$G_1/\ker f \cong \operatorname{Im} f$

$G_1 \xrightarrow{f} \operatorname{Im} f \subset G_2$

$\downarrow \quad \nearrow \bar{f}$

$G_1/\ker f$

$SL_n \triangleleft GL_n$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$

$S/_{S \cap I} \cong S+I/_I$

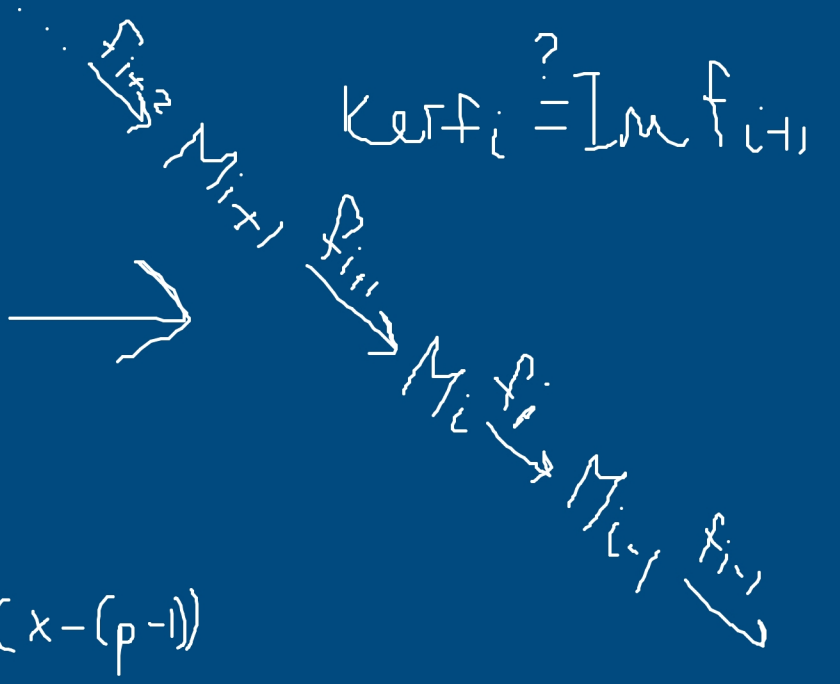
$R/_{I_1} \cong R/_{I_2} \times R/_{I_1}$

$I_1 \subset I_2 \subset I_3 \subset \dots$

$1+1+1+1+1+1+1+1=0$

$M/_K/_{L/K} \cong M/_L$

Abstract Algebra



$f(x) = x(x-1)(x-2)\dots(x-(p-1))$

Зміст

Попередні знання, які необхідні

Перед початком теорії груп наполегливо рекомендується згадати такі предмети:
• більшу частину теорії дискретної математики, як-от: теорія множин, відношень, трошки про відображення, трошки комбінаторики (останнє опціонально, але не завадить ніколи);
• більшу частину теорії чисел, зокрема: вся теорія про подільність, теорія про конгруентні числа, базові відомості про функції Ойлера;
• трошки теорії многочленів (залишив у PDF аналітичної геометрії);
• частину лінійної алгебри, особливо матриці. Для нормального засвоєння розділу 5 дуже бажано мати відомості про векторні простори.
Третє не сильно принципово, оскільки ми покриємо ще раз теорію многочленів уже в загальному представленні. Але просто для простої орієнтації варто пройтися трошки.

1 Теорія груп

У цьому розділі я почну одразу з означення групи, хоча є деякі корисні терміни: алгебраїчна структура, оператив, моноїд тощо. Але основна мета цього розділу – суто робота з групами, тому одразу даю більш розгорнуте означення.

1.1 Означення груп

Definition 1.1.1 Задана G – деяка множина, $*$ – деяка бінарна операція.
Групою назвемо пару $\langle G, * \rangle$, для якої виконуються такі властивості:
I. Замкненість відносно операції:

$$\forall a, b \in G : a * b \in G$$

II. Підпорядкована такими аксіомами:

1) $\forall a, b, c \in G : a * (b * c) = (a * b) * c$ – асоціативність
2) $\exists e \in G : a * e = e * a = a$ – існування нейтрального елементу
3) $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$ – існування оберненого елементу

Example 1.1.2 Розглянемо ось такі приклади груп:

G	$*$	e	a	a^{-1}
$\mathbb{Z}$	$+$	0	n	$-n$
$\mathbb{R} \setminus \{0\}$	$\cdot$	1	r	$\frac{1}{r}$
$\mathrm{Mat}_{n\times n}(\mathbb{R})$	$+$	O	A	$-A$
$\{-1, 1\}$	$\cdot$	1	$1, -1$	$1, -1$

Example 1.1.3 Ось така структура $\langle \mathrm{Mat}_{n\times n}(\mathbb{R}, \cdot \rangle$ уже не буде групою. Тому що для не для всіх матриц $A \in \mathrm{Mat}_{n\times n}$ існує оберненої матриці A^{-1}. Якщо $\det A = 0$, то нема оберненої.

Example 1.1.4 Але тепер розглянемо $\langle GL_n, \cdot \rangle$, де GL_n (general linear group) – множина матриць з $\mathrm{Mat}_{n\times n}(\mathbb{R})$ з ненульовими визначниками. Доведемо, що це утворює групу.
I. Нехай $A, B \in GL_n$, тобто $\det A \neq 0,\ \det B \neq 0$. Тоді звідси випливає, що $\det(AB) = \det A \cdot \det B \neq 0$, а тому звідси $AB \in GL_n$.
II. Перевіримо три аксіоми:
1) Нехай $A, B, C \in GL_n$, тоді звідси $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ (асоціативність кожних трьох матриць виконується із теорії матриць лінійної алгебри).
2) Існує матриця I – одинична матриця, причому $\det I = 1 \neq 0$, а тому $I \in GL_n$ та $A \cdot I = I \cdot A = A$.
3) Нехай $A \in GL_n$, тобто $\det A \neq 0$. Значить, існує $A^{-1} = \dfrac{1}{\det A}\overline{A}$, де $\overline{A}$ – приєднана матриця, для якої $A \cdot A^{-1} = A^{-1} \cdot A = I$.

Proposition 1.1.5 Задана $\langle G, * \rangle$ – група. Тоді виконуються такі пункти:
1) існуючий нейтральний елемент $e \in G$ – єдиний;
2) для кожного елемента $a \in G$ обернений елемент $a^{-1} \in G$ – єдиний.

Proof.
Покажемо виконання кожного пункту від супротивного.

1) !Припустимо, що існують два нейтральних елементи: $e_1, e_2 \in G$. Отримаємо такий ланцюг рівностей:
$e_1 = e_1 * e_2$ та $e_2 = e_1 * e_2$, а тому звідси $e_1 = e_2$.

2) !Припустимо, що для $a \in G$ існують два обернени $a_1^{-1}, a_2^{-1} \in G$. Отримаємо такий ланцюг рівностей:
$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}$.

У двох випадках отримали суперечність! ■

Definition 1.1.6 Задано $\langle G, * \rangle$ – група та $a \in G$. Нехай $n \in \mathbb{Z}$.
Степенем елемента a назвемо наступне:

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ разів}}$$
$$a^{-n} = (a^{-1})^n$$
$$a^0 = e$$

Proposition 1.1.7 Властивості
Задана $\langle G, * \rangle$ – група. Тоді виконуються наступне:
1) рівняння $a * x = b$ має єдиний розв'язок $x = a^{-1} * b$;
2) $a * x = b * x \iff a = b$ (тобто виконується скорочення);
3) $(a * b)^{-1} = b^{-1} * a^{-1}$;
4) $a^{n+m} = a^n * a^m$;
5) $(a^n)^m = a^{nm}$.
Доведення нескладні.

Definition 1.1.8 Задано $\langle G, * \rangle$ – група.
Вона називається **абелевою**, якщо

$$\forall a, b \in G : a * b = b * a \text{ – комутативність}$$

Example 1.1.9 Зокрема $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$, $\langle \{-1, 1\}, \cdot \rangle$ – абелеві групи.

1.2 Деякі інші корисні групи

1.2.1 Групи класів лишків

Розглянемо множину $\mathbb{Z}$ та будь-яке натуральне число $p \in \mathbb{N}$. Задамо відношення еквівалентності:

$$x \sim y \iff x \equiv y \pmod{p}$$

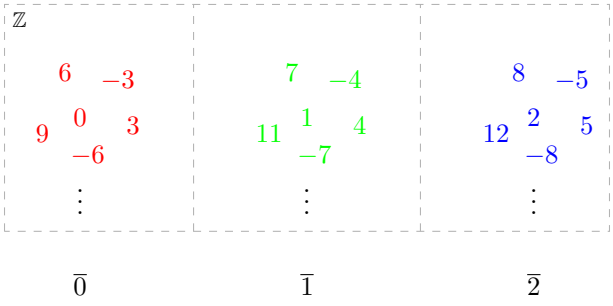
Ми вже її якось встигли профакторизувати ось так (див. дискретку):
$\mathbb{Z}/_{(\mathrm{mod}\ p)} = \{[0],\ [1],\ \ldots,\ [p-1]\}$, де
$[0] = \{\ldots, -2p, -p, 0, p, 2p, \ldots\}$
$[1] = \{\ldots, -2p+1, -p+1, 1, p+1, 2p+1, \ldots\}$
$\vdots$
$[p-1] = \{-p-1, -1, p-1, 2p-1, 3p-1), \ldots\}$.

Зробимо перепозначення $[k] = \overline{k}$, а також $\mathbb{Z}/_{(\mathrm{mod}\ p)} = \mathbb{Z}_p$.

Definition 1.2.1 Отримана фактормножина

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$
$$\overline{k} = \{\ldots, -2p+k, -p+k, k, p+k, 2p+k, \ldots\}$$

називається **класом лишків** за модулем p.



На прикладі проілюстрував множину $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

Theorem 1.2.2 $\langle \mathbb{Z}_p, + \rangle$ – абелева група, де операція визначається таким чином: $\overline{a} + \overline{b} \stackrel{\text{def.}}{=} \overline{a+b}$.

Proof.
Для початку треба з'ясувати, чи є коректно визначеною операція.
Тобто нехай $\overline{a} = \overline{c}$ та $\overline{b} = \overline{d}$. Хочемо довести, що $\overline{a+b} = \overline{c+d}$.
Маємо $a \equiv c \pmod{p}$ та $b \equiv d \pmod{p}$. А тому за властивостями конгруенції (див. теорію чисел), $a + b \equiv c + d \pmod{p}$. Тобто $\overline{a+b} = \overline{c+d}$.

А тепер час довести, що це абелева – група.
I. $\overline{a},\ \overline{b} \in \mathbb{Z}_p : \overline{a} + \overline{b} = \overline{a+b} \in \mathbb{Z}_p$ – тобто замкненість є, бо отримали, по суті, клас еквівалентності.
II. Перевіримо аксіоми груп.
1) $\forall \overline{a},\ \overline{b},\ \overline{c} \in \mathbb{Z}_p : \overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a + (b+c)} = \overline{(a+b)+c} = \overline{a+b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$ – тобто асоціативність є.
2) нейтральним елементом стане $\overline{0} \in \mathbb{Z}_p$, тому що $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$.
3) для $\overline{a} \in \mathbb{Z}_p$ оберненим елементом стане $\overline{a}^{-1} = \overline{p-a}$, бо $\overline{a} + \overline{a}^{-1} = \overline{a} + \overline{p-a} = \overline{a+p-a} = \overline{p} = \overline{0}$.
Для абелевої групи треба довести комутативність. Справді,
$\forall \overline{a}, \overline{b} \in \mathbb{Z}_p : \overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$ – тобто комутативність є. ■

Example 1.2.3 Є ще така штука як **таблиця Келі**, покажу на прикладі $\langle \mathbb{Z}_3, + \rangle$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Фактично кажучи, в таблиці Келі описуються всі можливі (у цьому випадку) додавання між двома об'єктами та їхні результати.

Theorem 1.2.4 $\langle \mathbb{Z}_p \setminus \{\overline{0}\}, \cdot \rangle$, де p – просте число – абелева група, де операція визначається таким чином: $\overline{a} \cdot \overline{b} \stackrel{\text{def.}}{=} \overline{a \cdot b}$.

Remark 1.2.5 Можна зауважити два обмеження: вилучення елемента $\overline{0}$ та необідність p бути простим. Обґрунтую обмеження прикладами.

Example 1.2.6 Маємо структуру $\langle \mathbb{Z}_p, \cdot \rangle$, яка не буде групою, тому що нема нейтрального елемента.
!Припустімо, що $\overline{e} \in \mathbb{Z}_p$ – це нейтральний елемент, тобто
$\forall \overline{a} \in \mathbb{Z}_p : \overline{a} \cdot \overline{e} = \overline{a}$. Звідси випливає, що $\overline{e} = \overline{1}$.
Водночас $\overline{0} = \overline{0} \cdot \overline{1} = \overline{1}$. Суперечність!

Example 1.2.7 Тепер маємо структуру $\langle \mathbb{Z}_p \setminus \{\overline{0}\}, \cdot \rangle$, де p – складене. Уже нейтральний елемент існує, утім все одно не буде групою.
Оскільки p – складене, то існує якийсь інший дільник $n \neq p, n \neq 1$. Тому звідси $p = nm \implies \overline{p} = \overline{n} \cdot \overline{m}$.
Але $\overline{p} = \overline{0}$, а тому $\overline{n} \cdot \overline{m} = \overline{0}$. А це означає, що хоча $\overline{m}, \overline{n} \in \mathbb{Z}_p$, але $\overline{mn} = \overline{0} \notin \mathbb{Z}_p$. Замкненості нема.

Тепер повернімося до нашої теореми та проведемо її доведення.

Proof.
I. Доведемо, що $\forall \overline{a},\ \overline{b} \in \mathbb{Z}_p \setminus \{\overline{0}\} : \overline{a} \cdot \overline{b} \in \mathbb{Z}_p \setminus \{\overline{0}\}$.
!Припустимо, що $\overline{a} \cdot \overline{b} \notin \mathbb{Z}_p \setminus \{\overline{0}\}$, тоді єдиний варіант – це $\overline{a}\overline{b} = \overline{ab} = \overline{0}$, тобто $p \mid ab$. А оскільки p – просте, то звідси або $p \mid a$, або $p \mid b$. У двох випадках отримаємо суперечність!
Отже, замкненість перевірена успішно.

II. Тепер доведемо виконання аксіом груп.
1) $\forall \overline{a},\ \overline{b},\ \overline{c} \in \mathbb{Z}_p \setminus \{\overline{0}\} : \overline{a}(\overline{b}\overline{c}) = \overline{a}\overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}\overline{c} = (\overline{a}\overline{b})\overline{c}$ – тобто асоціативність є;
2) нейтральним елементом стане $\overline{1} \in \mathbb{Z}_p \setminus \{\overline{0}\}$, тому що $\overline{a}\overline{1} = \overline{a \cdot 1} = \overline{a}$;
3) а ось з оберненим елементом ситуація складніша. Маємо $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$, розглянемо ось таку множину: $\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$. Спочатку покажемо, що тут всі елементи абсолютно різні.
!Припускаючи, що $\overline{k_1 a} = \overline{k_2 a}$ для $k_1 \neq k_2$, ми отримаємо $k_1 a \equiv k_2 a \pmod{p} \implies (k_1 - k_2)a \equiv 0 \pmod{p}$. У силу того, що p – просте, то або $p \mid a$, що точно неправда, або $p \mid k_1 - k_2$. Але це має

місце лише тоді, коли $k_1 = k_2$, оскільки $k_1, k_2 = \overline{1, p-1}$. Суперечність!
Отже, множина $\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$ містить різні елементи. Так само різні елементи містить $\mathbb{Z}_p \setminus \{\overline{0}\}$, тобто фактично ми отримали, що
$\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \mathbb{Z}_p \setminus \{\overline{0}\}$.
Таким чином, елемент серед елементів $\overline{ka}$, де $k = 1, 2, \ldots, p-1$, має бути елемент $\overline{1}$.
Тоді для $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$ знайдеться деякий $\overline{ka}$, для якого $\overline{ka} = \overline{k}\overline{a} = \overline{1}$, і от $\overline{k}$ буде деяким оберненим елементом.
Залишилось показати, що це абелева група. Справді,
$\forall \overline{a},\ \overline{b} \in \mathbb{Z}_p \setminus \{\overline{0}\} : \overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$ – тобто комутативність є. ■

Example 1.2.8 Тут теж будується **таблиця Келі**, покажу на $\langle \mathbb{Z}_5 \setminus \{\overline{0}\}, \cdot \rangle$.

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Фактично тут описується всі можливі множення між двома об'єктами та їхні результати. І ось тут таблиця Келі має сенс, тому що під час доведення ми не знайшли явної формули знаходження оберненого елементу, тому варто будувати табличку.

Але все ж таки повернімось назад до структури $\langle \mathbb{Z}_n \setminus \{\overline{0}\}, \cdot \rangle$, де $n \in \mathbb{N}$, що вже має нейтральний елемент $\overline{e} = \overline{1}$.

Lemma 1.2.9 $\overline{m} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ має обернений елемент $\iff \gcd(m, n) = 1$.

Proof.
$\boxed{\Rightarrow}$ Дано: $\overline{m} \in \mathbb{Z}_n\{\overline{0}\}$ має обернений, тобто $\exists \overline{x} \in \mathbb{Z}_n \setminus \{\overline{0}\} : \overline{m} \cdot \overline{x} = \overline{1}$.
Тобто $mx \equiv 1 \pmod{n}$ для деякого x. Із курсу теорії чисел, можемо сказати, що $\gcd(m, n) \mid 1 \implies \gcd(m, n) = 1$.

$\boxed{\Leftarrow}$ Дано: $\gcd(m, n) = 1$, тоді рівняння $mx \equiv 1 \pmod{n}$ матиме єдиний розв'язок x, із курсу теорії чисел. Мовою класів лишків, маємо
$\overline{mx} = \overline{m} \cdot \overline{x} = \overline{1}$. Таким чином, $\overline{m} \in \mathbb{Z}_n$ має обернений. ■

Познайомимось з ось такою множиною:

$$U_n = \{\overline{m} \in \mathbb{Z}_n | \gcd(m, n) = 1\}$$

Example 1.2.10 Зокрема маємо $U_9 = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

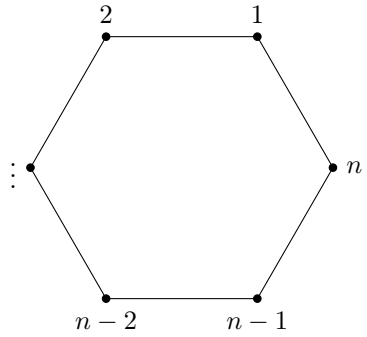
Theorem 1.2.11 $\langle U_n, \cdot \rangle$ – абелева група з операцією $\cdot$ як було в $\mathbb{Z}_n \setminus \{\overline{0}\}$.

Proof.
I. Із теорії чисел, відомо, що $\begin{cases} \gcd(a, n) = 1 \\ \gcd(b, n) = 1 \end{cases} \implies \gcd(ab, n) = 1$. А тому звідси $\forall \overline{a},\ \overline{b} \in U_n : \overline{ab} \in U_n$.
II. Комутативність, асоціативність аналогічно доводиться, як і в минулій теоремі. Нейтральний елемент досі $\overline{e} = \overline{1}$. Кожний елемент має обернений, бо $\overline{m} \in U_n \implies \gcd(m, n) = 1$. Тут спрацьовує лема. ■

1.2.2 Діедральні групи

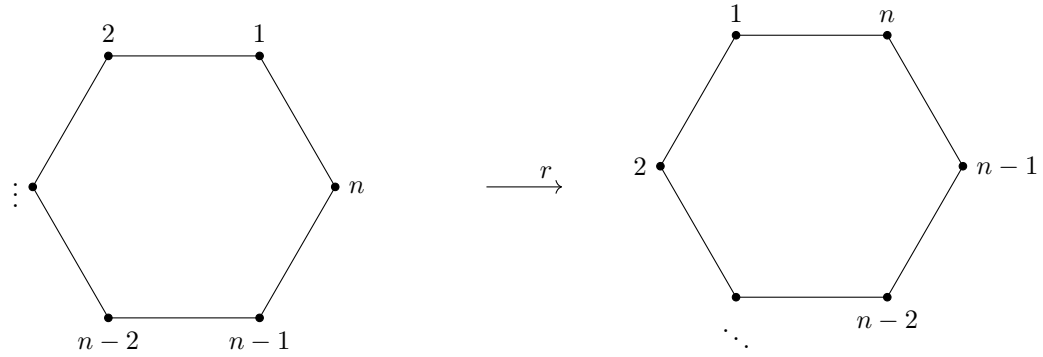
Definition 1.2.12 Дієдральною групою називають групу симетрій правильного n-кутника.
Позначення: D_n (інколи D_{2n}).

Розглянемо правильний n-кутник.



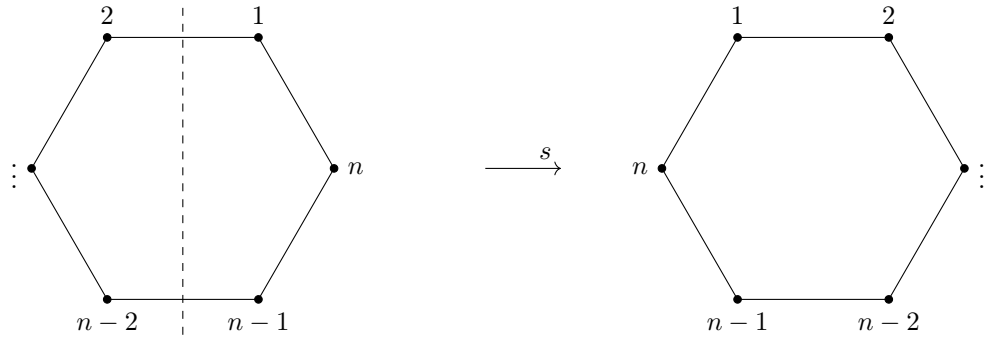
Над цією фігурою робитемо два перетворення (це всі симетрії):
1) обертання відносно центра фігури проти годинникової стрілки;
2) відбиття відносно осі, що проходить через центр фігури.

Зауважимо, що в цьому випадку $\operatorname{card} D_n = 2n$.
Щоб кожну вершину зсунути проти годинниковою стрілкою, треба на n-кутник застоувати обертання розміром $\dfrac{360^\circ}{n}$. Цю дію позначимо за r.



r^k – означає k разів застосувати обертання.
Ясно, що $r^n = e$ – повернемось до початкового положення.

Для правильних n-кутників всього рівно n вісів симетрій. Візьмемо якусь одну вісь та зробимо відбиття. Цю дію позначимо за s.



Ясно, що $s^2 = e$ – повернемось до початкового положення. Інші $n-1$ відбиття, які є в n-кутнику, виражаються через обраний вісь відбиття s та певну кількість обертань r, тобто маємо:
$s, rs, r^2s, \ldots, r^{n-1}s$.
Чому ці відбиття різні, тому що якби $r^k s = r^l s$, то було б обов'язоко $r^k = r^l$, що неможливо при $k \neq l$.
Також жодне з цих перетворень не є обертанням (тобто це дійсно відбиття), бо якби $r^l = r^k s$, то було б $s = r^{l-k}$, що неможливо. Адже симетрія змінює орієнтацію, а обертання – ні.

Із цих міркувань ми робимо висновок, що нам неважливо, який вісь відбиття треба брати.
Ще хочеться зауважити, що $rs = sr^{n-1}$, це теж саме, що $rsrs = e$. Уже було з'ясовано, що rs буде відбиттям, а тому звідси $(rs)^2 = e$.

Таким чином, ми отримаємо вид дієдральної групи:

$$D_n = \{\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{обертання}}, \underbrace{s, rs, r^2s, \ldots, r^{n-1}s}_{\text{відбиття}}\},$$

де $r^n = e,\ s^2 = e,\ rs = sr^{n-1}$.
Можна ще переписати це як $D_n = [s, r]$.

Theorem 1.2.13 $\langle D_n, \circ\rangle$ – справді група. Тут операція $\circ$ – композиція дій на n-кутник. (явно я це не вказував для зручності)

Remark 1.2.14 $\langle D_n, \circ\rangle$ – не абелева група в загальному випадку.
Принаймні тому, що $sr \neq rs$.

1.2.3 Групи кватерніонів

Розглядається ось така множина:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

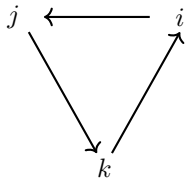
з операцією $\cdot$, яка працює ось таким чином:

$$i^2 = j^2 = k^2 = -1$$
$$ijk = -1$$

Тут числа $1, -1$ – природним чином задані, не абстрактно.

Theorem 1.2.15 $\langle Q_8, \cdot\rangle$ – група.

Proof.
На основі заданих правил, можна отримати ще такі співвідношення:
$ij = k \qquad ji = -k$
$jk = i \qquad kj = -i$
$ki = j \qquad ik = -j$
Дійсно,
$ij = (-ij)(-1) = (-ij)k^2 = -(ijk)k = -(-1)k = k$
$ji = ji(1) = ji(-ijk) = -(jiijk) = -k.$
На прикладі першого було пояснення.



Із цього випливає замкненість операції множення.
Покажемо асоціативність, тобто $x(yz) = (xy)z$.
Не втрачаючи загальності, припустимо $x = i$. Ми будемо розглядати випадки $y, z \in \{i, j, k\}$ – загалом 9 варіантів. Із одиницею всередині все зрозуміло, а мінусові не беремо, бо все те саме з точністю до знака. Якщо всі варіанти розписати, то можна переконатись в рівностях.
Нейтральним елеемнтом буде 1.
Залишились обернені елементи:

a	a^{-1}
± 1	± 1
i	$-i$
j	$-j$
k	$-k$

Доведено. ■

1.2.4 Симетричні групи

Definition 1.2.16 Перестановкою елементів множини $X \neq \emptyset$ називають бієкцію

$$\sigma \colon X \to X$$

Позначення: S_X – множина всіх перестановок на множині X.

Theorem 1.2.17 $\langle S_X, \circ \rangle$ – група, якщо $X \neq \emptyset$.

Спочатку наведемо кілька важливих лем.

Lemma 1.2.18 Задано $\sigma, \mu : X \to X$ – бієкції. Тоді $\sigma \circ \mu$ – бієкція.
Таким чином, це доводить замкненість. Тобто $\sigma, \mu \in S_X \implies \sigma \circ \mu \in S_X$.

Proof.
!Припустимо маємо $a \neq b$, але $\sigma \circ \mu(a) = \sigma \circ \mu(b)$. Тобто звідси $\sigma(\mu(a)) = \sigma(\mu(b)) \implies \mu(a) = \mu(b) \implies a = b$. Суперечність! Довели ін'єктивність.
Маємо $u \in X$, тоді $\exists a \in X : \sigma(a) = u$. Водночас для числа $a \in X : \exists k \in X : \mu(k) = a$. Отже, $\sigma \circ \mu(k) = \sigma(\mu(k)) = \sigma(a) = u$. Довели сюр'єкцію.
Отже, $\sigma \circ \mu$ – бієкція. ■

Lemma 1.2.19 Задано $\sigma \colon X \to X$ - бієкція. Тоді існує бієкція $\mu \colon X \to X$, для якого $\sigma(a) = b \iff \mu(b) = a$.
Таким чином, це доводить існування оберненого елементу. Тобто для кожного $\sigma \in S_X$ існуватиме $\mu \in S_X$, для якого $\sigma \circ \mu(b) = b, \forall b \in X$ та $\mu \circ \sigma(a) = a, \forall a \in X$.

Proof.
Відображення μ коректно визначено. Дійсно, якщо $\mu(b) = a_1$ та $\mu(b) = a_2$, то отримаємо звідси $\sigma(a_1) = b, \sigma(a_2) = b \implies a_1 = a_2$.
!Припустимо, що $b_1 \neq b_2$, але $\mu(b_1) = \mu(b_2)$. Позначимо $a_1 = \mu(b_1), a_2 = \mu(b_2)$. Тоді $b_1 = \sigma(a_1), b_2 = \sigma(a_2)$, а тому $b_1 = \sigma(a_1) = \sigma(a_2) = b_2$. Суперечність! Довели ін'єктивність.
Для кожного $a \in X$ існує елемент $b = \sigma(a)$, для якого $\mu(\sigma(a)) = a$. Довели сюр'єктивність.
Отже, μ – бієкція. ■

Далі відомо, що композиція будь-яких відображень – асоціативна. Нейтральним елементом буде відображення $\mathrm{id} \colon X \to X$, де виконано $\mathrm{id}(x) = x, \forall x \in X$.
Останні два міркування та дві вищезгадані леми доводять нашу теорему.

1.2.5 Групи перестановок

Один з найпоширеніших симетричних груп – це група $\langle S_{\{1,2,\ldots,n\}}, \circ \rangle$, що має ще позначення $\langle S_n, \circ \rangle$.
Перестановки $\sigma \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ мають ще таке позначення:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

де $\{i_1, i_2, \ldots, i_n\}$ – переставлені числа $\{1, 2, \ldots, n\}$. Тут $\sigma(k) = i_k$.

Remark 1.2.20 $\mathrm{card}(S_n) = n!$.

Example 1.2.21 Зокрема в групі $\langle S_3, \circ \rangle$ маються такі перестановки:
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$

Тотожна перестановка виглядає як $\varepsilon = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$.
Добутком двох перестановок σ, μ називається композиція відображень $\sigma \circ \mu$.

Example 1.2.22 Наприклад, $\mu = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Тоді

$$\sigma \circ \mu = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\mu \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Example 1.2.23 Маємо $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Знайти σ^{-1}.

Оскільки σ – бієкція, при цьому $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$, тоді $\sigma^{-1}(1) = 1, \sigma^{-1}(3) = 2, \sigma^{-1}(2) = 3$. Такий розв'язок каже нам наступне: ми просто рядки в перестановці σ поміняємо місцями, а далі верхній рядок переставимо за порядком. А тому звідси

$$\sigma^{-1} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Definition 1.2.24 Задано $\sigma \in S_n$ – перестановка.
Пара (i_j, i_k) називається **інверсією** перестановки σ, якщо

$$\text{при } j < k \text{ маємо } i_j > i_k$$

Example 1.2.25 Зокрема для $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ маємо такі інверсії: $(3,2), (3,1), (2,1), (5,4), (5,1), (4,1)$.

Definition 1.2.26 Перестановка $\sigma \in S_n$ називається **парною**, якщо

$$\text{кількість інверсії – парне число.}$$

Інакше перестановка називається **непарною**.
Парність перестановки визначається ось так:

$$l(\sigma) = \begin{cases} 1, & \sigma \text{ – парна} \\ 0, & \sigma \text{ – непарна} \end{cases}$$

Definition 1.2.27 Перестановка $\tau \in S_n$ називається **транспозицією**, якщо лише два елементи змінені місцями, тобто

$$\tau = \begin{pmatrix} 1 & \dots & k & \dots & j & \dots & n \\ 1 & \dots & j & \dots & k & \dots & n \end{pmatrix}$$

Особливе позначення: $\tau = (kj)$.

Lemma 1.2.28 Задано τ – транспозиція. Тоді $\tau^{-1} = \tau$.

Proof.
Маємо $\tau = \begin{pmatrix} 1 & \dots & k & \dots & j & \dots & n \\ 1 & \dots & j & \dots & k & \dots & n \end{pmatrix}$.
Тобто $\tau(p) = p$ при $p \notin \{k, j\}$, а тому в силу бієкції маємо $\tau^{-1}(p) = p$.
Також $\tau(k) = j, \tau(j) = k$, тоді в силу бієкції $\tau^{-1}(j) = k, \tau^{-1}(k) = j$.
Отже, $\tau^{-1} = \begin{pmatrix} 1 & \dots & k & \dots & j & \dots & n \\ 1 & \dots & j & \dots & k & \dots & n \end{pmatrix} = \tau$.
Висновок такий, що τ^{-1} також є транспозицією. ■

Theorem 1.2.29 Будь-яку перестановку $\sigma \in S_n$ можна записати як добуток транспозицій.

Remark 1.2.30 Ящо взяти перестановку $\sigma \in S_n$ та транспозицію $\tau = (jk)$, то звідси $\sigma \circ \tau$ – та сама перестановка σ, але елементи на j, k позиціях помінялися місцями. Тобто

$$\begin{pmatrix} 1 & \dots & j & \dots & k & \dots & n \\ i_1 & \dots & i_j & \dots & i_k & \dots & i_n \end{pmatrix} \circ \begin{pmatrix} 1 & \dots & j & \dots & k & \dots & n \\ 1 & \dots & k & \dots & j & \dots & n \end{pmatrix} = \begin{pmatrix} 1 & \dots & j & \dots & k & \dots & n \\ i_1 & \dots & i_k & \dots & i_j & \dots & i_n \end{pmatrix}$$

Proof.
Маємо перестановку $\sigma = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$. Використовуючи зауваження, ми будемо обирати такі транспозиції, щоб $\{i_1, \dots, i_n\}$ впорядкувати, тобто отримати $\{1, 2, \dots, n\}$.

Поставимо на місце число 1. Якщо $i_1 = 1$, то вже стоїть на місці. Інакше якщо $i_1 \neq 1$, то має знайтись інший $i_{k_1} = 1$ при $k_1 \neq 1$. Оберемо транспозицію, що міняє i_1, i_{k_1} місцями, я таку позначу за τ_1, тоді отримаємо $\sigma \circ \tau_1$ – перестановка, де тепер 1 стоїть на місці.
Аналогічно ставимо число 2. Якщо $i_2 = 2$, то вже стоїть на місці, а інакше аналогічно беремо відповідну транспозицію – отримаємо $\sigma \circ \tau_1 \circ \tau_2$, де вже $1, 2$ стоять на місцях.
$\vdots$
І так робимо, допоки не отримаємо ось таку рівність:
$\sigma \circ \tau_1 \circ \tau_2 \circ \cdots \circ \tau_m = \varepsilon$.
Цікаво зазначити, що $m \leq n - 1$. Із рівності отримаємо:
$\sigma = \tau_1^{-1} \circ \tau_2^{-1} \ldots \tau_m^{-1} = \tau_1 \circ \tau_2 \cdots \circ \tau_m$.
Отже, σ розклалась в добуток транспозицій. ■

Example 1.2.31 Зокрема для перестановки $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 3 & 2 \end{pmatrix}$ маємо таке представлення в добуток транспозицій: $\sigma = (51) \circ (52) \circ (63) \circ (65)$.
Це робиться за вищеописаним алгоритмом. Але ніхто не забороняє спочатку поставити на місце останній, потім передостанній і так до першого. Отримаємо іншу репрезентацію:
$\sigma = (62) \circ (35) \circ (23) \circ (12)$.
А ще ніхто не забороняє зробити ось так:
$\sigma = (62) \circ (35) \circ (23) \circ (12) \circ \underbrace{(13) \circ (13)}_{\varepsilon}$.
Висновок: розклад на транспозицію не є єдиним.
Але вже тут можна зауважити, що всюди однакова парність: парна кількість транспозицій.

