Solutions of exercise sheet 9

The content of the marked exercises **(*)** should be known for the exam.

1. **(*)** Let K be a field.

1. Suppose that $P \in K[X]$ is a non-zero polynomial of degree d. Prove that P has at most d roots in K. [*Hint:* Exercise 2.3 from Exercise sheet 8].
2. Is the previous point also true if K is just supposed to be a division ring? [*Hint:* Exercise 1 from Exercise sheet 6].
3. Now suppose that K is an infinite field, and that $P \in K[X]$ is such that $P(\alpha) = 0$ for every $\alpha \in K$. Prove: $P = 0$ in $K[X]$.
4. Still supposing that K is an infinite field, show that if $P \in K[X_1, \ldots, X_n]$ is such that for every $(\alpha_1, \ldots, \alpha_n) \in K^n$ one has $P(\alpha_1, \ldots, \alpha_n) = 0$, then $P = 0$ in $K[X_1, \ldots, X_n]$.

Solution:

1. Let $V(P) \subseteq K$ be the set of roots of the polynomial $P \in K[X]$. For every finite collection of distinct roots $\alpha_1, \ldots, \alpha_k \in V(P)$, we have that $(X - \alpha_i)|P$. Since the polynomials $X - \alpha_i$ have degree 1, and K is a field, we have that the only possible decompositions of $X - \alpha_i$ are of the form $c \cdot q(X)$ for some polynomial $q(X)$ of degree 1 and constant $c \in K \setminus \{0\} = K^\times$. Hence the polynomials $X - \alpha_i$ are distinct irreducible elements in $K[X]$ which all divide P. We claim that then

$$\prod_{i=1}^{k}(X - \alpha_i)|P \quad (*),$$

and being K a field we have $k = \deg(\prod_{i=1}^{k}(X - \alpha_i)) \leq \deg P = d$. Hence all finite subsets of $V(P)$ have cardinality $\leq d$, implying that $|V(P)| \leq d$, that is, P has at most d roots.

We are only left to prove the claim $(*)$. This is true more in general for any UFD A (and $A = K[X]$ is a UFD): if $\gamma_1, \ldots, \gamma_k$ are distinct irreducible elements dividing $f \in A$, then their product divides f as well. To prove it, we work by induction on k, the case $k = 1$ being trivial. So we can suppose that $\gamma_1 \cdot \cdots \cdot \gamma_{n-1}|f$, and write $f = \gamma_1 \cdot \cdots \cdot \gamma_{n-1} \cdot g$ for some $g \in A$. Decomposing g into irreducible and using uniqueness of decomposition into irreducible, we have that $\gamma_n|g$, and this gives our claim.

Please turn over!

2. No, it is not true. For example, the polynomial $X^2+1 \in \mathbb{H}[X]$ vanishes on $\mathbb{i}$, $\mathbb{j}$ and $\mathbb{k}$ (see Exercise 1 from Exercise sheet 6).
3. By contradiction, assume that $P \neq 0$. Then by Point 1 we have that P has less than $\deg(P)$ roots. Since every $\alpha \in K$ is a root, we get $\infty = |K| \leq \deg(P) < \infty$, contradiction.
4. We prove this by induction on n, the case $n=1$ being proved in previous point. So we can prove the statement by supposing that it holds for $n-1$. For $d = \deg_{X_n}(P)$ and some $a_i \in K[X_1, \ldots, X_{n-1}]$, we can write

$$P(X_1, \ldots, X_n) = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-1}) X_n^d.$$

Then for every $(\alpha_1, \ldots, \alpha_{n-1}) \in K^{n-1}$ we define

$$q_{\alpha_1,\ldots,\alpha_{n-1}}(Y) = P(\alpha_1, \ldots, \alpha_{n-1}, Y) = \sum_{i=0}^{d} a_i(\alpha_1, \ldots, \alpha_{n-1}) Y^d \in K[Y],$$

and we observe that by construction $q_{\alpha_1,\ldots,\alpha_{n-1}} \in K[Y]$ vanishes on all elements in K, so that by the previous point we have $q_{\alpha_1,\ldots,\alpha_{n-1}}(Y) = 0$, meaning that for all $i = 0, \ldots, d$ and $(\alpha_1, \ldots, \alpha_{n-1})$ we have $a_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$, so that inductive hypothesis (applied on all the a_i's) gives $a_i = 0$, which implies $P = 0$.

