MATH-F-303 handout 2: ring and fields

Rules: Exam problems would be similar to ones marked with ! sign. It is recommended to solve all unmarked and !-problems or to find the solution online. It's better to do it in order starting from the beginning, because the solutions are often contained in the previous problems. The problems with * are harder, and ** are very hard; don't be disappointed if you can't solve them, but feel free to try. Have fun!

2.1 Rings and fields

Consider some "numbers": real numbers, rational numbers, integer numbers. The "numbers" are equipped with the following algebraic operations:

a. Addition $+$, which is commutative (satisfies $x + y = y + x$) and makes the set of "numbers" into a group.

b. Multiplication, which is associative and commutative, but does not make the set of "numbers" into a group, because not all "numbers" are invertible; it is denoted by a dot, which is often omitted for brevity; one writes $x \cdot y$ or just xy.

Let us axiomatise these structures.

Definition 2.1. Let R be a set, equipped with two operations $R \times R \longrightarrow R$, "addition" $a, b \mapsto a + b$ and "multiplication" $a, b \mapsto a \cdot b$. Fix two elements 1 and 0 in R ("unit" and "zero"). The set $(R, +, \cdot, 1, 0)$ is called **a ring** if the following axioms hold.

a. R is a commutative group with respect to $+$, and 0 is unit in this group structure.

b. 1 is unit with respect to multiplication: $1 \cdot a = a \cdot 1 = a$ for all $a \in R$

c. Multiplication is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

d. Distributivity of multiplication with respect to addition: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

If the multiplication is commutative, we say that the ring R is commutative. Further on in this course, we shall assume commutativity in the rings by default. If, in addition, the multiplication is invertible for all $a \neq 0$, that is, $R \backslash \{0\}$ is a group with respect to multiplication, $(R, +, \cdot, 1, 0)$ is called **a field**.

Definition 2.2. Two rings R, R' are called **isomorphic** if there exists a bijection $j : R \longrightarrow R'$ which is compatible with addition and multiplication. In this case the map j is called **an isomorphism**. An isomorphism from a ring to itself is called **an automorphism**.

Definition 2.3. Subring of a ring R is a subset $R' \subset R$ which is a subgroup with respect to addition, contains 1, and is closed under multiplication.

Remark 2.1. The commutativity of multiplication in rings, and existence of unit, are assumed in these lectures, but the terminology might vary: everything depends on which domain of mathematics you operate with. Even associativity of multiplication might be dropped sometimes.

Exercise 2.1. Consider the following sets, equipped with standard operations of addition and multiplication. Check if they satisfy the ring axioms.

a. Integer numbers

b. Even integers

c. Rational numbers

d. Irrational real numbers

e. Finite decimal fractions

f. Pairs of integers, addition and multiplication pairwise.

g. Pairs of integers, addition pairwise, multiplication given by the formula $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$.

h. Pairs of integers, addition pairwise, multiplication given by the formula $(a,b)\cdot(c,d) = (ac+2bd, ad+bc)$.

i. Subsets of a set M, with addition given by symmetric difference, $A+B := (A\cup B)\backslash(A\cap B)$, multiplication $A\cdot B := A\cap B$.

j. Maps from a fixed set S to a fixed ring A, with operations $(f\cdot g)(s) := f(s)g(s)$, $(f+g)(s) := f(s)+g(s)$,

Exercise 2.2. Which rings considered in Exercise 2.1 are also fields?

Exercise 2.3. Let R be a ring. Consider the set of sequences

$$a = (a_0, a_1, \dots, a_i, \dots, 0, 0, \dots)$$

of elements $a_i \in R$ with finitely many non-zero elements. Define operations on this set as

$$(a+b)_i = a_i + b_i,$$
$$(a\cdots b)_i = \sum_{l+m=i} a_m b_l.$$

Prove that this set is a ring (in particular, prove associativity of multiplication).

Definition 2.4. The ring defined in Exercise 2.3 is called **polynomial ring of one variable** and denoted $R[x]$. Its elements are called “polynomials”. They are written as $a_0 + a_1x + \dots + a_nx^n$. Multiplication of two polynomials of form $P(x) = a_0 + a_1x + \dots + a_nx^n$ and $Q(x) = b_0 + b_1x + \dots + b_nx^n$ is given by $P(x)Q(x) = \sum_{i,j} a_ib_jx^{i+j}$.

Exercise 2.4. Fix an integer number $n > 1$. Division with remainders modulo n gives remainders 0, 1, 2, ... $n-1$. If two integer numbers have the same remainders modulo n, we write $a = b \mod n$. These numbers are called “equal modulo n”. We define addition and multiplication on the set of remainders $\mod n$ in such a way that

$$(x \mod n) + (y \mod n) = ((x+y) \mod n),$$
$$(x \mod n)\cdot(y \mod n) = (xy \mod n)$$

Prove that this definition is unambiguous, and the set of remainders is a ring.

Definition 2.5. The ring of reminders modulo n is denoted as $\mathbb{Z}/n\mathbb{Z}$.

