Prof. Dr. Özlem Imamoglu

Solutions Exercise sheet 0

1. Let K be a field, $\mathcal{I}$ be a set of indices and for every $i \in \mathcal{I}$ let $K_i \subset K$ be a subfield. Show that $\bigcap_{i\in\mathcal{I}} K_i$ is a subfield of K.

Solution: Set $K' := \bigcap_{i\in\mathcal{I}} K_i$. For each $i \in \mathcal{I}$ we have that $1 \in K_i$, so $1 \in K'$. Let $a, b, c \in K'$ be arbitrary elements with $c \neq 0$. For each $i \in \mathcal{I}$ we have that $a, b, c \in K_i$, and since K_i is a subfield of K, we have that $a + b, ab, -a, c^{-1}$ are again elements of K_i. Since i was arbitrary, we have that all those elements lie in K'. Hence K' is a subfield of K.

2. Decide which of the following quotient rings are isomorphic to each other:

(a) $R_1 := \mathbb{R}[X, Y]/(X^2)$

(b) $R_2 := \mathbb{R}[X, Y, Z]/(X, Y)$

(c) $R_3 := \mathbb{R}[X, Y, Z]/(Y^2, X + Z)$

(d) $R_4 := \mathbb{R}[X, Y]/(X + Y)$

(e) $R_5 := \mathbb{R}[X, Y, Z]/(XY)$

(f) $R_6 := \mathbb{R}[X, Y, Z]/(XY + 2X + Y + 2)$

Solution: We will analyze the properties of each ring separately. For each $1 \leqslant i \leqslant 6$ we will denote the residue class of a polynomial f in R_i by $\overline{f}$.

Since $X \notin (X^2)$, we have in R_1 that $\overline{X} \neq 0$. On the other hand, we have that $X^2 \in (X^2)$ and thus $\overline{X}^2 = 0$. Then $R_1 \neq 0$ and it contains a non-zero nilpotent element.

We have that $1 \notin (XY)$ and hence $R_5 \neq 0$. Since $X, Y \notin (X, Y)$ and $XY \in (XY)$ we have that $\overline{X} \cdot \overline{Y} = \overline{XY} = 0$ in R_5 with $\overline{X}, \overline{Y} \neq 0$, so R_5 has zero divisors. Next we claim that R_5 has no nilpotent elements. Consider an element $f \in \mathbb{R}[X, Y]$ with $\overline{f}$ being nilpotent. Then there exists $n \in \mathbb{N}$ with $\overline{f^n} = (\overline{f})^n = 0$ and hence $f^n \in (XY)$. In other words, f^n is divisible by XY. But then also f has to be divisible by XY, and thus $\overline{f} = 0$ and we obtain our claim.

Next, consider the evaluation homomorphism $\mathbb{R}[X, Y, Z] \to \mathbb{R}[Z], f \mapsto f(0, 0, Z)$. This homomorphism is surjective. The kernel consists of all polynomials only in variables X and Y, and is thus equal to (X, Y). By the first isomorphism theorem, we obtain an isomorphism $R_2 = \mathbb{R}[X, Y, Z]/(X, Y) \cong \mathbb{R}[Z]$.

Let $Z := X + Y$. Then $R_4 = \mathbb{R}[Z, Y]/(Z)$ and the rings R_2 and R_4 are isomorphic to each other.

Note that $R_6 := \mathbb{R}[X, Y, Z]/(XY + 2X + Y + 2) = \mathbb{R}[X, Y, Z]/((X + 1)(Y + 2))$, so that there is an isomorphism

$$\mathbb{R}[X, Y, Z]/((X + 1)(Y + 2)) \cong \mathbb{R}[X, Y, Z]/(XY),$$

and the rings R_5 and R_6 are isomorphic.

If we define $Q := X + Z$, then there is an isomorphism

$$R_3 \cong \mathbb{R}[X, Y, Q]/(Y^2, Q) \cong \mathbb{R}[X, Y]/(Y^2).$$

Then the rings R_1 and R_3 are isomorphic.

Finally, the properties above show that only $R_1 \cong R_3$ contain a non-zero nilpotent element, while $R_5 \cong R_6$ don't, so they can not be isomorphic to each other. Since $R_5 \cong R_6$ contain zero-divisors, but $R_2 \cong R_4$ are integral domains, they can not be isomorphic to each other either. Hence there are no further isomorphisms.

3. Let R be a commutative ring and let $\varphi : R \hookrightarrow \mathbb{Z}$ be a surjective ring homomorphism. Prove that the following statements are true or give a counter-example:

(a) $\text{image}(\varphi)$ is a prime ideal in $\mathbb{Z}$.

(b) For $\mathfrak{s}$ a prime ideal in $\mathbb{Z}$, $\varphi^{-1}(\mathfrak{s})$ is also a prime ideal in R.