2. Let $p \in \mathbb{Z}$ be a positive prime number.

1. Prove that there exists a unique ring map $\mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ sending $X \mapsto X$, and that it is surjective. For $f \in \mathbb{Z}[X]$, we denote by $\bar{f}$ its image via this map.
2. Let $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ be such that $p | a_i$ for $i \in \{0, \ldots, n-1\}$ and $p \nmid a_n$. Prove that $\bar{f}$ is a monomial in $\mathbb{Z}/p\mathbb{Z}[X]$, and deduce that if $f = gh$ in $\mathbb{Z}[X]$ with g and h non-constant polynomials, then $p^2 | a_0$ [Hint: $\mathbb{Z}/p\mathbb{Z}$ is a field, hence $\mathbb{Z}/p\mathbb{Z}[X]$ is a principal ideal domain].
3. Conclude: if $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ is such that $p^2 \nmid a_0$, $p \nmid a_n$, $p | a_i$ for $i \in \{0, \ldots, n-1\}$ and the coefficients $a_0, \ldots, a_n$ are coprime, then f is an irreducible polynomial in $\mathbb{Z}[X]$. (This is known as Eisenstein's Criterion).
4. For $n \in \mathbb{Z}_{>1}$, we denote by W_n the set of primitive n-th roots of unity, and define the n-th cyclotomic polynomial

$$\Phi_n(t) := \prod_{\zeta \in W_n} (X - \zeta) \in \mathbb{C}[X].$$

For $n = p$ a prime number, show that $\Phi_p(X) \in \mathbb{Z}[X]$, and that it is irreducible over $\mathbb{Z}[X]$. [*Hint:* First, find $(X-1)\Phi_p(X)$. Then take also in account the polynomial $Q(X) = \phi_p(X+1)$]

Solution:

See next page!

1. Let $B = \mathbb{Z}/p\mathbb{Z}[X]$. Applying Exercise 1 from Exercise sheet 8 (in particular, parts 4 and 8) with $A = \mathbb{Z}$, we have that for every $b \in B$ and ring homomorphism $s : \mathbb{Z} \to B$ there exists a unique ring homomorphism $\lambda : \mathbb{Z}[X] \to B$ such that $X \mapsto b$ and $\mathbb{Z} \ni m \mapsto s(m)$. Of course, this association $(b, s) \mapsto \lambda$ gives all the ring homomorphisms $\lambda : \mathbb{Z}[X] \to B$, as from λ we can recover $b = \lambda(X)$ and $s = \lambda|_{\mathbb{Z}}$. But since $(\mathbb{Z}, +)$ is generated as abelian group by $1_{\mathbb{Z}}$, which is mapped to 1_B by any ring map $s : \mathbb{Z} \to B$, there exists a unique ring homomorphism $\mathbb{Z} \to B$, and hence a unique ring homomorphism $\gamma : \mathbb{Z}[X] \to B$ sending $X \mapsto X$.

   More explicitly, we see that for $m \in \mathbb{Z}$ we have $\gamma(m) = \bar{m} := m + p\mathbb{Z}$, so that γ just reduces the coefficients of $f \in \mathbb{Z}[X]$ modulo p.

2. If $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ is such that $p|a_i$ for $i \in \{0, \ldots, n-1\}$ and $p \nmid a_n$, then $\bar{f} = \bar{a}_n X^n$ is a monomial, and as γ is a ring homomorphism, we have that $f = gh$ implies $\bar{f} = \bar{g}\bar{h}$. Since $B = \mathbb{Z}/p\mathbb{Z}[X]$ is a UFD (as it is a principal ideal domain) where $X \in B$ is an irreducible element (by reasoning on the degrees of possible divisors), we have that $\bar{g}, \bar{h}$ are monomials of some positive (by hypothesis) degrees d and e such that $d + e = n$. Then p divides all coefficients of g and h but the leading ones. Since the constant terms of f is the product of the constant terms of g and h, which are both divisible by p, we get that $p^2|a_0$.

3. This follows immediately by assuming by contradiction that f is not irreducible, meaning that $f = gh$ for some polynomials g, h which are not invertible. The two polynomials g and h need then to have positive degree, because if one of them were a non-invertible constant which would divide all the coefficients of f, contradiction with the fact that they are coprime. Then g, h have positive degree, and the previous point gives $p^2|a_0$, contradiction.