Lemma 1.2.32 Нехай задано $\sigma \in S_n$ – перестановка та τ – довільна транспозиція. Тоді σ та $\sigma \circ \tau$ мають різну парність, тобто $l(\sigma) \neq l(\sigma \circ \tau)$.

Proof.
$\sigma = \begin{pmatrix} 1 & \ldots & k & \ldots & j & \ldots & n \\ i_1 & \ldots & i_k & \ldots & i_j & \ldots & i_n \end{pmatrix}$ $\qquad$ $\sigma \circ \tau = \begin{pmatrix} 1 & \ldots & k & \ldots & j & \ldots & n \\ i_1 & \ldots & i_j & \ldots & i_k & \ldots & i_n \end{pmatrix}$.
Візьмемо пару (i_s, i_t) та розглянемо кілька випадків:
1. $(i_s, i_t) \neq (i_j, i_k)$. Тоді як і в σ, так і в $\sigma \circ \tau$ або пара (i_s, i_t) або буде інверсією, або не буде.
2. $(i_s, i_t) = \begin{bmatrix} (i_s, i_k) \\ (i_s, i_j) \end{bmatrix}$ при $1 \leq s < k$. Тоді аналогічно або пара (i_s, i_t) або буде інверсією, або не буде.
3. $(i_s, i_t) = \begin{bmatrix} (i_k, i_t) \\ (i_j, i_t) \end{bmatrix}$ при $j < t \leq n$ – абсолютно аналогічно до 2.
4. $(i_s, i_t) = (i_k, i_t)$ при $k < t < j$ або $(i_s, i_t) = (i_s, i_j)$ при $k < s < j$. Тоді наочно можна подивитись, що або (i_s, i_t) інверсія σ та не інверсія в $\tau \circ \sigma$, або навпаки. Кількість таких пар $j - k - 1$ кожному випадку.
5. $(i_s, i_t) = (i_k, i_j)$. Очевидно, що або (i_s, i_t) інверсія σ та не інверсія в $\tau \circ \sigma$, або навпаки.
Остаточно, всього $2 \cdot (j - k - 1) + 1$ пар з різною інверсійністю. Цього цілком достатньо, щоб сказати, що $l(\sigma) \neq l(\tau \circ \sigma)$. ■

Corollary 1.2.33 Перестановка $\sigma \in S_n$ – парна $\iff$ кількість транспозицій в розкладі – парна.

Corollary 1.2.34 Якщо $\sigma = \sigma_1 \circ \sigma_2$, то тоді $l(\sigma) = l(\sigma_1) \oplus l(\sigma_2)$ (під $\oplus$ мається на увазі сума за модулем 2).

Definition 1.2.35 Задано $\sigma \in S_n$ – перестановка.
Вона називається **циклом довжини** k, якщо

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$$
$$x \mapsto x, \ x \neq i_s$$

Позначення: $(i_1 i_2 \ldots i_k)$.
Множину $\{i_1, \ldots, i_k\}$ в деякій літературі називають **носієм** даного цикла.

Example 1.2.36 Зокрема перестановка $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$ буде циклом довжиною 3, тому що $2 \mapsto 4 \mapsto 5 \mapsto 2$, а також $1 \mapsto 1, 3 \mapsto 3$.
Отже, $\sigma = (245)$.

Remark 1.2.37 Перестановка $\varepsilon = (1)$ також є циклом, але довжини 1. Усі транспозиції – цикли довжини 2.

Definition 1.2.38 Задано цикли $(i_1 \dots i_k)$ та $(j_1 \dots j_m)$.
Вони називаються **незалежними**, якщо

$$\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_m\} = \emptyset$$

Тобто їхні носії не перетинаються між собою.

Example 1.2.39 Зокрема цикли $(23) \in S_6$ та $(456) \in S_6$ – незалежні.

Lemma 1.2.40 Задано $\sigma_1, \sigma \in S_n$ – цикли. Тоді $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.
Тобто цикли комутують між собою.
Вказівка: подивитися наочно.

Theorem 1.2.41 Будь-яку перестановку $\sigma \in S_n$ можна записати як добуток циклів єдиним чином.

Proof.
Маємо перестановку $\sigma \in S_n$. Побудуємо цикл ось таким чином:
$1 = i_0 \to \sigma(i_0) \to \sigma^2(i_0) \to \dots \to \sigma^{k_0-1}(i_0) \to \sigma^{k_0}(i_0) = i_0 = 1$.
Тут вважаємо, що всі числа до цього різні між собою.
Цей цикл обов'язково рано чи пізно почне повторюватись, починаючи з номера k_0, просто тому що у нас множина $\{1, 2, \dots, n\}$ скінченна.
Чи може таке статись, що $\sigma^{k_0}(i_0)$ потрапить в один з $\sigma^p(i_0), p = \overline{1, k_0}$ – ні, не може. Тому що маємо $\sigma^{p-1}(i_0) \mapsto \sigma^p(i_0)$, а якби також $\sigma^{k_0}(i_0) \mapsto \sigma^p(i_0)$, то порушувались би умова ін'єкції.
Отже, звідси маємо $\sigma^{k_0}(i_0) = i_0 = 1$. Знайшли один цикл.
Якщо так сталось, що $k_0 \neq n$, то тоді побудуємо новий ще один цикл аналогічним чином:
$j_0 \to \sigma(j_0) \to \dots \to \sigma^{k_1}(j_0) = j_0$.
Причому ми беремо таке j_0, що не співпадає зі значенням з першого циклу, бо тоді в нас буде той самий цикл.
До речі, цикли $(i_0, \sigma(i_0), \dots, \sigma^{k_0-1}(i_0))$ та $(j_0, \sigma(j_0), \dots, \sigma^{k_1-1}(j_0))$ будуть незалежними. Бо в іншому випадку знову буде порушення ін'єкції.
І так продовжуємо, допоки не охопимо всі числа.
Нарешті, зауважимо, що добуток всіх отриманих циклів – це σ. Причому даний розклад справді єдиним чином задається з точністю до комутативності циклів. Бо даний алгоритм визначає кожний цикл однозначно, до якого має входити кожне число $\{1, \dots, n\}$. ■

Example 1.2.42 Зокрема маємо $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 6 & 4 & 1 & 7 & 3 \end{pmatrix}$. Тоді
$1 \to 2 \to 5 \to 4 \to 6 \to 1$.
$3 \to 8 \to 3$
$7 \to 7$
Отже, $\sigma = (12546) \circ (38) \circ (7)$.
Зазвичай цикл довжини 1 в іноземних підручниках не пишуть, окрім тотожної перестановки. Тобто можна записати $\sigma = (12546) \circ (38)$.

Example 1.2.43 Повернімось до групи $\langle S_3, \circ \rangle$:
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.
Тепер ці перестановки можна записати більш компактно циклами:
$(1), (23), (12), (123), (132), (13)$

Corollary 1.2.44 $(i_1 i_2 i_3 \dots i_k) = (i_1 i_k) \circ \dots \circ (i_1 i_3) \circ (i_1 i_2)$.
Дивись зауваження, як діє перестановка на транспозицію.

До груп перестановок будемо неодноразово повертатися. Інші групи зустрічатимуться вже під час іншої теорії груп. Просто потрібний був певний арсенал для розгляду різних прикладів.

1.3 Підгрупи

Definition 1.3.1 Задані $\langle G, * \rangle$ – група та множина $H \subset G$.
Підмножина H називається **підгрупою**, якщо

$$\langle H, * \rangle \text{ – група,}$$

де операцію $*$ ми успадкували з групи G.
Позначення: $H \leq G$ (цим позначенням не користуватимуся, але таке є).

Example 1.3.2 Розглянемо кілька прикладів:
1. $\mathbb{Z}$ – підгрупа групи $\langle \mathbb{R}, + \rangle$.
2. SL_n (special linear group) – набір матриць з одничним визначником – підгрупа групи $\langle GL_n, \cdot \rangle$.
3. A_n – набір парних перестановок – підгрупа групи $\langle S_n, \circ \rangle$. Групу $\langle A_n, \circ \rangle$ називаються часто **знакозмінною групою**.

Remark 1.3.3 Якщо маємо групу $\langle G, * \rangle$, то у підгрупи H нейтральний елемент збігається з нейтральним елементом групи G.
Дійсно, припустимо, що $e' \in H, e \in G$ – різні нейтральні елементи. Тоді якщо $h \in H$, то $e' * h = h$ та оскільки $h \in G$, то $e * h = h$, тобто $e' * h = e * h \implies e' = e$.

Theorem 1.3.4 Критерій підгрупи
Задані $\langle G, * \rangle$ – група та множина $H \subset G$.

$$H \text{ – підгрупа } \iff \begin{cases} \forall a, b \in H : a * b \in H \\ \forall a \in H : a^{-1} \in H \end{cases} \quad \text{та (!) } H \neq \emptyset.$$

Proof.
$\boxed{\Rightarrow}$ Дано: H – підгрупа, тоді звідси $\langle H, * \rangle$ – група. А тому звідси випливають умови, що записані праворуч.

$\boxed{\Leftarrow}$ Дано: $\begin{cases} \forall a, b \in H : a * b \in H \\ \forall a \in H : a^{-1} \in H \end{cases}$. Доведемо, що $\langle H, * \rangle$ – група.
Ми уже маємо замкненість за умовою.
Нижче ми будемо брати елементи з H – і це легітимно, адже $H \neq \emptyset$.
$\forall a, b, c \in H \implies a, b, c \in G : a * (b * c) = (a * b) * c$ - тобто маємо асоціативність.
Оскільки $a \in H$, то звідси $a^{-1} \in H$, але водночас $a, a^{-1} \in G$, а тому звідси $a * a^{-1} = e$. Причому за першою умовою, $e \in H$.
Отже, нейтральний елемент існує. Автоматично існування оберненого елемента теж виконується. ■

Remark 1.3.5 Зазвичай критерій підгрупи записують в такому вигляді:

$$H \text{ – підгрупа } \iff \begin{cases} \forall a, b \in H : a * b \in H \\ \forall a \in H : a^{-1} \in H \\ e \in H \end{cases}.$$

Тобто замість $H \neq \emptyset$ ми пишемо $e \in H$. Еквівалентність неважка.

Corollary 1.3.6 Переписаний критерій
H – підгрупа $\iff \forall a, b \in H : a * b^{-1} \in H$, причому $H \neq \emptyset$.

Proof.
Нам достатньо показати, що $\begin{cases} \forall a, b \in H : a * b \in H \\ \forall a \in H : a^{-1} \in H \end{cases} \iff a * b^{-1} \in H.$
$\boxed{\Rightarrow}$ все ясно.
$\boxed{\Leftarrow}$ Дано: $\forall a, b \in H : a * b^{-1} \in H$.
Зауважимо, що $a * a^{-1} = e \in H$, рівність виконана, оскільки $a, a^{-1} \in G$. Тоді звідси
$\forall a \in H : a^{-1} = e * a^{-1} \in H$.
$\forall a, b \in H : a * b = a * (b^{-1})^{-1} \in H$. ■

Example 1.3.7 Покажемо, що A_n – підгрупа $\langle S_n, \circ \rangle$, завдяки критерію.
Беремо $\sigma_1, \sigma_2 \in A_n$, тобто σ_1, σ_2 – парні підстановки. Але σ_2^{-1} досі залишається парною. І парність зберігається при взятті композиції, тож $\sigma_1 \circ \sigma_2^{-1}$ залишається парною, тобто $\sigma_1 \circ \sigma_2^{-1} \in A_n$.
Отже, за критерієм, A_n – підгрупа групи $\langle S_n, \circ \rangle$.

Remark 1.3.8 Кожна група $\langle G, * \rangle$ (тут e – нейтральний елемент) має дві підгрупи: $\{e\}$ та G. Ці підгрупи ще називаються **тривіальними**. У іншій літературі G не називають тривіальною підгрупою.

Example 1.3.9 Задано групу $\langle G, * \rangle$ на $\{H_\alpha\}$ – деяка сім'я підгруп G (можливо, нескінченна). Виявляється, що $\bigcap\limits_\alpha H_\alpha$ – також підгрупа G.

Зауважимо для початку, що $e \in \bigcap\limits_\alpha H_\alpha$, тому що $\forall a \in H_\alpha : e \in H_\alpha$.

Нехай тепер $a, b \in \bigcap\limits_\alpha H_\alpha$, тобто $\forall \alpha : a, b \in H_\alpha$. Оскільки $\forall \alpha : H_\alpha$ – всі підгрупи G, то за критерієм, $a * b^{-1} \in H_\alpha, \forall \alpha \implies a * b^{-1} \in \bigcap\limits_\alpha H_\alpha$.

1.4 Підгрупи, породжені множиною

Definition 1.4.1 Задано $\langle G, * \rangle$ – група та $M \subset G$.
Підгрупа, що породжена множиною M, називають таку множину:

$$[M] = \bigcap_{\substack{H \text{ – підгрупа } G \\ H \supset M}} H$$

Альтернативне позначення: $\langle M \rangle$.

Remark 1.4.2 $[M]$ справді задає підгрупу G, як перетин якогось числа підгруп G (**Ex. 1.3.9**).

Proposition 1.4.3 $[M] = \{m = m_1^{\varepsilon_1} * \cdots * m_s^{\varepsilon_s} \mid s \geq 0, m_i \in M, \varepsilon_i = \pm 1\}$.
Важливо зауважити, що в добутку не обов'язково різні елементи.

Proof.
Позначимо $P = \{m = m_1^{\varepsilon_1} * \cdots * m_s^{\varepsilon_s} \mid m_i \in M, \varepsilon_i = \pm 1\}$.
Нехай H – один з підгруп G так, щоб $H \supset M$, тоді звідси будь-який $m_i \in H$, а в силу підгрупи $m_i^{\varepsilon_i} \in H \implies m_1^{\varepsilon_1} * \ldots m_s^{\varepsilon_s} \in H \implies P \subset [M]$.
Навпаки: зрозуміло, що $M \subset P$. Нам треба показати, щоб P - підгрупа G, тоді звідси буде $P \supset [M]$.

Покажемо, що P – підгрупа групи G. Маємо $u, v \in P$, тобто
$u = m_1^{\varepsilon_1} * \cdots * m_s^{\varepsilon_s} \qquad \varepsilon_i = \pm 1.$
$v = n_1^{\eta_1} * \cdots * n_t^{\eta_t} \qquad \eta_i = \pm 1.$
$\implies u * v = m_1^{\varepsilon_1} * \cdots * m_s^{\varepsilon_s} * n_1^{\eta_1} * \cdots * n_t^{\eta_t} = k_1^{\sigma_1} * \cdots * k_{s+t}^{\sigma_{s+t}}$, причому $\sigma_i = \pm 1$ та $k_i \in M$. Таким чином, $u * v \in P$.
$\implies u^{-1} = m_s^{-\varepsilon_s} * \cdots * m_1^{-\varepsilon_1}$, але все одно $-\varepsilon_i = \pm 1$, а також $m_i \in M$. Таким чином, $u^{-1} \in P$. ■

Remark 1.4.4 $[M]$ – найменша підгрупа, що містить множину M.

Example 1.4.5 Група $\langle S_n, \circ \rangle$ породжена транспозиціями.
Дійсно, якщо $\sigma \in S_n$, то тоді $\sigma = \omega_1 \circ \cdots \circ \omega_k$, де кожний ω – цикл. Водночас $\omega = \tau_1 \circ \cdots \circ \tau_m$, тобто ми кожний цикл розписали як добуток транспозиції.

Example 1.4.6 Оберемо множину $M = \{a\}$, $a \in G$ – отримаємо:
$[\{a\}] = \{a^{\varepsilon_1} * \cdots * a^{\varepsilon_s} | s \geq 0, \varepsilon_s = \pm 1\} = \{a^m \mid m \in \mathbb{Z}\} \overset{\text{позн.}}{=} \langle a \rangle$.
Тобто отримали циклічну підгрупу, породжена елементом $a \in G$, про це детально в наступному підрозділі.

1.5 Циклічні підгрупи

Definition 1.5.1 Задано $\langle G, * \rangle$ – група. Зафіксуємо $a \in G$.
Циклічною підгрупою, що породжена елементом $a \in G$, називають ось таку множину:

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

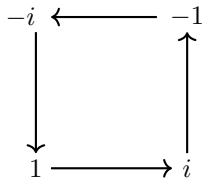
Водночас елементом a називають **твірною підгрупи** $\langle a \rangle \subset G$.
Альтернативне позначення: $[a]$, але поширеніше за всього використовують позначення в означенні.

Remark 1.5.2 $\langle a \rangle$ – дійсно підгрупа групи $\langle G, * \rangle$ (попередній підрозділ).

Definition 1.5.3 Задано $\langle G, * \rangle$ – група.
Група G називається **циклічною**, якщо

$$\exists a \in G : \langle a \rangle = G$$

Example 1.5.4 Маємо групу $\langle \mathbb{C} \setminus \{0\}, \cdot \rangle$. Знайдемо множину $\langle i \rangle$.
Можна зауважити, що $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$, а далі по колу, збільшуючи степінь на одиницю.



Отже, $\langle i \rangle = \{1, i, -1, -i\}$.

Remark 1.5.5 Між іншим, із нескінченної групи ми знайшли скінченну підгрупу.

Example 1.5.6 Маємо групу $\langle \mathbb{Z}_6, + \rangle$. Всі можливі циклічні підгрупи записані ось таким чином:
$[k] = [-k] = \{-2k, -k, 0, k, 2k, \dots\} \overset{\text{позн}}{=} k\mathbb{Z}$.

Example 1.5.7 Зауважимо, що $\langle 1 \rangle = \mathbb{Z}$, що доводить, що $\langle \mathbb{Z}, + \rangle$ – циклічна група.

Remark 1.5.8 Різниця між першими двома прикладами полягала в тому, що:
– в першій циклічній підгрупі рано чи пізно ми знайшли якийсь інший номер $n \in \mathbb{N}$, для якого $a^n = e$. У нашому випадку, $i^4 = 1$;
– в других циклічних підгрупах ми ніколи не знайдемо $n \in \mathbb{N}$, щоб $a^n = e$.

Definition 1.5.9 Задано $\langle G, * \rangle$ – група. Зафіксуємо $a \in G$.
Порядком елемента $a \in G$ називають таке найменше число n, для якого:

$$a^n = e$$

Позначення: $|a|$ або $\text{ord}(a)$. Якщо такого порядку не існує, то тоді кладемо $|a| = \infty$.
Порядком групи G називають просто її потужність:

$$|G| = \text{card}(G)$$

Example 1.5.10 Зокрема для групи $\langle \mathbb{C} \setminus \{0\}, \cdot \rangle$ та підгрупи $\langle i \rangle$ маємо $|i| = 4$. Для циклічної групи $\langle \mathbb{Z}, + \rangle$ маємо $|1| = \infty$.

Proposition 1.5.11 Задано $\langle G, * \rangle$ – група та $\langle a \rangle$ – циклічна підгрупа. Тоді $\text{ord}(a) = |\langle a \rangle|$.
Тобто порядок елемента a дорівнює порядку циклічної підгрупи $\langle a \rangle$

Proof.
Нехай $\text{ord}(a) = n$, тобто $a^n = e$. А це означає, що $a^m = a^k$ при $m \equiv k \pmod{n}$. Переконаємось, що $a^{k_1} \neq a^{k_2}$ при $0 \leq k_1 < k_2 \leq n - 1$.
!Припустимо, що $a^{k_1} = a^{k_2}$ при $k_1 < k_2$. У такому разі $a^{k_2 - k_1} = e$, що можливо лише при $k_2 - k_1 = 0 \implies k_1 = k_2$, але в нас $0 < k_2 - k_1 < n$. Суперечність!
Таким чином, $[a] = \{e, a, a^2, \dots, a^{n-1}\}$, а значить, $|[a]| = n$.

Нехай $\text{ord}(a) = \infty$, тобто $a^n \neq e$ для кожного $n \in \mathbb{N}$. Доведемо, що $a^{k_1} \neq a^{k_2}$ при $k_1 \neq k_2$.
!Припустимо, що $a^{k_1} = a^{k_2}$ при $k_1 \neq k_2$, але тоді $a^{k_1 - k_2} = e$.
Єдиний варіант - це вимагати $k_1 - k_2 = 0 \implies k_1 = k_2$. Суперечність!
Отже, $[a] = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots, \}$ - буде зліченна множина, а тому $|[a]| = \infty$. ■

Remark 1.5.12 $|a| = 1 \iff \langle a \rangle = \{e\}$.

Example 1.5.13 Розглянемо групу $\langle U_9, \cdot \rangle$ та циклічну підгрупу $\langle \overline{2} \rangle = \{\overline{2}, \overline{4}, \overline{8}, \overline{7}, \overline{5}\} = U_9$. Тоді $\text{ord}(\overline{2}) = 5$.
До речі, із теорії чисел важливо зауважити: 2 – первісний корінь (mod 9).

Theorem 1.5.14 Задано $\langle G, * \rangle$ – група та $a \in G$, причому $\text{ord}(a) = n$. Тоді $\langle a^m \rangle = \left\langle a^{\gcd(m,n)} \right\rangle$ для довільного $m \in \mathbb{N}$.

Proof.
Нехай $x \in \langle a^m \rangle$, тобто $x = (a^m)^k = a^{mk}$. Водночас $\gcd(m, n) = d$, тобто $d \mid m \implies m = dq$. Отже, $x = a^{dqk} = (a^d)^{qk} \implies x \in \left\langle a^d \right\rangle$.

Нехай $x \in \left\langle a^d \right\rangle$, тоді $x = (a^d)^k$. За рівністю Безу, $\gcd(m, n) = d = mx + ny$, тому $x = (a^d)^k = a^{dk} = a^{mkx+nky} = (a^m)^{kx}(a^n)^{ky} = (a^m)^{kx} \implies x \in \langle a^m \rangle$.
Отже, $\langle a^m \rangle = \left\langle a^{\gcd(m,n)} \right\rangle$. ■

Example 1.5.15 Маємо групу $\langle D_8, \circ \rangle$, зрозуміло $\text{ord}(r) = 8$. А за теоремою вище, $\left\langle r^6 \right\rangle = \left\langle r^{\gcd(8,6)} \right\rangle = \left\langle r^2 \right\rangle = \{e, r^2, r^4, r^6\}$. Ця теорема просто потрібна, щоб розглядати більш просту підгрупу за виглядом, хоча вони є однаковими.

Theorem 1.5.16 Задано $\langle G, * \rangle$ – циклічна група. Тоді будь-яка підгрупа H – також циклічна.

Proof.
Маємо $G = \langle g \rangle$ та H – деяка підгрупа. Розглянемо два випадки:
I. H – тривіальна підгрупа. Тоді або $H = \{e\} = \langle e \rangle$, або $H = G = \langle g \rangle$.
II. H – нетривіальна підгрупа. Нехай $m \in \mathbb{N}$ – найменше число, де $g^m \neq e$. Таке число існує, бо оскільки $H \neq \{e\}$, то він має містити якийсь елемент g^m, де тут може бути або додатний, або від'ємний степінь.
Якщо $m > 0$, то оберемо найменше таке число (Well-ordering principle).
Якщо $m < 0$, то тоді обов'язково існує $g^{-m} \in H$, оскільки H - підгрупа.
Покажемо, що $\langle g^m \rangle = H$.
Нехай $h \in H \subset G$, тоді $h = g^n$ для деякого $n \in \mathbb{Z}$. Поділимо n та m:
$n = mq + r$ при $0 \leq r < m$.
$h = g^n = g^{mq+r} = (g^m)^q g^r$.
Отже, $g^r = (g^m)^{-q} \cdot h$. Зауважимо, що $g^m \in H \implies (g^m)^{-q} \in H$, а також $h \in H$. Таким чином, елемент $g^r \in H$. Але тоді $r \geq m$, бо ми домовились, що m - найменший степінь для того, щоб $g^m \in H$. А тому вимагаємо $r = 0$. Тобто $h = g^n = g^{mq} = (g^m)^q \implies h \in \langle g^m \rangle$.
Нехай $h \in \langle g^m \rangle$, ну тоді звідси $h = (g^m)^k \in H$, бо $g^m \in H$.
Разом отримали $H = \langle g^m \rangle$. ■

Lemma 1.5.17 Задано $\langle G, * \rangle$ - група та $m = \text{ord}(g)$. Тоді $g^n = e \iff m \mid n$.
Без доведення. Така ж лема була в теорії чисел під час розмови про первісні корені. Доведення буквально слово в слово.

Proposition 1.5.18 Задано $\langle G, * \rangle = \langle g \rangle$ – циклічна група, $\text{ord}(g) = n$. Тоді $\text{ord}(g^m) = \dfrac{n}{\gcd(m, n)}$, тут $m < n$.
Без доведення за аналогічними причинами.

Example 1.5.19 Маємо $\langle \mathbb{Z}_n, + \rangle$. Тоді твірними групи $\mathbb{Z}_n$ будуть числа p, що взаємно прості з n.

Theorem 1.5.20 Задано $\langle G, * \rangle$ – циклічна група порядка n. Нехай $d \mid n$. Тоді існує єдина підгрупа H, для якого $|H| = d$.

Proof.
I. *Існування.*
Зауважимо, що $\left\langle g^{\frac{n}{d}} \right\rangle$ має рівно d елементів (за твердженням вище). Знайшли підгрупу $H = \left\langle g^{\frac{n}{d}} \right\rangle$.

II. *Єдиність.*
!Припустимо, що існує якась інша підгрупа H_1, для якого $|H_1| = d$. Тоді за попередньою теоремою, $H_1 = \langle g^m \rangle = \left\langle g^{\gcd(m,n)} \right\rangle$.
Отже, $d = |H_1| = |\left\langle g^{\gcd(m,n)} \right\rangle| = \dfrac{n}{\gcd(m, n)}$. Але тоді $\gcd(m, n) = \dfrac{n}{d}$, а звідси
$H_1 = \left\langle g^{\frac{n}{d}} \right\rangle = H$. Суперечність! ■

Corollary 1.5.21 Задано $\langle G, * \rangle$ – циклічна група порядка n. Нехай $d \mid n$. Тоді кількість елементів G порядка d складає $\varphi(d)$.

Theorem 1.5.22 Задано перестановку $\sigma \in S_n$, розкладемо на незалежні цикли $\sigma = \sigma_1 \dots \sigma_k$ – довжини відповідно $a_1, \dots, a_k$. Тоді $\operatorname{ord}(\sigma) = \operatorname{lcm}(a_1, \dots, a_k)$.

Proof.
Позначимо $m = \operatorname{ord}(\sigma)$ та $l = \operatorname{lcm}(a_1, \dots, a_k)$.
Перш за все, зауважимо, що $\operatorname{ord}(\sigma_i) = a_i$. А також маємо:
$l = q_1 a_1, \dots, l = q_k a_k$.
$\sigma^l = (\sigma_1 \dots \sigma_k)^l \overset{\text{цикли комутують}}{=} \sigma_1^l \dots \sigma_k^l = \sigma_1^{q_1 a_1} \dots \sigma_k^{q_k a_k} = \varepsilon \implies m \mid l$.
Також $\varepsilon = \sigma^m = \sigma_1^m \dots \sigma_k^m$.
Маємо все одно незалежні цикли, тобто вони не є між собою взаємно оберненими. А значить, єдиний варіант рівності – це $\sigma_i^m = \varepsilon \implies a_i \mid m$. Тоді m – спільне кратне чисел $a_1, \dots, a_k \implies l \mid m$. ■

Example 1.5.23 Зокрема $\sigma = (13)(254)$ із S_5 має $\operatorname{ord}(\sigma) = \operatorname{lcm}(2, 3) = 6$.

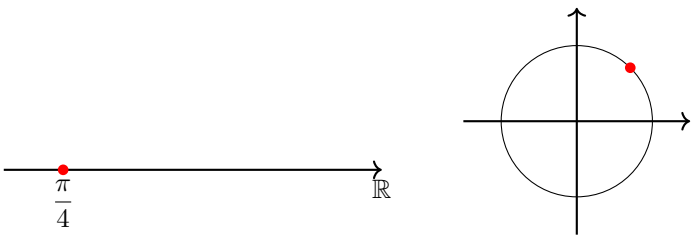
1.6 Гомоморфізм груп

Definition 1.6.1 Задано $\langle G_1, * \rangle$ та $\langle G_2, \star \rangle$ – групи.
Гомоморфізмом називають відображення $f \colon G_1 \to G_2$, для якого

$$\forall a, b \in G_1 : f(a * b) = f(a) \star f(b)$$

Example 1.6.2 Розглянемо кілька прикладів:
1. Маємо групи $\langle GL_n, \cdot \rangle$ та $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$. Розглянемо функцію $f \colon GL_n \to \mathbb{R} \setminus \{0\}$ таким чином:
$f(A) = \det A$.
Якщо взяти $A, B \in GL_n$, тобто оборотні матриці, то звідси
$f(AB) = \det(AB) = \det A \det B = f(A) f(B)$.

2. Маємо групи $\langle \mathbb{R}, + \rangle$ та $\langle \mathbb{T}, \cdot \rangle$, де множина $\mathbb{T}$ – набір комплексних чисел, для яких $|z| = 1$. Розглянемо функцію $\varphi \colon \mathbb{R} \to \mathbb{T}$ таким чином:
$\varphi(\theta) = \cos\theta + i \sin\theta$.
Якщо взяти кути $\alpha, \beta \in \mathbb{R}$, отримаємо
$\varphi(\alpha + \beta) = \cos(\alpha + \beta) + i \sin(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) =$
$= \cos\beta(\cos\alpha + i\sin\alpha) - \sin\beta(\sin\alpha - i\cos\alpha) = \cos\beta\varphi(\alpha) + i\sin\beta\varphi(\alpha) = \varphi(\alpha)\varphi(\beta)$.
Фактично кажучи, цим гомоморфізмом ми просто обертаємо дійсну числову лінію навколо кола одиничного радіусу.



Remark 1.6.3 Гомоморфізм перекладається як "одна форма". По суті кажучи, гомоморфізм – це функція, яка зберігає структуру групи.
Ми маємо $a, b \in G_1$, тоді згідно з групою, $a * b \in G_1$. А далі маємо відображення $f \colon G_1 \to G_2$, куди ми переводимось в іншу групу, з іншою операцією. Ці три елементи можна засунути в відображення та отримати $f(a), f(b) \in G_2$ та $f(a * b) \in G_2$. Ясно, що $f(a) \star f(b) \in G_2$, але додатково хотілось б, щоб це збігалось з $f(a * b)$.

Proposition 1.6.4 Категорія гомоморфізмів груп
Задані $\langle G, * \rangle, \langle H, \star \rangle, \langle K, \cdot \rangle$ – групи. Тоді виконуються наступне:
1) $\mathrm{id} \colon G \to G$ – гомоморфізм;
2) Якщо $\varphi \colon G \to H, \psi \colon H \to K$ – гомоморфізми, то $\psi \circ \varphi \colon G \to K$ – також гомоморфізм;
3) Операція композиції гомоморфізми груп – асоціативна.

Proof.
Покажемо виконання кожного пункту:

1) $\mathrm{id}(a*b) = a*b = \mathrm{id}(a)*\mathrm{id}(b)$ – тобто тут все зрозуміло.

2) Нехай $a, b \in G$, тоді справедливий такий ланцюг:
$\psi\circ\varphi(a*b) = \psi(\varphi(a*b)) \overset{\varphi\text{ – гомоморфізм}}{=} \psi(\varphi(a)\star\varphi(b)) \overset{\psi\text{ – гомоморфізм}}{=} \psi(\varphi(a))\cdot\psi(\varphi(b)) = \psi\circ\varphi(a)\cdot\psi\circ\varphi(b)$.
Отже, $\psi\circ\varphi$ дійсно задає гомоморфізм.

3) Будь-які відображення (зокрема гомоморфізми) асоціативні.

Всі пункти доведені. ■

Theorem 1.6.5 Властивості гомоморфізма
Задано $\langle G_1, *\rangle$ та $\langle G_2, \star\rangle$ – групи з нейтральними елементами e_1, e_2. Маємо $f\colon G_1 \to G_2$ – гомоморфізм, тоді виконуються такі пункти:
1) $f(e_1) = e_2$;
2) $\forall a \in G_1 : f(a^{-1}) = (f(a))^{-1}$;
3) $\mathrm{ord}(f(g)) \mid \mathrm{ord}(g)$, якщо $\mathrm{ord}(g) < \infty$;
4) Нехай H – підгрупа $\langle G_1, *\rangle$. Тоді $f(H)$ – підгрупа $\langle G_2, \star\rangle$;
5) Нехай K – підгрупа $\langle G_2, \star\rangle$. Тоді $f^{-1}(K)$ – підгрупа $\langle G_1, *\rangle$.

Proof.
Покажемо виконанна кожної властивості:

1) $f(e_1)\star e_2 = f(e_1) = f(e_1 * e_1) = f(e_1)\star f(e_1)$.
Тому за правилом скорочення, $e_2 = f(e_1)$.

2) $f(e_1) = f(a * a^{-1}) = f(a)\star f(a^{-1}) = e_2$.
Тому звідси $f(a^{-1}) = (f(a))^{-1}$.

3) Позначимо $\mathrm{ord}(g) = n$, тобто $g^n = e_1$.
Тоді $f(g^n) = (f(g))^n$, але тоді звідси $e_2 = f(e_1) = (f(g))^n$, тобто $\mathrm{ord}(f(g)) \mid n = \mathrm{ord}(g)$.

