Глава 1

Въведение

1.1 Множества и изображения.

1.1.1 Множества и операции с тях

Целта на този параграф е не да представи аксиоматичното изграждане на теория на множествата, а да запознае читателя с основни понятия и свойства касаещи множествата, от които ще имаме нужда по-нататък в курса по линейна алгебра и аналитична геометрия.

Понятието ***множество*** е базисно понятие и не се дефинира подобно на точка и права в геометрията. Ползваме го, когато разглеждаме няколко обекта, наричани ***елементи*** на множество. Например множеството на студентите в аудиторията, симпатизантите на спортен клуб, сградите в един град и други такива. Множествата ще бележим с главни букви, а техните елементи обикновено с малки букви. Ако множеството се състои от краен брой елементи го наричаме ***крайно***, а ако има безброй елементи - ***безкрайно***. Например множеството на целите числа $\mathbb{Z}$ е безкрайно.

Едно множество може да зададем като изредим неговите елементи или като ги опишем с някакво тяхно свойство. Например

$$A = \{1, 2, 3, 4, 5, 6, 7\} = \{n \mid n \text{ е естествено число ненадминаващо } 7\ \}.$$

Празно множество ще наричаме множеството без елементи. Бележим го със символа $\emptyset$. (То е математическа абстракция на липсата на много неща, с която се сблъскваме ежедневно!)

Фактът, че a е елемент (т.е. принадлежи) на множеството A бележим с $a \in A$, съответно $a \notin A$, когато не принадлежи. Ако всички елементи на множеството B са елементи и на A, казваме, че B е ***подмножество*** на

A и бележим с $B \subseteq A$ или $B \subset A$, когато искаме да подчертаем, че B се съдържа строго в A.

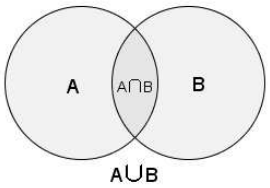
Под понятието ***мощност*** на множеството A, която бележим с $|A|$, се разбира броят на елементите на A, ако то е крайно или символът ∞, ако е безкрайно множество. Мощността на празното множество е нула.

Обединение на множества:

$$A \cup B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ или } x \in B\}.$$

В сила са следните свойства:

1) $A \cup A = A$; 2) $A \cup B = B \cup A$;
3) $A \cup (B \cup C) = (A \cup B) \cup C$; 4) $A \cup \emptyset = A$.



Фигура 1.1: Обединение и сечение на множествата A и B.

Сечение на множества:

$$A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ и } x \in B\}.$$

В сила са следните свойства:

1) $A \cap A = A$; 2) $A \cap B = B \cap A$;
3) $A \cap (B \cap C) = (A \cap B) \cap C$; 4) $A \cap \emptyset = \emptyset$;
5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; 6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
7) $A \cap (A \cup B) = A \cup (A \cap B) = A$;
8) $A \cup (B \cap C) = (A \cup B) \cap C$, ако $A \subseteq C$.

Допълнение на множество:

$$\overline{A} \stackrel{\text{def}}{=} \{x \in A \mid x \notin B\}.$$

Разлика на множества:

$$A \setminus B \stackrel{\text{def}}{=} \{x \mid x \notin A\}.$$

В сила е $A \setminus B = A \cap \overline{B}$.

Дефиниция 1.1.1 ***Декартово произведение*** *на множествата* $A_1, A_2, \ldots, A_k$ *наричаме съвкупността от всички наредени* k*-орки, т.е.*

$$\prod_{i=1}^{k} A_i = A_1 \times A_2 \times \ldots \times A_k \stackrel{\text{def}}{=} \{(a_1, a_2, \ldots, a_k) \mid a_i \in A_i,\ i = 1, \ldots, k\}$$

Твърдение 1.1.2 *Ако* $|A_i| < \infty$ *,*$i = 1, \ldots, k$*, то*

$$\left|\prod_{i=1}^{k} A_i\right| = \prod_{i=1}^{k} |A_i|.$$

Доказателство. С индукция по броя на множествата k. При $k = 1$ твърдението е очевидно вярно. Да предположим, че е вярно за $k - 1$. Ще го докажем и за k.
Да фиксираме произволен символ $a_k \in A_k$ и да разгледаме всички наредени k-орки с последен символ равен на a_k. Първите $k - 1$ символа във всяка наредена k-орка представляват елемент на $\prod_{i=1}^{k-1} A_i$. Следователно, съгласно индукционното допускане броят на k-орките с последен елемент a_k е $\prod_{i=1}^{k-1} |A_i|$. Тъй като за a_k имаме $|A_k|$ възможности, то общият брой на k-орките е $\prod_{i=1}^{k-1} |A_i|.|A_k|$.