4. If $\zeta \in \mathbb{C}$ is a p-th root of unity, then $\zeta \in \mathbb{C}^\times$, and $|\zeta|^p = 1$ (by Exercise 2.1 of Exercise sheet 2), so that $|\zeta| = 1$. Then we can write $\zeta = \exp(\vartheta i) = \cos(\vartheta) + i\sin(\vartheta)$ for some $\vartheta \in \mathbb{R}$, and get

$$1 = \zeta^p = \exp(p\vartheta i),$$

   which implies $\vartheta = 2k\pi/p$ for some $k \in \mathbb{Z}$. Notice that increasing k by p, the resulting ζ does not vary. Moreover, if ζ is a non-primitive root of unity, then it has as order (in $\mathbb{C}^\times$) a proper divisor of p, which gives $\zeta = 1$. So we have

$$W_p = \{\exp(2k\pi/p) : k = 1, \ldots, p-1\},$$

   and $(X-1) \cdot \phi_p(X) = \prod_{k=0}^{n}(X - \exp(2k\pi/p))$, a polynomial of degree p whose roots are all the p-th roots of unity. Since they are roots of $X^p - 1$, by applying Factorization Lemma as we did in Exercise 1.1 and using the fact that $\mathbb{C}[X]$ is a UFD, we can conclude that the two polynomials are the same up to a multiplicative constant, which has to be 1 (by comparing the leading coefficients). Hence

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X].$$

   Defining $Q(X) := \phi_p(X+1)$, we have that Q is irreducible if and only if ϕ_p is

Please turn over!

(since their factorizations are in a degree-preserving correspondence). But

$$Q(X) = \phi_p(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1},$$

and we claim that Q satisfies the conditions to apply Eisenstein's Criterion. Then Q is irreducible over $\mathbb{Z}[X]$, and so is $\phi_p(X)$.
To prove the claim on $Q(X)$, write $a_k = \binom{p}{k+1}$, so that $Q = \sum_{k=0}^{p-1} a_k X^k$. Then $a_{p-1} = \binom{p}{p} = 1$, so that $p \nmid a_{p-1}$ and the coefficients are all coprime. For $k = 0, \dots, p-2$, we have $1 \leq k+1 \leq p-1$, and we shall prove that in this case $p | \binom{p}{k+1}$. Indeed, one has

$$\binom{p}{k+1} = \frac{p \cdots (p-k)}{(k+1) \cdots 1},$$

and p appears as a factor only in the numerator, proving that this binomial coefficient is divisible by p. Finally, we have $a_0 = \binom{p}{1} = p$, so that $p^2 \nmid a_0$ and we have all the required conditions.

3. Let $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

1. Show that R is a ring, and determine $R^\times$. [*Hint:* Suppose that $\alpha \in R^\times$. What can we say about $|\alpha|^2$?]
2. Show that $2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ are two non-equivalent factorizations of $6 \in R$, so that R is not a UFD.
3. Prove that the ideal $\mathfrak{m} = (2, 1 + i\sqrt{5}) \subseteq R$ is maximal but not principal. [*Hint:* Compute $R/\mathfrak{m}$ and deduce that $\mathfrak{m}$ is maximal. Working by contradiction and using irreducibility of 2, you can prove that $\mathfrak{m}$ is not principal.]

Solution:

1. We define operations on R as in $\mathbb{C}$, and we want to check that R is a subring of $\mathbb{C}$. This is easily done by noticing that $0, 1 \in R$, and that for $a, b, c, d \in \mathbb{Z}$ one has

$$(a + bi\sqrt{5}) - (c + di\sqrt{5}) = (a - c) + (b - d)i\sqrt{5} \in R$$

and

$$(a + bi\sqrt{5}) \cdot (c + di\sqrt{5}) = (ac - 5bd) + (ad + bc)i\sqrt{5} \in R,$$

so that R is closed by multiplication, sum, and taking inverses. Let $\alpha = a + bi\sqrt{5} \in R$. Then $|\alpha|^2 = \alpha\bar{\alpha} = a^2 + 5b^2 \in \mathbb{Z}_{\geq 0}$. Then if $\alpha \in R^\times$, and $\alpha\beta = 1$, we get $1 = 1 \cdot \bar{1} = \alpha\beta\bar{\alpha}\bar{\beta} = |\alpha|^2|\beta|^2$, and $|\alpha|^2$ can only be equal to 1 (as also $|\beta|^2 \in \mathbb{Z}_{\geq 0}$). Then $5b^2 \leq a^2 + 5b^2 = 1$ implies that $b = 0$ and $a = \pm 1$, hence $R^\times = \{\pm 1\}$.