4) Маємо $x, y \in f(H)$, тобто $x = f(a), y = f(b)$ при деяких $a, b \in H$.
Тоді $x \star y^{-1} = f(a)\star(f(b))^{-1} = f(a)\star f(b^{-1}) = f(a * b^{-1})$, причому $a * b^{-1} \in H$.
Отже, $x \star y^{-1} \in H$.

5) Маємо $a, b \in f^{-1}(K)$, тобто $f(a), f(b) \in K$, а тому звідси
$f(a)\star(f(b))^{-1} = f(a * b^{-1}) \in K$, тобто $a * b^{-1} \in f^{-1}(K)$.

Всі властивості доведені. ■

Definition 1.6.6 Задані $\langle G_1, *\rangle, \langle G_2, \star\rangle$ – групи, а також $f\colon G_1 \to G_2$ – гомоморфізм.
Відображення f називається **ізоморфізмом**, якщо

$$f \text{ – бієктивне}$$

У такому разі групи G_1, G_2 називаються **ізоморфними**.
Позначення: $\langle G_1, *\rangle \cong \langle G_2, \star\rangle$ або часто позначають $G_1 \cong G_2$, якщо ясно, що за операції сховані.

Example 1.6.7 Маємо групи $\langle \mathbb{Z}_2, +\rangle$ та $\langle\{-1, 1\}, \cdot\rangle$. Розглянемо відображення $f\colon \mathbb{Z}_2 \to \{-1, 1\}$ таким чином: $f(\overline{0}) = 1$ та $f(\overline{1}) = -1$.
Ясно, що воно є гомоморфізмом, а також зрозуміло, що кожному елементу з $\{-1, 1\}$ ставиться у відповідність єдиний об'єкт з $\mathbb{Z}_2$. Тобто f – ізоморфізм, а значить, $\langle \mathbb{Z}_2, +\rangle \cong \langle\{-1, 1\}, \cdot\rangle$.

Theorem 1.6.8 Задано $\langle G, *\rangle$ – група та $[a]$ – циклічна підгрупа, $a \in G$. Відомо, що $|a| = n \in \mathbb{N}$. Тобто маємо $[a] = \{e, a, a^2, \ldots, a^{n-1}\}$. Тоді $\langle [a], *\rangle \cong \langle \mathbb{Z}_n, +\rangle$.

Proof.
Сконструюймо функцію $f\colon \mathbb{Z}_n \to [a]$ таким чином: $f(\overline{k}) = a^k$, де число $k = \overline{0, n-1}$.
Спочатку перевіримо, що це – гомоморфізм. І дійсно,
$\forall \overline{k}, \overline{m} \in \mathbb{Z}_n : f(\overline{k} + \overline{m}) = f(\overline{k+m}) = a^{k+m} = a^k * a^m = f(\overline{k}) * f(\overline{m})$.
А далі покажемо, що маємо бієкцію.
Сюр'єкція зрозуміло, що виконана.
Ін'єкція виконана, бо $f(\overline{k}) = f(\overline{m}) \implies a^k = a^m \implies k = m$, це було доведено колись вище.
Отже, f – ізоморфізм та $\langle [a], *\rangle \cong \langle \mathbb{Z}_n, +\rangle$. ■

Theorem 1.6.9 Задано $\langle G, * \rangle$ – група та $[a]$ – циклічна підгрупа, $a \in G$. Відомо, що $|a| = \infty$. Тоді $\langle [a], * \rangle \cong \langle \mathbb{Z}, + \rangle$.

Proof.
Сконструюймо функцію $f\colon \mathbb{Z} \to [a]$ таким чином: $f(k) = a^k$. А далі все майже аналогічно, як в попередній теоремі. ■

Theorem 1.6.10 Властивості ізоморфізма
Задані $\langle G_1, * \rangle, \langle G_2, \star \rangle$ – групи з нейтральними елементами e_1, e_2. Маємо $f\colon G_1 \to G_2$ – ізоморфізм, тоді виконуються такі пункти:
1) $f^{-1}\colon G_2 \to G_1$ – також ізоморфізм;
2) $\langle G_1, * \rangle$ – абелева (циклічна) $\iff$ $\langle G_2, \star \rangle$ – абелева (циклічна);
3) $\operatorname{ord}(g) = \operatorname{ord}(f(g))$.

Proof.
Доведемо виконання кожної властивості:

1) f – ізоморфізм, тобто бієктивний гомоморфізм, тоді f^{-1} – також бієктивне відображення. Залишилось довести, що теж гомоморфізм.
$\forall x, y \in G_2 : f^{-1}(x \star y) = f^{-1}(f(f^{-1}(x)) \star f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x) * f^{-1}(y))) = f^{-1}(x) * f^{-1}(y)$.

2) Нехай G_1 – абелева.
$\forall x, y \in G_2 : x \star y = f^{-1}(f(x)) \star f^{-1}(f(y)) = f^{-1}(f(x) * f(y)) = f^{-1}(f(y) * f(x)) = f^{-1}(f(y)) \star f^{-1}(f(x)) = y \star x$.
В зворотний бік аналогічно.
Нехай G_1 – циклічна, тобто $G_1 = [g]$.
Маємо $x \in G_2$, тоді $x = f(a)$ за сюр'єктивністю. Але $a \in G_1$, тоді звідси $a = g^n$, а тому $x = f(g^n)) = (f(g))^n$. Отже, $G_2 \subset [f(g)]$. Ясно, що $[f(g)] \subset G_2$, а тому $G_2 = [f(g)]$ – циклічна.
В зворотний бік аналогічно.

3) Оскільки f – гомоморфізм, то $\operatorname{ord}(f(g)) \mid \operatorname{ord}(g)$. Водночас $\operatorname{ord}(g) = \operatorname{ord}(f^{-1}(f(g)) \mid \operatorname{ord}(f(g))$, тому що f^{-1} – гомоморфізм. Отже, $\operatorname{ord}(g) = \operatorname{ord}(f(g))$.

Всі властивості доведені. ■

Example 1.6.11 Більш специфічний приклад: ми розглянемо групу $\langle S_n, \circ \rangle$ та покажемо, що S_n – не циклічна.
!Нехай $S_n = \langle \sigma \rangle$, тобто циклічна. Тоді $S_n \cong \mathbb{Z}_{n!}$. Тобто задається ізоморфізм, а значить за властивістю 2), оскільки $\mathbb{Z}_{n!}$ – абелева, то тоді S_n – абелева теж. І це суперечність!

Example 1.6.12 Знайти всі гомоморфізми $f\colon \mathbb{Z}_8 \to \mathbb{Z}_{12}$.
Зауважимо, що якщо f – гомоморфізм, то $f(\overline{k}) = kf(\overline{1})$ при $k = 0, 1, \ldots, 7$. Тобто нам достатньо зрозуміти, чому може дорівнювати $f(\overline{1})$, тим самим визначиться гомоморфізм.
Маємо $f(\overline{8}) = 8f(\overline{1}) = f(\overline{0}) = \overline{0}$. Таким чином, $8f(\overline{1}) \equiv 0 \pmod{12}$.
Розв'язавши конгруентне рівняння, отримаємо $f(\overline{1}) \in \{0, 3, 6, 9\}$.
Отже, ми знайшли 4 гомоморфізми:
$f_1(\overline{k}) = \overline{0},\ f_2(\overline{k}) = 3\overline{k},\ f_3(\overline{k}) = 6\overline{k},\ f_4(\overline{k}) = 9\overline{k}$.

Ще трошки про групу перестановок

Theorem 1.6.13 Теорема Келі
Задано $\langle G, * \rangle$ – група. Тоді існує підгрупа перестановок $H \subset S_G$, для якої $\langle G, * \rangle \cong \langle H, \circ \rangle$.

Proof.
Маємо $g \in G$, визначимо відображення $\lambda_g\colon G \to G$ таким чином: $\lambda_g(x) = g * x$. Покажемо, що $\lambda_g \in S_G$, що теж саме, що воно бієктивне.
$\lambda_g(x) = \lambda_g(y) \implies g * x = g * y \implies x = y$ – ін'єктивність є.
$\forall y \in G : \exists x = g^{-1} * y \in G : \lambda_g(x) = \lambda_g(g^{-1} * y) = g * (g^{-1} * y) = y$ – сюр'єктивність є.

Встановимо множину $H = \{\lambda_g \mid g \in G\}$, причому $H \subset S_G$. Покажемо, що це – підгрупа $\langle S_G, \circ \rangle$.
Асоціативність ясно, що виконується.
$\lambda_e(x) = e * x = x$ – нейтральний елемент – ясно.
$\forall \lambda_g : \exists \lambda_{g^{-1}} : \lambda_g \circ \lambda_{g^{-1}}(x) = \lambda_g(g^{-1} * x) = g * (g^{-1} * x) = x = \lambda_e(x)$ – оберненість є.

Нарешті, покажемо, що $G \cong H$, для цього треба встановити $\varphi\colon G \to H$ так, що $\varphi(g) = \lambda_g$. Це буде гомоморфізмом, бо
$\varphi(g*h) = \lambda_{g*h}$, але $\lambda_{g*h}(x) = (g*h)*x = g*(h*x) = \lambda_g(h*x) = \lambda_g \circ \lambda_h$, тобто $\varphi(g*h) = \varphi(g) \circ \varphi(h)$.
Ін'єкція та сюр'єкція над φ ясно, що виконується. Отже, $G \cong H$. ■

Example 1.6.14 Задані $\langle G, * \rangle, \langle H, \cdot \rangle$ – групи. Позначимо $\mathrm{Hom}(G, H)$ – множина всіх гомоморфізмів з G в H. Установимо для неї операцію $(f \cdot g)(x) = f(x) \cdot g(x), \forall x \in G$. Загалом $\langle \mathrm{Hom}(G, H), \cdot \rangle$ не задає групу.
Дійсно, нехай $f, g, h \in \mathrm{Hom}(G, H)$, тоді:
$(f \cdot g)(x_1 * x_2) = f(x_1 * x_2) \cdot g(x_1 * x_2) = (f(x_1) \cdot f(x_2)) \cdot (g(x_1) \cdot g(x_2))$.
$(f \cdot g)(x_1) \cdot (f \cdot g)(x_2) = f(x_1) \cdot g(x_1) \cdot f(x_2) \cdot g(x_2)$.
Тобто ми таким чином показали, що $f \cdot g$ не обов'язково може бути гомоморфізмом, тобто $f \cdot g \notin \mathrm{Hom}(G, H)$ – порушується замкненість.
Утім якщо попросити групу $\langle H, \cdot \rangle$ бути абелевою, то тоді замкненість вже буде працювати. Гомоморфізми між собою асоціативні. Нейтральний елемент – це гомоморфізм $\sigma\colon G \to H$, що задається як $\sigma(g) = e_H$. Для кожного гомоморфізму $f\colon G \to H$ його оберненим буде гомоморфізм $g\colon G \to H$, що задається як $g(x) = (f(x))^{-1}$.

Повернімося до п. 1.3.
Маючи означення гомоморфізму, ми можемо означення підгрупи написати більш закручено:

Proposition 1.6.15 Задано $\langle G, * \rangle$ – група та $H \subset G$. Нехай $\langle H, \cdot \rangle$ – група (поки що ми вважаємо, що це якась інша операція).
H – підгрупа $G \iff \imath\colon H \hookrightarrow G$ задає гомоморфізм.

Proof.
$\boxed{\Rightarrow}$ Дано: H – підгрупа G, тобто, насправді, $\cdot \equiv *$. Чоловічою мовою, операція на H така ж, що в й групі G. Нехай $h_1, h_2 \in H$.
$\imath(h_1 * h_2) = h_1 * h_2 = \imath(h_1) * \imath(h_2)$.

$\boxed{\Leftarrow}$ Дано: $\imath\colon H \to G$ задає гомоморфізм. Тобто $\forall h_1, h_2 \in H$:
$h_1 \cdot h_2 = \imath(h_1 \cdot h_2) = \imath(h_1) * \imath(h_2) = h_1 * h_2$.
Із точки зору бінарного відображення, ми довели, що $\cdot \equiv *|_H$. Таким чином, H – підгрупа G (бо успадкувала операцію). ■

1.7 Ядра, образи гомоморфізмів

Definition 1.7.1 Задані $\langle G_1, * \rangle, \langle G_2, \star \rangle$ – групи, $f\colon G_1 \to G_2$ – гомоморфізм.
Ядром гомоморфізма називають множину

$$\ker f = \{x \in G_1 : f(x) = e_2\}$$

Образом гомоморфізма називають множину

$$\mathrm{Im}\, f = \{f(x) : x \in G_1\}$$

Remark 1.7.2 $\ker f = f^{-1}(\{e_2\}), \qquad \mathrm{Im}\, f = f(G_1)$.
Таким чином, оскільки $\{e_2\}, G_1$ є тривіальними підгрупами для свої груп, то за властивостями гомоморфізма, $f^{-1}(\{e_2\}), f(G_1)$ будуть підгрупами для своїх груп як прообраз та образ відповідно.

Example 1.7.3 Розглянемо $\langle \mathbb{R}, + \rangle$ та $\langle \mathbb{T}, \cdot \rangle$ та гомоморфізм $\varphi(\theta) = \cos\theta + i \sin\theta \overset{\text{або}}{=} e^{i\theta}$. Знайдемо $\ker\varphi$ та $\mathrm{Im}\,\varphi$. Зауважу заздалегідь, що ми маємо нейтральні елементи $0 \in \mathbb{R}$ та $1 \in \mathbb{T}$.
$\theta \in \ker\varphi \implies \varphi(\theta) = e^{i\theta} = 1 \implies \theta = 2\pi k, k \in \mathbb{Z}$.
Отже, $\ker\varphi = \{2\pi k, k \in \mathbb{Z}\}$.
$z \in \mathrm{Im}\,\varphi \implies z = e^{i\theta}$, причому $|z| = 1$, бо $z \in \mathbb{T}$, але водночас $|e^{i\theta}| = 1$.
Отже, $\mathrm{Im}\,\varphi = \mathbb{T}$.

Theorem 1.7.4 Задані $\langle G_1, * \rangle, \langle G_2, \star \rangle$ – групи та $f\colon G_1 \to G_2$ – гомоморфізм.
f – ін'єктивний $\iff \ker f = \{e_1\}$.

Інколи ін'єктивний гомоморфізм називають **мономорфізмом**.

Proof.
$\boxed{\Rightarrow}$ Дано: f – ін'єктивний гомоморфізм, тож $f(x_1) = f(x_2) \implies x_1 = x_2$.
$x \in \ker f \implies f(x) = e_2 \implies x = e_2$. Таким чином, $\ker f = \{e_1\}$.

$\boxed{\Leftarrow}$ Дано: $\ker f = \{e_1\}$.
!Припустимо, що при $x_1 \neq x_2$ отримаємо $f(x_1) = f(x_2)$. Тоді $f(x_1) \star (f(x_2))^{-1} = f(x_1) \star f(x_2^{-1}) = f(x_1 * x_2^{-1}) = e_2$. Це означає, що $x_1 * x_2^{-1} \in \ker f$. А тому $x_1 * x_2^{-1} = e_1 \implies x_1 = x_2$. Суперечність!
Отже, $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$, тобто f - ін'єктивний. ■

Example 1.7.5 Гомоморфізм $\varphi\colon \mathbb{R} \to \mathbb{T}$, який задавався вище, тобто $\varphi(\theta) = \cos\theta + i\sin\theta$, не буде ін'єктивним, оскільки $\ker f$ містить інші елементи, окірм нейтрального 0.

1.8 Суміжні класи

Маємо $\langle G, * \rangle$, $\langle G', \star \rangle$ – групи та $f\colon G \to G'$ – гомоморфізм. Установимо відношення еквівалентності:
$g_1 \sim g_2 \iff f(g_1) = f(g_2)$.
Окремо пропишемо рівність, помноживши зліва на $(f(g))^{-1}$ – отримаємо:
$(f(g_1))^{-1} \star f(g_2) = e_{G'} \iff f(g_1^{-1}) \star f(g_2) = e_{G'} \iff f(g_1^{-1} * g_2) = e_{G'} \iff g_1^{-1} * g_2 \in \ker f$.
Таким чином, ми отримали $g_1 \sim g_2 \iff g_1^{-1} * g_2 \in \ker f$.
Але $\ker f$ – це один із підгруп G. Насправді, ми хочемо ці міркування повторити для кожної підгрупи.

Нехай H – підгрупа G, встановимо схоже відношення еквівалентності (неважко покати, що це дійсно задає відношення еквівалентності):
$g_1 \sim g_2 \iff g_1^{-1} * g_2 \in H$.
Після цього ми можемо розбити G на класи еквівалентності.

Definition 1.8.1 Лівим суміжним класом g за підгрупою H назвемо клас еквівалентності

$$g * H \overset{\text{def.}}{=} [g]$$

Таке позначення виправдане, оскільки лівий суміжний клас можна записати по-іншому:

Proposition 1.8.2 $g * H = \{g * h \mid h \in H\}$.

Proof.
Нехай $x \in g*H$, тобто звідси $x^{-1}*g \in H$. Але тоді $x = x*(x^{-1}*g)$, причому елемет $x \in G,\ x^{-1}*g \in H$. Тобто x потрапляє в праву множину.
Нехай x потрапяє в праву множину, тобто $x = g*h,\ h \in H$. Але тоді $h = g^{-1}*x \in H \implies x^{-1}*g \in H$, тобто $x \sim g$. Звідси $x \in g * H$. ■

Фактормножина $G/_\sim \overset{\text{позн.}}{=} G/_H$ буде містити всі ліві суміжні класи.

Proposition 1.8.3 $g_1 * H = g_2 * H \iff g_1^{-1} * g_2 \in H$.
Це випливає з того, що $g_1^{-1} * g_2 \in H \iff g_1 \sim g_2 \iff [g_1] = [g_2] \iff g_1 * H = g_2 * H$. У такому формулюванні ми будемо часто користуватися.

Повернімося до самого початку, до $g_1 \sim g_2 \iff f(g_1) = f(g_2)$. Праву рівність можна записати іншим способом, помноживши уже справа на $(f(g))^{-1}$ – отримаємо:
$f(g_2) \star (f(g_1))^{-1} = e_{G'} \iff f(g_2) \star f(g_1^{-1}) = e_{G'} \iff f(g_2 * g_1^{-1}) \in e_{G'} \iff g_2 * g_1^{-1} \in \ker f$.
Таким чином, ми отримали $g_1 \sim g_2 \iff g_2 * g_1^{-1} \in \ker f$.

Тепер для H можна задати інше відношення еквівалентності (знову неважко довести):
$g_1 \sim g_2 \iff g_2 * g_1^{-1} \in H$.
Ми потім знову розіб'ємо G на класи еквівалентності.

Definition 1.8.4 Правим суміжним класом g за підгрупою H назвемо клас еквівалентності

$$H * g \overset{\text{def.}}{=} [g]$$

Proposition 1.8.5 $H * g = \{h * g \mid h \in H\}$.
Аналогічне доведення, як було з лівим суміжним класом.

Фактормножина $G/_\sim \overset{\text{позн.}}{=} {}_H/G$ буде містити всі праві суміжні класи.

Proposition 1.8.6 $H * g_1 = H * g_2 \iff g_2 * g_1^{-1} \in H$.
Аналогічні міркування. Знову цим будемо частіше користуватися.

Example 1.8.7 Розглянемо тривіальні підгрупи групи $\langle G, * \rangle$. Знайдемо суміжні класи.
1. $g * \{e\} = \{e\} * g = \{g\}$, і це $\forall g \in G$;
2. $g * G = G * g = G$, і це $\forall g \in G$.

Коли в нас підгрупа $H = \ker f$, то тоді ліві та праві суміжні класи збігалися, тому все чудово. Виникає логічне питання, чи буде так з довільною підгрупою H. Відповідь: ні.

Example 1.8.8 Маємо $\langle S_3, \circ \rangle$ – група та підгрупа $H = \{(23), (1)\} \overset{\text{або}}{=} \langle (23) \rangle$. Знайдемо всі можливі як й ліві, так й праві суміжні класи:
$(1) \circ H = \{(23), (1)\}$ $\quad H \circ (1) = \{(23), (1)\}$
$(23) \circ H = \{(23), (1)\}$ $\quad H \circ (23) = \{(23), (1)\}$
$(13) \circ H = \{(132), (13)\}$ $\quad H \circ (13) = \{(123), (13)\}$
$(12) \circ H = \{(123), (12)\}$ $\quad H \circ (12) = \{(132), (12)\}$
$(123) \circ H = \{(123), (12)\}$ $\quad H \circ (123) = \{(123), (13)\}$
$(132) \circ H = \{(132), (13)\}$ $\quad H \circ (132) = \{(132), (12)\}$
Уже на цьому прикладі зауважимо, що загалом $g * H \neq H * g$.

За яких умов ці суміжні класи ще збігатимуться, дізнаємося згодом. Зараз кілька важливих наслідків із того, що ми зробили, та корисні твердження.

Corollary 1.8.9 Ліві суміжні класи між собою або не перетинаються, або збігаються. Так само праві суміжні класи між собою або не перетинаються, або збігаються.
Тому що класи еквівалентності або не перетинаються, або збігаються.

Corollary 1.8.10 $G = \bigcup\limits_{g \in G} g * H \qquad G = \bigcup\limits_{g \in G} H * g$.
Тому що класи еквівалентності утворюють розбиття множини.

Example 1.8.11 Зокрема за попереднім прикладом, маємо:
$S_3 = \{(23), (1)\} \cup \{(132), (13)\} \cup \{(123), (12)\}$ – об'єднання лівих суміжних класів;
$S_3 = \{(23), (1)\} \cup \{(123), (13)\} \cup \{(132), (12)\}$ – об'єднаяння правих суміжних класів.

Remark 1.8.12 Даний наслідок сформульовано окремо для лівих суміжних класів та правих. Мається на увазі, що $a * H$ та $H * b$ можуть мати непорожній перетин.
Зокрема з попереднього прикладу, $(13) \circ H \cap H \circ (12) = \{(132)\}$.

Proposition 1.8.13 $g_1 * H = g_2 * H \iff H * g_2^{-1} = H * g_1^{-1}$.

Proof.
$\boxed{\Rightarrow}$ Дано: $g_1 * H = g_2 * H$.
Нехай $x \in H * g_2^{-1}$, тоді $x = h * g_2^{-1}$ для деякого $h \in H$. Оскільки $g_2 \in g_2 * H$, то $g_2 \in g_1 * H \implies g_2 = g_1 * h'$ для деякого $h' \in H$. Отже, $x = h * (h')^{-1} * g_1^{-1}$, що означає $x \in H * g_1^{-1}$.
Нехай $x \in H * g_1^{-1}$, тоді аналогічним чином $x \in H * g_2^{-1}$.
Висновок: $H * g_2^{-1} = H * g_1^{-1}$.

$\boxed{\Leftarrow}$ *доведення є зеркальним.* ■

Proposition 1.8.14 Задано $\langle G, * \rangle$ – скінченна група, $H \subset G$ – підгрупа. Тоді для кожного елемента $g \in G$ виконується $\text{card}(g * H) = \text{card}(H)$.
Для правих суміжних класів аналогічне твердження.

Proof.
Припустимо, що $H = \{h_1, \ldots, h_k\}$ – всі різні. Тоді маємо $g * H = \{g * h_1, g * h_2, \ldots, g * h_k\}$. Єдине, що треба довести, – це те, що $g * h_i \neq g * h_j$ для кожних $i \neq j$.
!Припустимо, що $g * h_i = g * h_j$. Тоді автоматично звідси $h_i = h_j$. Ну але ж ми маємо різні елементи, тому суперечність!
Отже, $\text{card}(g * H) = k$. ■

Proposition 1.8.15 Задано $\langle G, * \rangle$ – скінченна група, $H \subset G$ – підгрупа.
Кількість лівих суміжних класів збігається з кількістю правих суміжних класів.

Proof.
Визначимо множини $\mathcal{L}_H = \{g * H \mid g \in G\}$ та $\mathcal{R}_H = \{H * g \mid g \in G\}$. Визначимо відображення $f \colon \mathcal{L}_H \to \mathcal{R}_H$ таким чином: $f(g * H) = H * g^{-1}$.
Воно визначено коректно. Дійсно, якщо $x * H = y * H$, то $f(x * H) = H * x^{-1} = H * y^{-1} = f(y * H)$.
Доведемо, що f задає бієкцію.
$f(x * H) = f(y * H) \implies H * x^{-1} = H * y^{-1} \implies x * H = y * H$ – ін'єктивно.
$\forall H * g \in \mathcal{R}_H : \exists g^{-1} * H \in \mathcal{L}_H : f(g^{-1} * H) = H * g$ – сюр'єктивно.
Тобто $\operatorname{card}(\mathcal{L}_H) = \operatorname{card}(\mathcal{R}_H)$. ■

Theorem 1.8.16 Теорема Лагранжа
Задано $\langle G, * \rangle$ – скінченна група та $H \subset G$ – підгрупа. Тоді $\operatorname{card}(H) \mid \operatorname{card}(G)$.

Proof.
Припускаємо, що $\operatorname{card}(G) = m$. Маємо $G = \bigcup_{k=1}^{n} g_k * H$, де число $n \leq m$. Сюди ми записали лише таку кількість суміжних класів, де вони не співпадають. Оскільки ці множини не перетинаються, то $\operatorname{card}(G) = \operatorname{card}(g_1 * H) + \cdots + \operatorname{card}(g_n * H) \overset{\text{Prp. 1.8.14}}{=} \operatorname{card}(H) + \cdots + \operatorname{card}(H) = n \cdot \operatorname{card}(H)$.
Отже, $\operatorname{card}(H) \mid \operatorname{card}(G)$. ■

Definition 1.8.17 Задано $\langle G, * \rangle$ – скінченна група, $H \subset G$ – підгрупа.
Індексом підгрупи H в групі G називають кількість суміжних класів.
Позначення: $i(H)$, але поширеніше бачу $[G : H]$.
(уже доводили, що кількість лівих та правих суміжних класів однакова, тому означення має сенс).

Corollary 1.8.18 $\operatorname{card}(G) = [G : H] \cdot \operatorname{card}(H)$.
Також можна записати це як $\operatorname{card}(G) = \operatorname{card}(G/_H) \cdot \operatorname{card}(H)$ або $\operatorname{card}(G) = \operatorname{card}({}_H/G) \cdot \operatorname{card}(H)$.

Example 1.8.19 Із теореми Лагранжа випливає, що група $\langle S_3, \circ \rangle$ не може містити підгрупи H, що складаються з 4 або 5 елементів.

Corollary 1.8.20 Наслідки з теореми Лагранжа
Задано $\langle G, * \rangle$ – скінченна група. Маємо наступні пункти:
1) Якщо $\operatorname{card}(G) = p$, де p – просте число, то тоді вона містить лише тривіальні підгрупи (тобто G – циклічна група);
2) $\operatorname{ord}(a) \mid \operatorname{card}(G)$ для кожного $a \in G$;
3) $a^{\operatorname{card}(G)} = e$, для кожного $a \in G$.
Вправа: довести.

Proposition 1.8.21 Задано $\langle G, * \rangle$ – група та H, K – підгрупи, причому $H \subset K \subset G$. Тоді
$[G : H] = [G : K] \cdot [K : H]$.

Proof.
$[G : H] \cdot \operatorname{card}(H) = \operatorname{card}(G) \qquad [G : K] \cdot \operatorname{card}(K) = \operatorname{card}(G)$.
Звідси випливає, що $[G : H] \cdot \operatorname{card}(H) = [G : K] \cdot \operatorname{card}(K)$.
Зауважимо, що H можна сприймати як підгрупу K (не просто G). А всі сужміжні класи $k * H \subset K$, а тому там є розбиття K на об'єднання суміжних класів $k * H$ – все коректно тоді буде.
$[K : H] \cdot \operatorname{card}(H) = \operatorname{card}(K)$. Підставивши це вище, отримаємо:
$[G : H] = [G : K] \cdot [K : H]$. ■

Theorem 1.8.22 Теорема Ейлера
Задані числа a, n так, що $\gcd(a, n) = 1$. Тоді $a^{\varphi(n)} \equiv 1 \pmod{n}$.
У теорії чисел це доводилось, але покажу інший спосіб.

Proof.
Маємо $\langle U_n, \cdot \rangle$ – скінченна група, причому $\operatorname{card}(U_n) = \varphi(n)$ за визначенням функції Ейлера. Тоді за наслідком теореми Лагранжа, $\overline{a}^{\operatorname{card}(U_n)} = \overline{a}^{\varphi(n)} = \overline{a^{\varphi(n)}} = \overline{1}$. Отже, $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

1.9 Нормальні підгрупи

Definition 1.9.1 Задано $\langle G, * \rangle$ та $H \subset G$ – підгрупа.
Підгрупа називається **нормальною** (або **нормальним дільником**), якщо:

$$\forall g \in G : g * H = H * g$$

Позначення: $H \triangleleft G$.

Remark 1.9.2 Еквівалентне означення: $\forall g \in G : H = g * H * g^{-1}$.

Example 1.9.3 Якщо $\langle G, * \rangle$ – абелева група, то будь-яка підгрупа $H \triangleleft G$.

Example 1.9.4 Для тривіальних підгруп групи $\langle G, * \rangle$ маємо $\{e\} \triangleleft G$ та $G \triangleleft G$. І це згідно з попередніми прикладами.

Example 1.9.5 Маємо $\langle S_3, \circ \rangle$ – група та підгрупа $H = \{(123), (132), (1)\} \overset{\text{або}}{=} \langle (123) \rangle$. У цьому випадку
$(1) \circ H = H \circ (1) = \{(123), (132), (1)\}$
$(23) \circ H = H \circ (23) = \{(23), (13), (12)\}$
$(13) \circ H = H \circ (13) = \{(23), (13), (12)\}$
$(12) \circ H = H \circ (12) = \{(23), (13), (12)\}$
$(123) \circ H = H \circ \varphi_1 = \{(123), (132), (1)\}$
$(132) \circ H = H \circ \varphi_2 = \{(123), (132), (1)\}$
Таким чином, $\{(123), (132), (1)\} \triangleleft S_3$.

Theorem 1.9.6 Критерій нормальної підгрупи
Задано $\langle G, * \rangle$ та $H \subset G$ – підгрупа. Тоді виконується:
$H \triangleleft G \iff \forall g \in G, \forall h \in H : g * h * g^{-1} \in H$.

Remark 1.9.7 Праву частину компактно можна записати таким чином: $\forall g \in G : g * H * g^{-1} \subset H$.

Proof.
$\boxed{\Rightarrow}$ Дано: $H \triangleleft G$.
Нехай $g \in G$ та $h \in H$, тоді звідси $g * h \in g * H \implies g * h \in H * g$, а тому $g * h = \tilde{h} * g \implies \tilde{h} = g * h * g^{-1} \in H$.

$\boxed{\Leftarrow}$ Дано: $\forall g \in G, \forall h \in H : g * h * g^{-1} \overset{\text{позн}}{=} \tilde{h} \in H$. Нам треба $g * H = H * g$.
$x \in g * H \implies x = g * h = g * h * (g^{-1} * g) = g * h * g^{-1} * g = \tilde{h} * g \implies x \in H * g$
$x \in H * g \implies x = h * g = g * g^{-1} * h * g = g * (g^{-1} * h * g) = g * \tilde{h} \implies x \in g * H$.
Таким чином, $g * H = H * g$, а звідси $H \triangleleft G$. ■

Corollary 1.9.8 Маємо $\langle G, * \rangle$ – група та $H \triangleleft G$. Тоді відношення еквівалентності $g_1 \sim_{\text{left}} g_2 \iff g_1^{-1} * g_2 \in H$ та $g_1 \sim_{\text{right}} g_2 \iff g_2 * g_1^{-1} \in H$ збігаються.

Proof.
Оскільки $H \triangleleft G$, то тоді ${}_H/G = G/_H$, оскільки суміжні класи рівні між собою. Тобто $[g]_{\text{left}} = [g]_{\text{right}}$.
Для збіжності двох різних відношень еквівалентності покажемо, що $g_1 \sim_{\text{right}} g_2 \iff g_1^{-1} * g_2 \in H$.
Нехай $g_1 \sim_{\text{right}} g_2$, тобто $g_1 \in [g_2]_{\text{right}} = [g_2]_{\text{left}}$, тобто $g_1 \sim_{\text{left}} g_2$, тобто $g_1^{-1} * g_2 \in H$.
Нехай $g_2 * g_1^{-1} \in H$, тобто $g_1 \sim_{\text{left}} g_2$, тобто $g_1 = [g_2]_{\text{left}} = [g_2]_{\text{right}}$, тобто $g_1 \sim_{\text{right}} g_2$. ■

Example 1.9.9 Маємо $\langle GL_n, \cdot \rangle$ – група.
1. Розглянемо підгрупу SL_n. Покажемо, що $SL_n \triangleleft GL_n$.
Нехай $A \in GL_n$, тобто $\det A \neq 0$. Розглянемо ще $B \in SL_n$, тоді маємо $\det B = 1$. Звідси
$\det\left(ABA^{-1}\right) = \det A \det B \det A^{-1} = \det A \det B \dfrac{1}{\det A} = \det B = 1$.
Таким чином, ми довели, що $ABA^{-1} \in SL_n$. Отже, $SL_n \triangleleft GL_n$.

2. Розглянемо підгрупу $H \subset GL_2$ – набір всіх нижньо трикутних матриць. Покажемо, що $H \not\triangleleft GL_2$.
Дійсно, візьмемо деяку матрицю $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in H$. Візьмемо також елемент $A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \in GL_2$.
Тоді $ABA^{-1} = \begin{pmatrix} -3 & 4 \\ 2 & -1 \end{pmatrix} \notin H$. Отже, $H \not\triangleleft GL_2$.

Example 1.9.10 Розглянемо $\langle S_n, \circ\rangle$. Доведемо, що $A_n \triangleleft S_n$.
Нехай $\sigma \in A_n, \theta \in S_n$. Хочемо, щоб $\theta \circ \sigma \circ \theta^{-1} \in A_n$. Дійсно, це так і буде. Уже відомо, що σ – парна перестановка. Перестановка σ, σ^{-1} мають однакову парність, а тому сума всіх парностей трьох перестановок буде парною.

Remark 1.9.11 Важливо – не забувати перевіряти, що H – підгрупа! У минулих прикладах явно цього не робили.

