ALGEBRA 2: divisibility in rings and Euclid's algorithm

Greatest common divisor

Let R be a ring.

Definition 2.1. **Divisors of zero** in ring R are the elements x, y such that $xy = 0$. R is called an **integral domain** if there are no divisors of zero in R.

Throughout this section all rings are supposed to be integral domains.

Definition 2.2. An invertible element in R is called a **unit** of ring R.

Exercise 2.1. Gauss integers are complex numbers of a form $x + y\sqrt{-1}$ where x, y are integers. Prove that they form a ring. It is denoted by $\mathbb{Z}[\sqrt{-1}\,]$.

Exercise 2.2. Describe all the unities in the ring of Gauss integers.

Hint. If a complex number z is invertible in $\mathbb{Z}[\sqrt{-1}\,]$ then $z\bar{z}$ is also invertible in $\mathbb{Z}[\sqrt{-1}\,]$.

Exercise 2.3. Let us fix a positive integer n. Consider a set of all complex numbers of the form $x + y\sqrt{-n}$ where x, y are integers. Prove that this is a ring.

Exercise 2.4 (*). Fix a positive integer n. Consider a set of all complex numbers of the form $\frac{x+y\sqrt{-3}}{2}$ where x, y are either both even or both odd. Prove that this is a ring and describe all unities. We will denote this ring by $\widetilde{\mathbb{Z}[\sqrt{-3}]}$.

Definition 2.3. Let R be a ring and $x, y \in R$ be elements of R. If $x = yz$ in R then one says that x is **divisible** by y in R and y **divides** x. The relation of divisibility is denoted by $x \,\vdots\, y$.

Definition 2.4. Let R be a ring and $x, y \in R$ be the elements of R. **Greatest common divisor** (GCD) of x, y is an element $z \in R$ such that z divides x and y and for all z' which divides x, z' divides z. x and y are called **coprime** if 1 is the greatest common divisor of x, y.

Strictly speaking, if one considers an arbitrary ring GCD may not exist for every pair of elements.

Exercise 2.5. Prove that if GCD exists then it is unique up to a unit: if z and z' are greatest common divisors x and y in a ring R, then $z = ez'$, where e is a unit of ring R.

Exercise 2.6. Let $\mathbb{Q}(2)$ be a set of all rational numbers, represented as fractions of the form $\frac{p}{q}$ with odd denominator q. Prove that this set is closed under multiplication and addition and forms a subring in the ring of rational numbers.

Exercise 2.7. Give an example of a non-invertible element in $\mathbb{Q}(2)$.

Exercise 2.8. Describe all unities of the ring $\mathbb{Q}(2)$.

Exercise 2.9 (!). Prove that in $\mathbb{Q}(2)$ for any two elements there exists a greatest common divisor of them.

Hint. Prove that any element of $\mathbb{Q}(2)$ can be represented in the form $e2^n$, where e is a unit.

Definition 2.5. Let p be an element of a ring R. It is called **prime**, if for any q, r with $p = qr$ either q, or r is a unit of the ring R.

Exercise 2.10. What are prime elements of $\mathbb{Q}(2)$?

Divisibility in the ring of integer numbers

Exercise 2.11. Let x, y be positive integer numbers and $z = (x - ky)$ be the remainder when x is divided by y. Prove that if $\mathrm{GCD}(y, z)$ exists then $\mathrm{GCD}(x, y)$ exists as well and $\mathrm{GCD}(x, y)=$ $\mathrm{GCD}(y, z)$.

Definition 2.6. The Euclid's algorithm takes two positive integer numbers x, y, $x > y$ and return a positive integer number z.

a. If x is divisible by y then algorithm stops and returns y.

b. If x is not divisible by y then algorithm loops, taking numbers $x_1 = y$, $y_1 = x - ky$ where $x - ky$ is the remainder when x is divided by y.

Exercise 2.12. Prove that the Euclid's algorithm terminates after finite number of iterations.

Exercise 2.13. Prove that the number returned by the Euclid's algorithm applied to integer numbers x, y is $\mathrm{GCD}(y, z)$

Exercise 2.14. Solve the problem 1.26 from ALGEBRA 1 (unless you have already solved it).

Exercise 2.15. Prove that the Euclid's algorithm applied to numbers x, y can be represented as a linear combination of x with y integer coefficients: $z = ax + by$.

Exercise 2.16. Let x, y be coprime integer numbers and p be a prime number. Suppose that xy is divisible by p^α for some natural number α. Prove that either x is divisible by p^α, or y is divisible by p^α.

