c = 2$, or $f = 2 - c$. Substituting into equation (3), we have

$$\begin{aligned} 4 &= c(2-c) \\ 4 &= 2c - c^2 \\ c^2 - 2c + 4 &= 0. \end{aligned}$$

The quadratic formula shows that this has no integer solution for c . Since c must be an integer, $b \neq 0$.

Neither case gives a solution for the coefficients. Hence p cannot factor as the product of two quadratic polynomials. Thus p is irreducible in $\mathbb{Z}[X]$. By Gauss' Lemma, q is irreducible in $\mathbb{Q}[X]$.

Aufgabe 2. Sei $\sqrt{-3} := \sqrt{3}\mathbb{i} \in \mathbb{C}$, $R := \mathbb{Z}[\sqrt{-3}]$ und $K = \mathrm{qf}(R)$.

(a) Zeige

$$R = \{a + b\sqrt{-3} \mid a,b \in \mathbb{Z}\}$$

und

$$K = \{a + b\sqrt{-3} \mid a,b \in \mathbb{Q}\}.$$

(b) Untersuche die Irreduzibilität von $X^2 + X + 1$ in $R[X]$ und in $K[X]$.

(c) Zeige, dass R nicht faktoriell ist.

Solution

Let $f = X^2 + X + 1$.

(a) That $R = \{a + b\sqrt{-3} \mid a,b \in \mathbb{Z}\}$ is clear from the definition.

Take $a,b \in \mathbb{Z}$ such that $x := a + b\sqrt{-3} \neq 0$. To show that $K = \{a + b\sqrt{-3} \mid a,b \in \mathbb{Q}\}$, we must show that x is invertible in $\{a + b\sqrt{-3} \mid a,b \in \mathbb{Q}\}$. Take $y = \frac{a - b\sqrt{-3}}{a^2+3b^2}$. If this is well defined, then it is clearly the inverse of x and an element of $\{a + b\sqrt{-3} \mid a,b \in \mathbb{Q}\}$. It is well defined if $a^2 + 3b^2 \neq 0$, which is clearly the case if either a or b is non-zero, and if $a = b = 0$, then $x = 0$.

(b) Over K (the fraction field of R), f factors as

$$f = \left(X - \frac{-1 + \sqrt{-3}}{2}\right)\left(X - \frac{-1 - \sqrt{-3}}{2}\right).$$

We will now show that f is irreducible in R. Since f is of degree 2, it is irreducible if and only if it has a root. Assume a root exists, of the form $\alpha = a + b\sqrt{-3}$ with $a,b \in \mathbb{Z}$. Then

$$0 = f(\alpha) = (a + b\sqrt{-3})^2 + a + b\sqrt{-3} + 1 = (a^2 - 3b^2 + a + 1) + (2ab - b^2)\sqrt{-3} = 0$$

Hence $a^2 - 3b^2 + a + 1 = 0$ and $2ab - b^2 = 0$. From $2ab - b^2 = 0$ we get either $b = 0$ or $2a - b = 0$.

Case $b = 0$. In this case we get that $a^2 + a + 1 = 0$ from the first equation. But we already know that $X^2 + X + 1$ has no roots in $\mathbb{Z}$.

Case $2a = b$. In this case we get that $-11a^2 + a + 1 = 0$. We can easily check with the equation for roots of a quadratic polynomial that $-11X^2 + X + 1 = 0$ has no roots in $\mathbb{Z}$.

In both cases we get a contradiction, hence f is irreducible over $\mathbb{Z}[\sqrt{-3}]$.

(c) f is irreducible over R, but not over its field of fractions K. Since $\deg f \geqslant 1$ this would be a contradiction to Gauss' Lemma if R was a unique factorization domain (faktorieller Ring). Therefore R is not a unique factorization domain.

Aufgabe 3. Sei K ein Körper und $v : K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung auf K mit zugehörigem Bewertungsring $\mathcal{O}_v$ und maximalem Ideal $\mathfrak{m}_v$.

Sei $\pi \in K$ mit $v(\pi) = 1$.