Example 1.9.12 Маємо $\langle G, *\rangle$ – група на H – підгрупа. Припустимо, що $G/_H = \{H, a * H\}$, тобто всього лише два лівих суміжних класи. Покажемо, що $H \triangleleft G$.

Нехай $g \in G$ та $h \in H$, нам треба довести $g * h * g^{-1} \in H$.
Відомо, що $G = H \sqcup (a * H)$. Значить, у нас будуть два випадки.
$g \in H$, тоді зрозуміло, що $g * h * g^{-1} \in H$ за замкненістю.
$g \in a*H$. Припустимо, що $g*h*g^{-1} \in g*H$, тобто звідси $g*h*g^{-1} = g*\bar{h},\ \bar{h} \in H$. Звідси отримаємо $g^{-1} = h^{-1} * \bar{h}$. Але ця рівність каже, що $g^{-1} \in H$, тож і $g \in H$. Значить, автоматично $g*h*g^{-1} \in H$.

Remark 1.9.13 Для груп $\langle G, *\rangle$ нехай відомо, що $K \triangleleft H$ та $H \triangleleft G$. Тоді із цього в жодному разі не випливає, що $K \triangleleft G$, тобто не виконана умова транзитивності.

Example 1.9.14 Зокрема маємо $\langle D_4, \circ\rangle$ - діедральну групу.
$[s] \triangleleft\ [s, r^2]$ та $[s, r^2] \triangleleft D_4$.
Але тут $[s] \not\triangleleft D_4$. І дійсно, для $s \in [s]$ та $r \in D_4$ маємо:
$rsr^{-1} = rsr^3 = r^2 s = sr^2 \notin [s]$.

Proposition 1.9.15 Ще одна властивість гомоморфізма
Задані $\langle G_1, *\rangle, \langle G_2, \star\rangle$ – групи та $f\colon G_1 \to G_2$ – гомоморфізм. Тоді якщо $N \triangleleft G_2$, то $f^{-1}(N) \triangleleft G_1$.

Proof.
Уже доводили, що $f^{-1}(N)$ буде підгрупою G_1.
Маємо $n \in f^{-1}(N)$ та $g \in G_1$. Тоді $f(n) \in N, f(g) \in G_2$. Оскільки N – нормальний дільник, то звідси $f(g) \star f(n) \star (f(g))^{-1} = f(g * n * g^{-1}) \in N$, а тому $g * n * g^{-1} \in f^{-1}(N)$.
Отже, $f^{-1}(N) \triangleleft G_1$. ■

Corollary 1.9.16 $\ker f \triangleleft G_1$.
Щоправда, за образ так не скажеш.

Example 1.9.17 Приклад, де $\operatorname{Im} f \not\triangleleft G_2$. Розглянемо $\langle H, \cdot\rangle$ – підгрупа всіх нижньотрикутних матриць, причому $H \subset GL_2$. Маємо гомоморфізм $f\colon H \to H$ заданий таким чином:
$f\left(\begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22}\end{pmatrix}\right) = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22}\end{pmatrix}$.
Беремо $A = \begin{pmatrix} 1 & 0 \\ 1 & 1\end{pmatrix} \in H$ та $A = \begin{pmatrix} 1 & 0 \\ 0 & 2\end{pmatrix} \in \operatorname{Im} f$, тоді
$\begin{pmatrix} 1 & 0 \\ 1 & 1\end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2\end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1\end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 2\end{pmatrix} \notin \operatorname{Im} f$.

1.10 Фактогрупи

Theorem 1.10.1 Задано $\langle G, *\rangle$ – група та підгрупа $H \triangleleft G$. На множині $G/_H$ визначимо операцію $*$ таким чином: $(g_1 * H) * (g_2 * H) \overset{\text{def.}}{=} (g_1 * g_2) * H$. Тоді структура $\langle G/_H, *\rangle$ формує групу.

Спочатку прокоментую наступну лему:

Lemma 1.10.2 Операція $*$ на множина $G/_H$ визначена коректно, тобто якщо $a_1 * H = a * H$ та $b_1 * H = b * H$, то звідси $(a_1 * b_1) * H = (a * b) * H$.

Proof.
$(a * b) * H = (a_1 * b_1) * H \iff (a * b) * (b_1^{-1} * a_1^{-1}) \overset{?}{\in} H$.
Оскільки $b_1 * H = b * H$, то звідси $b * b_1^{-1} \overset{\text{позн.}}{=} h_1 \in H$
Тоді $(a * b) * (b_1^{-1} * a_1^{-1}) = a * h_1 * a^{-1}\boxed{=}$
Оскільки $a * h_1 \in a * H = a_1 * H = H * a_1$, то звідси $a * h_1 = h_2 * a_1$
$\boxed{=} h_2 * a_1 * a^{-1}\boxed{=}$
Оскільки $a_1 * H = a * H$, то звідси $a_1 * a^{-1} \overset{\text{позн.}}{=} h_3 \in H$
$\boxed{=} h_2 * h_3 \in H$ за замкненістю операції. ■

Тепер ми можемо довести нашу теорему.

Proof.
$\forall a*H, b*H \in G/_H : (a*H)*(b*H) = (a*b)*H \in G/_H$ – тобто замкненість є.
$\forall a*H, b*H, c*H \in G/_H : (a*H)*[(b*H)*(c*H)] = (a*H)*[(b*c)*H] = (a*[b*c])*H = ([a*b]*c)*H = [(a*b)*H]*(c*H) = [(a*H)*(b*H)]*(c*H))$ – тобто асоціативність є
Нейтральним елементом стане $e*H = H \in G/_H$, тому що $(e*H)*(g*H) = (e*g)*H = g*H$.
Для $a*H \in G/_H$ оберненим елементом стане $(a*H)^{-1} = a^{-1}*H \in G/_H$, тому що $(a*H)*(a*H)^{-1} = (a*H)*(a^{-1}*H) = (a*a^{-1})*H = e*H = H$.
Означення групи перевірено. ■

Definition 1.10.3 Групу $\langle G/_H, * \rangle$ називають **факторгрупою** групи $\langle G, * \rangle$ за нормальною підгрупою $H \triangleleft G$, де операція $*$ визначена:

$$(g_1 * H) * (g_2 * H) \stackrel{\text{def.}}{=} (g_1 * g_2) * H$$

Example 1.10.4 Маємо $\langle \mathbb{R}, + \rangle$ та $\mathbb{Z} \triangleleft \mathbb{R}$. Знайдемо факторгрупу $\mathbb{R}/_{\mathbb{Z}}$.
Розглянемо суміжник клас $x + \mathbb{Z} = \{\dots, -2+x, -1+x, x, 1+x, 2+x, \dots\}$. Зауважимо, що дані суміжні класи будуть різними при $x \in [0, 1)$. При інших x суміжний клас збігатиметься.
Отже, $\mathbb{R}/_{\mathbb{Z}} = \{x + \mathbb{Z} \mid x \in [0, 1)\}$.
У нас зібрались такі множини:
- множина $0 + \mathbb{Z} = \mathbb{Z}$, де всі числа – цілі;
- решта множин $\alpha + \mathbb{Z}$ при $\alpha \in (0, 1)$, де всі числа – не цілі. Але в кожній такій множині описується своя причина, чому так. Наприклад, $0.5 + \mathbb{Z}$ має нецілі числа, тому що 0.5 – неціле число.

Example 1.10.5 Уже відомо, що $A_n \triangleleft S_n$. Знайдемо факторгрупу $S_n/_{A_n}$.
Розглянемо суміжний клас $\sigma \circ A_n$. Якщо $\sigma \in S_n$ – парна перестановка, то звідси $\sigma \circ A_n$ містить всі парні перестановки, тож $\sigma \circ A_n = A_n$. Якщо $\sigma \in S_n$ – непарна перестановка, то тоді $\sigma \circ A_n$ містить всі непарні перестановки, тож $\sigma \circ A_n = S_n \setminus A_n$. Інших суміжних класів нема.
Отже, $S_n/_{A_n} = \{A_n, S_n \setminus A_n\}$.

Corollary 1.10.6 $\text{card}(A_n) = \dfrac{n!}{2}$.

Ще одна мотиваційна причина, чому нас цікавлять саме нормальні підгрупи. Ми можемо спробувати окремо створити групу $\langle G/_H, * \rangle$ та $\langle {}_H/G, * \rangle$ із операцій, які були зазначені вище. Але ми прийдемо до провалу.

Example 1.10.7 Маємо $\langle S_3, \circ \rangle$ – група та підгрупа $H = \{(23), (1)\}$. Уже відомо, що $H \not\triangleleft S_3$. Ми уже знаходили всі ліві суміжні класи. Тому тепер розглянемо множину всіх лівих суміжних класів:
$S_3/_H = \{(1) \circ H, (23) \circ H, (13) \circ H, (12) \circ H, (123) \circ H, (132) \circ H\} \stackrel{\text{або}}{=} \{(1) \circ H, (13) \circ H, (12) \circ H\}$.
Хочеться скопіювати операцію $\circ$ та визначити для цієї множини так:
$(\sigma \circ H) \circ (\varphi \circ H) = (\sigma \circ \varphi) \circ H$.
Але дана операція не коректно визначеною, тобто не має сенс. Тому що візьмемо $((13) \circ H), ((132) \circ H)$ – дві однакові множини з різними іменами та $((12) \circ H), ((123) \circ H)$ – також дві однакові множини з різними іменами. Застосуємо операцію вище:
$((13) \circ H) \circ ((12) \circ H) = ((13) \circ (12)) \circ H = (132) \circ H$.
$((132) \circ H) \circ ((123) \circ H) = ((132) \circ (123)) \circ H = (1) \circ H$.
Проте отримали $(132) \circ H \neq (1) \circ H$.
Також слід зазначити, що отриманий $(132) \circ H \notin S_3/_H$.

Зараз наведемо приклад, де зворотне твердження теореми Лагранжа не працює.

Example 1.10.8 Маємо групу $\langle A_4, \circ \rangle$. Уже знаємо, що $\text{card}(A_4) = 12$.
!Припустимо, що існує підгрупа H, для якого $\text{card}(H) = 6$. Оскільки $[A_4 : H] = 2$, то тоді $H \triangleleft A_4$. Таким чином, $\forall g \in A_4 : \forall h \in H : g \circ h \circ g^{-1} \in H$.
Можна переконатися, що в групі A_4 всього 8 перестановок, що є циклами довжини 3, а тому принаймні один такий потрапить в H. Не втрачаючи загальності, нехай $(123) \in H$. Оскільки H – підгрупа, то $(123)^{-1} = (132) \in H$.
При $h = (123)$ та $g = (124)$ отримаємо $(243) \in H$ за нормальністю. Оскільки H – підгрупа, то $(243)^{-1} = (234) \in H$.
Також $(123) \circ (243) = (124) \in H$, так само $(124)^{-1} = (142) \in H$.
Разом елементи $(123), (132), (243), (234), (124), (142), (1) \ni H$. Отримали $\text{card}(H) > 6$ – суперечність!
Отже, хоч $6 = \text{card}(H) \mid \text{card}(A_4)$, але не існує підгрупи H, щоб $\text{card}(H) = 6$.

1.11 Прямі добутки

1.11.1 Зовнішній прямий добуток

Definition 1.11.1 Задані $\langle G_1, *_1\rangle$ та $\langle G_2, *_2\rangle$ – групи.
(Зовнішнім) прямим добутком двох груп називають множину

$$G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\},$$

на якій визначена операція $*$ таким чином:

$$(a, b) * (c, d) = (a *_1 c, b *_2 d)$$

Proposition 1.11.2 За умовами означення, $\langle G_1 \times G_2, *\rangle$ – група.
Вправа: довести.

Remark 1.11.3 Можна означення розширити до $G_1 \times G_2 \times \cdots \times G_n$ або навіть до $G_1 \times G_2 \times \dots$

Example 1.11.4 Маємо $\langle \mathbb{Z}_3 \times U_5 \times D_4, *\rangle$ - група, де під $*$ ховаються операції $(+, \cdot, \circ)$.
$(\overline{2}, \overline{3}, sr) * (\overline{2}, \overline{4}, sr^2) = (\overline{2} + \overline{2}, \overline{3} \cdot \overline{4}, (sr) \circ (sr^2)) = (\overline{1}, \overline{2}, r)$.

Example 1.11.5 Маємо $\langle \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots, *\rangle$, де під $*$ ховаються операції $(+, +, \dots)$.
$(\overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{1}, \overline{0}, \dots) * (\overline{0}, \overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{1}, \dots) = (\overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \dots)$.

Proposition 1.11.6 Задані $\langle G_1, *_1\rangle$ та $\langle G_2, *_2\rangle$ - групи. Відомо, що для $a \in G_1, b \in G_2$ маємо $\operatorname{ord}(a) = m, \operatorname{ord}(b) = n$. Тоді $\operatorname{ord}((a, b)) = \operatorname{lcm}(m, n)$, де елемент $(a, b) \in G_1 \times G_2$.

Proof.
Позначимо $k = \operatorname{ord}((a, b))$ та $l = \operatorname{lcm}(m, n)$. Маємо $l = ms,\ l = nt$ для деяких $s, t \in \mathbb{N}$. Тоді
$(a, b)^l = (a^l, b^l) = ((a^m)^s, (b^n)^t) = (e_1^s, e_2^t) = (e_1, e_2)$. Отримали $k \mid n$.
А з іншого боку, $(e_1, e_2) = (a, b)^k = (a^k, b^k) \implies a^k = e_1, b^k = e_2$.
Отримали $m \mid k, n \mid k$, а тому k - спільне кратне. А отже, $l \mid k$.
Нарешті, $l = k$. ■

Corollary 1.11.7 $\operatorname{ord}((g_1, \dots, g_n)) = \operatorname{lcm}(\operatorname{ord}(g_1), \dots, \operatorname{ord}(g_n))$.

Example 1.11.8 Маємо елемент $(\overline{9}, \overline{12}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{20}$. Тоді $\operatorname{ord}((\overline{9}, \overline{12})) = \operatorname{lcm}(\operatorname{ord}(\overline{9}), \operatorname{ord}(\overline{12})) = \operatorname{lcm}(4, 5) = 20$.

Theorem 1.11.9 Задані $\langle G_1, *_1\rangle$ та $\langle G_2, *_2\rangle$ – групи. Маємо групу $\langle G_1 \times G_2, *\rangle$ – прямий добуток. Тоді $\hat{G}_1, \hat{G}_2 \triangleleft G_1 \times G_2$, де
$\hat{G}_1 = \{(g_1, e_{G_2}) \mid g_1 \in G_1\} \qquad \hat{G}_2 = \{(e_{G_1}, g_2) \mid g_2 \in G_2\}$.
Більш того, $\hat{G}_1 \cong G_1$ та $\hat{G}_2 \cong G_2$.

Proof.
Ми будемо доводити лише для випадку $\hat{G}_1$, оскільки з $\hat{G}_2$ аналогічно.
Нехай $\hat{g}_1, \hat{h}_1 \in \hat{G}_1$, тобто $\hat{g}_1 = (g_1, e_{G_2}),\ \hat{h}_1 = (h_1, e_{G_2})$. Тоді $\hat{g}_1 * (\hat{h}_1)^{-1} = (g_1 *_1 h_1^{-1}, e_{G_2})$. Оскільки $g_1 * h_1^{-1} \in G_1$, то тоді $\hat{g}_1 * (\hat{h}_1)^{-1} \in \hat{G}_1$. Отже, дійсно $\hat{G}_1$ – підгрупа $G_1 \times G_2$.
Нехай $(g_1, g_2) \in G_1 \times G_2$ та $(h_1, e_{G_2}) \in \hat{G}_1$. Тоді
$(g_1, g_2) * (h_1, e_{G_2}) * (g_1^{-1}, g_2^{-1}) = (g_1 *_1 h_1 *_1 g_1^{-1}, e_{G_2})$, причому $g_1 *_1 h_1 *_1 g_1^{-1} \in G_1$. Отже, цей добуток $(g_1, g_2) * (h_1, e_{G_2}) * (g_1^{-1}, g_2^{-1}) \in \hat{G}_1$.
Установимо відображення $\varphi\colon G_1 \to \hat{G}_1$ таким чином: $\varphi(g_1) = (g_1, e_{G_2})$. Відносно зрозуміло, що це задає гомоморфізм, залишилося довести бієктивність.
$\varphi(g_1) = \varphi(g_2) \implies (g_1, e_{G_2}) = (g_2, e_{G_2}) \implies g_1 = g_2$ – ін'єктивність є.
$x \in \hat{G}_1 \implies x = (g_1, e_{G_2}) \implies \exists g_1 \in G : \varphi(g_1) = (g_1, e_{G_2}) = x$ – сюр'єктивність є.
Отже, ми довели $\hat{G}_1 \cong G_1$. ■

Theorem 1.11.10 Задані числа $m, n \in \mathbb{N}$. Тоді виконується:
$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m, n) = 1$.

Proof.
$\boxed{\Rightarrow}$ Дано: $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Оскільки $\mathbb{Z}_{mn}$ циклічна, то тоді звідси $\mathbb{Z}_n \times \mathbb{Z}_m$ – циклічна. Тоді існує елемент $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, для якого $\mathbb{Z}_m \times \mathbb{Z}_n = [(a, b)]$. Зауважимо, що

$mn = |\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| = \text{ord}((a,b)) = \text{lcm}(\text{ord}(a), \text{ord}(b)) \leq \text{lcm}(m,n) = \dfrac{mn}{\gcd(m,n)}$.
А тому єдиний варіант – це мати $\gcd(m,n) = 1$.
Пояснення першої нерівності: $\text{ord}(a) \mid m$ та $\text{ord}(b) \mid n$. Але тоді звідси $\text{ord}(a), \text{ord}(b) \mid \text{lcm}(m,n)$, тобто $\text{lcm}(m,n)$ – спільне кратне чисел $\text{ord}(a), \text{ord}(b)$, а значить, $\text{lcm}(\text{ord}(a), \text{ord}(b)) \mid \text{lcm}(m,n)$. Власне, звідси $\text{lcm}(\text{ord}(a), \text{ord}(b)) \leq \text{lcm}(m,n)$.

$\boxed{\Leftarrow}$ Дано: $\gcd(m,n) = 1$.
Візьмемо $(\overline{1}, \overline{1}) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Зауважимо, що $\text{ord}((\overline{1}, \overline{1})) = \text{lcm}(\text{ord}(\overline{1}), \text{ord}(\overline{1})) = \text{lcm}(m,n) = mn$.
Тоді звідси $\mathbb{Z}_{mn} \cong [(1,1)] = \mathbb{Z}_m \times \mathbb{Z}_n$ (як циклічни підгрупи). ■

Example 1.11.11 $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_{30}$.
$\mathbb{Z}_6 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_{15}$

1.11.2 Внутрішній прямий добуток

Proposition 1.11.12 Задано $\langle G, * \rangle$ – група, H – підгрупа G та $N \triangleleft G$.
Тоді $H * N \overset{\text{def.}}{=} \{h * n \mid h \in H, n \in N\}$ – підгрупа групи G. Причому також додатково $H * N = N * H$.

Proof.
Ясно, що множина $H * N$ непорожня. Тож нехай $x, y \in H * N$. Тобто $x = h_1 * n_1, y = h_2 * n_2$.
Тоді $x * y^{-1} = h_1 * n_1 * n_2^{-1} * h_2^{-1} = h_1 * n * h_2^{-1} = h_1 * h_2^{-1} * (h_2 * n * h_2^{-1}) = \tilde{h} * \tilde{n}$.
Ясно, що $\tilde{h} \in H$ та $\tilde{n} \in N$. Отже, $x * y^{-1} \in H * N$.

Нехай $x \in H * N$, тобто $x = h * n$ при $h \in H, n \in N$. Оскільки $h \in G$ та $n \in N$, то в силу нормованості $h * n * h^{-1} = \tilde{n} \in K$, звідси $x = h * n = (h * n * h^{-1}) * h = \tilde{n} * h$. Отже, $x \in N * H$.
Нехай $x \in N * H$, тобто $x = n * h$ при $n \in N, h \in H$. Приблизним чином, як минулого разу, отримаємо $x = h * h^{-1} * n * h = h * \tilde{n}$, де $\tilde{n} \in N$. Отже, $x \in H * N$. ■

Remark 1.11.13 Принципово, щоб хоча б одна з підгруп H, N була нормальною.
Зокрема маємо дієдральну групу D_3, дві підгрупи $H = [s]$, $N = [sr]$, тобто маємо $H = \{e, s\}$ та $N = \{e, sr\}$. Звідси $HN = \{e, s, sr, r\}$, що не є підгрупою, бо $sr \cdot r = sr^2 \notin HN$.

Definition 1.11.14 Задані $\langle G, * \rangle$ – група та N_1, N_2 – підгрупи G.
Кажуть, що G є **внутрішнім прямим добутком** N_1, N_2, якщо

$$\forall a \in N_1, \forall b \in N_2 : a * b = b * a$$
$$\forall g \in G : \exists! a \in N_1 : \exists! b \in N_2 : g = a * b$$

Theorem 1.11.15 Критерій внутрішнього прямого добутка
Задані $\langle G, * \rangle$ – група та та N_1, N_2 – підгрупи G.

$$G \text{ – внутрішній прямий добуток } N_1, N_2 \iff \begin{cases} N_1, N_2 \triangleleft G \\ N_1 \cap N_2 = \{e\} \\ G = N_1 * N_2 \end{cases}.$$

Proof.
$\boxed{\Rightarrow}$ Дано: G - внутрішній прямий добуток N_1, N_2.
Нехай $n \in N_1$ та $g \in G \implies g = a * b$ при $a \in N_1, b \in N_2$. Тоді
$g * n * g^{-1} = a * b * n * b^{-1} * a^{-1} = b * (\underbrace{a * n * a^{-1}}_{\in N_1}) * b^{-1} = (a * n * a^{-1}) * b * b^{-1}$
$= a * n * a^{-1} \in N_1$.
Аналогічно $n \in N_2, g \in G \implies g * n * g^{-1} \in N_2$.
Отже, $N_1, N_2 \triangleleft G$.
Нехай $x \in N_1 \cap N_2$. Ми маємо $x = x * e = e * x$ - два розклади. Оскільки $x \in N_1$, разом $e \in N_1$, то в силу єдиності розкладу, $x = e$.
Отже, $N_1 \cap N_2 = \{e\}$. Рівність $G = N_1 * N_2$ є цілком зрозумілою.

$\boxed{\Leftarrow}$ Дано: $\begin{cases} N_1, N_2 \triangleleft G \\ N_1 \cap N_2 = \{e\} \\ G = N_1 * N_2 \end{cases}$.

Розглянемо $z = b * a * b^{-1} * a^{-1}$ (такий вираз називається комутатором).
Із одного боку, $z \in N_1$, тому що $b*a*b^{-1} \in N_1$ в силу того, що $N_1 \triangleleft G$, а також $a \in N_1 \implies a^{-1} \in N_1$.
Із іншого боку, $z \in N_2$, тому що $a * b^{-1} * a^{-1} \in N_2$ в силу того, що $N_2 \triangleleft G$, а також $b \in N_2$.
Разом маємо $z \in N_1 \cap N_2 \implies z = e \implies b * a * b^{-1} * a^{-1} = e$.
Отже, $b * a = a * b$.
!Припустимо, що $g \in G$ має два розклади. Тобто $g = a * b = c * d$. Тут $a, c \in N_1, b, d \in N_2$. Тоді $c^{-1} * a = d * b^{-1}$.
Оскільки $a \in N_1, c \in N_1 \implies c^{-1} \in N_1$, то звідси $d * b^{-1} \in N_1 \implies d * b^{-1} \in N_1 \cap N_2 \implies d * b^{-1} = e \implies d = b$.
А звідси $a = c$. Суперечність!
Таким чином, $g \in G$ має єдиний розклад та $a * b = b * a$, звідси G – внутрішній добуток N_1, N_2. ■

Corollary 1.11.16 Маємо $\langle G_1 \times G_2, * \rangle$. Тоді $\hat{G}_1, \hat{G}_2$ утворює внутрішній прямий добуток.

Proof.
Ми вже знаємо, що $\hat{G}_1, \hat{G}_2 \triangleleft G_1 \times G_2$.
Також якщо $x \in \hat{G}_1 \cap \hat{G}_2$, то $x = (g_1, e_{G_2}), x = (e_{G_1}, g_2)$. Звідси $g_1 = e_{G_1}, g_2 = e_{G_2} \implies x = (e_{G_1}, e_{G_2})$.
Також якщо $(g_1, g_2) \in G_1 \times G_2$, тоді $(g_1, g_2) = (g_1, e_{G_2}) * (e_{G_1}, g_2)$. Значить, $G_1 \times G_2 = \hat{G}_1 * \hat{G}_2$. ■

Remark 1.11.17 Внутрішній прямий добуток групи $\langle G, * \rangle$ можна узагальнити підгрупами $N_1, \ldots, N_k$. Зокрема означення буде таким:

$$\forall a_i \in N_i, \forall b_j \in N_j : i \neq j : a_i * a_j = a_j * a_i$$
$$\forall g \in G : \exists! a_i \in N_i : g = a_1 * \cdots * a_k$$

Theorem 1.11.18 Критерій внутрішнього прямого добутка (≥ 2)
Задані $\langle G, * \rangle$ – група та та $N_1, \ldots, N_k$ - підгрупи G.

$$G \text{ - внутрішній прямий добуток } N_1, \ldots, N_k \iff \begin{cases} N_1, \ldots, N_k \triangleleft G \\ N_i \cap (N_1 * \cdots * N_{i-1} * N_{i+1} * \cdots * N_k) = \{e\} \\ G = N_1 * \cdots * N_k \end{cases} .$$

Theorem 1.11.19 Задано $\langle G, * \rangle$ – група, що є внутрішнім прямим добутком підгруп N_1, N_2. Тоді $G \cong N_1 \times N_2$. Розгорнуто кажучи, $N_1 * N_2 \cong N_2 \times N_2$.

Proof.
Визначимо функцію $f \colon N_1 \times N_2 \to \underset{=G}{N_1 * N_2}$ таким чином:
$f(n_1, n_2) = n_1 * n_2$.
Це буде гомоморфізмом, тому що $\forall (a, b), (c, d) \in N_1 \times N_2$:
$f((a, b) * (c, d)) = f(a * c, b * d) = (a * c) * (b * d) = (a * b) * (c * d) = f(a, b) * f(c, d)$.
Залишилось довести, що f – ізоморфізм.
$f(a, b) = f(c, d) \implies a * b = c * d \implies c^{-1} * a = d * b^{-1}$.
Маємо $c^{-1} * a \in N_1$ а $d * b^{-1} \in N_2$. Отже, $c^{-1} * a \in N_1 \cap N_2 \implies c^{-1} * a = e \implies a = c$. Аналогічно $b = d$. Отже, $(a, b) = (c, d)$ – довели ін'єктивність.
Нехай $y \in G$, тобто $y = a * b$. Тоді $f(a, b) = a * b = y$ – довели сюр'єктивність.
Таким чином, $G = N_1 * N_2 \cong N_1 \times N_2$. ■

Example 1.11.20 Маємо $\langle D_{2n}, \circ \rangle$ – дієдральна група при n – непарне. Розглянемо такі нормальні дільники:
$N_1 = [s, r^2] = \{e, r^2, \ldots, r^{2n-2}, s, sr^2, \ldots, sr^{2n-2}\} \cong D_n$.
$N_2 = [r^n] = \{e, r^n\} \cong \mathbb{Z}_2$.
Зауважимо, що $N_1 \cap N_2 = \{e\}$. Також маємо $D_{2n} = N_1 N_2$: достатньо подивитись на множину $r^n * \{e, r^2, \ldots, r^{2n-2}\}$.
Таким чином, $D_{2n} \cong D_n \times \mathbb{Z}_2$.

Theorem 1.11.21 Задано $\langle G, * \rangle$ – скінченна група та H, K – підгрупи. Тоді $\text{card}(H * K) = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Proof.
Зауважимо, що $H \cap K$ – підгрупа K, тоді звідси $K = ((H \cap K) * k_1) \sqcup \cdots \sqcup ((H \cap K) * k_n)$. Таким чином, $|K| = |H \cap K| \cdot n$.

Хочемо тепер довести, що $H * K = H * k_1 \sqcup \cdots \sqcup H * k_n$.
Нехай $x = h * k \in H * K$. Оскільки $k \in K$, то тоді $k = l * k_j$ для деякого $l \in H \cap K$ та $j = \overline{1,n}$. Але тоді $h * k = (h * l) * k_j \in H * k_j$, оскільки елемент $h, l \in H \implies h * l \in H$. Разом отримали $x \in H * k_1 \sqcup \cdots \sqcup H * k_n$.
Нехай $x \in H * k_1 \sqcup \cdots \sqcup H * k_n$, тобто $x = h * k_j$, але це автоматично $x \in H * K$.
Залишилося припустити, що $(H * k_i) \cap (H * k_j) \neq \emptyset$ при різних i, j. Тобто існує елемент $x \in (H * k_i) \cap (H * k_j)$, а отже, $x = h * k_i = h' * k_j$ при деяких $h, h' \in H$. Звідси випливає, що $(h')^{-1} * h = k_j * k_i^{-1}$. Зауважимо, що $k_j * k_i^{-1} \in K$, але також $k_j * k_i^{-1} = (h')^{-1} * h \in H$. Разом отримали $k_j * k_i^{-1} \in H \cap K$. Але мовою суміжних класів, це означає $k_j * (H \cap K) = k_i * (H \cap K)$. Рівність можлива лише при $i = j$. Отже, $k_i = k_j$.
Власне, остаточно $H * K = (H * k_1) \sqcup \cdots \sqcup (H * k_n)$, але тоді $\operatorname{card}(H * K) = |H * k_1| + \cdots + |H * k_n| = n \cdot |H|$.
$\operatorname{card}(H * K) = n \cdot |H| = \dfrac{|K|}{|H \cap K|} \cdot |H| = \dfrac{|H| \cdot |K|}{|H \cap K|}$. ■

Example 1.11.22 Припустимо $|G| = 28$. Група G має підгрупи H_1, H_2, причому $|H_1| = 7,\ |H_2| = 4$. Зауважимо, що $|H_1 \cap H_2| \mid 7$ та $|H_1 \cap H_2| \mid 4$, тоді звідси єдиний варіант $H_1 \cap H_2 = \{e\}$. Отже, $\operatorname{card}(H_1 * H_2) = 28 = |G|$. Звідси випливає, що $G = H_1 * H_2$.

1.12 Основні теореми про ізоморфізм

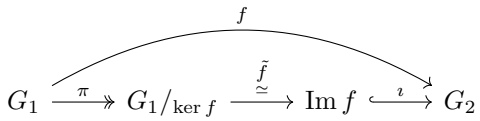
Наша мета розкласти відображення в канонічному вигляді, але цього разу ми маємо справу з гомоморфізмом.

Lemma 1.12.1 Маємо $\langle G, * \rangle$ – група та $N \triangleleft G$. Розглянемо факторвідображення $\pi \colon G \to G/_N$, тобто $\pi(g) = g * N$. Тоді π – гомоморфізм. Крім того, $\ker \pi = N$.
Відображення π називають **проєкцією** (або **природним гомоморфізмом**).

Proof.
Дійсно, $\forall x, y \in G : \pi(x * y) = (x * y) * N = (x * N) * (y * N) = \pi(x) * \pi(y)$.
$\ker \pi = \pi^{-1}(e * N) = \{g \in G : g * N = e * N\} = \{g \in G : g \in N\} = N$. ■

Lemma 1.12.2 Маємо $\langle G, * \rangle$ - група та $H \subset G$ – підгрупа. Розглянемо вкладення $\imath \colon H \to G$. Тоді $\imath$ – гомоморфізм.
Відображення $\imath$ називають **гомоморфізмом вкладень.**
Див. підрозділ 1.3.

Theorem 1.12.3 Задано $\langle G_1, * \rangle$ та $\langle G_2, \star \rangle$ – групи та $f \colon G_1 \to G_2$ – гомоморфізм. Тоді існує єдиний ізоморфізм $\tilde{f} \colon G_1/_{\ker f} \to \operatorname{Im} f$, для якого $\imath \circ \tilde{f} \circ \rho = f$.



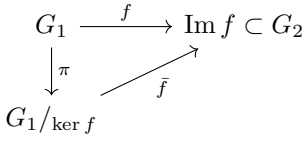
Тут π – проєкція та $\imath$ – вкладення. Більш детально, відображення $\tilde{f}(g * \ker f) = f(g)$.

Remark 1.12.4 Відомо $\ker f \triangleleft G_1$. Ми встановлювали відношення еквівалентності $g_1 \sim g_2 \iff g_1 * g_2^{-1} \in \ker f$ та отримували $G_1/_{\ker f}$. Але можна записати $g_1 \sim g_2 \iff f(g_1) = f(g_2)$. Тобто, по суті кажучи, ми можемо функцію декомпозувати, як це було в дискретній математиці.

Proof.
Насправді, все вже майже доведено. Тільки треба показати, що $\tilde{f}$ буде гомоморфізмом. Дійсно, нехай $g * \ker f, h * \ker f \in G_1/_{\ker f}$. Тоді
$\tilde{f}((g * \ker f) * (h * \ker f)) = \tilde{f}((g * h) * \ker f) = f(x * y) = f(x) * f(y) = \tilde{f}(x * \ker f) * \tilde{f}(y * \ker f)$. ■

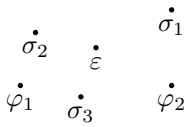
1.12.1 Перша теорема про ізоморфізм

Theorem 1.12.5 Перша теорема про ізоморфізм
Задано $\langle G_1, * \rangle$ та $\langle G_2, \star \rangle$ – групи та $f \colon G_1 \to G_2$ – гомоморфізм. Тоді $G_1/_{\ker f} \cong \operatorname{Im} f$. Ізоморфізм задається діаграмою нижче.

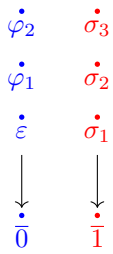


Тут $\bar{f}(g * \ker f) = f(g)$.
Тут нічого нового не написано, тупо попередня теорема.