(c) For $\mathfrak{r}$ a prime ideal in R with $\ker(\varphi) \subseteq \mathfrak{r}$, $\varphi(\mathfrak{r})$ is also a prime ideal in $\mathbb{Z}$.

Solution: (a) This is wrong: let $R := \mathbb{Z}$ and let φ be the identity. Then $\text{image}(\varphi) = \mathbb{Z}$, which is not a prime ideal in $\mathbb{Z}$ as it is equal to the whole ring $\mathbb{Z}$.

(b) Note that $\varphi^{-1}(\mathfrak{s})$ can not be the entire ring R, since then $\varphi(\varphi^{-1}(\mathfrak{s})) = \mathbb{Z} \subseteq \mathfrak{s}$ and $\mathfrak{s}$ would not be a prime ideal in $\mathbb{Z}$.

Let $a, b \in R$ be such that $ab \in \varphi^{-1}(\mathfrak{s})$. Then $\varphi(a)\varphi(b) = \varphi(ab) \in \mathfrak{s}$ and since $\mathfrak{s}$ is a prime ideal, we have that $\varphi(a) \in \mathfrak{s}$ or $\varphi(b) \in \mathfrak{s}$. This implies that $a \in \varphi^{-1}(\mathfrak{s})$ or $b \in \varphi^{-1}(\mathfrak{s})$.

(c) Let $a, b \in \mathbb{Z}$ and $ab \in \varphi(\mathfrak{r})$ be arbitrary. We want to show that $a \in \varphi(\mathfrak{r})$ or $b \in \varphi(\mathfrak{r})$. Since φ is surjective, there exist $r, s \in R$ such that $\varphi(r) = a$ and $\varphi(s) = b$. Further, there exists $c \in \mathfrak{r}$ with $\varphi(c) = ab$. Then $\varphi(c) = ab = \varphi(r)\varphi(s)$, and since φ is a ring homomorphism, we obtain $\varphi(c - rs) = 0$, so $c - rs \in \ker(\varphi)$.

By assumption $\ker(\varphi) \subseteq \mathfrak{r}$, so that $rs - c \in \mathfrak{r}$. Then $rs \in \mathfrak{r}$ and since $\mathfrak{r}$ is a prime ideal, we have that $r \in \mathfrak{r}$ or $s \in \mathfrak{r}$. This implies $a \in \varphi(\mathfrak{r})$ or $b \in \varphi(\mathfrak{r})$, so $\varphi(\mathfrak{r})$ is a prime ideal.

4. Show that any finite integral domain is a field.

Solution: Let $a \in R$ be a non zero element of an integral domain R. Since R does not have any zero divisors, $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x = y$. Hence the map $\varphi : R \to R$ which sends x to ax is injective. Since R is finite the map φ is also surjective. In particular there is a $b \in R$ such that $ab = 1$

5. Let R and S be rings with 1 and $\varphi : R \to S$ be a nonzero map which satisfies $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$, $\forall a, b \in R$. Show that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor. Hence if S has no zero divisors then $\varphi(1_R) = 1_S$.

Solution: Since $\varphi(ab) = \varphi(a)\varphi(b)$, $\varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R)\varphi(1_R)$. Hence $\varphi(1_R) = \varphi(1_R)1_S = \varphi(1_R)\varphi(1_R)$. It then follows that $\varphi(1_R)[1_S - \varphi(1_R)] = 0$. Since φ is a non zero map it follows that $\varphi(1_R) \neq 0$ and hence it is a zero divisor.

(Note $\varphi(1_R) = 0 \Rightarrow \varphi(r) = \varphi(r)\varphi(1_R) = 0$, $\forall r \in R$)

6. Let $\varphi : R \to Q$ be a surjective ring homomorphism. Prove that there is a one-to-one correspondence between the ideals of Q and the ideals of R that contain $\ker(\varphi)$.

Solution: By the first isomorphism theorem, we have that there is an isomorphism $R/\ker(\varphi) \to Q$, so it suffices to prove that there is a one-to-one correspondence between ideals of R containing $\ker(\varphi)$ and ideals of $R/\ker(\varphi)$. Let $\pi : R \to R/\ker(\varphi)$ denote the natural projection. Given an ideal $\mathfrak{a} \subseteq R$ with $\ker(\varphi) \subseteq \mathfrak{a}$, we let

$$\pi(\mathfrak{a}) = \{\pi(a) \mid a \in \mathfrak{a}\} = \{a + \ker(\varphi) \mid a \in \mathfrak{a}\} \subseteq R/\ker(\varphi).$$

Given an ideal $\mathfrak{b} \subseteq R/\ker(\varphi)$, we will make it correspond to

$$\pi^{-1}(\mathfrak{b}) = \{b \in R \mid \pi(b) \in \mathfrak{b}\}.$$

Note that any ideal $\mathfrak{b}$ of $R/\ker(\varphi)$ contains the zero-element, $0_{R/\ker(\varphi)} = \ker(\varphi) \in \mathfrak{b}$. Hence for each $k \in \ker(\varphi)$ we have $\pi(k) = \ker(\varphi) \in \mathfrak{b}$, and thus $\ker(\varphi) \subseteq \pi^{-1}(\mathfrak{b})$.