Exercise 2.5 (!). Prove that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Hint. Use Euclidean algorithm (see below).

Exercise 2.6. Construct fields of

a. 2

b. 3

c. (*) 4 elements.

Exercise 2.7 (*). Prove that there is no field of 6 elements.

Definition 2.6. **Zero divisors** in a ring R are two non-zero elements $x, y \in R$ such that $xy = 0$.

Exercise 2.8. Let R be a finite ring without zero divisors. Prove that R is a field.

Exercise 2.9. Let p be a prime. Prove that a ring of p elements is unique up to an isomorphism.

Definition 2.7. Recall that **order** of an element g of a group is the number of elements in the subgroup $\{e, g, g^{-1}, g^2, g^{-2}, g^3 ...\}$ generated by g. **Characteristic** of a field k is 0 if $1 \in k$ has infinite order, and order of 1 in the additive group of k if 1 has finite order.

Exercise 2.10. Let p be a characteristic of a field k. Prove that p is prime or 0.

Exercise 2.11 (*). Let k be a field of characteristic p. Prove that the **Frobenius map** $x \mapsto x^p$ preserves addition and multiplication.

Definition 2.8. Let $P(t) \in R[x]$ be a polynomial over a ring R, $P = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ **Root** of $P(x)$ is $r \in R$ such that $P(r) = a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r + a_0 = 0$.

Definition 2.9. Let $a, b \in R$ be elements of a ring. We say that a **is divisible by** b of $a = bc$ for some $c \in R$.

Exercise 2.12 (!). Let α be a root of a polynomial $P(t)$ in $k[t]$. Prove that $P(t)$ is divisible by $t - \alpha \in k[t]$.

Hint. Use the long division of polynolials:

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

Exercise 2.13 (!). (Bézout theorem)
Prove that a non-zero polynomial over a field cannot have more than n different roots.

Hint. Use the previous exercise.

Exercise 2.14. Using long division of polynomials, consider **the set of remainders in** $k[x]$ **modulo** $P(x) \in k[x]$**,** denoted as $k[x] \mod k(x)$ Prove that it is a ring.

2.2 Complex numbers

Definition 2.10. The field of real numbers is denoted by $\mathbb{R}$, the ring of integers is $\mathbb{Z}$. Let $\mathbb{C}$ be the set of pairs of real numbers $(a,b) \in \mathbb{R}^2$, with addition $(a,b)+(c,d)=(a+c,b+d)$ and multiplication

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc).$$

Elements of $\mathbb{C}$ are called **complex numbers**.

Exercise 2.15 (!). Prove that $\mathbb{C}$ is a ring which is isomorphic to $\mathbb{R}[x] \mod P(x)$, where $P(x)=x^2+1$.

Exercise 2.16. Prove that an equation $x^2+1=0$ has precisely 2 solutions in $\mathbb{C}$.

Exercise 2.17. Choose a solution of $x^2+1=0$, and denote it by $\sqrt{-1}$. Prove that any complex number can be unambiguously expressed as $z=a+b\sqrt{-1}$.

Exercise 2.18. Let $z=a+b\sqrt{-1}$ be a complex number. Its **complex conjugate** is $\bar{z}:=a-b\sqrt{-1}$. Prove that the map $z \longrightarrow \bar{z}$ is an isomorphism of the ring $\mathbb{C}$ with itself.

Exercise 2.19. Prove that for any non-zero $z=a+b\sqrt{-1}$, the number $z\bar{z}=a^2+b^2$ is real and invertible.

Definition 2.11. Absolute value $|z|$ of a complex number is $|z|:=\sqrt{z\bar{z}}$.

Exercise 2.20. Let $z':=\bar{z}|z|^{-2}$. Prove that $zz'=1$.

Remark 2.2. This implies that $\mathbb{C}$ is a field.

Exercise 2.21 (!). Prove that $|z_1|-|z_2| \leqslant |z_1-z_2| \leqslant |z_1|+|z_2|$ for any $z_1,z_2 \in \mathbb{C}$.

Exercise 2.22. Prove that $|z_1z_2|=|z_1||z_2|$.

Exercise 2.23 (!). Let z be a complex number satisfying $|z|=1$. We identify $\mathbb{C}$ with the complex plane $\mathbb{R}^2$ in the standard way. Consider the map $t \longrightarrow zt$ as a map from $\mathbb{R}^2$ to $\mathbb{R}^2$. Prove that it is a rotation of angle ϕ, where ϕ satisfies $z=\cos\phi+\sqrt{-1}\sin\phi$.

Exercise 2.24. Find all automorphisms of $\mathbb{C}$ which act as identity on $\mathbb{R}\subset\mathbb{C}$.

Exercise 2.25 (!). In the definition of complex numbers, replace

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc).$$

by

$$(a,b)\cdot(c,d)=(ac+bd,ad+bc).$$

a. Prove that this is a ring.

b. Denote this ring by $\mathbb{R}_2$. Find all solutions of $z^2=1$ in $\mathbb{R}_2$.

c. Find all solutions of $z^2=0$ in $\mathbb{R}_2$.

d. Find zero divisors in $\mathbb{R}_2$.