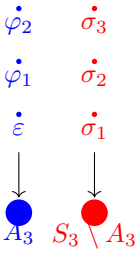
Example 1.12.6 Розглянемо групу $\langle S_3, \circ \rangle$. Для початку картина цих елементів виглядає приблизно так:



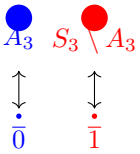
Хотілось би їх організувати під певними властивостями. Розглянемо гомоморфізм $f\colon S_3 \to \mathbb{Z}_2$, який працює ось так:
$f(\sigma) = \overline{0}$, коли σ – парна
$f(\sigma) = \overline{1}$, коли σ – непарна.
Тепер ці елементи ми хоч якось згрупуємо:



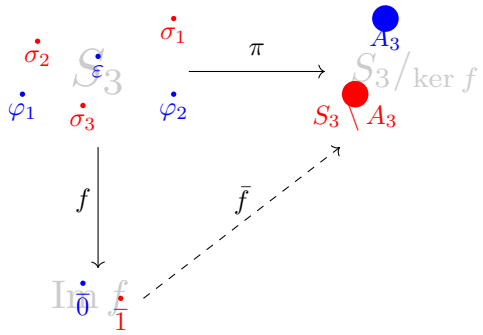
Тепер ми розглядаємо множину $S_3/_{\ker f}$ і зауважуємо, що складається з двох множин, тобто $S_3/_{\ker f} = \{\{\varepsilon, \varphi_1, \varphi_2\}, \{\sigma_1, \sigma_2, \sigma_3\}\} = \{A_n, S_n \setminus A_n\} = S_3/_{A_3}$.
Якщо розглянути проєкцію $\pi\colon S_3 \to S_3/_{\ker f}$, то буде така картина:



Тому очікується, що отримаємо ізоморфізм $\bar{f}\colon S_3/_{\ker f} \to \underset{=\mathbb{Z}_2}{\operatorname{Im} f}$, який описує останній малюнок:



Резюмувати цей приклад можна ось таким крупним малюнком:



Таким чином, $S_3/_{A_3} \cong \mathbb{Z}_2$.

Example 1.12.7 Маємо гомоморфізм $f\colon \mathbb{Z} \to \mathbb{Z}_n$ таким чином: $f(m) = \overline{m}$.
Зрозуміло, що $\operatorname{Im} f = \mathbb{Z}_n$ та $\ker f = n\mathbb{Z}$. Отже, маємо $\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n$.
Насправді, якщо уважно подивитись, то $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$. Тож коли кажуть про адитивну групу класів лишків $\langle \mathbb{Z}/_{n\mathbb{Z}}, + \rangle$, то здебільшого беруть таке позначення.

Example 1.12.8 Маємо гомоморфізм $f\colon D_n \to \mathbb{Z}_2$, що задається так: $r \overset{f}{\mapsto} \overline{0}$ та $s \overset{f}{\mapsto} \overline{1}$. Для інших елементів можна порахувати. Наприклад, $f(sr^2) = f(s) + f(r) + f(r) = \overline{1} + \overline{0} + \overline{0} = \overline{1}$.
Можна зауважити, що $\operatorname{Im} f = \mathbb{Z}_2$ та $\ker f = [r]$. Отже, маємо $D_n/_{[r]} \cong \mathbb{Z}_2$.

Example 1.12.9 Маємо гомоморфізм $\det\colon GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$. Тут групи – мультиплікативні.
Можна показати, що $\operatorname{Im} \det = \mathbb{R} \setminus \{0\}$. Справді, $x \in \mathbb{R} \setminus \{0\}$:

$$\det \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} = x \text{ при } x \neq 0.$$

Також неважко показати, що $\ker \det = SL_n(\mathbb{R})$. Отже, $GL_n(\mathbb{R})/_{SL_n(\mathbb{R})} \cong \mathbb{R} \setminus \{0\}$.

1.12.2 Друга теорема про ізоморфізм

Lemma 1.12.10 Задано $\langle G, * \rangle$ – група, H – підгрупа G та $N \lhd G$. Тоді $N \lhd H * N$.

Proof.
Вимога $N \lhd G$ виправдується тим, що $H * N$ стає групою. А там вже неважко переконатися, що N буде підгрупою $H * N$.
Нехай $u \in H * N$, тобто $u = h * n$, та $\tilde{n} \in N$. Хочемо довести, що $u * \tilde{n} * u^{-1} \in H * N$.
Маємо $u * \tilde{n} * u^{-1} = h * n * \tilde{n} * n^{-1} * h^{-1} = h * \bar{n} * h^{-1}$. Але оскільки $h \in G$ та $N \lhd G$, то $u * \tilde{n} * u^{-1} \in N$, тоді автоматично $u * \tilde{n} * u^{-1} \in H * N$. ■

Theorem 1.12.11 Друга теорема про ізоморфізм
Задано $\langle G, * \rangle$ – група, H - підгрупа G та $N \lhd G$. Тоді $H/_{H \cap N} \cong (H * N)/_N$.

Proof.
Установимо відображення $\varphi\colon H \to (H * N)/_N$ таким чином: $h \mapsto h * N$. Ясно, що це гомоморфізм.
Тоді за першою теоремою про ізоморфізм, $H/_{\ker \varphi} \cong \operatorname{Im} \varphi$.
Доведемо, що $\ker \varphi = H \cap N$. Маємо $h \in \ker \varphi$, тоді $\varphi(h) = e * N \iff h * N = N \iff h \in N$. Але оскільки $\ker \varphi \lhd H$, то звідси $h \in H$, але водночс $h \in N$. Тож $h \in H \cap N$. Остаточно звідси $\ker \varphi = H \cap N$. До речі, $H \cap N = \ker \varphi \lhd H$.
Доведемо, що $\operatorname{Im} \varphi = (H * N)/_N$, а це теж саме, що показати, що φ буде сюр'єктивним відображенням. Нехай $(h * n)N \in (H * N)/_N$. Треба зауважити, що $(h * n) * N = h * N$, просто тому що $h^{-1} * (h * n) = n \in N$. Тобто ми знайшли $h \in H$, для якого $\varphi(h) = h * N = (h * n) * N$.
Нарешті, $H/_{H \cap N} \cong (H * N)/_N$. ■

1.12.3 Третя теорема про ізоморфізм

Theorem 1.12.12 Теорема про відповідність
Задано $\langle G, * \rangle$ – група та $N \lhd G$. Тоді існує бієкція $F\colon U_1 \to U_2$, де окремо $U_1 = \{H$ - підгрупа $G \mid$

$H \supset N\}$, а також $U_2 = \{K$ - підгрупа $G/_N\}$.
Тобто ця теорема каже, що є взаємна однозначність між підгрупами G, що містять N, а також підгрупами $G/_N$.

Хтось ще інколи це називає четвертою теоремою про ізоморфізм.

Proof.
Установимо відображення $F\colon U_1 \to U_2$ за правилом $F(H) = \pi(H)$, де $\pi\colon G \to G/_N$ – природний гомоморфізм. Можна зауважити, що $\pi(H) = \{g * N \mid g \in H\} = H/_N$ (оскільки $N = \ker\pi$, тоді автоматично $N \lhd H$). Покажемо, що це бієктивне відображення.
Нехай K – підгрупа $G/_N$. Побудуємо множину $H = \{g \in G \mid g * N \in K\}$. Доведемо, що $H \in U_1$, тобто треба довести, що H – підгрупа G, а також $H \supset N$.
Для початку $H \neq \emptyset$, оскільки $e \in H$, просто тому що $e * N \in K$ в силу того, що K – підгрупа $G/_N$.
Нехай $x, y \in H$, тобто $x * N, y * N \in K$. Тоді звідси $(x * N) * (y * N)^{-1} \in K$, просто тому що K – підгрупа $G/_N$. Але з іншого боку $(x * N) * (y * N)^{-1} = (x * y^{-1}) * N \in K$, а тому $x * y^{-1} \in H$.
Далі, $H \supset N$, тому що K містить елемент $e * N = N$, а тому H має всі елементи з N.
Нарешті, зауважимо, що $K = H/_N$, за побудовою підгрупи.
Отже, для кожної $K \in U_2$ знайшли $H \in U_1$, де $F(H) = \pi(H) = H/_N = K$ – сюр'єктивність доведена.
Нехай $F(H_1) = F(H_2)$, тобто $H_1/_N = H_2/_N$. Доведемо, що $H_1 = H_2$.
Маємо $x \in H_1$, тоді $x * N \in H_1/_N = H_2/_N$, але тоді звідси $x \in H_2$. У зворотний бік абсолютно аналогічно – ін'єктивність доведена. ■

Lemma 1.12.13 Задано $\langle G, *\rangle$ – група, $M, N \lhd G$ та N – підгрупа M. Тоді $N \lhd M$.

Proof.
Дійсно, нехай $n \in N$ та $m \in M$. Тоді автоматично $m \in G$. Оскільки $N \lhd G$, то звідси $m * n * m^{-1} \in N$.
Отже, $N \lhd M$. ■

Theorem 1.12.14 Третя теорема про ізоморфізм
Задано $\langle G, *\rangle$ – група, $M, N \lhd G$ та N – підгрупа M. Тоді $G/_N/_{M/_N} \cong G/_M$.

Proof.
Перш за все, M – підгрупа G, що містить N, тож за відповідністю, $M/_N$ – підгрупа $G/_N$, причому вона буде нормальною, оскільки $M \lhd G$. Тому далі все буде коректно визначено.
Розглянемо відображення $\varphi\colon G \to G/_N/_{M/_N}$ таким чином: $\varphi = \pi_2 \circ \pi_1$. Тут дві проєкції $\pi_1\colon G \to G/_N$ та $\pi_2\colon G/_N \to G/_N/_{M/_N}$. Відображення φ – сюр'єктивний гомоморфізм, як композиція сюр'єктивних гомоморфізмів. Знайдемо ядро:
$\ker\varphi = \{g \in G \mid \varphi(g) = e * G/_M\} = \{g \in G \mid (g * N) * M/_N = M/_N\} = \{g \in G \mid g * N \in M/_N\} = M$.
Щодо останньої рівності. Нехай $g \in G$ такий, що $g * N \in M/_N$. Тож $g * N = m * N$ при деякому $m \in M$, звідси $g = m * n$ при деякому $n \in N$. Але оскільки N – підгрупа M, то звідси $g \in M$.
Тепер нехай $g \in M$, звідси автоматично $g * N \in M/_N$.
За першою теоремою про ізоморфізм, $G/_M \cong G/_N/_{M/_N}$. ■

2 Просунуті матеріали з теорії груп

2.1 Дія групи, орбіта

Definition 2.1.1 Задано $\langle G, * \rangle$ – групу та множину $A \neq \emptyset$.
Дією групи G на множину A назвемо відображення $\rho\colon G \times A \to A$, що підпорядкована умовами:

$$\forall a \in A : \rho(e_G, a) = a;$$
$$\forall g_1, g_2 \in G : \rho(g_1 * g_2, a) = \rho(g_1, \rho(g_2, a))$$

Remark 2.1.2 Частіше за всього замість $\rho(g, a)$, пишуть ga. Тобто умови переписуються так:
$e_G a = a$
$(g_1 * g_2)a = g_1(g_2 a)$.

Example 2.1.3 Візьмемо дієдральну групу D_4 та множину $\mathbb{R}^2$. Ми встановимо дію таким чином:
$r \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, де дана матриця описує матрицю повороту на 90° проти годинникової стрілки відносно початку координат.
$s \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, де дана матриця описує відбиття площини по OY.
$e \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, де дана матриця нічого не змінює.

Решта дій буде композицією, яка описується множення матриць. Наприклад, $r^2 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$.

Proposition 2.1.4 Задано $\langle G, * \rangle$ – групу та множину $A \neq \emptyset$. Кожна дія ρ групи G на множину A задає гомоморфізм $\sigma\colon G \to S_A$ формулою $\sigma(g)(a) = \rho(g, a), \forall a \in A$.
Навпаки теж працює: кожний гомоморфізм $\sigma\colon G \to S_A$ задає дію групи G на множину A.

Proof.
$\boxed{\Rightarrow}$ Дано: $\rho\colon G \times A \to A$ – дія. Для кожного $g \in G$ формула $\sigma(g)(a) = \rho(g, a)$ буде визначати відображення $\sigma(g)\colon A \to A$. Я хочу пересвідчитись, що це $\sigma(g) \in S_A$, тобто $\sigma(g)$ задає бієкцію на A.
Для нейтрального елемента $\sigma(e_G)(a) = \rho(e_G, a) = a$, для всіх $a \in A$, тобто $\sigma(e_G) = \mathrm{id}_A$.
Для кожних $g_1, g_2 \in G$ маємо наступне:
$\sigma(g_1 * g_2)(a) = \rho(g_1 * g_2, a) = \rho(g_1, \rho(g_2, a)) = \sigma(g_1)[\sigma(g_2)(a)] = (\sigma(g_1) \circ \sigma(g_2))(a)$ – виконано для всіх $a \in A$, тобто $\sigma(g_1 * g_2) = \sigma(g_1) \circ \sigma(g_2)$. Зокрема отримаємо $\sigma(g * g^{-1}) = \sigma(g) \circ \sigma(g^{-1}) = \sigma(e_G) = \mathrm{id}_A$.
Тобто для $\sigma(g)$ знайшовся обернене відображення. Отже, $\sigma(g) \in S_A$.
До речі, ми вже довели $\sigma(g_1 * g_2) = \sigma(g_1) \circ \sigma(g_2)$, тобто σ – гомоморфізм.

$\boxed{\Leftarrow}$ Дано: $\sigma\colon G \to S_A$ – гомоморфізм. Доведемо, це задає дію. Позначимо $\rho(g, a) = \sigma(g)(a)$.
Оскільки σ – гомоморфізм, то звідси $\sigma(e_G) = \mathrm{id}_A$, зокрема це означає, що $\sigma(e_G)(a) = \rho(e_G, a) = a$.
За аналогічною причиною $\sigma(g_1 * g_2) = \sigma(g_1) \circ \sigma(g_2)$, зокрема це означає, що $\rho(g_1 * g_2, a) = \sigma(g_1)(\sigma(g_2)(a)) = \rho(g_1, \sigma(g_2)(a)) = \rho(g_1, \rho(g_2, a))$. ■

Example 2.1.5 Маємо групу $[r]$ – підгрупа дієдральної групи D_3. Маємо $A = \{1, 2, 3\}$, де ці числа відповідають вершинами рівностороннього трикутника.
1. Дію ρ групи $[r]$ на множину A задамо таким чином: r діє на елемент $a \in A$ як поворот трикутника проти годинникової стрілки. Наприклад, $\rho(r^2, 1) = 2,\ \rho(r^2, 2) = 3,\ \rho(r^2, 3) = 1$.
За твердженням, ця дія ρ відповідає гомоморфізму $\sigma\colon [r] \to S_3$ таким чином:

$$e \mapsto \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases}, \ r \mapsto \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases}, \ r^2 \mapsto \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}.$$

Візьмемо іншу підгрупу $[s]$.
2. Дію ρ групи $[s]$ на множину A задамо таким чином: r діє на елемент $a \in A$ як відбиття трикутника відносно осі, що проходить через цю вершину. Наприклад, $\rho(s, 1) = 1,\ \rho(s, 2) = 3,\ \rho(s, 3) = 2$.
За твердженням, це дія ρ відповідає гомоморфізму $\sigma\colon [s] \to S_3$ таким чином:

$$e \mapsto \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases}, \ s \mapsto \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases}$$

Definition 2.1.6 Задано $\langle G, * \rangle$ – групу, що діє на множину $A \neq \emptyset$.
Орбітою елемента $a \in A$ називають таку підмножину:

$$\mathrm{Orb}_G(a) = \{ga \mid g \in G\}$$

Тобто ми фіксуємо елемент $a \in A$ та розглядаємо всі можливі дії.

Remark 2.1.7 Зрозуміло, що $a \in \mathrm{Orb}_G(a)$, просто тому що $e_G a = a$. Тобто $\mathrm{Orb}_G(a) \neq \emptyset$.

Definition 2.1.8 Орбіта називатиметься **тривіальною**, якщо

$$\mathrm{Orb}_G(a) = \{a\}$$

Example 2.1.9 Зокрема по нашому прикладу, якщо взяти другу дію групи $[s]$ на множину A, отримаємо $\mathrm{Orb}_{[s]}(1) = \{1\}$. Також $\mathrm{Orb}_{[s]}(2) = \mathrm{Orb}_{[s]}(3) = \{2, 3\}$.

Proposition 2.1.10 $\mathrm{Orb}_G(a)$ утворюють розбиття множини A.

Proof.
Припустимо, що $\mathrm{Orb}_G(a) \cap \mathrm{Orb}_G(b) \neq \emptyset$ для деяких $a, b \in A$. Значить, мається там $c \in \mathrm{Orb}_G(a) \cap \mathrm{Orb}_G(b)$ таким чином, що $c = g_1 a = g_2 b$ для $g_1, g_2 \in G$. Ми зараз доведемо, що $\mathrm{Orb}_G(a) = \mathrm{Orb}_G(b)$. Нехай $x \in \mathrm{Orb}_G(a)$, тобто $x = ga$ для деякого $g \in A$. Але детально розглянемо $g_1 a = g_2 b$, навіть запишу як $\rho(g_1, a) = \rho(g_2, b)$. Зауважимо:
$a = \rho(e_G, a) = \rho(g_1^{-1} * g_1, a) = \rho(g_1^{-1}, \rho(g_1, a)) = \rho(g_1^{-1}, \rho(g_2, b)) = \rho(g_1^{-1} * g_2, b) \implies a = (g_1^{-1} * g_2)b$.
Значить, тоді $x = g((g_1^{-1} * g_2)b) = [g * (g_1^{-1} * g_2)]b$, причому тут $g * (g_1^{-1} * g_2) \in G$, а тому звідси $x \in \mathrm{Orb}_G(b)$.
Аналогічним чином із $x \in \mathrm{Orb}_G(a)$ випливає $x \in \mathrm{Orb}_G(b)$. ■

Definition 2.1.11 Дія групи $\langle G, * \rangle$ на множину A називається **транзитивною**, якщо

$$\forall a, b \in A : \exists g \in G : b = ga$$

Тобто між будь-якими двома елементами можна законектитися, завдяки елементу, який діє.

Remark 2.1.12 Дія групи $\langle G, * \rangle$ на множину A транзитивна $\iff$ тобто має єдину орбіту.

Example 2.1.13 Узявши першу дію з минулого прикладу, там $\mathrm{Orb}_{[r]}(1) = A$ – і це єдина орбіта в принципі. Тобто дія $[r]$ на A транзитивна.

Definition 2.1.14 Дія групи $\langle G, * \rangle$ на множині A називається **точною** (**faithful action**), якщо

$$\nexists g \in G \setminus \{e\} : ga = a, \forall a \in A$$

Proposition 2.1.15 Дія групи $\langle G, * \rangle$ на множині A точна $\iff$ $\sigma \colon G \to S_A$ – ін'єктивне.
Вправа: довести.

Example 2.1.16 Всі дії з того прикладу – точні.

Definition 2.1.17 Дія групи $\langle G, * \rangle$ на множині A називається **вільною** (**free action**), якщо

$$\forall a \in A : ga \neq a, \forall g \in G \setminus \{e\}$$

Remark 2.1.18 Будь-яка вільна дія – точна дія.

Example 2.1.19 Знову повертаємось до прикладу вище. Перша дія – вільна, а друга дія – ні.

Example 2.1.20 Нехай $\langle G, * \rangle$ – група. Розглянемо операцію G як відображення $\rho \colon G \times G \to G$ таким чином: $\rho(g_1, g_2) = g_1 * g_2$. Тоді
$\rho(e, g) = e * g = g$
$\rho(g_1 * g_2, h) = (g_1 * g_2) * h = g_1 * (g_2 * h) = \rho(g_1, g_2 * h) = \rho(g_1, \rho(g_2, h))$.
Отже, ρ буде дією. Ще кажуть, що **група G діє на собі множенням зліва**.
Така дія – вільна. Дійсно, якщо $g, h \in G$ такі, що $g * h = h$, то миттєво $g = e$.

Theorem 2.1.21 Теорема Келі
Задано $\langle G, * \rangle$ – група. Тоді існує підгрупа перестановок $H \subset S_G$, для якої $\langle G, * \rangle \cong \langle H, \circ \rangle$.
Уже така теорема була. Доведемо з іншого боку цю теорему.

Proof.
Розглянемо дію G на собі множенням зліва. Тоді вона задає гомоморфзм $\sigma \colon G \to S_G$ формулою $\sigma(g)(a) = g * a, \forall a \in G$. Але оскільки дія – вільна (тому автоматично точна), то $\ker \sigma = \{e\}$, тому що відображення ін'єктивне. Тоді $G \cong \mathrm{Im}\, \sigma$, причому $\mathrm{Im}\, \sigma$ – шукана підгрупа S_G. ■

2.2 Спряженість та центр групи

Definition 2.2.1 Задано $\langle G, * \rangle$ – група та $a \in G$.
Елемент $y \in G$ називається **спряженим до** a, якщо

$$\exists x \in G : y = x * a * x^{-1}$$

Позначення: $y = a^x$.

Proposition 2.2.2 Відношення спряженості утворює відношення еквівалентності.

Proof.
$g = e * g * e^{-1}$, для $e \in G$ – виконується рефлексивність.
$h = x * g * x^{-1} \iff g = x^{-1} * h * x = x^{-1} * h * (x^{-1})^{-1}$ – виконується симетричність.
$h = x * g * x^{-1}, k = y * h * y^{-1} \implies k = y * x * g * x^{-1} * y^{-1} = (y * x) * g * (y * x)^{-1}$ – виконується транзитивність.
Отже, $a \sim y \iff y = x * a * x^{-1}$ для деякого $x \in G$. ■

Proposition 2.2.3 Відображення $\rho \colon G \times G \to G$, що задається як $\rho(g, a) = a^g$, задає дію групи $\langle G, * \rangle$ на собі.

Proof.
$\rho(e, a) = a^e = e * a * e^{-1} = a$.
$\rho(g_1 * g_2, a) = a^{g_1 * g_2} = (g_1 * g_2) * a * (g_1 * g_2)^{-1} = g_1 * (g_2 * a * g_2^{-1}) * g_1^{-1} = \rho(g_1, g_2 * a * g_2^{-1}) = \rho(g_1, \rho(g_2, a))$.
Значить, $\rho(g, a) = a^g$ справді задає дію. ■

Proposition 2.2.4 Властивості спряженості
Виконуються такі властивості:
1) $(a^x)^y = a^{x*y}$;
2) $(a * b)^x = a^x * b^x$;
3) $(a^x)^{-1} = (a^{-1})^x$.
1) доводили під час доведення транзитивності. 2) та 3) неважко.

Позначення: $a^G = \{x * a * x^{-1} \mid x \in G\}$ – клас спряжених елементів з a.
Можна зауважити, що, насправді, $a^G = \mathrm{Orb}_G(a)$.

Example 2.2.5 Розглянемо кілька прикладів:
1. $e^G = \{e\}$ для кожної групи $\langle G, * \rangle$.
2. a^G містить один елемент $\iff \langle G, * \rangle$ – абелева група (неважко).
3. Розглянемо групу $\langle GL_n(\mathbb{C}), \cdot \rangle$. Тоді $B^{GL_n(\mathbb{C})}$ – клас спряжених елементів з B – це всі матриці A, що подібні з матрицею B. Для такихх матриць жорданова нормальна форма однакова.
4. Розглянемо групу $\langle Q_8, \cdot \rangle$ – кватерніони. Маємо класи спряженостей:
$1^{Q_8} = \{1\} \qquad (-1)^{Q_8} = \{-1\} \qquad i^{Q_8} = \{-i, i\}$ (аналогічно j, k).

Definition 2.2.6 Задано $\langle G, * \rangle$ – група.
Центром групи G будемо називати таку множину:

$$Z(G) = \{a \in G : \forall x \in G : a * x = x * a\}$$

Елементи $a \in Z(G)$ називають **центральними елементами** групи G.

Remark 2.2.7 Спряженість не точна дія – це теж саме, що сказати, що $\exists g \in G \setminus \{e\} : \forall a \in A : g * a * g^{-1} = a \iff g * a = a * g$. Це теж саме, що сказати, що $g \in Z(G)$.
Отже, спряженість не точна дія $\iff Z(G) \neq \emptyset$.

Remark 2.2.8 Оскільки $e \in Z(G)$, то вже автоматично $Z(G) \neq \emptyset$, тому звідси спряженість автоматично не точна дія (внаслідок чого не вільна дія).

Remark 2.2.9 $a^G = \{a\}$, тобто орбіта – тривіальна $\iff a \in Z(G)$.

Proposition 2.2.10 Задано $\langle G, * \rangle$ – група.
$\langle G, * \rangle$ – абелева $\iff Z(G) = G$.
Зрозуміло.

Example 2.2.11 Зокрема маємо такі приклади:
$Z(S_3) = \{\varepsilon\}$;
$Z(Q_8) = \{1, -1\}$.

Theorem 2.2.12 Задано $\langle G, * \rangle$ – група. Тоді $Z(G) \triangleleft G$, причому $Z(G)$ абелева.

Proof.
Нехай $a, b \in Z(G)$, хочемо показати $a * b^{-1} \in Z(G)$. Справді,
$a * b^{-1} * x = a * b^{-1} * x * b * b^{-1} = a * b^{-1} * b * x * b^{-1} = a * x * b^{-1} = x * a * b^{-1}$.
Нехай тепер $g \in G, h \in Z(G)$, хочемо показати $h * g * h^{-1} \in Z(G)$.
$g * h * g^{-1} * x = g * g^{-1} * h * x = h * x = x * h = x * h * g * g^{-1} = x * g * h * g^{-1}$.
Абелевість $Z(G)$ доводиться миттєво. ■

Proposition 2.2.13 Інший критерій нормальної підгрупи
Задано $\langle G, * \rangle$ – група та H – підгрупа.
$H \triangleleft G \iff H = \bigcup\limits_{h \in H} h^G$.

Proof.
Позначимо $\tilde{H}$ – об'єднання класів спряженості елементів групи H. Тобто $\tilde{H} = \bigcup\limits_{h \in H} h^G$. Звідси отримаємо $\tilde{H} = \bigcup\limits_{g \in G} g * H * g^{-1}$.
$\boxed{\Rightarrow}$ Дано: H – нормальна, тобто $g * H * g^{-1} = H$, але тоді звідси $\tilde{H} = H$.
$\boxed{\Leftarrow}$ Дано: $\tilde{H} = H$, тоді $\forall g \in G : g * H * g^{-1} \subset \tilde{H} = H$, тобто $H \triangleleft G$. ■

2.3 Стабілізатори

Definition 2.3.1 Задано $\langle G, * \rangle$ – група та A – множина. Нехай є дія групи G на множині A.
Стабілізатором елемента $a \in A$ називається підгрупа

$$\mathrm{Stab}_G(a) = \{g \in G \mid ga = a\}$$

Тобто тут всі елементи групи g, для яких точка $a \in A$ буде нерухомою.

Proposition 2.3.2 $\mathrm{Stab}_G(a)$ – підгрупа G.

Proof.
Ясно, що ця множина непорожня, бо $e \in \mathrm{Stab}_G(a)$.
Нехай $u, v \in \mathrm{Stab}_G(a)$, тобто $ua = a,\ va = a$.
$(u * v)a = u(va) = ua = a \implies u * v \in \mathrm{Stab}_G(a)$;
$a = ea = (u^{-1} * u)a = u^{-1}(ua) = u^{-1}a \implies u^{-1} \in \mathrm{Stab}_G(a)$. ■

Lemma 2.3.3 Існує бієкція $\mathrm{Orb}_G(a) \to G/_{\mathrm{Stab}_G(a)}$.

Remark 2.3.4 Хоча $\mathrm{Stab}_G(a) \not\triangleleft G$ загалом, але множина $G/_{\mathrm{Stab}_G(a)}$ все одно визначається як просто клас всіх суміжних класів (тут будуть ліві суміжні).

Proof.
Установимо відображення $\alpha \colon G/_{\mathrm{Stab}_G(a)} \to \mathrm{Orb}_G(a)$ таким чином: $\alpha(g * \mathrm{Stab}_G(a)) = ga$.
Це відображення коректно визначено. Маємо $g_1 * \mathrm{Stab}_G(a) = g_2 * \mathrm{Stab}_G(a)$. Маємо $g_1 * g_2^{-1} \in \mathrm{Stab}_G(a)$, тобто звідси $(g_1 * g_2^{-1})a = a$, а звідси отримаємо $g_1 a = g_2 a$.
Нехай $\alpha(g_1 * \mathrm{Stab}_G(a)) = \alpha(g_2 * \mathrm{Stab}_G(a))$, тобто $g_1 a = g_2 a$, тоді звідси $(g_1 * g_2^{-1})a = a$, тобто $g_1 * g_2^{-1} \in \mathrm{Stab}_G(a)$ або $g_1 * \mathrm{Stab}_G(a) = g_2 * \mathrm{Stab}_G(a)$.
Нехай $x \in \mathrm{Orb}_G(a)$, тобто $x = ga$. Тоді існує $g * \mathrm{Stab}_G(a) \in G/_{\mathrm{Stab}_G(a)}$, де $\alpha(g * \mathrm{Stab}_G(a)) = ga = x$.
Довели, що α – бієктивне відображення. ■

Із даної леми випливає миттєвво теорема:

Theorem 2.3.5 Задано $\langle G, * \rangle$ – скінченна група та A – множина. Маємо дію групи G на A. Тоді $\mathrm{card}(\mathrm{Orb}_G(a)) = [G : \mathrm{Stab}_G(a)]$.

Example 2.3.6 Маємо циклічну групу G порядка 35, що діє на множину A, де $\text{card}(A) = 4$. За щойно доведеною теоремою, $\text{card}(\text{Orb}_G(a)) = [G : \text{Stab}_G(a)]$, тобто $\text{card}(\text{Orb}_G(a)) \mid \text{card}(G) = 35$, звідси маємо $\text{card}(\text{Orb}_G(a)) \in \{1, 5, 7, 35\}$.
Водночас $\text{Orb}_G(a) \subset A$, тобто $\text{card}(\text{Orb}_G(a)) \leq 4$.
Разом отримаємо $\text{card}(\text{Orb}_G(a)) = 1$, тож дія групи G на A буде тривіальною, бо всі орбіти – тривіальні.

Definition 2.3.7 Задано $\langle G, * \rangle$ – скінченна група та A – множина. Маємо дію групи G на A.
Елемент $a \in A$ називається **нерухомою точкою дії групи** G, якщо

$$\text{Stab}_G(a) = G$$

Або інакше кажучи, $\text{card}(\text{Orb}_G(a)) = 1$. Тобто якщо орбіта тривіальна, то точка a є нерухомою.

Corollary 2.3.8 Задано $\langle G, * \rangle$ – p-група та A – множина. Нехай є дія групи G на множині A. Позначимо F за множину всіх нерухомих точок цієї дії. Тоді $\text{card}(F) \equiv \text{card}(A) \pmod{p}$.

Proof.
Ми вже знаємо, що $|G| = [G : \text{Stab}_G(a)]|\text{Stab}_G(a)|$ за теоремою Лагранжа, а також ми знаємо, що $[G : \text{Stab}_G(a)] = |\text{Orb}_G(a)|$. Маючи той факт, що G є p-групою (тобто $|G| = p^r$), то отримаємо $|\text{Orb}_G(a)| \mid p^r$. В силу того, що p – просте, то звідси $|\text{Orb}_G(a)| \in \{1, p, p^2, \ldots, p^r\}$.
За умовою, F – множина нерухомих точок, тобто $F = \{a \in A : |\text{Orb}_G(a)| = 1\}$. Із цього випливатиме, що $\forall a \in A \setminus F : |\text{Orb}_G(a)| \mid p$. Ми вже знаємо, що множина A розбивається орбітами. Доведемо, що множина $A \setminus F$ теж розбивається орбітами тільки елементами з $A \setminus F$.
Якщо $x \in A \setminus F$, то $x \in \text{Orb}_G(a)$, причому обов'язково $a \in A \setminus F$ (у протилежному випадку x сама стане нерухомою точкою, чого ми не вимагали). Якщо $x \in \text{Orb}_G(a)$, де a не є нерухомою, то тоді $x \in A \setminus F$; бо якби x була нерухомою, то, маючи $x = ga$ та $x = gx$, отримали би $x = a$, а це означало б нерухомість точки a, чого ми не вимагали.
Отже, $A \setminus F = \bigsqcup_{a \in A \setminus F} \text{Orb}_G(a) \implies p \mid |A \setminus F| \implies |A| = |A \setminus F| + |F| \equiv |F| \pmod{p}$. ■

Corollary 2.3.9 Задано $\langle G, * \rangle$ – скінченна група та $a \in G$. Тоді $\text{card}(a^G) \mid \text{card}(G)$.

Proof.
Група G діє сама на себе спряженням та $\text{Orb}_G(a) = a^G$. Ми вже знаємо, що $\text{card}(\text{Orb}_G(a)) \mid \text{card}(G)$, але це те, що ми хотіли. ■

2.4 Централізатори та p-групи

Definition 2.4.1 Задано $\langle G, * \rangle$ - група та елемент $a \in G$.
Централізатором елемента a називають таку множину:

$$Z_G(a) = \{g \in G : a * g = g * a\}$$

Інколи ще позначають $C_G(a)$.

Remark 2.4.2 Зауважимо, що $a * g = g * a \iff g * a * g^{-1} = a$.
Якщо розглянути дію спряження, то тоді отримаємо наступне:
$\text{Stab}_G(a) = \{g \in G \mid g * a * g^{-1} = a\} = \{g \in G \mid a * g = g * a\} = Z_G(a)$.
Висновок: централізатором елемента a називають стабілізатор елемента a при дії групи G собою спряженням. Коротше, отримали частинний випадок.

Remark 2.4.3 $a^G = \text{Orb}_G(a) = [G : \text{Stab}_G(a)] = [G : Z_G(a)]$

Remark 2.4.4 $Z(G) = \bigcap_{a \in G} Z_G(a)$ *(вправа: довести)*

Theorem 2.4.5 Задано $\langle G, * \rangle$ – група. Нехай $\Gamma_0 \subset G$ містить рівно по одному представнику від кожного класа спряжності елемента G. Позначимо $\Gamma = \Gamma_0 \setminus Z(G)$. Тоді
$\text{card}(G) = \sum_{a \in \Gamma_0} [G : Z_G(a)] \overset{\text{або}}{=} \text{card}(Z(G)) + \sum_{a \in \Gamma} [G : Z_G(a)]$.