1.1.2 Изображения

Дефиниция 1.1.3 *Нека* A *и* B *са две множества. Казваме, че е зададено* ***изображение*** φ ***на множеството*** A ***в множеството*** B*, когато е дадено правило, по което на всеки елемент* $a \in A$ *се съпоставя точно един елемент* $b \in B$*. Бележим* $\varphi : A \longrightarrow B$, $A \xrightarrow{\varphi} B$, *или* $b = \varphi(a)$*. Множеството* A *се нарича* ***дефиниционна област*** *на* φ*, елементът* b *-* ***образ*** *на* a*, и* a *съответно* ***първообраз*** *на* b

Терминът ***функция*** е синоним на изображение, но ние ще го използваме главно за изображения на числови множества, т.е. когато A и B са числови множества.
Образ на φ наричаме подмножеството $\operatorname{Im}\varphi$ на B състоящо се от образите на всички елементи на A при действието на φ, т.е.

$$\operatorname{Im}\varphi \ = \ \{\varphi(a) \mid a \in A\}.$$

Две изображения $\varphi : A \longrightarrow B$ и $\psi : C \longrightarrow D$ считаме ***равни (съвпадащи)***, когато $A \equiv C$ и $\varphi(a) = \psi(a)$ за всяка $a \in A$.

Дефиниция 1.1.4 *Нека $C \subset A$. Казваме, че изображението $\psi : C \longrightarrow B$ е* ***ограничение (рестрикция)*** *на $\varphi : A \longrightarrow B$, ако*

Пример 1.1.1 Нека X е произволно множество. Изображение $\mathcal{E}_X$ на X в себе си зададено с правилото $\mathcal{E}_X(x) = x$ за всяко $x \in X$. Това изображение се нарича ***единично (тъждествено) изображение на*** X.

Пример 1.1.2 Изображение f на множеството на естествените числа $\mathbb{N}$ в множеството $E = \{-1, 1\}$ зададено с правилото $f(n) = (-1)^n$.

Пример 1.1.3 Нека $A = \{1, 2, 3\}$ и $B = \{1, 7, 15, 19\}$. Изображение $\varphi : A \longrightarrow B$ на зададено с правилото $\varphi(1) = 1,\ \varphi(2) = 7,\ \varphi(3) = 19$.

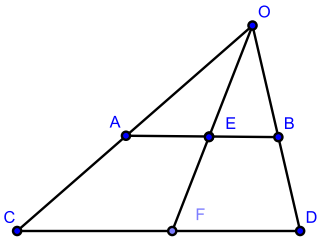
Дефиниция 1.1.5 *Изображението $\varphi : A \longrightarrow B$ се нарича* ***изображение върху (сюрекция)****, ако всеки елемент от B има първообраз, т.е. ако $Im\,\varphi = \varphi(A) = B$.*

Сюрекция е изображението от Пример 1.1.2.

Дефиниция 1.1.6 *Изображението $\varphi : A \longrightarrow B$ се нарича* ***инекция (инективно)****, ако различните елементи отиват в различни, т.е. от $x \neq y$ следва $\varphi(x) \neq \varphi(y)$.*

Инективно е изображението от Пример 1.1.3.

Дефиниция 1.1.7 *Изображение, което е едновременно инективно и сюрективно се нарича* ***биекция (взаимно-еднозначно)****, т.е. $\varphi : A \longrightarrow B$ е биективно, когато всеки елемент на B има и то единствен първообраз.*



Фигура 1.2: Пример на взаимно-еднозначно изображение.