Exercise 2.17 (!). Deduce that prime multipliers decomposition is unique: if a positive integer number x can be represented in two ways as a product of prime numbers then these two ways only differ by an order of multipliers.

Hint. Present x as a product $p_i^{\alpha_i}$ where p_i are different prime numbers and use the previous problem to prove that α_i can be defined in unique fashion.

Unique factorization ring

Definition 2.7. Let R be a ring. Two decompositions of $r \in R$ into prime multipliers $r = p_1 p_2 \dots p_k$, $r = q_1 q_2 \dots q_k$ are called equivalent if $r = q_1 q_2 \dots q_k$ can be obtained after by permuting p_i and by multiplying p_i by ring unit. It is said that R is a **unique factorization ring**, if for any $r \in R$ there exists decomposition of r into the product of prime elements which is unique up to equivalence.

Exercise 2.18 (!). Let a ring R admits decomposition into prime multipliers and for each pair of elements x, y there exists a GCD in this ring. Let z be represented in R as a linear combination of x, y: $z = ax + by$ where $a, b \in R$. Prove that R is a unique factoriazation ring.

Hint. Use the hint to the problem 2.17.

Exercise 2.19. Consider a positive number n. Consider a ring $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{C}$ of complex numbers of the form $z = x + y\sqrt{-n}$ where x and y are integer. Prove that $|z|^2$ is integer for all $z \in \mathbb{Z}[\sqrt{-n}]$.

Exercise 2.20. Prove that z is a unit in $\mathbb{Z}[\sqrt{-n}]$ iff $|z|^2 = 1$.

Hint. $|z^{-1}|^2 = (|z|^2)^{-1}$.

Exercise 2.21. Let z be an element of $\mathbb{Z}[\sqrt{-n}]$ such that $|z|^2$ is prime in $\mathbb{Z}$. Prove that z is prime in $\mathbb{Z}[\sqrt{-n}]$.

Hint. $|zz'|^2 = |z|^2|z'|^2$.

Exercise 2.22 (!). Consider the ring $\mathbb{Z}[\sqrt{-3}]$. Prove that 2 and $1 \pm \sqrt{-3}$ are primes. Deduce that $\mathbb{Z}[\sqrt{-3}]$ is not a unique factorization ring.

Hint. Use the equality $2^2 = 4$.

Division with remainder in rings

Definition 2.8. Let R be a ring. It is said that **division with remainder is defined** in R if for every pair x, y, $y \neq 0$ in R there are elements $z, k \in R$ defined such that $z = x - ky$. In this case z is called **remainder** and k is called **factor**.

Examples. Division with remainder is defined in the ring of integer numbers. Division with remainder is defined as well in the ring of polynomials $k[t]$ over a field k:

$$\begin{array}{r|l} x^2 + 2x - 12 & x+5 \\ \cline{2-2} x^2 + 5x \phantom{{}-12} & x-3 \\ \cline{1-1} -3x - 12 & \\ -3x - 15 & \\ \cline{1-1} 3 & \end{array}$$

Definition 2.9. Let division with remainder be defined in the ring R. **Euclid's algorithm in** R is applied to a pair x, y of non-zero elements in R and is defined recursively. If x is divisible by y Euclid's algorithm stops and returns y. If x is not divisible by y then Euclid's algorithm is applied to y, z, where z is a remainder when x is divided by y. This process can be infinite, a priori.

Exercise 2.23 (!). Let division with remainder be defined in a ring R. Suppose that Euclid's algorithm applied to a pair $x, y \in R$ stopped in some finite number of steps and returned $z \in R$. Prove that

a. $z = ax + by$ for some $a, b \in R$.

b. z is the greatest common divisor of x and y.

Hint. Proof for the arbitrary ring is the same as in the case of ring of natural numbers.

Definition 2.10. Let R be a ring. It is said that **there exists a Euclid's algorithm in** R or that R **is Euclidean** if division with remainder is defined in R and for all $x, y \in R$ Euclid's algorithm stops in finite number of steps.

Exercise 2.24 (!). Let there exists a prime multipliers decomposition and an Euclid's algorithm in a ring R. Prove that R is a unique factorization ring.

Hint. Use the previous problems.

Exercise 2.25. Prove that the ring $k[t]$ of polynomials over a field k.

Exercise 2.26. Prove that an equation $x \cdot y = 0$ has a solution (for $x, y \neq 0$) in $k[t] \mod P$ if and only if a polynomial P is irreducible.