Proof.
Маємо дію групи G на собі – і це спряження.
Робимо нагадування, що $a^G = \mathrm{Orb}_G(a)$.
Зауважимо, що $Z(G)$ у цьому випадку – це множина нерухомих точок. А це означає, що $Z(G)$ містить точки групи G, орбіти яких одноелементні. Справді,
$Z(G) = \{a \in G : \forall g \in G : ga = ag\} = \{a \in G : \forall g \in G : gag^{-1} = a\} = \{a \in G : a^G = \{a\}\} = \{a \in G : \mathrm{Orb}_G(a) = \{a\}\}$.
Ми знаємо, що G розбивається орбітами, тобто $G = \bigsqcup_{a \in \Gamma_0} \mathrm{Orb}_G(a)$. Отже,

$$\mathrm{card}(G) = \sum_{a \in \Gamma_0} \mathrm{card}(\mathrm{Orb}_G(a)) \overset{\text{або}}{=} \mathrm{card}(Z(G)) + \sum_{a \in \Gamma} \mathrm{card}(\mathrm{Orb}_G(a)).$$

Але ми знаємо, що $\mathrm{card}(\mathrm{Orb}_G(a)) = [G : \mathrm{Stab}_G(a)] = [G : Z_G(a)]$. ■

Corollary 2.4.6 Задано $G \neq \{e\}$ – p-група. Тоді $Z(G) \neq \{e\}$.

Proof.
Відомо, що $\mathrm{card}(G) = [G : Z_G(a)]\,\mathrm{card}(Z_G(a))$. Оскільки $\mathrm{card}(G) = p^r$,
$r > 1$, то тоді отримаємо $p \mid [G : Z_G(a)]$ для всіх $a \in \Gamma$, тому що в цьому випадку $[G : Z_G(a)] = \mathrm{card}(\mathrm{Orb}_G(a)) > 1$ (ми беремо ті точки, де орбіта містить більше одного елементу). Тоді
$\mathrm{card}(Z(g)) = \mathrm{card}(G) - \sum_{a \in \Gamma} [G : Z_G(a)] \implies p \mid \mathrm{card}(Z(g))$. ■

Corollary 2.4.7 Задано G – група порядку p^2. Тоді G – абелева.

Proof.
Ми маємо нетривіальну p-групу G, а тому $Z(G)$ також буде нетривіальною. Оскільки $Z(G)$ є підгрупою G, то звідси $\mathrm{card}(Z(G)) \in \{p, p^2\}$.
!Припустимо, що $\mathrm{card}(Z(G)) = p$, тобто існує елемент $a \in G \setminus Z(G)$. Оскільки $\{a\} \cup Z(G) \subset Z_G(a)$, то звідси $\mathrm{card}(Z_G(a)) > p$. Оскільки відомо, що $\mathrm{card}(Z_G(a)) \mid \mathrm{card}(G) = p^2$, то тоді обов'язково $\mathrm{card}(Z_G(a)) = p^2$, тобто звідси $Z_G(a) = G$. Отримали $a \in Z(G)$ – суперечність!
Залишається єдиний варіант – це $\mathrm{card}(Z(G)) = p^2$, звідси $Z(G) = G$, що й означає, що група G – абелева. ■

Remark 2.4.8 Якщо G має порядок $p^k, k > 2$, то ми не можемо сказати загалом, що G – абелева група.
Зокрема дієдральна група D_4 містить $8 = 2^3$ елементів, але не абелева. Ну дійсно, $sr \cdot r \neq r \cdot sr$.

2.5 Нормалізатори

Маємо $\langle G, * \rangle$ – група та множина 2^G (клас всіх підмножин G). Буде група G діяти на 2^G таким чином:
$\rho(g, S) = g * S * g^{-1} \overset{\text{def.}}{=} \{g * s * g^{-1} \mid s \in S\}$ – це теж тіпа спряження.

Definition 2.5.1 Задано $\langle G, * \rangle$ – група та елемент H – підгрупа G.
Нормалізатором підгрупи H називають таку множину:

$$N_G(H) = \{g \in G : g * H * g^{-1} = H\}$$

Зважаючи, яку ми дію задали, тут насправді $N_G(H) = \mathrm{Stab}_G(H)$.

Remark 2.5.2 Нормалізатор – це в деякому сенсі узагальнення централізатора. Якщо в централізаторі ми фіксували $a \in G$, тобто одноточкову множину $\{a\}$, то в нормалізаторі ми фіксуємо аж підгрупу H групи G.

Proposition 2.5.3 $N_G(H)$ – найбільша підгрупа G, що містить H та при цьому $H \triangleleft N_G(H)$.

Proof.
Спочатку нехай $g_1, g_2 \in N_G(H)$, тобто $g_1 * H * g_1^{-1} = H$ та $g_2 * H * g_2^{-1} = H$. Звідси отримаємо:
$(g_1 * g_2) * H * (g_1 * g_2)^{-1} = g_1 * (g_2 * H * g_2^{-1}) * g_1^{-1} = g_1 * H * g_1^{-1} = H$
$g_1 * H * g_1^{-1} = H \implies H * g_1^{-1} = g_1^{-1} * H \implies H = g_1^{-1} * H * (g_1^{-1})^{-1}$.
Довели, що $g_1 * g_2, g_1^{-1} \in H$.
Тепер доведемо, що $N_G(H) \supset H$.

Нехай $a \in H$, тоді автоматично $a^{-1} \in H$. Але тоді
$a * H * a^{-1} = a * (H * a^{-1}) \overset{a^{-1} \in H}{=} a * H \overset{a \in H}{=} H$.
Таким чином, $a \in N_G(H)$. Той факт, що $H \lhd N_G(H)$, доводиться легко.
!Припустимо тепер, що існує $M \supset N_G(H)$ – більша підгрупа G, що містить H та $H \lhd M$. Але тоді за нормальністю, $\forall m \in M : H = m * H * m^{-1}$, тобто автоматично $m \in N_G(H)$, а тому $M \subset N_G(H)$. ■

Definition 2.5.4 Задано $\langle G, * \rangle$ – група, де $G \neq \{e\}$.
Група називається **простою**, якщо в неї нема власних нормальних підгруп, відмінних від $\{e\}$.

Remark 2.5.5 Тобто $\{e\}$ уже не буде простою групою.

2.6 Теореми Сілова

Definition 2.6.1 Задано $\langle G, * \rangle$ – скінченна група та p – просте число. Із порядка $|G|$ відокремимо найбільший можливий степінь простого числа p, тобто буде $|G| = p^r \cdot m$, де $m \nmid p$.
p-підгрупою Сілова називають підгрупу порядка p^r (найбільша p-підгрупа).

Theorem 2.6.2 Перша теорема Сілова
Задано $\langle G, * \rangle$ – скінченна група та p – просте число. Відомо, що існує $k \in \mathbb{N}$, для якого $p^k \mid |G|$. Тоді група G містить підгрупу порядка p^k.

Як наслідок, у кожній скінченній групі існує p-сіловська підгрупа.

Proof.
!Припустимо, що існує скінченна група $\langle G, * \rangle$, просте число p, для яких хоч й існує $k \in \mathbb{N}$, для якого $p^k \mid |G|$, але при цьому G не містить підгрупу порядка p^k.
Ми оберемо групу G з найменшим можливим порядком $|G|$, щоб виконувалося те, що ми припустили. Тоді для всіх інших груп з меншим порядком, ніж $|G|$, I теорема Сілова виконуватиметься. Хочемо довести, що $p \mid |Z(G)|$, де нам вже відомо, що $|G| = |Z(G)| + \sum_{a \in \Gamma} [G : Z_G(a)]$. Для цього залишилося довести, що p ділить будь-який індекс підгрупи G.
!!Припустимо, що існує нетривіальна підгрупа H, для якої $p \nmid [G : H]$. Оскільки відомо, що $p^k \mid |G|$, то тоді обов'язково $p^k \mid |H|$ із теореми Лагранжа. Оскільки $|H| < |G|$, то тоді працює I теорема Сілова: H містить підгрупу порядка p^k. Зрозуміло, що G також – суперечність!!
Із цього випливає зокрема, що $p \mid [G : Z_G(a)]$ для всіх $a \in \Gamma$.
Отже, маємо $p \mid |Z(G)|$. За теоремою Коші абелевих груп, знайдеться елемент $g \in Z(G)$, для якого $\text{ord}(g) = p$. Але тоді $[g] \lhd G$ в силу того, що $[g] \subset Z(G)$.
Тому розглянемо групу $G' = G/_{[g]}$. За теоремою Лагранжа, $|G'| = \dfrac{|G|}{p}$. Оскільки $p^k \mid |G|$, тоді $p^{k-1} \mid |G'|$. Оскільки також $|G'| < |G|$, то працює I теорема Сілова: G' містить підгрупу H' порядка p^{k-1}. Але за відповідністю, H' відповідає $H \supset [g]$ – підгрупа G, зокрема тоді $H' = H/_{[g]}$.
Нарешті, $|H| = p|H'| = p^k$, звідси G містить підгрупу H порядка p^k – суперечність! ■

Theorem 2.6.3 Друга теорема Сілова
Задано $\langle G, * \rangle$ – скінченна група та p – просте число. Оберемо P – p-підгрупу Сілова. Нехай H – p-підгрупа G. Тоді існує елемент $g \in G$, для якого $H \subset g * P * g^{-1}$.

Як наслідок, якщо P_1, P_2 – дві p-підгрупи Сілова, то тоді вони є спряженими: $\exists g \in G : P_2 = g * P_1 * g^{-1}$.

Proof.
Розглянемо дію групи H множенням зліва на множини суміжних класів $G/_P$. У нас буде $h(a * P) = (h * a) * P$. Оскільки $|G/_P| = [G : P]$, тобто це буде взаємно просте число з p, то звідси дана дія містить нерухомі точки, за **Crl. 2.3.8**. Оберемо $a * P \in G/_P$ – нерухома точка, тобто $h * a * P = a * P$, для всіх $h \in H$.
$\forall h \in H : h * a * P = a * P \implies \forall h \in H : a^{-1} * h * a * P = P \implies \forall h \in H : a^{-1} * h * a \in P \implies a^{-1} * H * a \subset P \implies H \subset a * P * a^{-1}$. ■

Для наступної теореми над знадобиться корисна лема.

Lemma 2.6.4 Задано $\langle G, * \rangle$ – скінченна група та H – підгрупа. Нехай H діє на $G/_H$ множенням лівих суміжних класів.
$a * H \in G/_H$ – нерухома точка $\iff a * H \subset N_G(H)$.
Значить, кількість нерухомих точок даної дії дорівнює $[N_G(H) : H]$.

Proof.
Аналогічно, як це було з другою теоремою Сілова, доведемо, що
$a * H$ – нерухома точка $\iff H \subset a * H * a^{-1}$.
Останнє еквівалентне тому, що $a \in N_G(H)$ (див. означення нормальних підгруп). А це теж саме, що $a * H \subset N_G(H)$.
Нарешті, оскільки $H \triangleleft N_G(H)$, то звідси $[N_G(H) : H]$ – кількість нерухомих точок. ■

Theorem 2.6.5 Третя теорема Сілова
Задано $\langle G, * \rangle$ – скінченна група та p – просте число. Маємо $|G| = p^r m,\ p \nmid m$. Позначимо N за кількість p-підгруп Сілова групи G. Тоді $N \mid m$ та $N \equiv 1 \pmod{p}$.

Proof.
За першою теоремою Сілова, бодай одна p-підгрупи Сілова P існує.
За другою теоремою Сілова, множина всіх p-підгруп Сілова – це множина всіх спряжених до P. Якщо розглядати дію групи G спряженням на 2^G, то отримаємо, що $\mathrm{Orb}_G(P)$ – це та сама множина, яка описує множину всіх спряжених до P, а до того ж $\mathrm{Stab}_G(P) = N_G(P)$. За умовою, $N = |\mathrm{Orb}_G(P)|$, тоді ми знаємо, що $|\mathrm{Orb}_G(P)| = N = [G : N_G(P)]$.
Спочатку доведемо, що $N \mid m$. Дійсно,
$m = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P] = N_p \cdot [N_G(P) : P]$.
Залишилося довести, що $N \equiv 1 \pmod{p}$.
Нехай P діє на $G/_P$ множенням лівих суміжних класів. Позначимо F за множину нерухомих точок. Тоді за лемою, $|F| = [N_G(P) : P]$. Оскільки P є p-підгрупою, то звідси $|F| \equiv |G/_P| \pmod{p}$. Але тоді
$[N_G(P) : P] \equiv m \pmod{p}$.
$N_p \cdot [N_G(P) : P] = N_p \cdot m \equiv m \pmod{p}$.
Утім оскільки $p \nmid m$, то автоматом $N_p \equiv 1 \pmod{p}$. ■

2.7 Застосування теорем Сілова

Theorem 2.7.1 Теорема Коші
Задано $\langle G, * \rangle$ – скінченна група та p – просте число, причому $p \mid |G|$. Тоді існує елемент $g \in G$, для якого $\mathrm{ord}(g) = p$.

Proof.
За першою теоремою Сілова, існує підгрупа H групи G, для якої $|H| = p$. За наслідком теореми Лагранжа, така підгрупа – циклічна, тож $H = [h]$. Причому $h \in G$, а також $\mathrm{ord}(h) = p$. ■

2.8 Простота знакозмінної групи

Lemma 2.8.1 A_n породжена циклами довжини 3.

Proof.
Якщо $\sigma \in A_n$, то це парна перестановка, а тому кількість транспозицій – парна. Розіб'ємо їх на пари. Нам достатньо довести, що добуток двох довільних транспозицій формує цикл довжини 3.
Нехай (ij), (kl) – транспозиції. Кілька випадків:
1) $\mathrm{card}(\{i, j\} \cap \{k, l\}) = 2$, тобто фактично $(ij) = (kl)$. Звідси випливає, що $(ij) \circ (kl) = (ij)^2 = \varepsilon = (123)^3$;
2) $\mathrm{card}(\{i, j\} \cap \{k, l\}) = 1$, тут не втрачаючи загальності, нехай $j = l$. Тоді звідси $(ij) \circ (kj) = (ijk)$;
3) $\{i, j\} \cap \{k, l\} = \emptyset$, тобто ці транспозиції незалежні. Звідси отримаємо $(ij) \circ (kl) = (ijk) \circ (jkl)$. ■

Lemma 2.8.2 Спряженість в S_n
Нехай $\tau \in S_n$, а також $\sigma \in S_n$, причому
$\sigma = (a_1 \dots a_r) \circ (b_1 \dots b_s) \circ \dots \circ (c_1 \dots c_l)$.
Тоді $\tau \circ \sigma \circ \tau^{-1} = (\tau(a_1) \dots \tau(a_r)) \circ (\tau(b_1) \dots \tau(b_s)) \circ \dots \circ (\tau(c_1) \dots \tau(c_l))$.

Proof.
Легко зауважити, що виконуєтсья наступне:
$\tau \circ \sigma \circ \tau^{-1} = \tau \circ (a_1 \dots a_r) \circ \tau^{-1} \circ \tau \circ (b_1 \dots b_s) \circ \tau^{-1} \circ \dots \circ \tau \circ (c_1 \dots c_l) \circ \tau^{-1}$.
Отже, достатньо довести лему лише для циклів:
$\tau \circ (a_1 \dots a_r) \circ \tau^{-1} = (\tau(a_1) \dots \tau(a_r))$.
Позначимо $\sigma = \tau(a_1 \dots a_r)\tau^{-1}$. Припустимо, що $\tau(a_i) = b_i$. Хочемо довести, що $\sigma = (b_1, \dots, b_r)$.
$\sigma(b_i) = \tau(a_1 \dots a_r)\tau^{-1}(b_i) = \tau(a_1 \dots a_r)(a_i) = \tau(a_{i+1}) = b_{i+1}$.
$\sigma(k) = \tau(a_1 \dots a_r)\tau^{-1}(k) = \tau(a_1 \dots a_r)(m) = \tau(m) = k$ при $k \notin \{b_1, \dots, b_r\}$. Зауважимо, що $\tau(m) = k$, при цьому також $m \notin \{b_1, \dots, b_r\}$. ■

Definition 2.8.3 Типом перестановки $\sigma \in S_n$ називають розбиття числа n, що відповідає набору довжин незалежних циклів (включаючи цикл довжини 1), добутком яких є σ.

Example 2.8.4 Маємо $\sigma = (14) \circ (23756)$. Тоді його типом буде розбиття $8 = 2 + 5 + 1$.

Corollary 2.8.5 Маємо перестановки $\sigma, \sigma' \in S_n$.
σ, σ' – спряжені $\iff$ σ, σ' мають однаковий тип.

Proof.
$\boxed{\Rightarrow}$ *див. попередню лему.*

$\boxed{\Leftarrow}$ Дано: σ, σ' мають однаковий тип $n = r + s + \dots + t$.
$\sigma = (a_1 \dots a_r) \circ (b_1 \dots b_s) \circ \dots \circ (c_1 \dots c_l)$;
$\sigma' = (a'_1 \dots a'_r) \circ (b'_1 \dots b'_s) \circ \dots \circ (c'_1 \dots c'_l)$.
Визначимо відображення $\tau\colon \{1, \dots, n\} \to \{1, \dots, n\}$ таким чином:
$\tau(a_i) = a'_i,\ \tau(b_j) = b'_j,\ \tau(c_k) = c'_k$.
Зауважимо, що воно задає бієкцію в силу того, що три носії кожної перестановки утворюють розбиття $\{1, \dots, n\}$. Таким чином, $\tau \in S_n$. Нарешті,
$\tau \circ \sigma \circ \tau^{-1} = (\tau(a_1) \dots \tau(a_r)) \circ (\tau(b_1) \dots \tau(b_s)) \circ \dots \circ (\tau(c_1) \dots \tau(c_l)) =$
$= (a'_1 \dots a'_r) \circ (b'_1 \dots b'_s) \circ \dots \circ (c'_1 \dots c'_l) = \sigma'$. ■

Example 2.8.6 Розглянемо групу S_3, де всього два цикли довжини 3:
$\sigma_1 = (123),\ \sigma_2 = (132)$, причому другий цикл $\sigma_2 = \sigma_1^2$.
Знаючи, що A_3 породжена циклами довжини 3 та результатом вище, отримаємо, що $A_3 = [\sigma_1]$. Оскільки $|A_3| = 3$, то вона містить лише тривіальні підгрупи, а тому це – проста група.

Example 2.8.7 Розглянемо групу S_4 та всі перестановки вигляду $2 + 2$. Їх всього три: $\sigma_1 = (12)(34),\ \sigma_2 = (13)(24),\ \sigma_3 = (14)(23)$.
Зауважимо, що всі $\sigma_1, \sigma_2, \sigma_3 \in A_n$, причому кожний з них має порядок 2 (тому що $\sigma_i^{-1} = \sigma_i$). Також зазначимо, що $\sigma_i\sigma_j = \sigma_k$ при різних $i, j, k \in \{1, 2, 3\}$.
Разом із цими результатами, множина $K = \{\varepsilon, \sigma_1, \sigma_2, \sigma_3\}$ утворює підгрупу A_4. Більш того, $K \triangleleft A_4$, тому що всі перестановки одного типу – спряжені. Тобто $\forall \tau \in S_4 : \tau \circ K \circ \tau^{-1} = K$.
Отже, A_4 – не проста група, бо існує нетривіальна підгрупа $K \subsetneq A_4$ (бо $(123) \in A_4 \setminus K$).

Definition 2.8.8 Отримана підгрупа K називається **четвертою групою Кляйна**. Вона складається з 4 елементів, кожний з який оборотний самому себе.

Lemma 2.8.9 Всі цикли довжини 3 спряжені в $A_n,\ n \geq 5$.

Proof.
Нехай $\sigma = (ijk)$. Достатньо довести, що σ спряжена з елементом (123). Для цього зафіксуємо бієкцію $\tau\colon \{1, \dots, n\} \to \{1, \dots, n\}$ таким чином: $\tau(i) = 1, \tau(j) = 2, \tau(k) = 3$. Звідси
$\tau \circ \sigma \circ \tau^{-1} = (\tau(i)\tau(j)\tau(k)) = (123)$.
$\tau \in A_n \implies$ доведено.
$\tau \notin A_n \implies$ розглянемо перестановку $\tilde{\tau} = (45) \circ \tau$. Тепер $\tilde{\tau} \in A_n$, причому $\tilde{\tau}(i) = \tilde{\tau}(i) = 1, \tilde{\tau}(j) = \tilde{\tau}(j) = 2, \tilde{\tau}(k) = \tilde{\tau}(k) = 3$. ■

Remark 2.8.10 Питання, що відбувається з $n \in \{3, 4\}$.
Для $A_3 = \{(1), (123), (132)\}$ зауважимо, що (123) не спряжений з (132) в групі A_3. Тому що який б $\tau \in A_3$ я не взяв, $(123) \neq \tau(132)\tau^{-1}$.
Для A_4 кількість класів спряженості ділить $|A_n| = 12$, кількість 3-циклів тут всього 8. Значить, всі вони не лежать в одному класу спряженості.

Lemma 2.8.11 Задано перестановку $\sigma \in A_n, n \geq 5$, причому $\sigma \neq \varepsilon$. Припустимо, що σ не є циклом довжини 3. Тоді існує перестановка $\tau \in A_n$, для якої $\tau\sigma\tau^{-1}\sigma^{-1} \neq \varepsilon$ та має більше нерухомих точок, аніж σ.

Proof.
1. Припустимо, що σ розписується як добуток неперетинних транспозицій. Тоді цих транспозицій хоча б 2 штуки, оскільки перестановка – парна та нетотожна. Не втрачаючи загальності, нехай $\sigma = (12)(34)\rho$, де перестановка ρ – це (можливо) добуток решти транспозицій, що має уже нерухомі точки $1, 2, 3, 4$. Оскільки $n \geq 5$, покладемо $\tau = (345) \in A_n$.
Нехай $f \in \{1, 2, \ldots, n\}$ – нерухома точка σ. Тоді автоматично $f \geq 5$, бо в протилежному випадку вона буде рухомою через (12) або (34).
Якщо нерухома точка $f \geq 6$ для σ, то вона буде нерухомою точкою для
$\tau\sigma\tau^{-1}\sigma^{-1}$, оскільки
$\tau\sigma\tau^{-1}\sigma^{-1}(f) = \tau\sigma\tau^{-1}(f) = \tau\sigma(f) = \tau(f) = f.$
Також зауважимо, що $1, 2$ – нерухомі точки для $\tau\sigma\tau^{-1}\sigma^{-1}$:
$\tau\sigma\tau^{-1}\sigma^{-1}(1) = \tau\sigma\tau^{-1}(2) = \tau\sigma(2) = \tau(1) = 1.$
$\tau\sigma\tau^{-1}\sigma^{-1}(2) = \tau\sigma\tau^{-1}(1) = \tau\sigma(1) = \tau(2) = 2.$
Отже, $\tau\sigma\tau^{-1}\sigma^{-1}$ має більше фіксованих точок, аніж σ. Нарешті,
$\tau\sigma\tau^{-1}\sigma^{-1}(3) = \tau\sigma\tau^{-1}(4) = \tau\sigma(3) = \tau(4) = 5.$
Отже, $\tau\sigma\tau^{-1}\sigma^{-1} \neq \varepsilon$.

2. Припустимо, що σ не розписується як добуток неперетинних транспозицій. Тоді існує цикл довжини хоча б три. Не втрачаючи загальності, нехай $\sigma = (123\ldots)\rho$, де ρ діє на підмножину $\{4, \ldots, n\}$. За умовою леми, $\sigma \neq (123)$, тобто не є 3-циклом. Значить, σ рухає ще хоча би дві точки. Не втрачаючи загальності, це будуть $4, 5$.
Бо якби це було не так, то $\sigma = (123r)$ для деякого r, але $\sigma \notin A_n$, що неможливо.
Нехай $f\{1, 2, \ldots, n\}$ – нерухома точка σ. Тода автоматично $f \geq 6$.
Якщо нерухома точка $f \geq 6$ для σ, то аналогічними міркуваннями вона буде нерухомою для $\tau\sigma\tau^{-1}\sigma^{-1}$. Більше того, точка $f = 2$ також нерухома для $\tau\sigma\tau^{-1}\sigma^{-1}$. Отже, $\tau\sigma\tau^{-1}\sigma^{-1}$ містить більше нерухомих точок, аніж σ. Нарешті,
$\tau\sigma\tau^{-1}\sigma^{-1}(3) = \tau\sigma\tau^{-1}(2) = \tau\sigma(2) = \tau(3) = 4.$
Отже, $\tau\sigma\tau^{-1}\sigma^{-1} \neq \varepsilon$.

3. Залишилося довести, що якщо $\tilde{\sigma}$ задовольняє лемі, то будь-яка спряжена перестановка до σ також задовольняє лемі.
Нехай $\sigma \in A_n$, не є 3-циклом та $\sigma \neq \varepsilon$. За умовою, $\tilde{\sigma} = \alpha\sigma\alpha^{-1},\ \alpha \in S_n$. Звідси, оскільки вони мають однаковий тип перестановки, то:
1) $\tilde{\sigma} \in A_n$;
2) кількість нерухомих точок $\tilde{\sigma}$ така сама, як в σ;
3) $\tilde{\sigma}$ також не 3-цикл та $\tilde{\sigma} \neq \varepsilon$.
Отже, вона підпорядковується умовам леми, а для цієї перестановки лема працює. Тобто існує $\tilde{\tau} \in A_n$, для якої $\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\tilde{\sigma}^{-1} \neq \varepsilon$ та має більше нерухомих точок, аніж $\tilde{\sigma}$.
Розглянемо перестановку $\tau = \alpha^{-1}\tilde{\tau}\alpha$. Оскільки вона спряжена до $\tilde{\tau}$, то $\tau \in A_n$. Також $\alpha^{-1}\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\tilde{\sigma}^{-1}\alpha = \tau\sigma\tau^{-1}\sigma^{-1}$.
Спочатку треба довести, що $\forall\beta \in S_n : \alpha^{-1}\beta^{-1}\alpha = (\alpha^{-1}\beta\alpha)^{-1}$. Дійсно,
$\varepsilon = \alpha^{-1}\alpha = \alpha^{-1}\beta^{-1}\beta\alpha = \alpha^{-1}\beta^{-1}\alpha\alpha^{-1}\beta\alpha$
$\varepsilon = \alpha^{-1}\beta\alpha\alpha^{-1}\beta^{-1}\alpha$ (аналогічним чином).
Далі запаситися терпінням:
$\alpha^{-1}(\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\tilde{\sigma}^{-1})\alpha = (\alpha^{-1}\tilde{\tau}\alpha)(\alpha^{-1}\tilde{\sigma}\alpha)(\alpha^{-1}\tilde{\tau}^{-1}\alpha)(\alpha^{-1}\tilde{\sigma}^{-1}\alpha) =$
$= \tau\sigma(\alpha^{-1}\tilde{\tau}\alpha)^{-1}(\alpha^{-1}\tilde{\sigma}\alpha)^{-1} = \tau\sigma\tau^{-1}\sigma^{-1}.$
У силу спряженості такої перестановки ми доведемо, що кількість нерухомих точок у $\tau\sigma\tau^{-1}\sigma^{-1}$ така сама, як і в $(\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\tilde{\sigma}^{-1})$. Значить, теж має більше нерухомих точок, ніж σ. ■

Theorem 2.8.12 A_n – проста при $n \geq 5$.

Proof.
Достатньо довести, що якщо $n \geq 5$, то кожна нетривіальна нормальна підгрупа $N \triangleleft A_n$ містить 3-цикл.
Тому що всі 3-цикли спряжені в A_n. Оскільки $N \triangleleft A_n$ та містить 3-цикл, то N містить усі 3-цикли. Тобто N породжує A_n, тобто $N = A_n$, що завершить доведення.

Розглянемо $N \triangleleft A_n$, причому $N \neq \{\varepsilon\}$. Оберемо нетотожний $\sigma \in N$ – перестановка з найбільшим числом нерухомих точок.
!Припустимо, що σ не є 3-циклом. Тоді існує перестановка $\tau \in A_n$, для яких $\tau\sigma\tau^{-1}\sigma^{-1} \neq \varepsilon$ та місить більше нерухомих точок, аніж σ. При цьому оскільки $\sigma^{-1} \in N$ та $\tau\sigma\tau^{-1} \in N$ в силу нормованості, то звідси $\tau\sigma\tau^{-1}\sigma^{-1} \in N$. Суперечність!
Тож σ має бути 3-циклом обов'язково. ■

2.9 Комутанти

Definition 2.9.1 Задано $\langle G, * \rangle$ – група та $x, y \in G$.
Комутатором x, y назвемо об'єкт

$$[x, y] = x * y * x^{-1} * y^{-1}$$

Proposition 2.9.2 Властивості комутаторів
Нехай $\langle G, * \rangle$, $\langle H, \star \rangle$ – групи. Справедливі такі пункти:
1) $x * y = [x, y] * (y * x)$;
2) x, y комутують між собою $\iff [x, y] = e$;
3) $[x, y]^{-1} = [y, x]$;
4) $[x^g, y^g] = [x, y]^g, g \in G$;
5) Нехай $\varphi\colon G \to H$ – гомоморфізм груп. Тоді $\varphi([x, y]) = [\varphi(x), \varphi[y])$.

Proof.
Доведемо кожну властивість:

1) $x * y = x * y * x^{-1} * y^{-1} * y * x = [x, y] * y * x$

2) Якщо x, y комутують, тобто $x * y = y * x$, то звідси $[x, y] = x * y * x^{-1} * y^{-1} = y * x * x^{-1} * y^{-1} = e$.
Якщо $[x, y] = e$, тобто $x * y * x^{-1} * y^{-1} = e$, то звідси $x * y = y * x$

3) $[x, y]^{-1} = (x * y * x^{-1} * y^{-1})^{-1} = y * x * y^{-1} * x^{-1} = [y, x]$

4) $[x^g, y^g] = x^g * y^g * (x^g)^{-1} * (y^g)^{-1} =$
$= (g^{-1} * x * g) * (g^{-1} * y * g) * (g^{-1} * x^{-1} * g) * (g^{-1} * y^{-1} * g) =$
$= g^{-1} * (x * y * x^{-1} * y^{-1}) * g = g^{-1} * [x, y] * g = [x, y]^g$

5) $\varphi([x, y]) = \varphi(x * y * x^{-1} * y^{-1}) = \varphi(x) \star \varphi(y) \star \varphi(x^{-1}) \star \varphi(y^{-1}) =$
$= \varphi(x) \star \varphi(y) \star (\varphi(x))^{-1} \star (\varphi(y))^{-1} = [\varphi(x), \varphi(y)].$

Всі властивості доведені. ■

Remark 2.9.3 Перша властивість каже, що комутатор x, y – тіпа коректуючий множник, що дозволяє переставляти x, y місцями.

Definition 2.9.4 Задано $\langle G, * \rangle$ – група.
Комутантом (або **похідною**) групи G називають підгрупу

$$G' = \langle [x, y] \mid x \in G, y \in G \rangle$$

Тобто це підгрупа, породжена комутаторами.

Remark 2.9.5 Ми знаємо, що в породжуючих елементах там фігурує добуток елементів, деякі з них є оборотними. Але за властивістю 3), оборотний до комутатора – теж комутатор. Внаслідок цього можна записати
$G' = \{[x_1, y_1] * \cdots * [x_n, y_n] \mid x_i, y_i \in G, n \in \mathbb{N}\}$

Remark 2.9.6 Принципово, що комутатори породжують підгрупу. Якщо залишити просто множину комутаторів, то вона вже не буде підгрупою, оскільки порушується замкненість.
Зокрема розглянемо $SL_2(\mathbb{R})$. Скоро доведемо, що $SL_2(\mathbb{R})' = SL_2(\mathbb{R})$. Серед них $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ не є комутатором.

Remark 2.9.7 G – абелева група $\iff G' = \{e\}$.
Отже, комутант – це така собі міра неабелевості груп.

Definition 2.9.8 Задано $\langle G, * \rangle$ – група та K, H – підгрупи G.
Взаємним комутантом назвемо таку підгрупу

$$[K, H] = \langle [x, y] \mid x \in K, y \in H \rangle$$

Remark 2.9.9 $[K, K] = K'$.
Відповідно ми можемо писати $[G, G] = G'$ для кожної групи. До речі, таке позначення $[G, G]$ є загально прийнятим в західній літературі.

Proposition 2.9.10 Задано $\langle G, * \rangle, \langle H, \star \rangle$ – групи та $\varphi \colon G \to H$ – гомоморфізм. Тоді $\varphi(G')$ буде підгрупою H'.
Ба більше, якщо φ – сюр'єктивний, то $\varphi(G') = H'$.

Proof.
Нехай $u, v \in \varphi(G')$, тобто для них існують елементи $a, b \in G'$, для яких $\varphi(a) = u, \varphi(b) = v$. Але оскільки $a, b \in G'$, то тоді $a = [x_1, y_1], b = [x_2, y_2]$ при $x_1, x_2, y_1, y_2 \in G$.
Із іншого боку, $u = \varphi([x_1, y_1]) = [\varphi(x_1), \varphi(y_1)]$ та $v = \varphi([x_2, y_2]) = [\varphi(x_2), \varphi(y_2)]$. Звідси випливає, що $u \star v^{-1} = [\varphi(x_1), \varphi(y_1)][\varphi(y_2), \varphi(x_2)] \in H'$
$u \star v^{-1} = \varphi(a) \star (\varphi(b))^{-1} = \varphi(a * b^{-1}) = \varphi([x_1, y_1] * [y_2, x_2])$.
Тобто ми знайшли елемент $a * b^{-1} \in G'$, для якого $\varphi(a * b^{-1}) = u \star v^{-1}$, тобто $u \star v^{-1} \in \varphi(G')$.

Тепер нехай φ – сюр'єктивне. Нехай $h_1, h_2 \in H$, тобто звідси $\varphi(a) = h_1, \varphi(b) = h_2$ для деяких $a, b \in G$. Отже,
$\varphi([a, b]) = [\varphi(a), \varphi(b)] = [h_1, h_2] \in \varphi(G')$.
Якщо взяти елемент $u \in H'$, то це буде добуток комутаторів, кожний з яких потрапляє уже в $\varphi(G')$.
Отже, $u \in G'$. Отримали $\varphi(G') = H'$. ■

Corollary 2.9.11 Нехай $K \triangleleft G$. Тоді $K' \triangleleft G$.