Пример 1.1.4 Пример на взаимно-еднозначно изображение е изображението на отсечката AB върху отсечката CD съпоставящо на точката E точката F посредством правата OE (виж фигура 1.2)

Дефиниция 1.1.8 ***Композиция (произведение)*** *на изображенията* $\varphi : A \longrightarrow B$ *и* $\psi : B \longrightarrow C$ *наричаме изображението* $\eta : A \longrightarrow C$ *зададено с* $x \neq y$ *следва* $\eta(x) = \psi(\varphi(x)),\ x \in A$. *Бележим* $\eta = \psi\varphi$.

Нека $\varphi : A \longrightarrow B$ и $\mathcal{E}_A$ и $\mathcal{E}_B$ са единичните изображения на A и B, съответно. Очевидно $\varphi\mathcal{E}_A = \mathcal{E}_B\varphi = \varphi$.

Твърдение 1.1.9 *Композицията на две изображения е асоциативна, т.е., ако* $\varphi : A \longrightarrow B,\quad \psi : B \longrightarrow C$ *и* $\quad \eta : C \longrightarrow D$, *то* $\eta(\psi\varphi) = (\eta\psi)\varphi$.

Доказателство. За всяко $a \in A$ е в сила

$$[\eta(\psi\varphi)](a) = \eta[(\psi\varphi)(a)] = \eta[\psi(\varphi(a)) = [(\eta\psi)\varphi](a).$$

Упражнение 1.1.1 *Докажете, че композицията на биекции е също биекция.*

Дефиниция 1.1.10 *Изображението* $\varphi : A \longrightarrow B$ *се нарича* ***обратимо****, ако съществува изображение* $\psi : B \longrightarrow A$, *такова че* $\psi\varphi = \mathcal{E}_A$ *и* $\varphi\psi = \mathcal{E}_B$. *Изображението* ψ *се нарича* ***обратно изображение*** *на* φ.

Ще отбележим, че ако обратното изображение на φ съществува, то то е единствено. Наистина, нека η и ψ са две обратни изображения на φ, т.е. $\psi\varphi = \mathcal{E}_A$ и $\varphi\psi = \mathcal{E}_B$. Тогава

$$\psi = \psi\mathcal{E}_B = \psi(\varphi\eta) = (\psi\varphi)\eta = \mathcal{E}_A\eta = \eta.$$

Единственото обратно изображение на φ (ако съществува) ще бележим с φ^{-1}.

Твърдение 1.1.11 *Едно изображение е обратимо тогава и само тогава, когато е взаимно-еднозначно.*

Доказателство. *Необходимост.* Нека $\varphi : A \longrightarrow B$ е обратимо, т.е. съществува $\psi : B \longrightarrow A$, такова че $\psi\varphi = \mathcal{E}_A$ и $\varphi\psi = \mathcal{E}_B$. От $\psi\varphi = \mathcal{E}_A$ следва, че φ е инекция, а ψ сюрекция. Наистина предположението $\varphi(a_1) = \varphi(a_2),\ a_1, a_2 \in A$ влече

$$a_1 = \mathcal{E}_A(a_1) = \psi\varphi(a_1) = \psi\varphi(a_2) = \mathcal{E}_A(a_2) = a_2.$$

Също така за всяко $a \in A$ имаме $\psi(\varphi(a)) = (\psi\varphi)(a) = \mathcal{E}_A(a) = a$, т.е. $\varphi(a) \in B$ е първообраз на a.

Аналогично от $\varphi\psi = \mathcal{E}_B$ следва, че φ е сюрекция, а ψ инекция. Следователно φ и ψ са биекции.

Достатъчност. Нека φ е биекция. Тогава за всяко $b \in B$ съществува и то единствено $a \in A$, такова че $b = \varphi(a)$. Разглеждаме изображението $\psi : B \longrightarrow A$, което съпоставя на b елемента a, където $b = \varphi(a)$. Тогава ψ е обратно на φ изображение, тъй като $(\psi\varphi)(a) = \psi(\varphi(a)) = \psi(b) = a$ и $(\varphi\psi)(b) = \varphi(\psi(b)) = \varphi(a) = b$, т.е. $\psi\varphi = \mathcal{E}_A$ и $\varphi\psi = \mathcal{E}_B$.

1.2 Комплексни числа. Числови полета.