The integer part $[z]$ of a complex number $z = x + y\sqrt{-1}$ is defined as $[x + 0.5] + [y + 0.5]\sqrt{-1}$ where $[\ ]$ denotes an operation of taking an integer part of a real number (if one interprets complex numbers as points on a plane $\mathbb{R}^2$ then $[z]$ is a point with integer coordinates closest to z). Division with remainder in the ring of Gauss integers $\mathbb{Z}[\sqrt{-1}\,]$ is defined as follows: the factor of z_1 and z_2 equals $[\frac{z_1}{z_2}]$ and the remainder equals $z_1 - [\frac{z_1}{z_2}]z_2$.

Exercise 2.27. Prove that $\left| z_1 - \left[\frac{z_1}{z_2}\right] z_2 \right| < |z_2|$.

Exercise 2.28. Prove that in the ring of Gauss integers $\mathbb{Z}[\sqrt{-1}\,]$ Euclid's algorithm always terminates.

Hint. Use the previous problem. Deduce that with every step of the Euclid's algorithm a quantity $\min(|z_1|^2, |z_2|^2)$ decreases.

Let $R = \mathbb{Z}[\sqrt{-n}]$ or $R = \widetilde{\mathbb{Z}[\sqrt{-3}]}$. For any $z \in \mathbb{C}$ let us denote by $[z]_R$ a point of a complex plane corresponding to point from R closest to z. If there are several such points let us take a point with greatest $Re[z]_R$, if still there are several such points, let us take one with the greatest $Im[z]_R$. Define the division of z_1 by z_2 with remainder in such a way that the factor of z_1 and z_2 is $[\frac{z_1}{z_2}]_R$ and the remainder is $z_1 - [\frac{z_1}{z_2}]_R z_2$.

Exercise 2.29 (*). Prove that if $n = 1$ then it is the usual division with remainder in $\mathbb{Z}[\sqrt{-1}\,]$

Exercise 2.30 (*). Let $|z - [z]_R| < 1$ for all $z \in \mathbb{C}$. Prove that with every step of the Euclid's algorithm a quantity $|z_2|^2$ decreases.

Exercise 2.31 (*). Let for any point $z \in \mathbb{C}$ there exist $r \in R$ such that $|r - z| < 1$. Prove that R is Euclidean.

Exercise 2.32 (*). Prove that the following rings are Euclidean: $\mathbb{Z}[\sqrt{-2}]$, $\widetilde{\mathbb{Z}[\sqrt{-3}]}$.

Exercise 2.33. Decompose the number 2 into prime multipliers in $\mathbb{Z}[\sqrt{-1}\,]$.

Hint. Use the problem 2.21.

Exercise 2.34 (*). Decompose the numbers 3, 5, 7 into prime multipliers in $\mathbb{Z}[\sqrt{-1}\,]$.

Exercise 2.35 (*). Prove that a prime number in $\mathbb{Z}$ of the form $p = 4k + 3$ is prime in $\mathbb{Z}[\sqrt{-1}\,]$.

Hint. Prove that p cannot be represented as a sum of squares.

Exercise 2.36. Let $z = a + b\sqrt{-1}$ be a Gauss integer which is not divisible by $1 + \sqrt{-1}$. Suppose that a and b are coprime. Prove that z and $\overline{z}$ are coprime.

Hint. Prove that if a and b are coprime in $\mathbb{Z}$ then 2 can be represented as a linear combination $a+b\sqrt{-1}$, $a-b\sqrt{-1}$.

Exercise 2.37 (!). Let a, b, c be coprime numbers such that $a^2+b^2=c^2$. Prove that $c=|z|^2$ for some $z \in \mathbb{Z}[\sqrt{-1}\,]$.

Hint. Use the fact that $c^2=(a+b\sqrt{-1}\,)(a-b\sqrt{-1}\,)$ and a, b are coprime. Apply the uniqueness of prime multipliers decomposition in $\mathbb{Z}[\sqrt{-1}\,]$ and deduct that every prime multiplier of $a+b\sqrt{-1}$, $a-b\sqrt{-1}$ appears twice in the decomposition.

Exercise 2.38 (!). Find all triples of integer numbers a, b, c such that $a^2+b^2=c^2$ ("find" means "write a formula that gives all such triples when one substitutes its variables with integer numbers").

Hint. Use the previous problem.

Exercise 2.39 (*). Find all triples of coprime numbers a, b, c such that $a^2+2b^2=c^2$.

Exercise 2.40. Use the uniqueness of prime multipliers decomposition in $\mathbb{Z}[\sqrt{-2}]$

Exercise 2.41 (**). Find all triples of coprime numbers a, b, c such that $a^2+3b^2=c^2$.