Proof.
Нехай $k \in K'$ та $g \in G$, тобто маємо
$k = [u_1, v_1] * \cdots * [u_n, v_n]$, причому $u_i, v_i \in K$.
$g * k * g^{-1} = g * [u_1, v_1] * g^{-1} * g * [u_2, v_2] * g^{-1} * \cdots * g * [u_n, v_n] * g^{-1}$.
Отже, достатньо показати, що $g * [u_1, v_1] * g^{-1} = [u_1, v_1]^g = [u_1^g, v_1^g] \in K$. Дійсно, так воно й буде, оскільки $u_1^g, v_1^g \in K$ в силу $K \triangleleft G$.
Внаслідок цього доведемо $g * k * g^{-1} \in K$. ■

Corollary 2.9.12 $G' \triangleleft G$.

Theorem 2.9.13 Основна теорема про комутанти
Задано $\langle G, * \rangle$ – група. Тоді
1) $G/_{G'}$ – абелева група;
2) $H \triangleleft G$, причому $G/_H$ – абелева $\iff$ G' – підгрупа H, що уже є підгрупою G (тобто H – проміжкова підгрупа між G', G).

Proof.
1) Розглянемо проєкцію $\pi \colon G \to G/_{G'}$, при цьому відомо, що $\ker \pi = G'$. Оберемо будь-які $x * G', y * G' \in G/_{G'}$. Тоді

$$[x * G', y * G'] = [\pi(x), \pi(y)] = \pi([x, y]) \overset{[x,y] \in G' = \ker \pi}{=} e * G'.$$

За властивістю 2), звідси $(x * G') * (y * G') = (y * G') * (x * G')$, довели абелевість.

2) Доведення буде в обидві сторони.
$\boxed{\Rightarrow}$ Дано: $H \triangleleft G$, причому $G/_H$ – абелева.
Нехай $a, b \in G$, тоді звідси $[a * H, b * H] \overset{G/_H - \text{ абелева}}{=} e * H = H$. Із іншого боку, $[a * H, b * H] = [a, b] * H$.
Отже, отримали $[a, b] \in H$.
Отже, ми отримали, що всі комутатори потрапляють в H. Множина G' породжується комутаторами не просто в G, а тепер у H. Таким чином, G' – підгрупа H.

$\boxed{\Leftarrow}$ Дано: G' – підгрупа H.
Зауважимо, що $[H, G] \subset [G, G] = G'$. Тобто звідси $\forall h \in H, \forall x \in G : h * x * h^{-1} * x^{-1} \in H$. Отже, $x * h * x^{-1} = h^{-1} * h * x * h * x^{-1} \in H$.

Таким чином, $H \triangleleft G$, залишилося довести абелевість $G/_H$.
Маємо $a*H, b*H \in G/_H \implies [a*H, b*H] = [a,b]*H$. Але $[a,b] \in G' \subset H$ за умовою, тож $[a*H, b*H] = e*H = H$. Тобто $a*H, b*H$ комутують між собою. ■

Corollary 2.9.14 G' – найменша нормальна підгрупа G, для якої $G/_{G'}$ – абелева.

Example 2.9.15 Розглянемо групу S_n та знайдемо його комутатор.
Зазначимо, що $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ завжди парна перестановка, оскільки σ, σ^{-1} мають однакову парність (так само й τ, τ^{-1}). Отже, $S_n' \subset A_n$.
Із іншого боку, ми знаємо, що A_n породжується 3-циклами. Кожний 3-цикл подамо в такому вигляді:
$(ijk) = (ij)(ik)(ij)(ik) = (ij)(ik)(ij)^{-1}(ik)^{-1} = [(ij),(ik)] \in S_n'$.
Отже, отримаємо $A_n \subset S_n'$.
Висновок: $S_n' = A_n$.

Example 2.9.16 Знайдемо комутатор групи $G = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix} \middle| a,b,c \in \mathbb{R}, c \neq 0 \right\}$ (це дійсно підгрупа $GL_3(\mathbb{R})$, неважко переконатися).
Розглянемо комутатор довільних двох матриць
$$\left[\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix}, \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & y & z \end{pmatrix} \right] \overset{\text{перевірити}}{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -bz+b+cy-y & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \xi & 1 \end{pmatrix}.$$
Таким чином, кожний комутант – одинична матриця, але на третьому рядку та другому стовпчику розташоване число. Множення таких матриць приведе до матриці такої ж форми. Отже, $G' \subset \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \xi & 1 \end{pmatrix} \middle| \xi \in \mathbb{R} \right\}$.
Із іншого боку, погравшись трошки, отримаємо, що
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \xi & 1 \end{pmatrix} = \left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2\xi & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -\xi & 2 \end{pmatrix} \right],$$
тобто кожна матриця такого типу розписується як комутатор. Значить, $\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \xi & 1 \end{pmatrix} \middle| \xi \in \mathbb{R} \right\} \subset G'$.
Звідси отримаємо $G' = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \xi & 1 \end{pmatrix} \middle| \xi \in \mathbb{R} \right\}$.

Example 2.9.17 Знайдемо комутатор діедральної групи D_n.
Зауважимо, що $r^{2k} = [r^k, s]$, тож звідси випливає, що $\langle r^2 \rangle \subset D_n'$.
Із іншого боку, $\langle r^2 \rangle \triangleleft D_n$, при цьому $D_n/_{\langle r^2 \rangle}$ буде абелевою, оскільки його порядок або 2, або 4 в залежності від парності n-кутника. Отже, $D_n' \subset \langle r^2 \rangle$.
Висновок: $D_n' = \langle r^2 \rangle$.

Example 2.9.18

2.10 Нормальні замикання

Definition 2.10.1 Задано $\langle G, * \rangle$ – група та $M \subset G$.
Нормальним замиканням множини M в групі G, називають таку множину:

$$\mathrm{ncl}_G(M) = \bigcap_{\substack{H \triangleleft G \\ H \supset M}} H$$

Альтернативне позначення: $\langle M \rangle_n$.
Тобто $\mathrm{ncl}_G(M)$ – найменша нормальна підгрупа G (легітимним чином є підгрупою), що містить M.

Theorem 2.10.2 Задано $\langle G, * \rangle$ – група та $M \subset G$.
Тоді $\mathrm{ncl}_G(M) = \langle M^G \rangle$, у цьому випадку $M^G = \{m^x \mid m \in M, x \in G\}$.

Proof.
$\langle M^G \rangle \subset \mathrm{ncl}_G(M)$
Дійсно, нехай $m^x \in \langle M^G \rangle$. Оскільки $m \in M$, то звідси $m \in \mathrm{ncl}_G(M)$. Але водночас $x \in G$ та $\mathrm{ncl}_G(M) \triangleleft G$, звідси $m^x = x^{-1} * m * x \in \mathrm{ncl}_G(M)$.
Якщо взяти елемент $u \in \langle M^G \rangle$, то він розписується на добуток елементі $m^x \in \mathrm{ncl}_G(M)$. Таким чином, $u \in \mathrm{ncl}_G(M)$.

$\mathrm{ncl}_G(M) \subset \langle M^G \rangle$.
Достатньо довести, що $\langle M^G \rangle \triangleleft G$ та $M^G \supset M$.
Те, що $M^G \subset M$, це зрозуміло просто через те, що $e \in G$.
Для першого зауважимо, що для $x \in G$ виконується така рівність:
$\left(\langle M^G \rangle\right)^x = \langle (M^G)^x \rangle = \langle M^{G*x} \rangle = \langle M^G \rangle$.
Ця рівність свідчить про те, що $M^G \triangleleft G$.
Тоді $\mathrm{ncl}_G(M) \subset \langle M^G \rangle$, бо друга множина в цьому перетині. ■

Theorem 2.10.3 Про побудову комутанта підгрупи, що породжена множиною
Задано $G = \langle M \rangle$. Тоді $G' = \mathrm{ncl}_G(M')$, тут позначили
$M' = \{[m_1, m_2] \mid m_1, m_2 \in M\}$.

Proof.
$\mathrm{ncl}_G(M') \subset G'$.
За попередньою теоремою, $\mathrm{ncl}_G(M')$ породжується елементами $[m_1, m_2]^x, x \in G$. Зрозуміло, що $[m_1, m_2] \in G'$, але $G' \triangleleft G$. Отже, $[m_1, m_2]^x \in G'$.
Кожний елемнт $u \in \mathrm{ncl}_G(M')$ записується як добуток з елементів $[m_1, m_2]^x \in G'$. Значить, $u \in G'$.

$G' \subset \mathrm{ncl}_G(M')$.
Ми вже знаємо, що $G' \subset \mathrm{ncl}_G(M') \subset G \iff \mathrm{ncl}_G(M') \triangleleft G$ та $G/_{\mathrm{ncl}_G(M')}$ – абелева (основа теорема про комутант). Перша умова вже виконана, залишилася друга.
Розглянемо проєкцію $\pi \colon G \to G/_{\mathrm{ncl}_G(M')}$. Зауважимо, що
$[m_1, m_2] * \mathrm{ncl}_G(M') = [m_1 * \mathrm{ncl}_G(M'), m_2 * \mathrm{ncl}_G(M')]$. Оскільки $[m_1, m_2] \in \mathrm{ncl}_G(M')$, то звідси $[m_1 * \mathrm{ncl}_G(M'), m_2 * \mathrm{ncl}_G(M')] = e * \mathrm{ncl}_G(M')$. Отже, два суміжні класи комутують.
За еквівалентністю, $G' \subset \mathrm{ncl}_G(M)$. ■

2.11 Розв'язні групи

Definition 2.11.1 Група G називається **розв'язною**, якщо допускається ось такий ряд

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\},$$

причому кожна $G_i/_{G_{i+1}}$ – нетривіальна абелева група.

Example 2.11.2 Розглянемо купа прикладів:
1. Кожна абелева група – розв'язна, оскільки існує ланцюг $G \triangleright \{e\}$.

2. S_3 – розв'язна, оскільки $S_3 \triangleright [(123)] \triangleright \{\varepsilon\}$, причому $S_3/_{[(123)]}$ буде абелевою, оскільки там всього 2 елементи; $[(123)]/\{e\} \cong [(123)]$ буде абелевою.

3. S_4 – розв'язна, оскільки $S_4 \triangleright A_4 \triangleright V \triangleright \{\varepsilon\}$, де передостання V – група Кляйна. Теж зрозуміло, що кожна факторгрупа – абелева.

4. p-група G – розв'язні. (TODO: ?)

Theorem 2.11.3 Теорема Фейта-Томпсона
Задано G – група, причому $|G|$ – непарний порядок. Тоді G – розв'язний.
Без доведення. Стаття містить десь 250 сторінок доведення.

Example 2.11.4 $A_n, n \geq 5$ – нерозв'язні, оскільки вона є простою.

Proposition 2.11.5 Задано G – розв'язна група та H – підгрупа G. Тоді H – також розв'язна.

Proof.
Маємо $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\}$, всі $G_i/_{G_{i+1}}$ – нетривіальні абелеві групи.
Розглянемо $H_i = G_i \cap H$. Зауважимо, що $H_{i+1} \subsetneq H_i$ – підгрупа. Також $H_{i+1} \triangleleft H_i$, просто тому що $G_{i+1} \triangleleft G_i$. Також якщо розглянути таку композицію гомоморфізмів $H_i \hookrightarrow G_i \twoheadrightarrow G_i/_{G_{i+1}}$, то тоді H_i буде ядром даної композиції. Значить, за першою теоремою про ізоморфізм, існує бієкція (а тому й ін'єкція) $H_i/_{H_{i+1}} \hookrightarrow G_i/_{G_{i+1}}$. Отже, $H_i/_{H_{i+1}}$ – абелева, оскільки це (в силу ін'єкції) сприймається як підгрупа абелевої групи. ■

Proposition 2.11.6 Задано G – група та G' – гомоморфний образ групи G. Тоді G' – також розв'язна.

Proof.
За умовою, існує сюр'єкція $\varphi\colon G \to G'$, тоді за першою теоремою про ізоморфізм, $G' \cong G/_{\ker\varphi}$. Нам треба довести, що $G/_{\ker\varphi}$ – розв'язна.
Більш загально: якщо $K \triangleleft G$ при G – розв'язна, то $G/_K$ – розв'язна.
Оскільки $K \triangleleft G$, то звідси G_iK – підгрупа G. Також уже доводили, що $K \triangleleft G_iK$. Тому можна розглянути ланцюг
$G/_K \supsetneq G_1K/_K \supsetneq G_2K/_K \supsetneq \cdots \supsetneq G_rK/_K = K/_K = \{e\}$.
Оскільки $G_{i+1} \triangleleft G_i$, то тоді звідси $G_{i+1}K \triangleleft G_iK$. За третьою теоремою про ізоморфзм, $G_{i+1}K/_K \triangleleft G_iK/_K$, а також $(G_iK/_K)/_{(G_{i+1}K/_K)} \cong G_iK/_{G_{i+1}K}$.
Отже, залишилося довести, що $G_iK/_{G_{i+1}K}$ – абелева група.
Розглянемо відображення $\alpha\colon G_i \hookrightarrow G_iK \twoheadrightarrow G_iK/_{G_{i+1}K}$, яке є сюр'єктивним. Дійсно, для кожного $gkG_iK \in G_iK/_{G_{i+1}K}$ існує елемент $g \in G$, для якого $\alpha(g) \overset{\text{def.}}{=} gG_{i+1}K = gkG_{i+1}K$. Остання рівність виконана, тому що $g^{-1}gk = k \in K \subset G_{i+1}K$. Також можна показати, що $\ker\alpha \supset G_{i+1}$, але тоді в нас індукується сюр'єктивний гомоморфізм $G_i/_{G_{i+1}} \twoheadrightarrow G_iK/_{G_{i+1}K}$. Оскільки $G_i/_{G_{i+1}}$ – абелева, то тоді $G_iK/_{G_{i+1}K}$ – абелева. ■

Theorem 2.11.7 $S_n, n \geq 5$ – не розв'язна група.

Proof.
!Припустимо, що S_n – все ж таки розв'язна. Але оскільки A_n – підгрупа S_n, то A_n теж буде розв'язною – суперечність! ■

Взагалі-то кажучи, деякі автори можуть дати альтернативне означення, саме через комутатори.

Definition 2.11.8 Задано G – група та G' – похідна групи G. Таким же чином можна визначити другу похідну $G'' = (G')'$, третю похідну $G''' = (G'')'$ тощо. У нас утвориться **похідний ряд**

$$G \triangleright G' \triangleright G'' \triangleright \dots$$

Група G називається **розв'язною**, якщо

$$\exists n \in \mathbb{N} : G^{(n)} = \{e\}$$

Proposition 2.11.9 Два означення розв'язних груп еквівалентні.

Proof.
TODO: обдумати ■

Lemma 2.11.10 Задано G – група та H, K – підгрупи. Довести, що $[H, K] \triangleleft H, K$.

Definition 2.11.11 Задано G – група та $G_1 = [G, G],\ G_2 = [G_1, G], \dots$ У нас утвориться **нижній центральний ряд**

$$G \triangleright G_1 \triangleright G_2 \dots$$

Група G називається **нільпотентною**, якщо

$$\exists n \in \mathbb{N} : G_n = \{e\}$$

Proposition 2.11.12 Задано G – нільпотентна група. Тоді G – розв'язна.

Proof.
За МІ ми доведемо, що $\forall n \in \mathbb{N} : G^{(n)} \subset G_n$.
База: $n = 1$, тоді отримаємо $G' \subset [G, G] = G'$.
Припущення: $G^{(k)} \subset G_k$.
Крок: $G^{(k+1)} = (G^{(k)})' = [G^{(k)}, G^{(k)}] \subset [G_k, G^{(k)}] \subset [G_k, G] = G_{k+1}$.
МІ доведено. А тепер якщо G – нільпотентна, то $\exists n \in \mathbb{N} : G_n = \{e\}$. Звідси $G^{(n)} \subset G_n = \{e\} \implies G^{(n)} = \{e\}$.
Отже, G – розв'язна група. ■

Theorem 2.11.13 Нехай G – група та $K \triangleleft G$.
G – розв'язна $\iff$ K та $G/_K$ – розв'язні.

Proof.
$\boxed{\Rightarrow}$ випливає з двох тверджень вище.

$\boxed{\Leftarrow}$ Дано: $K, G/_K$ – розв'язні. Маємо $K^{(n)} = (G/_K)^{(l)}\{e\}$.
Розглянемо $\pi \colon G \to G/_K$ – сюр'єктивне. Нам уже відомо, що $\pi(G') = (G/_K)'$, тоді можна звузити до $\pi|_{G'} \colon G' \to (G/_K)'$, що залишається сюр'єктивним. Так продовжуємо до $\pi|_{G^{(l)}} \colon G^{(l)} \to (G/_K)^{(l)} = \{e\}$. Звідси випливає, що $G^{(l)}$ – підгрупа $\ker \pi = K$. Але можна довести, що $G^{(l+n)}$ – підгрупа $K^{(n)} = \{e\}$. Тому звідси G – розв'язна. ■

3 Теорія кілець

3.1 Означення кільця

Definition 3.1.1 Задана R – деяка множина та дві бінарні операції $+, \cdot$.
Кільцем назвемо трійку $\langle R, +, \cdot \rangle$, для якої виконуються властивості:
I. $\forall a, b \in R : a + b \in R$ – замкненість відносно $+$;
II. $\forall a, b \in R : a \cdot b \in R$ – замкненість відносно $\cdot$;
III. Підпорядкована такими аксіомами:

1)	$\forall a, b, c \in R : a + (b + c) = (a + b) + c$	– асоціативність додавання
2)	$\forall a, b, c \in R : a + b = b + a$	– комутативність додавання
3)	$\exists 0 \in R : a + 0 = a$	– існування нейтрального елементу за додаванням
4)	$\forall a \in R : \exists (-a) \in R : a + (-a) = 0$	– існування оберненого елементу за додаванням
5)	$\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$	– асоціативність множення
6)	$\forall a, b, c \in R : \begin{matrix}(a+b)\cdot c = (a\cdot c) + (b\cdot c)\\ c\cdot(a+b) = (c\cdot a) + (c\cdot b)\end{matrix}$	– дистрибутивність множення відносно додавання

$0 \in R$ називають **нулем кільця**; $(-a) \in R$ називають **протилежним елементом** $a \in R$.

Remark 3.1.2 Якщо взяти структуру $\langle R, + \rangle$, то вона формує абелеву групу. Зокрема звідси випливає єдиність 0 та єдиність протилежного елементу $(-a)$ для кожного $a \in R$.

Example 3.1.3 Розглянемо ось такі приклади кілець:

R	$+$	$\cdot$	0	a	$-a$
$\mathbb{R}$	$+$	$\cdot$	0	x	$-x$
$\mathbb{R}[x]$	$+$	$\cdot$	$0(x)$	$f(x)$	$-f(x)$
$\mathbb{Z}_n$	$+$	$\cdot$	$\overline{0}$	$\overline{a}$	$\overline{n-a}$
$\mathcal{K}$	$\triangle$	$\cap$	$\emptyset$	A	A

Операція $+, \cdot$ в першому визначається стандартним чином.

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$
$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$
припускаємо, що $n < m$
$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_m x^m$
$f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + (a_0 b_m + a_1 b_{m-1} + \cdots + a_{m-1} b_1 + a_m b_0)x^m$,
тут вважаємо $a_k = 0$ при $k > n$.

$\overline{a} + \overline{b} = \overline{a + b}$
$\overline{a} \cdot \overline{b} = \overline{ab}$

Example 3.1.4 Окремо перевіримо, що $\langle \mathcal{K}, \triangle, \cap \rangle$ – кільце як структура, де $\mathcal{K}$ – кільце множин. Те, що $\mathcal{K}$ – замкнена відносно $\triangle, \cap$, випливає з властивостей кільця з теорії міри. Решта аксіом доводиться аксіоматично зі знань теорії множин, зокрема:
1) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$
2) $A \triangle B = B \triangle A$
3) $A \triangle \emptyset = A$
4) $A \triangle A = \emptyset$
5) $A \cap (B \cap C) = (A \cap B) \cap C$
6) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ та $(B \triangle C) \cap A = (B \cap A) \triangle (C \cap A)$
Ми маємо, що $\emptyset$ - нуль кільця, а от протилежним елементом до A буде сама ж A.

Proposition 3.1.5 Властивості
Задано $\langle R, +, \cdot \rangle$ – кільце. Тоді виконуються такі пункти:
1) $\forall a \in R : 0 \cdot a = a \cdot 0 = 0$;
2) $\forall a, b \in R : a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;
3) $(-1) \cdot a = -a$.

Proof.
Покажемо виконання кожної властивості:

1) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. За правилом скорочення відносно плюса, $0 \cdot a = 0$.

2) Доведемо, що $a \cdot (-b)$ – протилежний елемент до $a \cdot b$. Дійсно,
$(a \cdot b) + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$.
Отже, $a \cdot (-b) = -(a \cdot b)$.

3) $-a = -(a \cdot 1) = (-1) \cdot a$.

Всі властивості доведені. ■

3.2 Підкільця

Definition 3.2.1 Задано $\langle R, +, \cdot \rangle$ – кільце та множину $R_1 \subset R$.
Воно називається **підкільцем**, якщо

$$\langle R_1, +, \cdot \rangle \text{ – кільце,}$$

де операцію $+$ та операцію $\cdot$ ми успадкували з R.

Remark 3.2.2 Оскільки $\langle R, + \rangle$ – абелева група, то звідси, за означенням, $\langle R_1, + \rangle$ буде підгрупою, а тому в них будуть однакові нульові елементи.

Для визначення підкільця є ідентичний критерій, що з теорії груп, просто буде додаткова умова.

Theorem 3.2.3 Критерій підкільця
Задано $\langle R, +, \cdot \rangle$ – кільце та множину $R_1 \subset R$.

$$R_1 \text{ – підкільце } \iff \begin{cases} \forall a, b \in R_1 : a + b \in R_1 \\ \forall a, b \in R_1 : a \cdot b \in R_1 \\ \forall a \in R_1 : -a \in R_1 \end{cases} \quad \text{та } R_1 \neq \emptyset.$$

Вправа: довести.

Corollary 3.2.4 Переписаний критерій

$$R_1 \text{ – підкільце } \iff \begin{cases} \forall a, b \in R_1 : a - b \in R_1 \\ a \cdot b \in R_1 \end{cases} \quad \text{та } R_1 \neq \emptyset.$$

Remark 3.2.5 Під виразом $a - b$ мається на увазі $a + (-1) \cdot b$.

Example 3.2.6 Зокрема $\mathbb{Z}, \mathbb{Q}$ – підкільця кільця $\langle \mathbb{R}, +, \cdot \rangle$.

Example 3.2.7 Маємо $\langle \mathbb{R}[x], +, \cdot \rangle$ – кільце. Розглянемо $\mathbb{R}_n[x]$ – многочлени до степені n. $\mathbb{R}_n[x]$ вже не буде підкільцем, тому що $f(x) = g(x) = x^n \in \mathbb{R}_n[x]$, але $f(x) \cdot g(x) = x^{2n} \notin \mathbb{R}_n[x]$.

Example 3.2.8 Маємо $\langle \mathbb{Z}, +, \cdot \rangle$ – кільце, множина $n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ – підкільце.

Remark 3.2.9 Кожне кільце $\langle R, +, \cdot \rangle$ має два **тривіальних** підкільця: $\{0\}$ та R.

3.3 Основні класифікації кілець

3.3.1 Комутативні кільця

Definition 3.3.1 Задано $\langle R, +, \cdot \rangle$ – кільце.
Воно називається **комутативним**, якщо

$$\forall a, b \in R : a \cdot b = b \cdot a \text{ – комутативність множення}$$

У протилежному випадку – **некомутативним**.

Example 3.3.2 Зокрема $\langle \mathbb{R}, +, \cdot \rangle$ – комутативне кільце.

Example 3.3.3 А ось $\langle \mathrm{Mat}_{n \times n}(\mathbb{R}), +, \cdot \rangle$ – некомутативне кільце.

3.3.2 Кільця з одиницею

Definition 3.3.4 Задано $\langle R, +, \cdot \rangle$ – кільце.
Воно називається **кільцем з одиницею**, якщо

$$\exists 1 \in R : a \cdot 1 = 1 \cdot a = a$$

Тобто 1 – нейтральний елемент за множенням.

Proposition 3.3.5 Якщо задано $\langle R, +, \cdot \rangle$ – кільце з одиницею, то ця одиниця – єдина.

Proof.
!Припустимо, що існують дві одиниці $1, 1' \in R$, тоді маємо:
$1 \cdot 1' = 1$, але з іншого боку, $1 \cdot 1' = 1'$, а тому вони рівні. Суперечність! ■

Example 3.3.6 Зокрема $\langle \mathbb{R}[x], +, \cdot \rangle$ – кільце з одиницею $1(x) \equiv 1$.

Example 3.3.7 А ось $\langle \mathcal{K}, \triangle, \cap \rangle$ – кільце, але без одиниці.
Якщо припустити, що деяка множина I – одиниця кільця, то тоді має виконуватись $A \cap I = I \cap A = A$ для кожної множини $A \in \mathcal{K}$. Але це можливо лише тоді, коли $A \subset I$. У нас в кільці може існувати елемент $A \cup I \in \mathcal{K}$, для якого $A \cup I \supset I$, а також $(A \cup I) \cap I \neq A$. Прийшли до суперечності.
Тобто $\langle \mathcal{K}, \triangle, \cap \rangle$ не може бути кільцем з одиницею.

Example 3.3.8 Але можна показати, що $\langle \mathcal{A}, \triangle, \cap \rangle$ – кільце з одиницею $\iff$ $\mathcal{A}$ – алгебра множин. Причому одиницею кільця буде універсальна множина U.

Lemma 3.3.9 Задано $\langle R, +, \cdot \rangle$ – ненульове кільце з одиницею. Тоді $0 \neq 1$.

Proof.
!Припустимо, що все ж таки $0 = 1$. Тоді
$a \cdot 1 = 1 \cdot a = a$
$a \cdot 0 = 0 \cdot a = 0$
Єдина можливість тоді – це $a = 0$. Але кільце в нас ненульове. Суперечність! ■

Remark 3.3.10 Але кільце $\langle \{0\}, +, \cdot \rangle$ має одиницю $1 = 0$ – тобто співпадає з нулем кільця.

Definition 3.3.11 Задано $\langle R, +, \cdot \rangle$ – кільце з одиницею.
Елемент $a \in R$ називають **оборотним** в кільці R, якщо

$$\exists a^{-1} \in R : a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Водночас a^{-1} називають **оберненим** до a в кільці R.

Remark 3.3.12 Не всі $a \in R$ – оборотні в кільці з одиницею. Зокрема $0 \in R$, але от $a \cdot 0 = 0 \cdot a = 0 \neq 1$ – і це взагалі $\forall a \in R$.

Remark 3.3.13 Зате у будь-якого ненульового кільця з одиницею $\langle R, +, \cdot \rangle$ елементи $1, -1$ будуть завжди оборотними. Дійсно, якщо покласти $1^{-1} = 1$ та $(-1)^{-1} = -1$, то означення оберненості виконується.

Позначення: $R^\times$ – множина всіх оборотних елементів кільця $\langle R, +, \cdot \rangle$.

Example 3.3.14 Розглянемо кілька прикладів:

R	$R^\times$
$\mathbb{R}$	$\mathbb{R} \setminus \{0\}$
$\mathbb{Z}$	$\{-1, 1\}$
$\mathbb{Z}_p$	$\mathbb{Z}_p \setminus \{0\}$
$\mathbb{Z}_n$	U_n
$M_{n \times n}(\mathbb{R})$	GL_n

Більш детальне пояснення:
1. Тут всі ненульові елементи оборотні, бо
$a \cdot \dfrac{1}{a} = 1$, де елемент $a^{-1} = \dfrac{1}{a}$.

2. Тут лише, 1, -1 оборотні. В інакшому випадку якщо припустити, що для $n \in \mathbb{Z}$ знайдеться обернений $n^{-1} \in \mathbb{Z}$, то маємо $n \cdot n^{-1} = 1 \implies n^{-1} = \frac{1}{n}$. Але тоді $n^{-1} \in \mathbb{Z}$ лише в тому випадку, коли $n = \pm 1$.

3-4. Обернений елемент $\overline{m} \in \mathbb{Z}_n$ існує $\iff \gcd(m, n) = 1$.

5. Оборотними будуть ті матриці, які мають ненульові визначники.

Example 3.3.15 Розглянемо гаусові числа $\langle \mathbb{Z}[i], +, \cdot \rangle$, де множина $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z},\ i^2 = -1\}$ (це дійсно комутативне кільце, неважко довести).
Нехай $a \in (\mathbb{Z}[i])^\times$, тоді звідси $\exists b \in \mathbb{Z}[i] : ab = 1$.
Позначимо $a = x + iy, b = u + iv$, причому $u, v, x, y \in \mathbb{Z}$. Тоді
$(xu - yv) + i(xv + yu) = 1 \iff \begin{cases} xu - yv = 1 \\ xv + yu = 0 \end{cases}$.
Спочатку випадок $v = 0$ перед тим, як будемо домножувати. Матимемо:
$\begin{cases} xu = 1 \\ yu = 0 \end{cases} \iff \begin{cases} x = \pm 1 \\ u = \pm 1 \\ y = 0 \end{cases}$.
Домножимо перше рівняння на $v \neq 0$, а з другого виразимо $xv = -yu$, отримаємо:
$-yu^2 - yv^2 = 1 \iff y(u - v)(u + v) = -1$.
Рівняння в цілих числах, а тому ця рівність можлива: або всі -1, або один -1 і решта два 1. Будуть чотири випадки, серед яких спрацює один:
$\begin{cases} y = 1 \\ u - v = -1 \\ u + v = 1 \end{cases} \implies y = 1, u = 0, v = -1, x = 0.$
Таким чином, отримали такі числа: або $a = 1, b = 1$, або $a = -1, b = -1$, або $a = i, b = -i$.
Разом отримаємо, що $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$.

Theorem 3.3.16 Задано $\langle R, +, \cdot \rangle$ – кільце з одиницею. Тоді $\langle R^\times, \cdot \rangle$ – мультиплікативна група кільця – група.

Proof.
Маємо $a, b \in R^\times$, тоді вони мають обернені елементи a^{-1}, b^{-1}. Щоб довести, що $a \cdot b \in R^\times$, треба показати, що існує $(a \cdot b)^{-1}$. І дійсно, якщо покласти $(a \cdot b)^{-1} = b^{-1}a^{-1}$, то маємо
$(ab) \cdot (ab)^{-1} = (ab) \cdot (b^{-1}a^{-1})(a \cdot 1 \cdot a^{-1}) = a \cdot a^{-1} = 1$.
Отже, замкненість відносно $\cdot$ вже є.
Маємо асоціативність автоматично, за означенням кільця.
Нейтральний елемент - це $1 \in R^\times$, просто тому що $1^{-1} = 1$, а тому $1 \in R^\times$, а також $a \cdot 1 = a$.
Маємо $a \in R^\times$. Покажемо, що $\exists a^{-1} \in R^\times$, для якого $a \cdot a^{-1} = 1$.
Дійсно, для $a \in R^\times$ є обернений $a^{-1} \in R^\times$, водночас для нього є обернений $(a^{-1})^{-1} \overset{\text{покладемо}}{=} a$, а тому $a^{-1} \in R^\times$. ■

Example 3.3.17 Зокрема $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ – група. Тепер це можна позначити як $\langle \mathbb{R}^\times, \cdot \rangle$.

3.3.3 Області цілісності

Definition 3.3.18 Задано $\langle R, +, \cdot \rangle$ – кільце.
Елементи $a \neq 0, b \neq 0$ називають **дільниками нуля**, якщо

$$ab = 0$$

Тут a, b – відповідно лівий та правий дільники нуля.

Example 3.3.19 Розглянемо кілька прикладів:
1. $\langle \mathbb{Z}_6, +, \cdot \rangle$ має три дільників нуля: $\overline{2}, \overline{3}, \overline{4}$ – тому що $\overline{2} \cdot \overline{3} = \overline{2} \cdot \overline{4} = \overline{3} \cdot \overline{4} = \overline{0}$. Причому тут не вказується, чи лівий чи правий в силу комутативності операції $\cdot$ на цьому кільці.

2. $\langle \mathbb{R}, +, \cdot \rangle$ не має дільників нуля.
Якщо припустити, що такий існує дільник нуля $a \in \mathbb{R}$, то тоді знайдеться елемент $b \in \mathbb{R}$, для якого $ab = 0$, але тоді або $a = 0$, або $b = 0$ – неможливо.

Theorem 3.3.20 Задано $\langle R, +, \cdot \rangle$ – кільце з одиницею. Тоді жодний оборотний елемент не є дільником нуля.

Proof.
!Припустимо, що існує такий обернений елемент $a \in R^\times$, який є лівим дільником нуля. Тобто ми маємо:
$a \cdot a^{-1} = 1$
$a \cdot b = 0$, для деякого $b \in R \setminus \{0\}$.
Але тоді $b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = 0 \cdot a^{-1} = 0$. Суперечність!
Тобто висновок: дільникі одиниці – ніколи не дільники нуля. ■

Remark 3.3.21 Але якщо елемент – не дільник нуля, то не обов'язково, що воно оборотне.

Example 3.3.22 Маємо $\langle \mathbb{Z}, +, \cdot \rangle$. Жодний ненульовий елемент – не дільник нуля, серед них лише $1, -1$ – оборотні.

Theorem 3.3.23 Задано $\langle R, +, \cdot \rangle$ – кільце.
Можна використовувати закони скорочення відносно множення $\iff$ кільце не містить взагалі дільників нуля.

Під законами скорочення маю на увазі: $\begin{cases} ax = bx \iff a = b \\ xa = xb \iff a = b \end{cases}$ – відповідно праве та ліве скорочення, де $x \neq 0$ та $a, b \in R$.

Proof.
$\boxed{\Rightarrow}$ Дано: можна юзати закон скорочення.
!Припустимо, що існує один дільник нуля $a \in R$ (скажімо, лівий), тобто $ab = 0$ для $b \neq 0$. Але тоді $a \cdot b = a \cdot 0$, і за правилом (лівого) скорочення, $b = 0$. Суперечність!
Ми показали таким чином, що якщо можна юзати лише лівий закон скорочення, то тоді кільце не має дільників нуля.