В историческото развитие на човешката цивилизация понятието ***число*** се е променяло и разширявало. Може да кажем, че целите числа съпътстват човечеството от най-дълбоко древност. В можеството $\mathbb{Z}$ на целите числа (наричано ***пръстен на целите числа***) за всеки два елемента са възможни три аритметични операции - събиране, изваждане и умножение, но не винаги можем да разделим на ненулево число (деление на 0 разбира се е невъзможно). Това неудобство е довело твърде скоро до появата на рационалните числа $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b > 0\}$ (a и b считаме взаимнопрости: $(a, b) = 1$). Символът $\frac{a}{b}$ означава a на брой една b-та части. В ***полето на рационалните числа*** (както се нарича съвкупността на рационалните числа) вече можем и да делим на произволен ненулев елемент.

Нуждата да се извлича квадратен корен (и по-общо да се решават уравнения от вида $x^n = a$) в резултат на икономическото и технологично развитие е довела до ***полето на реалните числа*** $\mathbb{R}$. Реалните числа се представят с точките от права (наричана ***реална ос***), в която е фиксирана точка съответстваща на нулата и е избрана посока на нарастване на числата. Изказано по строго, съществува взаимно-еднозначно съответствие между реалните числа и точките от една права.

Реалните числа служат добре на практиката, но остава един математически проблем - уравнението $x^2 = -1$ (и безброй още уравнения) нямат решение. Затова полето на реалните числа се разширява до ***полето на комплексните числа*** $\mathbb{C}$, където, както ще видим в следващия параграф, този проблем вече не съществува.

Да припомним, че за произволни реални числа a, b, c са в сила следните свойства:

1. $a + b = b + a$,

2. $(a+b)+c = a+(b+c)$,
3. $a+0 = a$,
4. $a+(-a) = 0$,
5. $ab = ba$,
6. $(ab)c = a(bc)$,
7. $a(b+c) = ab+ac$,
8. $1 \cdot a = a$
9. ако $a \neq 0$, то съществува единствено a^{-1} : $aa^{-1} = 1$
10. $0 \cdot a = 0$ и $(-1) \cdot a = -a$.

Разширявайки $\mathbb{R}$ до полето на комплексните числа ще искаме тези свойства да останат в сила и за новото множество като при това уравнението $x^2 = -1$ да има решение. За целта да разгледаме съвкупността от всички наредени двойки реални числа, т.е.

$$\mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}.$$

$\mathbb{R}$ ще отъждествяваме с подмножеството $(\mathbb{R},0) = \{(a,0) \mid a \in \mathbb{R}\}$, т.е. $\mathbb{R} \subset \mathbb{R}^2$. Въвеждаме операциите събиране, изваждане и умножение по следния начин:

$$\begin{aligned} (a,b) \pm (c,d) &= (a \pm c, b \pm d), \\ (a,b) \cdot (c,d) &= (ac - bd,\ ad + bc) \end{aligned} \tag{1.2.1}$$

Лесно се проверява, че при така дефинираните операции в $\mathbb{R}^2$ всички свойства от 1 до 8 и 10 са в сила. Изпълнено е и

$$(a,0) \cdot (b,0) = (ab,0), \quad (a,0) \pm (b,0) = (a \pm b,\ 0),$$

т.е. ново-дефинираните операции съвпадат върху $\mathbb{R}$ с неговите операции. Проверката на свойство 9 ще направим по-долу. Сега да забележим, че

$$(0,1)^2 = (0,1) \cdot (0,1) = (-1,0).$$

Следователно елементът $i = (0,1)$ удовлетворява $i^2 = -1$. Очевидно и $-i = (0,-1)$ е също корен на $x^2 = -1$.

Дефиниция 1.2.1 *Множеството* $\mathbb{R}^2$ *с въведените чрез (1.2.1) операции се нарича* **поле на комплексните числа** *и бележим с* $\mathbb{C}$.

Тъй като

$$b.i = (b,0)\cdot(0,1) = (0,b),$$

то в сила е

$$a + b.i = (a,0) + (0,b) = (a,b)$$

и затова оттук нататък ще ползваме $a + b.i$ за означаване на комплексните числа вместо наредената двойка (a,b).