(a) Zeige, dass $k \mapsto (\pi^k)$ eine Bijektion zwischen $\mathbb{N}_0$ und der Menge der Ideale $I \neq \{0\}$ von $\mathcal{O}_v$ definiert.

(b) Zeige, dass π bis auf Assoziiertheit das einzige irreduzible Element in $\mathcal{O}_v$ ist.

Solution

(a) We will show that all non-zero ideals of $\mathcal{O}_v$ are of the form (π^n) for some $0 \neq n \in \mathbb{N}_0$ and that $(\pi^n) \neq (\pi^m)$ for all $n,m \in \mathbb{N}_0$ with $n \neq m$. Then the bijection is clear.

Note first that for all elements $a \in K^\times$, $v(a) + v(a^{-1}) = v(a \cdot a^{-1}) = v(0)$ and hence

$$v(a) = -v(a^{-1}),$$

and moreover, it is easy to show that

$$v(a^n) = nv(a)$$

for $n \in \mathbb{Z}$.

Take $0 \neq a \in \mathcal{O}_v$. If $v(a) = 0$ then $a \in \mathcal{O}_v^\times$ and trivially we have that $a = u\pi^0$ for some $u \in \mathcal{O}_v^\times$. Assume now that $v(a) = n > 0$. We have that $v(\pi^n) = n$, and hence $v(a^{-1}\pi^n) = v(a^{-1}) + v(\pi^n) = 0$. Therefore $a^{-1}\pi^n = u$ for some $u \in \mathcal{O}_v^\times$. Hence $a = u\pi^n$.

Let I be an non-zero ideal of $\mathcal{O}_v$ and assume $a \in I$ such that $v(a) \leqslant v(b)$ for all $b \in I$. If $a = 0$ then $v(a) = \infty$ and hence $v(b) = \infty$ for all $b \in I$, and therefore $I = \{0\}$, a contradiction. Hence $a \neq 0$.

From the above we have that $a = u\pi^n$ for some $n \in \mathbb{N}_0$ and $u \in \mathcal{O}^\times$. We also have that for all $b \in I$,

$$v(ba^{-1}) = v(b) + v(a^{-1}) \geqslant 0,$$

and hence $ba^{-1} \in \mathcal{O}_v$, therefore $b = ac = \pi^n uc \in (\pi^n)$ for some $c \in \mathcal{O}_v$. Hence $I \subseteq (\pi^n)$, and clearly $I \supseteq (\pi^n)$ as $a \in I$.

We now show that $(\pi^n) \neq (\pi^m)$ for all $n,m \in \mathbb{N}_0$ with $n \neq m$. Assume that $(\pi^n) = (\pi^m)$. Then $\pi^m = \pi^n \cdot a$ and $\pi^m \cdot b = \pi^n$ for some $a,b \in \mathcal{O}_v$. Taking valuations we see that $m = v(\pi^m) = v(\pi^n) + v(a) = n + v(a)$. So $v(a) = m - n \geqslant 0$ as $a \in \mathcal{O}_v$, hence $m \geqslant n$. Similarly $v(b) = n - m \geqslant 0$, and hence $n \geqslant m$, and hence $n = m$.

(b) Assume that $\pi = ab$ for some $a,b \in \mathcal{O}_v$. Then

$$v(\pi) = 1 = v(a) + v(b).$$

But $a,b \in \mathcal{O}_v$, and hence $v(a),v(b) \geqslant 0$. So, if $v(a) + v(b) = 1$, we must have that $v(a) = 0$ or $v(b) = 0$, so either a or b is a unit. Hence π is irreducible.

That π is the only irreducible element up to associativity goes as follows. Suppose $p \in \mathcal{O}_v$ is irreducible. Then by the argument in (a), $p = u\pi^n$ for some $n \in \mathbb{N}_0$ and $u \in \mathcal{O}_v^\times$. Since $p \notin \mathcal{O}_v^\times$, we have $n \geqslant 1$. Further, since p is irreducible and $p = (u\pi)(\pi^{n-1})$, we have that $\pi^{n-1} \in \mathcal{O}_v^\times$, which implies that $n = 1$, hence $p = u\pi$, i.e. $p \cong \pi$.