
Sheet 5

If you want your solutions to be corrected, upload them on URM by the end of June 1.
Write your name and matriculation number on each sheet. If you upload the exercises as a group,
only one person can do it instead of the whole group.

The exercises marked with * might be more complicated or involved than the others.

Exercise 5.1 Consider the rings

$$\mathbf{F}_2, \quad \mathbf{R}[x], \quad \mathbf{Z}[x], \quad \mathbf{Z}[\sqrt{7}], \quad \mathbf{Z}[\sqrt{5}].$$

Which of these is a Dedekind domain? Motivate your answer.

Exercise 5.2 Let A be a Dedekind domain and let $I = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$ and $J = \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_s^{m_s}$ be two nonzero ideals, written in terms of their unique factorization into pairwise distinct, non-zero prime ideals.

- (i) Write the unique factorization of the ideal $I \cap J$.
- (ii) Write the unique factorization of the ideal $I + J$.
- (iii) Show that $I + J = A$ if and only if $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \cap \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\} = \emptyset$.

Exercise 5.3 Let A be a Dedekind domain and assume that A has a unique non-zero prime ideal \mathfrak{p} . Then A is called a discrete valuation ring (DVR). Let also $F = \text{Frac } A$.

- (i) Show that \mathfrak{p} is principal: there is a $t \in \mathfrak{p}$ such that $\mathfrak{p} = (t)$. Show that A is a PID.
- (ii) Show that any non-zero $x \in F^\times$ can be written uniquely as $a = u \cdot t^{v(x)}$ where $u \in A^\times$ and $v(x) \in \mathbf{Z}$.
- (iii) Show that the function $v: F^\times \rightarrow \mathbf{Z}_{\geq 0}$ is a discrete valuation. This means that v is surjective and that for all $x, y \in F$ it holds that
 - $v(x + y) \geq \min\{v(x), v(y)\}$.
 - $v(xy) = v(x) + v(y)$.

Conversely, let F be a field and $v: F^\times \rightarrow \mathbf{Z}$ be a discrete valuation.

- (iv) Show that $A = \{x \in F \mid v(x) \geq 0\} \cup \{0\}$ is a discrete valuation ring with unique non-zero prime ideal given by $\mathfrak{p} = \{x \in F \mid v(x) \geq 1\} \cup \{0\}$.

Let now $p \in \mathbf{Z}$ be a fixed prime number. Then any $x \in \mathbf{Q}^\times$ can be written uniquely as $x = p^{v_p(x)} \cdot \frac{n}{m}$ where $v_p(x) \in \mathbf{Z}$ and $n, m \in \mathbf{Z}$ are coprime with p . This defines a map

$$v_p: \mathbf{Q}^\times \rightarrow \mathbf{Z}$$

called the p -adic valuation.

- (v) Show that v_p is a discrete valuation and that the corresponding discrete valuation ring is the ring of fractions where p does not divide the denominator. More precisely, this is the ring $\mathbf{Z}_{(p)} = \{\frac{a}{b} \mid p \nmid b\} \cup \{0\}$.

Turn the sheet

Exercise 5.4 Let $\alpha \in \mathbf{C}$ be integral over \mathbf{Z} and let $m_{\alpha, \mathbf{Q}}(x) \in \mathbf{Z}[x]$ be its minimal polynomial. Consider the extension $\mathbf{Z} \subseteq \mathbf{Z}[\alpha]$ and the evaluation map

$$\text{ev}_\alpha: \mathbf{Z}[x] \longrightarrow \mathbf{Z}[\alpha], \quad f(x) \mapsto f(\alpha)$$

- (i) Show that the evaluation map induces an isomorphism $\mathbf{Z}[x]/(m_{\alpha, \mathbf{Q}}(x)) \cong \mathbf{Z}[\alpha]$ and prove that $\mathbf{Z}[\alpha]$ is a free \mathbf{Z} -module of rank $n = \deg m_{\alpha, \mathbf{Q}}(x)$.
- (ii) If $f_1(x), \dots, f_r(x) \in \mathbf{Z}[x]$ show that the evaluation map induces an isomorphism $\mathbf{Z}[x]/(f_1(x), \dots, f_r(x), m_{\alpha, \mathbf{Q}}(x)) \cong \mathbf{Z}[\alpha]/(f_1(\alpha), \dots, f_r(\alpha))$.
- (iii) If $p \in \mathbf{Z}$ is a prime number and $f_1(x), \dots, f_r(x) \in \mathbf{Z}[x]$, denote by $\bar{f}_i(x) \in \mathbf{F}_p[x]$ the polynomial where all coefficients are taken modulo p . Show that the evaluation map induces isomorphisms

$$\begin{aligned} \mathbf{Z}[\alpha]/(p, f_1(\alpha), \dots, f_r(\alpha)) &\cong \mathbf{Z}[x]/(p, f_1(x), \dots, f_r(x), m_{\alpha, \mathbf{Q}}(x)) \\ &\cong \mathbf{F}_p[x]/(\bar{f}_1(x), \dots, \bar{f}_r(x), \bar{m}_{\alpha, \mathbf{Q}}(x)). \end{aligned}$$

Consider now the polynomial $f(x) = x^3 + 10x + 1$ and let $\alpha \in \mathbf{C}$ be a root of $f(x)$.

- (iv) Find all prime ideals in the three rings $\mathbf{Z}[\alpha]/2\mathbf{Z}[\alpha]$, $\mathbf{Z}[\alpha]/3\mathbf{Z}[\alpha]$ and $\mathbf{Z}[\alpha]/5\mathbf{Z}[\alpha]$.