При това означение равенствата (1.2.1) добиват вида

$$\begin{aligned} (a+bi) \pm (c+di) &= (a \pm c) + (b \pm d)i, \\ (a+bi).(c+di) &= (ac-bd) + (ad+bc)i \end{aligned} \tag{1.2.2}$$

Реалните числа a и b се наричат съответно ***реална*** и ***имагинерна*** част на $z = a + bi$. Бележим с $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$.

Да дефинираме ***модул (норма)*** на комплексното число $z = a+bi$ като положителното реално число

$$|z| \stackrel{\text{def}}{=} \sqrt{a^2+b^2}.$$

Очевидно $z = 0$ тогава и само тогава, когато $|z| = 0$.

За всеки две комплексни числа $z_1 = a + bi$ и $z_2 = c + di$ е в сила

$$|z_1 z_2|^2 = (ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2) = |z_1|^2|z_2|^2.$$

Следователно

$$|z_1 z_2| = |z_1||z_2|. \tag{1.2.3}$$

В частност получаваме, че

$$z_1 z_2 = 0 \qquad \Longrightarrow \qquad z_1 = 0 \ \text{ или } \ z_2 = 0.$$

Сега да проверим, че свойство 9 е в сила, което по същество означава, че в $\mathbb{C}$ можем да извършваме операцията деление. Наистина, нека $z = a+bi \neq 0$ и

$$z_1 = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} = \frac{1}{a^2+b^2}(a-bi) = \frac{a-bi}{|z|^2}.$$

Тогава

$$z_1 z = z z_1 = \frac{1}{a^2+b^2}(a+bi)(a-bi) = \frac{1}{a^2+b^2}(a^2+b^2) = 1.$$

Ако предположим, че съществува z_2 със същото свойство, то $z(z_1 - z_2) = 0$, откъдето $z_1 = z_2$.

Дефиниция 1.2.2 *Еднозначно определеното число*

$$z^{-1} = \frac{a - bi}{|z|^2} = \frac{a - bi}{a^2 + b^2}$$

със свойството $zz^{-1} = z^{-1}z = 1$ *се нарича* ***обратно (реципрочно)*** *число на* z

Произведението $z_1^{-1}z_2$ е решение на уравнението $z_1 x = z_2$ и обратно всяко решение на това уравнение има вида $x = z_1^{-1}z_2$. Това решение се нарича ***частно*** от делението на z_2 на z_1.

Числото

$$\overline{z} = a - b\,i$$

се нарича ***комплексно спрегнато*** на $z = a + b\,i$ и е в сила

$$z\overline{z} = |z|^2 \qquad \text{и} \qquad z^{-1} = \frac{\overline{z}}{|z|^2}.$$

Числата z и $\overline{z}$ са корените на квадратното уравнение

$$X^2 - 2aX + |z|^2 = 0. \tag{1.2.4}$$

Представянето на комплексните числа във вида $z = a + b\,i$, където $a, b \in \mathbb{R}$, се нарича ***алгебричен вид*** на комплексните числа за разлика от така наречения ***геометричен вид***. Последният е представяне на комплексните числа основаващо се на интерпретацията им като точки в равнината.

Да разгледаме равнината със зададена в нея правоъгълна координатна система Oxy. На всяка точка от равнината Z съответстват двойка координати (a, b). Дефинираме взаимно-еднозначно съответствие между точките в равнината и комплексните числа като на точката Z съпоставяме комплексното число $z = a + b\,i$. Питагоровата теорема ни дава, че

$$r = |OZ| = \sqrt{a^2 + b^2} = |z|.$$

Ако означим с φ ъгълът от оста Ox до OZ мерен в посока обратна на движението на часовниковата стрелка, то

$$a = r\cos\varphi, \qquad \text{и} \qquad b = r\sin\varphi.$$

Следователно

$$z = a + b\,i = r(\cos\varphi + i\,\sin\varphi). \tag{1.2.5}$$

Представянето на комплексните числа във вида зададен с уравнение (1.2.5) се нарича геометричен вид на z. Ъгълът φ се нарича ***аргумент*** на z, а $r = |z|$ - модул. Очевидно

$$\overline{z} = r(\cos\varphi - i\,\sin\varphi) = r(\cos(-\varphi) + i\,\sin(-\varphi)).$$

Твърдение 1.2.3 *Ако* $z_1 = r_1(\cos\varphi_1 + i\,\sin\varphi_1)$ *и* $z_2 = r_1(\cos\varphi_2 + i\,\sin\varphi_2)$, *то*

$$z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\,\sin(\varphi_1 + \varphi_2)) \tag{1.2.6}$$

Доказателство. Доказателството следва от тригонометричните формулите за $\cos(\varphi_1 + \varphi_2)$ и $\sin(\varphi_1 + \varphi_2)$ и правилото за умножение на комплексни числа.

