Humboldt-Universität zu Berlin
Institut für Mathematik
Dr. D. Agostini, M. Sc. L. Lerer
L. Mädje

Zahlentheorie

SoSe 2019

Exercise Sheet 3

If you want your solutions to be corrected, you should hand them in by Monday, May 6.
Please write your name and immatriculation number on top of every exercise.

Exercise 3.1 (5 points) Conclude the example in the lecture, by showing that for a squarefree integer $d \in \mathbb{Z}$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \mod 4. \\ \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \mod 4. \end{cases}$$

Exercise 3.2 (5 points) Prove the following extension of the integrality criterion that we had in the lectures. Let R be an integrally closed domain, $F = \operatorname{Frac} R$ its field of fractions and K/F a finite extension. For $\alpha \in K$, show that α is integral over R if and only if its minimal polynomial $m_\alpha(x)$ over F has coefficients in R.

Exercise 3.3 (2+2+1+2 points) Let R be a ring and M an R-module. Prove the following facts:

a) If M is noetherian, then any submodule $M' \subseteq M$ and any quotient module $M'' = M/M'$ are noetherian as well.

b) If N is another R-module, and both M, N are noetherian, then the direct sum $M \oplus N$ is noetherian as well.

c) M is finitely generated if and only if there is a surjective homomorphism $R^{\oplus r} \to M$, hence, if and only if M is a quotient of $R^{\oplus r}$.

d) Assume that R is noetherian. Then M is noetherian if and only if it is finitely generated.

Exercise 3.4 (5+5 points)

a) Prove that the number ring $\mathbb{Z}[\sqrt{2}]$ has infinitely many units by considering $1 + \sqrt{2}$. Conclude that the equation $x^2 - 2y^2 = 1$ has infinitely many integer solutions.

b) Let $\alpha = \sqrt[4]{2}$. Use the trace $\operatorname{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}$ to show that $\sqrt{3} \notin \mathbb{Q}(\alpha)$. *Hint*: write $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$ and show iteratively that $a = 0, b = 0, c = 0$, then derive a contradiction.

Turn the sheet.

Exercise 3.5 (5+5+2+2+2+2 points) Let R be an Euclidean domain (for example $R = \mathbb{Z}, K[X], \mathbb{Z}[i]$) and $A = (a_{ij})$ an $m \times n$ matrix with coefficients in R. We want to show that with elementary row and column operations, the matrix can be brought into the so-called *Smith normal form*: this is the block matrix

$$\begin{pmatrix} D & O \\ O & O \end{pmatrix} \qquad \text{where} \qquad D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_s \end{pmatrix}, \text{ with } d_i \neq 0,\ d_1 | d_2 | \dots | d_s.$$

Recall that the elementary row operations are: exchange two rows, multiply a row by an invertible element in R, add to a row another row multiplied by an arbitrary element of R. The elementary columns operations are the same.

a) Prove that row and column operations do not change $d = \gcd(a_{ij})$, up to multiplication by units in R.

b) Let $f\colon R \setminus \{0\} \to \mathbb{N}$ be the Euclidean function of R, and set $m = \min\{f(a_{ij}) \mid a_{ij \neq 0}\}$. Prove by induction on m that with row and columnt operations we can put the matrix A in the form

$$\begin{pmatrix} d & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Hint: For the induction step, use the Euclidean division, together with row and column operations. It can be useful to start with a simple matrix $A = \begin{pmatrix} a & b \end{pmatrix}$.

c) Prove that with row and column operations the matrix can be put into the form

$$\begin{pmatrix} d & 0 & 0 & \dots \\ 0 & a_{22} & a_{23} & \dots \\ 0 & a_{32} & a_{33} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

d) Conclude that with row and column operation we can put the matrix into Smith normal form.

Now let M be a finitely generated module over R.

f) Show that $M = \operatorname{coker}(\phi\colon R^{\oplus n} \to R^{\oplus m})$ for a certain map ϕ between free R-modules. *Hint*: look at the kernel of a map $R^{\oplus n} \to M$ as in 3.2.c and use noetherianity.

g) Let A be a matrix representing ϕ. Using a Smith normal form of A, prove that $M \cong R^{\oplus r} \oplus R/(d_1) \oplus \cdots \oplus R/(d_s)$ for $d_1 | d_2 | \dots | d_s$.

Furthermore, the d_i appearing in the Smith normal form of a matrix are unique up to multiplication by units in R. A way to see this is to notice that

$$d_1 \cdot d_2 \dots d_r = \gcd(\text{ all } r \times r \text{ minors of } A) \tag{1}$$

and then observe that the quantity on the right is unchanged by row and column operations. The Smith normal form exists also for arbitrary matrices over PID, but then row and column operations are not sufficient anymore. Then (3.3.g) holds also for modules over PID. For details, see `https://en.wikipedia.org/wiki/Smith_normal_form`.