See next page!

2. Let us first prove that 2 is irreducible. Suppose that $2 = \alpha\beta$ for $\alpha, \beta \in R$. Then we have $4 = |\alpha|^2|\beta|^2$, and $|\alpha|^2, |\beta|^2 \in \mathbb{Z}_{\geq 0}$. Moreover, we have seen before in proving the previous point that if $|\alpha|^2 = 1$ we get $\alpha = \pm 1 \in R^\times$, and the same holds for β. Hence the only possibility for the factorization $\alpha\beta = 2$ to be proper is that $|\alpha| = |\beta| = 2$, which is not possible since $5b^2 \leq a^2 + 5b^2 = 2$ implies $b = 0$, and $a^2 = 2$ which cannot hold. Then 2 is an irreducible element of R.

   As 2 clearly does not divide $1 \pm i\sqrt{5}$ (as $(1 \pm i\sqrt{5})/2 \in \mathbb{Q}[i\sqrt{5}]$ has non-integer coefficients, so that it cannot lie in R because $1, i\sqrt{5}$ are $\mathbb{Q}$-linear independent elements in $\mathbb{C}$), we get that the two given factorizations of 6 cannot be equivalent, so that R is not a UFD.

3. Let $A = R/\mathfrak{m}$. Notice that $i\sqrt{5} + \mathfrak{m} = -1 + \mathfrak{m} = 1 + \mathfrak{m}$, so that $a + bi\sqrt{5} + \mathfrak{m} = a + b + \mathfrak{m}$. This suggests that $A \cong \mathbb{Z}/2\mathbb{Z}$ via

$$\phi : A = \frac{R}{\mathfrak{m}} \to \frac{\mathbb{Z}}{2\mathbb{Z}}$$
$$a + bi\sqrt{5} + \mathfrak{m} \mapsto a + b + 2\mathbb{Z}.$$

   Let us prove that the above is indeed a ring isomorphism. First, notice that we have

$$a + bi\sqrt{5}\mathfrak{m} = a' + b'i\sqrt{5}\mathfrak{m} \iff (a - a') - (b - b') \in 2\mathbb{Z} \iff$$
$$\iff (a - a') + (b - b') \in 2\mathbb{Z} \iff (a - b) - (a' - b') \in 2\mathbb{Z},$$

   which implies that ϕ is a well defined injective map. It is clear that ϕ is additive, and that $\phi(0) = 0$, $\phi(1) = 1$, so that ϕ is surjective. Finally, we check multiplicativity:

$$\begin{aligned}\phi((a + bi\sqrt{5} + \mathfrak{m})(c + di\sqrt{5} + \mathfrak{m})) &= \phi((ac - 5bd) + (ad + bc)i\sqrt{5} + \mathfrak{m}) = \\ &= ac + bd + ad + bc + 2\mathbb{Z} = (a + b + 2\mathbb{Z})(c + d + 2\mathbb{Z}) \\ &= \phi(a + bi\sqrt{5} + \mathfrak{m}) \cdot \phi(c + di\sqrt{5} + \mathfrak{m}).\end{aligned}$$

   Then $R/\mathfrak{m}$ is isomorphic to the field $\mathbb{Z}/2\mathbb{Z}$, implying that $\mathfrak{m}$ is maximal in R.

   Now we prove by contradiction that $\mathfrak{m}$ is not principal. Suppose by contradiction that $\mathfrak{m} = (\gamma)$. We have $\gamma \notin R^\times$ (else it would generate the unit ideal R), and that $\gamma | 2$, so that being 2 irreducible we have $\gamma = 2 \cdot u$, for some $u \in R^\times$ (explicitly, $\gamma = \pm 2$), so that $(2, 1 + i\sqrt{5}) = (\gamma) = (2)$. Then $2 | 1 + i\sqrt{5}$, which is false. Contradiction. Hence $\mathfrak{m}$ is not a principal ideal.