Като следствие получаваме правилото за повдигане на степен:

Твърдение 1.2.4 *Ако* $z = r(\cos\varphi + i\,\sin\varphi)$ *и* n *е естествено число, то*

$$z^n = r^n(\cos(n\varphi) + i\,\sin(n\varphi)). \tag{1.2.7}$$

Твърдение 1.2.5 *Ако* $z = r(\cos\varphi + i\,\sin\varphi)$ *и* n *е естествено число, то уравнението* $x^n = z$ *има точно* n *решения* $u_0, u_1, \ldots, u_{n-1}$, *където*

$$u_k = \sqrt[n]{r}(\cos\frac{2k\pi + \varphi}{n} + i\,\sin\frac{2k\pi + \varphi}{n}), \qquad k = 0, 1, \ldots, n-1. \tag{1.2.8}$$

Доказателство. Свойствата на тригонометричните функции ни дават веднага, че $u_{k+n} = u_k$ за всяка k, а $u_0, u_1, \ldots, u_{n-1}$, са различни помежду си. Освен това формули (1.2.7) ни дават

$$u_k^n = r(\cos(2k\pi + \varphi) + i\,\sin(2k\pi + \varphi)) = z.$$

Но едно уравнение от n-степен има най-много n корена (виж следващия параграф), следователно $u_0, u_1, \ldots, u_{n-1}$ са всички n-ти корени от z.

Следствие 1.2.6 *Всички корени на* $x^n = 1$ *се дават с*

$$\xi_k = \cos\frac{2k\pi}{n} + i\,\sin\frac{2k\pi}{n} \qquad k = 0, 1, \ldots, n-1.$$

Числата $\{\xi_k\}$ се наричат ***n-ти корени на единицата***. Изобразени като точки в равнината те лежат на окръжност с радиус 1 и представляват множеството от върхове на правилен n ъгълник.

Пример 1.2.1 Нека $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Да намерим $\sqrt{z}$.

Модулът на z е $|z| = \frac{1}{4} + \frac{3}{4} = 1$, а аргументът φ се определя като решение на системата от две уравнения

$$\cos\varphi = \frac{1}{2}, \qquad \sin\varphi = \frac{\sqrt{3}}{2}.$$

Следователно

$$\varphi = \frac{\pi}{3} \quad \text{и} \quad z = \cos\frac{\pi}{3} + i\,\sin\frac{\pi}{3}.$$

Съгласно (1.2.8) квадратните корени от z са

$$\begin{aligned} u_0 &= \cos\frac{\pi}{6} + i\,\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i \\ u_1 &= \cos\frac{7\pi}{6} + i\,\sin\frac{7\pi}{6} = -\frac{\sqrt{3}}{2} - \frac{1}{2}i = -u_0 \end{aligned}$$

Дефиниция 1.2.7 ***Числово поле*** *наричаме всяко подмножество на комплексните числа, което е затворено относно четирите аритметични операции, т.е. сумата, разликата, произведението и частното на всеки два негови елемента принадлежи на същото подмножество.*

Очевидно Q, $\mathbb{R}$ и $\mathbb{C}$ са числови полета. Но такова е и

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Упражнение 1.2.1 *Покажете, че $\mathbb{Q}(\sqrt{2})$ е числово поле.*

1.3 Полиноми над числово поле.

Строгото математическо изграждане на пръстена от полиномите на една променлива излиза извън целите и рамката на настоящия курс. Затова ще ги въведем по начин макар и не много логически издържан, но близък до този използван в средното училище и интуитивно по ясен.