Exercise 2.26 (!). In the definition of complex numbers, replace

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc).$$

by

$$(a,b)\cdot(c,d)=(ac,ad+bc).$$

a. Prove that this is a ring.

b. Denote this ring by $\mathbb{R}_\varepsilon$. Find all solutions of $z^2=1$ in $\mathbb{R}_2$.

c. Find all solutions of $z^2=0$ in $\mathbb{R}_2$.

Exercise 2.27 (*). For the previous two examples of the rings, find all solutions of the equation $z^2=z$.

2.3 Gaussian integers

Definition 2.12. An element $v\in R$ of a ring is called **invertible** of there exists $w\in R$ such that $vw=1$.

Definition 2.13. Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ are complex numbers of form $x+y\sqrt{-1}$.

Exercise 2.28. Find all invertible elements in the ring of Gaussian integers.

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

Exercise 2.29 (!). Let $n>0$ be a positive integer number, and $\mathbb{Z}[\sqrt{-n}]$ the set of complex numbers of form $x+y\sqrt{-n}$, where $x,y\in\mathbb{Z}$. Prove that it is a subring of complex numbers, and find all invertible elements.

Exercise 2.30 (*). Let n be a positive, integer number, and A the set of numbers of form $\frac{x+y\sqrt{-n}}{2}$, where both x,y are even or odd. Assume that $n=3 \mod 4$. Prove that A is a subring of complex numbers. Find all invertible elements in A.

2.4 Divisibility and primes

Definition 2.14. Let $x,y\in R$ be elements of a ring. **Greatest common divisor** $\mathsf{GCD}(a,b)$ is $z\in R$ such that x and y are divisible by z, and for any z' such that x and y are divisible by z', z is also divisible by z'. **Lowest common denominator** $\mathsf{LCD}(a,b)$ is $a\in R$ which is divisible by x and y, and for any a' divisible by x and y, a' is divisible by a.

Remark 2.3. A caution: in arbitrary rings, GCDs and LCDs do not always exist.

Definition 2.15. An element $p\in R$ of a ring is called **prime** if for any q such that $p=qu$, either q or u is invertible.

Exercise 2.31. Prove that if $\mathsf{GCD}(a,b)$ or $\mathsf{LCD}(a,b)$ exists, it is exists up to an invertible elements: if z,z' are both $\mathsf{GCD}(a,b)$ or $\mathsf{LCD}(a,b)$, then $z=z'u$, where u is invertible.

Exercise 2.32. Let $\mathbb{Q}(2)$ be the set of all rational numbers represented by the fractions $\frac{p}{q}$ with odd q. Prove that it is a subring of rationals.

Exercise 2.33. Describe all invertible elements in $\mathbb{Q}(2)$.

Exercise 2.34. Describe all non-invertible primes in $\mathbb{Q}(2)$.

Exercise 2.35. Prove that $\mathbb{Q}(2)$ contains greatest common divisor and lowest common denominator of any two elements.

2.5 Prime decomposition and Euclidean algorithm

Definition 2.16. Euclidean algorithm takes two positive integers $x, y \in Z^{>0}$ and produces a positive integer z as follows.

A: If x is divisible by y, algorithm stops and gives y as its result.

B: Otherwise, we return to A: above, with x and y replaced by x_1 and y_1, with $x_1 = y$, $y_1 = x - ky$, where $x - ky$ is a remainder of division x by y.

Exercise 2.36. Prove that algorithm of Euclides finishes its work after a finite number of iterations.

Exercise 2.37. Prove that result of application of Euclidean algorithm to integers x, y can be expressed as $z = ax + by$, where a, b are integers. Prove that z is a divisor of a and b.

Hint. Use induction.

Exercise 2.38. Let x, y be integers, and $z = x - ky$. Prove that if $\mathsf{GCD}(z, y)$ exists, $\mathsf{GCD}(x, y)$ also exists, and $\mathsf{GCD}(x, y) = \mathsf{GCD}(z, y)$.

Exercise 2.39. Prove that the result of application of the Euclidean algorithm is equal to $\mathsf{GCD}(x, y)$.

Hint. Use the previous exercise

Exercise 2.40. Let p be a prime integer. Prove that all non-zero remainders modulo p are invertible.

Hint. Let y is not divisible by p. Using the algorithm of Euclides, solve an equation $1 = pa + yb$, where a, b are integers.

Exercise 2.41. Let x, y be integers without non-trivial common denominators, and p a prime. Suppose that xy is divisible by p^α for some integer $\alpha > 0$. Prove that either x is divisible by p^α or y divisible by p^α.

Hint. Use the previous exercise.

Exercise 2.42 (!). Deduce the uniqueness of prime decomposition: if x is represented as a product of primes in two different ways, these two different ways are different only by the order of prime multipliers.

Hint. Use the previous exercise.