Universität Wien
Prof. B. Szendrői

Commutative algebra and algebraic geometry
— Exercise Sheet 1 with hints —

WS 2023

All rings R are commutative and unital. The symbol k denotes a field.

Exercise 1. Let R be a domain. Prove that $R[x]$ is also a domain. Describe its field of fractions.

Exercise 2. Let R be a ring.

(1) Prove that if $r \in R$ is nilpotent, then $1-a \in U(R)$, where $U(R)$ denotes the group of units of R. Is the converse also true?
(2) Prove that if $r_1 \in R$ is idempotent (meaning $r_1^2 = r_1$), then $r_2 = 1 - r_1$ is also idempotent, and orthogonal to r_1 in the sense that $r_1 r_2 = 0$. Prove that R as an R-module decomposes as a direct sum of two R-submodules $r_1 R, r_2 R$.

Exercise 3. Let S be a subring of the ring $\mathbb{Q}$ of rational numbers.

(1) Let p be a prime number dividing a denominator n for an element $r = m/n \in S$ with (m, n) relatively prime integers. Prove that $1/p \in S$.
(2) Deduce that S is the subset of $\mathbb{Q}$ defined by the condition that all prime factors of the denominator n of an element $r = m/n \in S$ with (m, n) relatively prime integers must belong to a fixed set of primes $\mathcal{P}$.

Thus *subrings of $\mathbb{Q}$ are classified by subsets of the set of all prime numbers.*

Exercise 4. Prove that the ring $\mathbb{Z}[i]$ is a Euclidean domain (hence PID and UFD). Find the set of irreducibles of $\mathbb{Z}[i]$.

Exercise 5. Prove that the following rings are not principal ideal domains: $\mathbb{Z}[x], \mathbb{Z}[\sqrt{-5}], k[x, y]$.

Exercise 6. Prove that the following rings are not Noetherian.

(1) The subring $R \subset k[x, y]$ of polynomials of the form $f(x, y) = a + yg(x, y)$, with $a \in k$.
(2) The ring[1] of algebraic integers, consisting of all complex numbers that are roots of a monic polynomial equation over $\mathbb{Z}$.

[1]Extra exercise: prove that this set forms a ring.

Exercise 7. (Optional, challenging exercise) Let $\mathrm{Int}(\mathbb{Z})$ be the subring of $\mathbb{Q}[x]$ consisting of polynomials that take integer values on all integers.

(1) Show that for all natural numbers $n \geq 0$, the polynomial
$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$
is in $\mathrm{Int}(\mathbb{Z})$. So $\mathrm{Int}(\mathbb{Z})$ is strictly larger than its obvious subring $\mathbb{Z}[x]$.
(2) Show that the polynomials $\{\binom{x}{n} : n \in \mathbb{N}\}$ form a $\mathbb{Z}$-basis for the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$.
(3) Show that the ring $\mathrm{Int}(\mathbb{Z})$ is not Noetherian.

For more details on the amazing properties of this ring, see *What are Rings of Integer-Valued Polynomials?* by Michael Steward.

Hint for Exercise 1. Consider the field $R(x)$ of rational functions in one variable: the field of fractions $f(x)/g(x)$ where $f, g \in R[x]$ are polynomials, g not (idenfically) zero, and we are allowed to simplify by common factors.

Hint for Exercise 2. (1) Use $1/(1-a) = 1 + a + a^2 + \ldots$. For the converse, take a nontrivial unit in $R = \mathbb{Z}$. (2) Straightforward computation. For the last part, $x = r_1x + r_2x$, whereas uniqueness of decomposition comes from orthogonality and idempotence of the r_i.

Hint for Exercise 3. (1) Use Bezout's lemma: since m, n are relatively prime, there exist integers a, b such that $ma+nb = 1$. So $1/n = b+(m/n)a \in S$ and so $1/p \in S$. (2) Let $\mathcal{P}$ be the set of primes appearing as a factor of a reduced denominator of an element $m/n \in S$. By (1), for $p \in \mathcal{P}$, $1/p \in S$. Now it's easy to see that S must be the ring described.

Hint for Exercise 4. For (1), the norm is simply absolute value $|a+ib| = a^2+b^2$. A geometric argument shows that there is division with remainder with smaller norm. For (2), use the fact that a prime number p that is congruent to 1 modulo 4 can always be written as a sum of two integer squares, for example $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$. (Lagrange's theorem, taught in number theory classes.)

Hint for Exercise 6. (1) Consider the ideal $(y, xy, xy^2, \ldots)$ of R. (2) This will follow from material in the section on integral extensions; alternatively, use the theory of symmetric functions.

Hint for Exercise 7. (1) For $x \geq 0$ integer, $\binom{x}{n}$ is the answer to a combinatorial question and thus a (non-negative) integer. For $x < 0$, re-write the product in the numerator as a sign times a product of non-negative integer terms to see that the whole expression is a sign times a (positive) binomial coefficient. (2) Prove first that $\{\binom{x}{n} : n \in \mathbb{N}\}$ forms a linearly independent set over $\mathbb{Z}$ and also $\mathbb{Q}$, and that it forms a $\mathbb{Q}$-basis of $\mathbb{Q}[x]$. Now if $f \in \mathrm{Int}(\mathbb{Z})$, we can definitely write
$$f(x) = \sum_{k=0}^{n} a_k \binom{x}{k}$$
with $a_k \in \mathbb{Q}$. We need $a_k \in \mathbb{Z}$. Substitute $x = 0$. Proceed by induction. For (3), consider the ideal $I \lhd \mathrm{Int}(\mathbb{Z})$ generated by the elements $\binom{x}{p_i}$, for p_i the i-th prime.