Нека $\mathbb{F}$ е числово поле. Формални произведения от вида

$$a.\underbrace{x.x\ldots x}_{n} = ax^n,$$

където $a \in \mathbb{F}$, а x е символ (буква) се наричат ***едночлени*** на ***независимата променлива*** x. Естественото число n се нарича *степен* на едночлена. Всяко число $a \in \mathbb{F}$ го отъждествяваме с едночлен от нулева степен: $a = ax^0$. Два едночлена от вида ax^n и bx^n наричаме ***подобни*** и дефинираме сума (разлика) на два подобни едночлена по правилото $ax^n \pm bx^n = (a \pm b)x^n$. Под произведение на едночлените ax^n и bx^m разбираме едночлена abx^{n+m} от степен $n + m$.

Сумите (формални) $a(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ от едночлени на независимата променлива x се наричат ***полиноми (многочлени) на независимата променлива*** x. Ако $a_0 \neq 0$, то казваме, че полиномът е от степен $\deg a(x) = n$. В противния случай казваме, че $a(x)$ е с формална степен n.

Продължаваме операциите мужду едночлените до операции между полиноми, така че да са изпълнени дистрибутивният, асоциативният и комутативният закони, т.е. ако $a(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ и $b(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$, то

$$a(x) \pm b(x) \stackrel{\text{def}}{=} (a_0 \pm b_0)x^n + (a_1 \pm b_1)x^{n-1} + \cdots + (a_{n-1} \pm b_{n-1})x + (a_n \pm b_n)$$

Аналогично, искаме резултатът от умножението на два полинома да съвпада с това, което се получава като разкрием скобите и приведем подобните членове. Следователно произведението на два полинома $a(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ и $b(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$, трябва да се дефинира като полином

$$c(x) = a(x)b(x) = c_0x^{m+n} + c_1x^{m+n-1} + \cdots + c_{n+m-1}x + c_{n+m},$$

където

$$\begin{aligned}
c_0 &= a_0b_0 \\
c_1 &= a_0b_1 + a_1b_0 \\
&\cdots \\
c_k &= a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 \qquad \text{(коефициентът пред } x^{n-k}\text{)} \\
&\cdots \\
c_{n+m-1} &= a_{n-1}b_m + a_nb_{m-1} \\
c_{n+m} &= a_nb_m
\end{aligned}$$

При пресмятането на c_k стойностите на a_i и b_j считаме нули, ако $i > n$, съответно $j > m$.

Така въведената съвкупност от полиноми с коефициенти от $\mathbb{F}$ се нарича ***пръстен от полиномите на*** x ***над числовото поле*** $\mathbb{F}$ и бележим с $\mathbb{F}[x]$.

Дефиниция 1.3.1 *Нека* $f(x), g(x) \in \mathbb{F}[x]$. *Казваме, че полиномът* $g(x)$ *дели* $f(x)$, *когато съществува полином* $h(x) \in \mathbb{F}[x]$ *така че е изпълнено* $f(x) = g(x)h(x)$. *Бележим* $g(x) \mid f(x)$.

Твърдение 1.3.2 *За всеки два полинома* $a(x), b(x) \in \mathbb{F}[x]$ *съществуват полиноми* $q(x)$ *и* $r(x)$, *такива че*

$$a(x) = b(x)q(x) + r(x), \qquad r(x) = 0 \text{ или } \deg r(x) < \deg b(x).$$

($q(x)$ *се нарича* ***частно****, а* $r(x)$ *-* ***остатък****.)*

Доказателство. С индукция по степента n на $a(x)$. Нека $b(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$. Ако $n < m$, то полагаме $q(x) = 0$ и $r(x) = a(x)$. Очевидно в този случай $\deg r(x) < \deg b(x)$. Да предположим, че твърдението е вярно за степени на $a(x)$ по-малки от n. Ще го докажем за $\deg a(x) = n$. Полиномът $\frac{a_0}{b_0}x^{n-m}b(x)$ има старши едночлен a_0x^n и съгласно индукционното допускане получаваме

$$a(x) - \frac{a_0}{b_0}x^{n-m}b(x) = a_1'x^{n-1} + \cdots + a_n' = q_1(x)b(x) + r_1(x),$$

където $\deg r_1(x) < \deg b(x)$. Полагайки

$$q(x) = \frac{a_0}{b_0}x^{n-m} + q_1(x) \qquad \text{и} \qquad r(x) = r_1(x)$$

получаваме исканото твърдение.

