Home assignment 5: Factorial rings

Rules: This is a class assignment for the next week. Exercises with [*] are extra hard and not necessary to follow the rest. Exercises with [!] are non-trivial, fundamental and necessary for further work.

5.1 Euclidean algorithm

Definition 5.1. Let R be a ring, and $\nu: \ R\backslash 0 \longrightarrow \mathbb{Z}^{\geqslant 0}$ a function satisfying $\nu(xy) = \nu(x)\nu(y)$ ("Euclidean norm function"). We say that R is **Euclidean ring** if for any $p, q \in R$ such that p is not divisible by q, there exists a relation ("division with reminder") $p = qs + r$ with $\nu(r) < \nu(q)$.

Exercise 5.1. Prove that the ring $\mathbb{Z}$ of integers is Euclidean, with $\nu(x) = |x|$.

Exercise 5.2. Prove that the ring $k[t]$ of polynomials over a field k is Euclidean, with $\nu(P(t)) = 2^{\deg P(t)}$.

Hint. Use division with reminder.

Exercise 5.3. Prove that the ring $\mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$ of Gaussian integers is Euclidean, with $\nu(x) = |x|$.

Hint. Approximate a quotient $\frac{p}{q}$ of two Gaussian integers by a Gaussian integer s such that $\left|\frac{p}{q} - s\right| \leqslant 2^{-1/2}$.

Exercise 5.4. Prove that the ring $\mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$ is Euclidean, with $\nu(x) = |x|$.

Hint. Approximate a quotient $\frac{p}{q}$ of two elements of $\mathbb{Z}[\sqrt{-2}]$ by $s \in \mathbb{Z}[\sqrt{-2}]$ such that $\left|\frac{p}{q} - s\right| \leqslant \frac{\sqrt{3}}{2}$.

Exercise 5.5. Let R be a Euclidean ring, and $p, q \in R$. Prove that there exists $u \in R$, such that p and q are divisible by u, and $u = ap + bq$.[1]

Hint. Use the Euclidean algorithm.

5.2 Factorial rings

Definition 5.2. An ideal $I \subset R$ is called **finitely generated** if there is a finite subset $a_1, ..., a_n \in I$ such that any element $v \in I$ can be expressed as $\sum_{i=1}^n a_i b_i$, for some $b_i \in R$. An ideal I is called **principal** if $I = rR$, that is, I is all elements of R divisible by $r \in R$. Such an ideal is denoted (r). A ring R is called **principal ideal ring** if all finitely-generated ideals of R are principal.

[1] Such u is called **the greatest common divisor**.

Exercise 5.6. Let R be a Euclidean ring, $a, b \in R$, and I an ideal generated by a, b. Prove that $I = (u)$, where u is the greatest common divisor of a, b.

Exercise 5.7. Prove that any Euclidean ring is a principal ideal ring.

Hint. Use the previous exercise.

Definition 5.3. An element r of a ring R is called **prime** if the corresponding principal ideal (r) is prime.

Definition 5.4. Let $a, b \in R$. If a divides b, we write $a|b$. If a is divisible by b, we write $a \vdots b$.

Exercise 5.8. Prove that r is prime if and only if for any $a, b \in R$ such that $ab \vdots r$ one has $a \vdots r$ or $b \vdots r$.

Exercise 5.9. Let R be a Euclidean ring, $r \in R$ indivisible element, and $a \in R$ not dividing r. Prove that there exist $x, y \in R$ such that $ax + ry = 1$.

Exercise 5.10. Let R be a Euclidean ring, and $a, b, r \in R$ satisfy $ab \vdots r$, where r is indivisible. Prove that either $a \vdots r$ or $b \vdots r$.

Hint. Use the previous exercise.

Exercise 5.11. Let R be a Euclidean ring, and $a = p_1^{\alpha_1} ... p_n^{\alpha_n}$ be a decomposition of $a \in R$ onto a product of primes. Prove that this decomposition is unique up to invertible factors and permutation of p_i.

Definition 5.5. A ring with this property is called “unique factorization ring”, or “factorial ring”.

Exercise 5.12. Prove that any principal ideal ring is factorial.