Claim: If $\mathfrak{a}$ is an ideal of R with $\ker(\varphi) \subseteq \mathfrak{a}$, then $\pi(\mathfrak{a})$ is an ideal of $R/\ker(\varphi)$.

Let $\mathfrak{a}$ be an ideal of R. Let $a + \ker(\varphi) \in \pi(\mathfrak{a})$ and $r + \ker(\varphi) \in R/\ker(\varphi)$, with $a \in \mathfrak{a}$. Then we have $(r + \ker(\varphi))(a + \ker(\varphi)) = ra + \ker(\varphi) = \pi(ra)$. Since $\mathfrak{a}$ is an ideal, and $a \in \mathfrak{a}$ and $r \in R$, then $ra \in \mathfrak{a}$, so also $\pi(ra) \in \pi(\mathfrak{a})$.

Let $a + \ker(\varphi), a' + \ker(\varphi) \in \pi(\mathfrak{a})$, with $a, a' \in \mathfrak{a}$. Then $a + a' \in \mathfrak{a}$, so $(a + \ker(\varphi)) + (a' + \ker(\varphi)) = (a + a') + \ker(\varphi) = \pi(a + a') \in \pi(\mathfrak{a})$. Thus we obtain our claim.

Claim: If $\mathfrak{b}$ is an ideal of $R/\ker(\varphi)$, then $\pi^{-1}(\mathfrak{b})$ is an ideal of R which contains $\ker(\varphi)$.

Let $\mathfrak{b}$ be an ideal of $R/\ker(\varphi)$, $a \in \pi^{-1}(\mathfrak{b})$, and $r \in R$. Then $\pi(a) \in \mathfrak{b}$, so $\pi(ar) = \pi(a)\pi(r) \in \mathfrak{b}$, since $\mathfrak{b}$ is an ideal. Thus $ra \in \pi^{-1}(\mathfrak{b})$.

If $a, a' \in \pi^{-1}(\mathfrak{b})$, then $\pi(a + a') = (a + a') + \ker(\varphi) = a + \ker(\varphi) + a' + \ker(\varphi) = \mathfrak{b}$, as $\ker(\varphi) \subseteq \mathfrak{b}$. So we have $a + a' \in \pi^{-1}(\mathfrak{b})$. Thus $\pi^{-1}(\mathfrak{b})$ is an ideal of R. We have already seen that $\ker(\varphi) \subseteq \pi^{-1}(\mathfrak{b})$.

For an ideal $\mathfrak{b} \subseteq R/\ker(\varphi)$, let us denote $\overline{\Pi} : \mathfrak{b} \mapsto \pi^{-1}(\mathfrak{b})$. Similarly, we will write Π for the map sending an ideal $\mathfrak{a} \subseteq R$ with $\ker(\varphi) \subseteq \mathfrak{a}$, to $\pi(\mathfrak{a})$.

If $\overline{\Pi} \circ \Pi$ and $\Pi \circ \overline{\Pi}$ are both the identity, then Π is a bijection.

Let $\mathfrak{a}$ be an ideal of R that contains $\ker(\varphi)$. We have that $\mathfrak{a} \subseteq \overline{\Pi}(\Pi(\mathfrak{a}))$ holds, because it holds for any subset and any function. Now, let $c \in \overline{\Pi}(\Pi(\mathfrak{a}))$. Then $c \in \pi^{-1}(\pi(\mathfrak{a}))$ and $\pi(c) \in \pi(\mathfrak{a})$. Hence there exists $a \in \mathfrak{a}$ such that $\pi(c) = \pi(a)$; hence $\pi(c - a) \in \ker(\pi) \subseteq \mathfrak{a}$. Thus, $c - a \in \mathfrak{a}$, and since $a \in \mathfrak{a}$, we have that $c \in \mathfrak{a}$. Thus $\overline{\Pi}(\Pi(\mathfrak{a})) \subseteq \mathfrak{a}$, and we obtain $\overline{\Pi} \circ \Pi = \mathrm{id}$.

Conversely, if $\mathfrak{b}$ is an ideal of $R/\ker(\varphi)$, then $\Pi(\overline{\Pi}(\mathfrak{b})) = \mathfrak{b}$, because π is onto and this equality holds for any surjective function. This proves the desired correspondence.