Дефиниция 1.3.3 *Под стойност на полинома* $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}[x]$ *в точката* $a \in \mathbb{F}$ *разбираме числото*

$$f(a) = a_0a^n + a_1a^{n-1} + \cdots + a_{n-1}a + a_n.$$

Ако $f(a) = 0$, *то казваме че* a *е* ***корен (нула)*** *на* $f(x)$.

Лема 1.3.4 *Числото* $a \in \mathbb{F}$ *е корен на* $f(x) \in \mathbb{F}[x]$ *тогава и само тогава, когато* $(x - a) \mid f(x)$, *т.е.* $f(x) = (x - a)g(x)$.

Доказателство. *Необходимост.* Нека $a \in \mathbb{F}$ е корен. Тогава съгласно Твърдение 1.3.2

$$f(x) = (x-a)g(x) + r, \qquad \deg r < 1.$$

Следователно $r \in \mathbb{F}$ и като заместим $x = a$ получаваме $r = f(a) = 0$.
Достатъчност. Очевидна. Полагаме $x = a$.

Дефиниция 1.3.5 *Казваме, че $a \in \mathbb{F}$ е* ***k-кратен корен*** *на $f(x) \in \mathbb{F}[x]$, ако*

$$f(x) = (x-a)^k g(x), \quad но \quad (x-a)^{k+1} \nmid f(x), \tag{1.3.1}$$

т.е. $g(a) \neq 0$.

Нека $a(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}[x]$ и $c \in \mathbb{F}$, то както видяхме при доказателството на Лема

$$a(x) = (x-c)b(x) + a(c). \tag{1.3.2}$$

Сега ще опишем един ефективен алгоритъм за намиране на стойността $a(c)$ и коефициентите на частното $b(x) = b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}$, който е известен в литературата под името правило на Хорнер

Правило на Хорнер

	a_0	a_1	$\ldots$	a_k	$\ldots$	a_{n-1}	a_n
c	b_0	b_1	$\ldots$	b_k	$\ldots$	b_{n-1}	$a(c)$

където

$$b_0 = a_0,\ b_1 = cb_0 + a_1,\ \ldots,\ b_k = cb_{k-1} + a_k,\ \ldots,\ a(c) = cb_{n-1} + a_n. \tag{1.3.3}$$

Равенства (1.3.3) се получават като в (1.3.2) се разкрият скобите и се приравнят коефициентите пред съответните степени на x от двете страни на равенството.

Твърдение 1.3.6 *Нека $a(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ е полином с цели коефициенти. Ако рационалното число $c = \frac{p}{q}$, $(p,q) = 1$, е корен на $a(x)$, то $p \mid a_n$, а $q \mid a_0$.*

Доказателство. От $a(\frac{p}{q}) = 0$ получаваме равенството

$$a_0p^n + a_1p^{n-1}q + \cdots + a_{n-1}pq^{n-1} + a_nq^n = 0,$$

което дава $p \mid a_nq^n$, съответно $q \mid a_0p^n$. Вземайки предвид, че p и q са взаимнопрости, получаваме $p \mid a_n$ и $q \mid a_0$.

Горното твърдение в съчетание с правилото на Хорнер дава ефективен начин да намираме цели корени на полиноми над $\mathbb{Z}$.

Пример 1.3.1 Като илюстрация на гореказаното да намерим корените на $a(x) = x^4 - x^2 - 12$. Тъй като старшият коефициент е 1, то ако полиномът има рационален корен, то той ще бъде цяло число и дели 12. Следователно трябва да бъде някое от числата $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. Очевидно ± 1 не са корени. Да приложим правилото на Хорнер за $c = 2$.

	1	0	−1	0	−12
2	1	2	3	6	0
−2	1	0	3	0	

След първата проверка получаваме, че 2 е корен и $a(x) = (x-2)(x^3 + 2x^2 + 3x + 6)$. Тъй като всички коефициенти на частното $b(x) = x^3 + 2x^2 + 3x + 6$ са положителни, то очевидно 2 не му е корен, т.е. не е двоен корен на $a(x)$. На следващата стъпка проверяваме дали -2 е корен на $b(x)$. Резултатът е положителен и новото частно е $x^2 + 3$, т.е. $a(x) = (x-2)(x+2)(x^2+3)$.