$\boxed{\Leftarrow}$ Дано: нема дільників нуля. Тоді беремо $a, b, x \in R$ так, що $x \neq 0$.
$ax = bx \iff (a - b) \cdot x = 0 \iff a - b = 0 \iff a = b$.
Всі еквівалетності виконуються в силу відсутності дільників нуля.
Аналогічно доводиться, що $xa = xb \iff a = b$. ■

Remark 3.3.24 Взагалі-то кажучи, у кільці $\langle R, +, \cdot \rangle$ не обов'язково вимагати, щоб жодний елемент не був дільником нуля. Достатньо, щоб $x \in R \setminus \{0\}$, на який ми скорочуємо, не був дільником нуля.

Theorem 3.3.25 Задано $\langle R, +, \cdot \rangle$ – скінченне (!) кільце з одиницею. Нехай $a \in R$ – не дільник нуля. Тоді a – оборотний.

Proof.
Розглянемо випадок $\operatorname{card} R = n > 1$, бо коли один, то нема шо доводити.
Маємо $a \in R, a \neq 0$ – не дільник нуля. Шукати обернений елемент будемо за таким же принципом, як це було в **Th. 1.2.4**.
Розглянемо множину $a \cdot R = \{a \cdot b \mid b \in R\}$. Покажемо, що тут всі n елементів – різні. Дійсно,
$a \cdot b_1 = a \cdot b_2 \implies a \cdot (b_1 - b_2) = 0 \overset{a \text{ не дільник}}{\implies} b_1 - b_2 = 0 \implies b_1 = b_2$.
Отже, по-перше, $\operatorname{card} R = \operatorname{card}(a \cdot R) = n$, а також по-друге, $a \cdot R \subset R$.
Тобто звідси $a \cdot R = R$.
Оскільки $1 \in R$, то один з елементів $a \cdot b \in a \cdot R$ має співпадати з 1. Отже, $\exists b \in R : a \cdot b = 1$ - довели існування правого оберненого.
Аналогічно якщо розглянути $R \cdot a = \{b \cdot a, b \in R\}$, то доведемо існування лівого оберненого.
Оскільки $\langle R, \cdot \rangle$ утворює моноїд та праві, ліві обернені існують, то вони рівні. Тобто звідси
$\forall a \in R : \exists a^{-1} = b \in R : a \cdot a^{-1} = a^{-1} \cdot a = 1$. ■

Example 3.3.26 Розглянемо $\langle \mathbb{Z}_p, +, \cdot \rangle$ – кільце, де p - просте. Воно не має дільників нуля, тому що $\overline{k_1} \cdot \overline{k_2} = \overline{k_1 \cdot k_2} = \overline{0} \implies k_1 \cdot k_2 \equiv 0 \pmod{p} \implies p \mid k_1 \cdot k_2$, тобто або $p \mid k_1 \implies \overline{k_1} = \overline{0}$; або $p \mid k_2 \implies \overline{k_2} = \overline{0}$. Тоді звідси випливає, що всі ці елементи – оборотні, тобто $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$.
Це як по-іншому можна було довести існування обернених елементів.

Definition 3.3.27 Задано $\langle R, +, \cdot \rangle$ – комутативне кільце з одиницею.
Воно називається **областю цілісності** (**integral domain**), якщо

$$R \text{ не містить дільників нуля}$$

Example 3.3.28 Зокрема наступні кільця будуть областями цілісності:
1. $\langle \mathbb{Z}, +, \cdot \rangle$;
2. $\langle \mathbb{Z}_p, +, \cdot \rangle$ (тут p – просте число).
Але от кільце $\langle \mathbb{Z}_6, +, \cdot \rangle$ уже не буде областю цілісності, бо там є дільники нуля за прикладом вище.

3.3.4 Поле

Definition 3.3.29 Задано $\langle F, +, \cdot \rangle$ – ненульове комутативне кільце з 1.
Воно називається **полем**, якщо

$$F^\times = F \setminus \{0\},$$

тобто всі ненульові елементи – оборотні.

Example 3.3.30 Зокрема наступні структури будуть полями:
1. $\langle \mathbb{Q}, +, \cdot \rangle$;
2. $\left\langle \mathbb{Q}(\sqrt{2}), +, \cdot \right\rangle$, тут маємо $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Corollary 3.3.31 Будь-яке поле – область цілісності.
Випливає з **Th. 3.3.20**.

Remark 3.3.32 Але не кожна область цілісності – поле. Наприклад, $\langle \mathbb{Z}, +, \cdot \rangle$.

Theorem 3.3.33 Задано скінченну область цілісності, там не менше 2 елементів. Тоді вона – поле.
Випливає з **Th. 3.3.25**.

Example 3.3.34 Зокрема $\langle \mathbb{Z}_p, +, \cdot \rangle$, де p – просте, буде полем.
А от якщо p – складене, то тоді вже полем не буде. Тому що має дільник. Дісно, $p = k \cdot m$, раз воно складене. Тоді $\overline{0} = \overline{p} = \overline{k \cdot m} = \overline{k} \cdot \overline{m}$.

Це були лише основні класифікації кілець. Із іншими більш цікавими кільцями ознаймомимося вже пізніше.

3.4 Характеристика

Definition 3.4.1 Задано $\langle R, +, \cdot \rangle$ – ненульове кільце.
Характеристикою кільця називають найменше число $n \in \mathbb{N}$, для якого

$$\forall r \in R : \underbrace{r + \cdots + r}_{n \text{ разів}} = 0$$

Позначення: $n = \operatorname{char}(R)$.
Якщо такого $n \in \mathbb{N}$ не існує, то тоді $\operatorname{char}(R) \overset{\text{def.}}{=} 0$.

Remark 3.4.2 Інколи ще скорочують $\underbrace{r + \cdots + r}_{n \text{ разів}} = n \cdot r$. Як на мене, це позначення призводить до плутанини, тому уникатиму.

Example 3.4.3 Зокрема в кільці $\langle \mathbb{R}, +, \cdot \rangle$ маємо $\operatorname{char}(\mathbb{R}) = 0$ (зрозуміло).

Proposition 3.4.4 Задано $\langle R, +, \cdot \rangle$ – кільце з одиницею. Відомо, що $\operatorname{ord}_{\langle R, + \rangle}(1) = n$. Тоді $\operatorname{char} R = n$.

Proof.
Позначимо $\operatorname{char} = m$. Тоді $\underbrace{1 + \cdots + 1}_{m \text{ разів}} = 0 \implies \operatorname{ord}(1) = n \mid m \implies n \leq m$.
Водночас $\underbrace{r + \cdots + r}_{n \text{ разів}} = r(\underbrace{1 + \cdots + 1}_{n \text{ разів}}) = r \cdot 0 = 0 \implies m \geq n$.
Отже, $m = n$. ■

Remark 3.4.5 Отже, коли ми маємо $\langle R, +, \cdot \rangle$ – ненульове кільце з одиницею, то характеристикою назвають найменше число $n \in \mathbb{N}$, для якого

$$\underbrace{1 + \cdots + 1}_{n \text{ разів}} = 0$$

або 0, якщо такого найменшого нема. І саме ось таке означення дають більшість авторів.

Example 3.4.6 Зокрема в кільці $\langle \mathbb{Z}_n, +, \cdot \rangle$ маємо $\operatorname{char}(\mathbb{Z}_n) = n$.

Proposition 3.4.7 Задано $\langle R, +, \cdot \rangle$ – область цілісності. Тоді $\operatorname{char}(R) \in \{0, p\}$. У цьому випадку p – просте число.

Proof.
Якщо $\operatorname{char} R = 0$, то нема що доводити. Тому припустимо $\operatorname{char} R = n$.
!Припустимо, що n – складене число, тоді $n = ab$, причому $1 < a, b < n$.
$0 = \underbrace{1 + \cdots + 1}_{n \text{ разів}} = \underbrace{\underbrace{1 + \cdots + 1}_{a \text{ разів}} + \cdots + \underbrace{1 + \cdots + 1}_{a \text{ разів}}}_{b \text{ разів}} = (\underbrace{1 + \cdots + 1}_{a \text{ разів}})(\underbrace{1 + \cdots + 1}_{b \text{ разів}})$.
В останній рівності ми скористались дитрибутивністю, коли виносили $\underbrace{1 + \cdots + 1}_{a \text{ разів}}$. Тепер оскільки ми знаходимось в області цілісноті, то тоді або $\underbrace{1 + \cdots + 1}_{a \text{ разів}} = 0$, або $\underbrace{1 + \cdots + 1}_{b \text{ разів}} = 0$. Звідси отримаємо або $a \geq n$, або $b \geq n$. У двох випадках суперечність!
Отже, n може бути лише простим числом. ■

3.5 Кільце многочленів

Задано $\langle R, +, \cdot \rangle$ – будь-яке кільце. Визначимо таку множину:

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \geq 0, a_i \in R\},$$

де елемент $f \in R[x]$ – многочлен, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Даний об'єкт можна ще записати таким чином: $f(x) = \sum_{i \geq 0} a_i x^i$, де у випадку $i > n$ матимемо $a_i = 0$.

Нехай $f(x) = \sum_{i \geq 0} a_i x^i,\ g(x) = \sum_{i \geq 0} b_i x^i$. Ми визначимо такі операції:

$$f(x) + g(x) = \sum_{i \geq 0} (a_i + b_i) x^i$$

$$f(x) \cdot g(x) = \sum_{i \geq 0} \left(\sum_{r+s=i} a_r \cdot b_s \right) x^i$$

Це такі самі операції, як з многочлени з дійсними коефіцієнтами. Зрозуміло, що множина – замкнена відносно цих операцій.

Theorem 3.5.1 $\langle R[x], +, \cdot \rangle$ – (комутативне з одиницею) кільце $\iff$ $\langle R, +, \cdot \rangle$ – (комутативне з одиницею) кільце.

Proof.
Буде раціональніше спочатку довести в зворотному напрямку.
$\boxed{\Leftarrow}$ Дано $\langle R, +, \cdot \rangle$ – кільце. Наша мета: $\langle R[x], +, \cdot \rangle$ – кільце.
Візьмемо многочлени $f, g, h \in R[x]$, тобто $f(x) = \sum_{i \geq 0} a_i x^i \quad g(x) = \sum_{i \geq 0} b_i x^i \quad h(x) = \sum_{i \geq 0} c_i x^i$.
1. $f(x) + (g(x) + h(x)) = f(x) + \sum_{i \geq 0} (b_i + c_i) x^i = \sum_{i \geq 0} (a_i + (b_i + c_i)) x^i \overset{\text{1) для } R}{=} \sum_{i \geq 0} ((a_i + b_i) + c_i) x^i =$
$(f(x) + g(x)) + \sum_{i \geq 0} c_i x^i = (f(x) + g(x)) + h(x)$.
2. $f(x) + g(x) = \sum_{i \geq 0} (a_i + b_i) x^i \overset{\text{2) для } R}{=} \sum_{i \geq 0} (b_i + a_i) x^i = g(x) + f(x)$.

3. Маємо $\mathbf{0}(x) = 0$, тобто $\mathbf{0}(x) = \sum\limits_{i\geq 0} 0x^i$, де 0 - це нуль кільця R. Тоді

$f(x) + \mathbf{0}(x) = \sum\limits_{i\geq 0}(a_i + 0)x^i \overset{\text{3) для } R}{=} \sum\limits_{i\geq 0} a_i x^i = f(x).$

4. Для $f \in R[x]$ існує $-f \in R[x]$, що $(-f)(x) = \sum\limits_{i\geq 0}(-a_i)x^i \in R[x]$. Оскільки $a_i \in R, i \geq 0$, то за 4), існують $-a_i \in R$ для яких виконується рівність 4). Тоді

$f(x) + (-f)(x) = \sum\limits_{i\geq 0}(a_i + (-a_i))x^i \overset{\text{4) для } R}{=} \sum\limits_{i\geq 0} 0x^i = \mathbf{0}(x).$

5. $f(x) \cdot (g(x) \cdot h(x)) \overset{?}{=} (f(x) \cdot g(x)) \cdot h(x)$ – доволі складна рівність.

$g(x) \cdot h(x) = \sum\limits_{i\geq 0} d_i x^i$, де $\quad d_i = \sum\limits_{r+s=i} b_r c_s$

$f(x) \cdot (g(x) \cdot h(x)) = \sum\limits_{i\geq 0} u_i x^i$, де

$$u_i = \sum_{r+s=i} a_r d_s = \sum_{r+s=i} a_r \left(\sum_{\xi+\eta=s} b_\xi c_\eta \right) = \sum_{r+s=i} \sum_{\xi+\eta=s} a_r b_\xi c_\eta = \sum_{\xi+\eta+r=i} a_r b_\xi c_\eta.$$

$f(x) \cdot g(x) = \sum\limits_{i\geq 0} \tilde{d}_i x^i$, де $\quad \tilde{d}_i = \sum\limits_{r+s=i} a_r b_s$

$(f(x) \cdot g(x)) \cdot h(x) = \sum\limits_{i\geq 0} v_i x^i$, де

$$v_i = \sum_{r+s=i} d_r c_s = \sum_{r+s=i} \left(\sum_{\xi+\eta=r} a_\xi b_\eta \right) c_s = \sum_{r+s=i} \sum_{\xi+\eta=r} a_\xi b_\eta c_s = \sum_{\eta+s+\xi=i} a_\xi b_\eta c_s.$$

Якщо уважно придивитися, то можна зауважити, що $u_v = v_i$, тоді

$f(x) \cdot (g(x) \cdot h(x)) = \sum\limits_{i\geq 0} u_i x^i = \sum\limits_{i\geq 0} v_i x^i = (f(x) \cdot g(x)) \cdot h(x).$

Слід також зауважити, що ми користувалися спочатку 6) для R, а в кінці 5) для R, просто останнє я це явно не вказав.

$$6.\ f(x) \cdot (g(x) + h(x)) = \sum_{i\geq 0} \left(\sum_{r+s=i} a_r (b_s + c_s) \right) x^i = \sum_{i\geq 0} \left(\sum_{r+s=i} a_r b_s + \sum_{r+s=i} a_r c_s \right) x^i =$$

$$= \sum_{i\geq 0} \left(\sum_{r+s=i} a_r b_s \right) x^i + \sum_{i\geq 0} \left(\sum_{r+s=i} a_r c_s \right) x^i = f \cdot g(x) + f(x) \cdot h(x).$$

Аналогічно $(f(x) + g(x)) \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x)$.

Тепер нехай $\langle R, +, \cdot \rangle$ додатково комутативне кільце з одиницею. Тоді для $f, g \in R[x]$ маємо:

$$f(x) \cdot g(x) = \sum_{i\geq 0} \left(\sum_{r+s=i} a_r b_s \right) x^i = \sum_{i\geq 0} \left(\sum_{s+r=i} b_s a_r \right) x^i = g \cdot f.$$

Маємо $\mathbf{1}(x) = 1$, тобто $\mathbf{1}(x) = 1 + \sum\limits_{i\geq 1} 0x^n$, де 1 - це одиниця кільця R.

$$f(x) \cdot \mathbf{1}(x) = \sum_{i\geq 0} \left(\sum_{\substack{r+s=i \\ s>0}} a_r \cdot 0 + \sum_{\substack{r+s=i \\ s=0}} a_r \cdot 1 \right) x^i = \sum_{i\geq 0} a_i x^i = f(x).$$

Висновок: $\langle R[x], +, \cdot \rangle$ – (комутативне з одиницею) кільце.

$\boxed{\Rightarrow}$ Дано: $\langle R[x], +, \cdot \rangle$ – (комутативне з одиницею) кільце. Варто зауважити, що коли $u \in R$, то автоматично $u \in R[x]$. Тому що $u = u + 0x + 0x^2 + \ldots$ Ну тобто, по суті кажучи, ми маємо $R \subset R[x]$. Треба лише довести, що R є підкільцем $R[x]$, але це неважко. ■

Corollary 3.5.2 $\langle R[x], +, \cdot \rangle$ – область цілісності $\iff$ $\langle R, +, \cdot \rangle$ – область цілісності.

Proof.
$\boxed{\Leftarrow}$ Дано: $\langle R, +, \cdot\rangle$ – область цілісності. По суті, все, що нам залишилось довести, – це відсутність дільників нуля в $R[x]$.
!Припустимо, що $f \in R[x], f \neq \mathbf{0}$ – дільник нуля, тобто $\exists g \in R[x], g \neq \mathbf{0}$, для якого $f \cdot g = \mathbf{0}$. Тобто маємо $(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_kx^k) = 0$. Маємо старший коефіцієнт a_nb_k після множення. Оскільки многочлен нульовий, то це означає, що всі коефіцієнти, зокрема $a_nb_k = 0$. Але нам відомо, що $a_n, b_k \neq 0$, а тому a_n – дільник нуля – суперечить умові того, що R – область цілісності!

$\boxed{\Rightarrow}$ Дано: $\langle R[x], +, \cdot\rangle$ – область цілісності.
!Припустимо, що $u \in R, u \neq 0$ – дільник нуля, тобто $\exists v \in R, v \neq 0$, для якого $uv = 0$. Але u,v можна сприймати як многочлени, і тоді u - дільник нуля в $R[x]$ - суперечність! ■

Remark 3.5.3 Якщо R – кільце, тобто $R[x]$ – теж кільце (некомутативне), то нам варто вважати, що x комутує з усіма елементами $a \in R$. Це робиться, аби можна було розкривати дужки.

Example 3.5.4 Зокрема маємо $\mathbb{Z}/_{2\mathbb{Z}}[x]$ – кільце. Маємо многочлен $f(x) = x(x+\bar{1}) = x^2+\bar{1}x = x^2+x$. Можна зауважити, що $\forall x \in \mathbb{Z}/_{2\mathbb{Z}} : f(x) = \bar{0}$. Але в жодному разі $f(x) \neq \mathbf{0}(x)$ як многочлени. У функціональному сенсі вони рівні, але об'єкти різні.

Remark 3.5.5 Маємо $\langle R, +, \cdot, \rangle$ – кільце, ну тоді вже ясно, що $\langle R[x], +, \cdot, \rangle$ – кільце. Але можна піти далі та утворити нове кільце $\langle R[x][y], +, \cdot, \rangle$. Подивимось, що з себе представляє об'єкт $f \in R[x][y]$.
$(f(x))(y) = \sum\limits_{j\geq 0} a_jy^j$, при цьому $a_j \in R[x]$, тобто $a_j(x) = \sum\limits_{i\geq 0} b_{ij}x^i$.

$$(f(x))(y) = \sum_{j\geq 0} \left(\sum_{i\geq 0} b_{ij}x^j \right) y^i.$$

Далі $(f(x))(y)$ можна позначити за $f(x, y)$, а тому звідси отримаємо **многочлен з двома змінними**:
$f(x, y) = \sum\limits_{i,j\geq 0} b_{ij}x^iy^j$.
Надалі можна $R[x][y]$ позначити як $R[x, y]$.

Можна далі продовжити цей процес та утворити кільце $R[x_1, x_2, \ldots, x_n]$.

Про кільце многочленів ми ще будемо розмовляти неодноразово.

3.6 Гомоморфізм кілець

Definition 3.6.1 Задано $\langle R_1, +, \cdot\rangle$ та $\langle R_2, \oplus, \odot\rangle$ – кільця.
Гомоморфізмом (кілець) називають відображення $f\colon R_1 \to R_2$, для якого

$$\forall a, b \in R_1 : f(a + b) = f(a) \oplus f(b)$$
$$\forall a, b \in R_1 : f(a \cdot b) = f(a) \odot f(b)$$

Example 3.6.2 Між будь-якими кільцями $\langle R_1, +, \cdot\rangle$ та $\langle R_2, +, \cdot\rangle$ можна встановити нульовий гомоморфізм $O\colon R_1 \to R_2$ таким чином: $O(x) = 0, \forall x \in R_1$.

Example 3.6.3 Freshman's dream (мрія першокурсника)
Задано $\langle R, +, \cdot\rangle$ – комутативне кільце з одиницею, причому $\mathrm{char}(R) = p$, де p – просте число. Розглянемо відображення Фробеніуса $\varphi\colon R \to R$ як $\varphi(r) = r^p$. Воно задає гомоморфізм.
$\varphi(a + b) = (a + b)^p = a^p + C_p^1a^{p-1}b + \cdots + C_p^{p-1}ab^{p-1} + b^p\boxed{=}$.
Зауважимо, що $p \mid C_p^k$ при $k \in \{1, \ldots, p - 1\}$. Вправа з теорії чисел.
А далі скористаємось тим, що $\mathrm{char}(R) = p$.
$\boxed{=} a^p + 0 + \cdots + 0 + b^p = a^p + b^p = \varphi(a) + \varphi(b)$.
$\varphi(ab) = (ab)^p = a^pb^p = \varphi(a)\varphi(b)$.
Всі рівності виконуються лише за умовою комутативності кільця.

У загальному випадку це не працює. Можна взяти кільце $\langle \mathbb{R}, +, \cdot\rangle$ з нулевою характеристикою. Там $(a + b)^2 \neq a^2 + b^2$.

Proposition 3.6.4 Категорія гомоморфізмів кілець
Задані R, S, T – кільця. Тоді виконуються наступне:
1) $\mathrm{id}\colon R \to R$ – гомоморфізм;
2) Якщо $\varphi\colon R \to S, \psi\colon S \to T$ – гомоморфізми, то $\psi \circ \varphi\colon R \to T$ – також гомоморфізм;
3) Операція композиції гомоморфізмів кілець – асоціативна.
Все що треба показати – це збереження множення (неважко). Все решта виконується в силу категорії гомоморфізма груп.

Theorem 3.6.5 Властивості гомоморфізма
Задано $\langle R_1, +, \cdot\rangle$ та $\langle R_2, \oplus, \odot\rangle$ – кільця. Маємо $f\colon R_1 \to R_2$ – гомоморфізм кілець, тоді виконуються такі пункти:
1) $f(0_{R_1}) = 0_{R_2}$;
2) $\forall a \in R_1 : f(-a) = -f(a)$;
3) Нехай S – підкільце $\langle R_1, +, \cdot\rangle$. Тоді $f(S)$ – підкільце $\langle R_2, \oplus, \odot\rangle$;
4) Нехай T – підкільце $\langle R_2, \oplus, \odot\rangle$. Тоді $f^{-1}(T)$ – підкільце $\langle R_1, +, \cdot\rangle$.
Перші дві властивості випливають з властивостей гомоморфізма груп (якщо викинути операцію множення). Решта дві доводяться майже аналогічно, як було це з групами.

Theorem 3.6.6 Задано $\langle R_1, +, \cdot\rangle$ та $\langle R_2, \oplus, \odot\rangle$ – кільця та $f\colon R_1 \to R_2$ – сюр'єктивний гомоморфізм. Тоді якщо J – ідеал R_1, то $f(J)$ – ідеал R_2.
Вправа: довести.

Corollary 3.6.7 Задано $\langle R_1, +, \cdot\rangle$ та $\langle R_2, \oplus, \odot\rangle$ - кільця та $f : R_1 \to R_2$ - гомоморфізм. Тоді
1. $\ker f$ - ідеал R_1;
2. $\mathrm{Im}\, f$ - підкільце кільця R_2.

Definition 3.6.8 Задані $\langle R_1, +, \cdot\rangle, \langle R_2, \oplus, \odot\rangle$ – кільця, а також $f\colon R_1 \to R_2$ – гомоморфізм кілець. Відображення f називається **ізоморфізмом**, якщо

$$f \text{ – бієктивне}$$

У такому разі кільця R_1, R_2 називаються **ізоморфними**.
Позначення: $\langle R_1, +, \cdot\rangle \cong \langle R_2, \oplus, \odot\rangle$.

Example 3.6.9 $m\mathbb{Z} \cong n\mathbb{Z}$ в сенсі груп при $m \neq n$ (припускаємо всюди $m, n \geq 0$), просто тому що це дві циклічні групи, що $\cong \mathbb{Z}$.
Але $m\mathbb{Z} \ncong n\mathbb{Z}$ в сенсі кілець при $m \neq n$.
!Припустимо, що існує ізоморфізм кілець $f\colon m\mathbb{Z} \to n\mathbb{Z}$. Маємо:
$f(m^2) = f(m)f(m) = \underbrace{f(m) + \cdots + f(m)}_{m \text{ разів}} = mf(m)$.
$\Longrightarrow\ f(m)(f(m) - m)) = 0$. Оскільки $n\mathbb{Z}$ – це область цілісності, то тоді або $f(m) = 0$, або $f(m) = m$.
I. $f(m) = 0$, тоді $f(km) = 0, \forall km \in m\mathbb{Z}$, це ніфіга не ізоморфізм.
II. $f(m) = m$, а це можливо лише при $n \mid m$. Тобто $m = kn$, маємо $f(kn) = kn$. Оскільки f – сюр'єктивний, то $n = f(u \cdot kn) = uf(kn) = ukn$. Ці два елементи $n, ukn \in n\mathbb{Z}$ і вони рівні лише при $uk = 1$. Але $k \neq 1$, тоді рівність така неможлива.
Отримали суперечність у двох випадках!

Theorem 3.6.10 Властивості ізоморфізма
Задані $\langle R_1, +, \cdot\rangle, \langle R_2, \oplus, \odot\rangle$ – кільця. Маємо $f\colon R_1 \to R_2$ – ізоморфізм, тоді:
1) $f^{-1}\colon R_2 \to R_1$ – також ізоморфізм;
2) $\langle R_1, +, \cdot\rangle$ – комутативне $\iff \langle R_2, \oplus, \odot\rangle$ – комутативне;
3) $a \in R_1$ – дільник нуля $\iff f(a)$ – дільник нуля;

Corollary 3.6.11 $\langle R_1, +, \cdot\rangle$ – область цілісності (поле) $\iff \langle R_2, \oplus, \odot\rangle$ – область цілісності (поле).

Definition 3.6.12 Задані $\langle R_1, +, \cdot\rangle, \langle R_2, \oplus, \odot\rangle$ – кільця, $f\colon R_1 \to R_2$ – гомоморфізм.
Ядром гомоморфізма називають множину

$$\ker f = \{x \in R_1 : f(x) = 0_{R_2}\}$$

Образом гомоморфізма називають множину

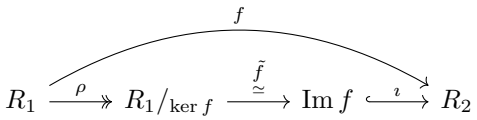
$$\mathrm{Im}\, f = \{f(x) : x \in R_1\}$$

Remark 3.6.13 $\ker f = f^{-1}(\{0_{R_2}\}), \qquad \operatorname{Im} f = f(R_1)$.
Таким чином, оскільки $\{0_{R_2}\}, R_2$ є тривіальними підкільцями для своїх кілець, то за властивостями гомоморфізма, $f^{-1}(\{0_{R_2}\}), f(S_1)$ будуть підкільцями для своїх кілець як прообраз та образ відповідно.

Theorem 3.6.14 Задані $\langle R_1, +, \cdot\rangle, \langle R_2, \oplus, \odot\rangle$ – кільця та $f\colon R_1 \to R_2$ – гомоморфізм.
f – ін'єктивне $\iff \ker f = \{0_{R_1}\}$.
Вправа: довести.

Аналогічно будується **основна теорема про гомоморфізми кілець**

Theorem 3.6.15 Задано $\langle R_1, +, \cdot\rangle$ та $\langle R_2, \oplus, \odot\rangle$ - кільця та $f : R_1 \to R_2$ - гомоморфізм. Тоді існує єдиний ізоморфізм кілець $\tilde{f}\colon G_1/_{\ker f} \to \operatorname{Im} f$, для якого $\imath \circ \tilde{f} \circ \rho = f$.



Тут ρ - природний гомоморфізм кілець та $\imath$ - гомоморфізм кілець вкладення.

Proof.
Лише достатньо показати, що $\tilde{f}(x \cdot y) = \tilde{f}(x) \cdot \tilde{f}(y)$ - це неважко. Також варто це зроби для інших гомоморфізмів. Це неважко.
А далі все решта випливає з основної теореми про гомоморфізм груп. ■

Example 3.6.16 Маємо кільце $\langle \mathbb{R}[x], +, \cdot\rangle$ та головний ідеал $(x-a), a \in \mathbb{R}$. Розглянемо гомоморфізм $f : \mathbb{R}[x] \to \mathbb{R}$ таким чином:
$f(p) = p(a)$.
Тобто беремо кожний многочлен та відображуємо на цей же многочлен в точці $a \in \mathbb{R}$.
$\ker f = \{p \in \mathbb{R}[x] : p(a) = 0\} = (x - a)$.
$\operatorname{Im} f = \{p(a) | p \in \mathbb{R}[x]\} = \mathbb{R}$.
Застосувавши основну теорему про гомоморфізм, отримаємо, що
$\mathbb{R}[x]/_{(x-a)} \cong \mathbb{R}$.
А ізоморфізм задається таким чином:
$\varphi(p + (x - a)) = p(a)$, де
$p + (x - a) = \{p(x) + r(x) | r \in (x - a)\} = \{p(x) + q(x)(x - a) | q \in \mathbb{R}[x]\}$

Example 3.6.17 Маємо кільце $\langle \mathbb{R}[x], +, \cdot\rangle$ та головний ідеал
$(ax^2 + bx + c), a \neq 0, b, c \in \mathbb{R}$, причому $D < 0$. Розглянемо гомоморфізм $f : \mathbb{R}[x] \to \mathbb{C}$ таким чином:
$p \overset{f}{\mapsto} p(z)$, де z - комплексний корінь $ax^2 + bx + c$.
$\ker f = \{p \in \mathbb{R}[x] : p(z) = 0\} = (ax^2 + bx + c)$.
$\operatorname{Im} f = \{p(z) | p \in \mathbb{R}[x]\} = \mathbb{C}$.
Застосувавши основну теорему про гомоморфізм, отримаємо, що
$\mathbb{R}[x]/_{(ax^2+bx+c)} \cong \mathbb{C}$.
А ізоморфізм задається таким чином:
$\varphi(p + (ax^2 + bx + c)) = p(z)$, тобто беремо всі многочлени, де значення дорівнює $p(z)$.

Example 3.6.18 Маємо кільце $\langle \mathbb{R}[x], +, \cdot\rangle$ та головний ідеал:
1. $(x - a)(x - b), a, b \in \mathbb{R}, a \neq b$. Розглянемо гомоморфізм $f : \mathbb{R}[x] \to M_{2\times 2}$ таким чином:
$f(p) = p\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

Аналогічно можна показати, що $\mathbb{R}/_{(x-a)(x-b)} \cong \left\{ \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} | a_1, a_2 \in \mathbb{R} \right\}$.

2. $(x - a)^2, a \in \mathbb{R}$. Розглянемо гомоморфізм $f : \mathbb{R}[x] \to M_{2\times 2}$ таким чином:
$f(p) = p\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ - клітина Жордана.

Аналогічно можна показати, що $\mathbb{R}/_{(x-a)^2} \cong \left\{ \begin{pmatrix} a_1 & a_2 \\ 0 & a_1 \end{pmatrix} | a_1, a_2 \in \mathbb{R} \right\}$.

3.7 Ідеал кільця. Породжені ідеали

Definition 3.7.1 Задано $\langle R, +, \cdot\rangle$ – кільце.
Ідеалом даного кільця назвемо множину $\emptyset \neq J \subset R$, для якої

$$\langle J, +\rangle \text{ – підгрупа групи } \langle R, +\rangle$$
$$\forall r \in R : \forall j \in J : rj, jr \in J$$

Remark 3.7.2 Можна сказати, що ідеал кільця – це такий собі аналог нормального дільника групи в теорії груп.

Remark 3.7.3 Інколи розрізняють: ліві ідеали, коли $rj \in J$, та праві ідеали, коли $jr \in J$. Якщо ідеал одночасно лівий та правий, інколи це називають двостороннім ідеалом.

Example 3.7.4 Розглянемо кільце $\langle \mathbb{Z}, +, \cdot\rangle$. Воно має ідеали $n\mathbb{Z}$, де $n \in \mathbb{N} \cup \{0\}$, тому що
$n\mathbb{Z}$ - підгрупа групи $\langle \mathbb{Z}, +\rangle$;
$\forall m \in \mathbb{Z} : \forall k \in n\mathbb{Z}$ маємо $k = nl$, а тому звідси $mk = km = n(lm) \in n\mathbb{Z}$.

Example 3.7.5 $\{0\}, R$ – ідеали кільця $\langle R, +, \cdot\rangle$, вони ще називаються **тривіальними ідеалами**.

Remark 3.7.6 Якщо J – ідеал, то J буде підкільцем R. Навпаки – ні.
Зокрема $\mathbb{Z}$ буде підкільцем $\langle \mathbb{R}, +, \cdot\rangle$, але не ідеалом, тому що $3 \cdot \sqrt{2} \notin \mathbb{Z}$.

Proposition 3.7.7 Задано $\langle R, +, \cdot\rangle$ – кільце з одиницею та J – ідеал, для якого $1 \in J$. Тоді $J = R$.

Proof.
Те, що $J \subset R$, – це за означенням.
Оскільки J – ідеал, то тоді для числа $1 \in J : \forall x \in R : x \cdot 1 = 1 \cdot x = x \in J$. Тобто $R \subset J$. ■

Proposition 3.7.8 Ще одна властивість гомоморфізма
Задано $\langle R_1, +, \cdot\rangle, \langle R_2, \oplus, \odot\rangle$ – кільця та $f\colon R_1 \to R_2$ – гомоморфізм. Нехай J – ідеал $\langle R_2, \oplus, \odot\rangle$. Тоді $f^{-1}(J)$ – ідеал $\langle R_1, +, \cdot\rangle$.

Corollary 3.7.9 $\ker f$ – ідеал R_1.

Remark 3.7.10 Варто зауважити, що якщо J – ідеал R_1, то не обов'язково $f(J)$ буде ідеалом R_2. Зокрема можна розглянути вкладення $\imath\colon \mathbb{Z} \to \mathbb{Q}$, а в якості ідеалу взяти $J = 2\mathbb{Z}$. Тоді $\imath(J) = J$ не буде ідеалом $\mathbb{Q}$.
Можна взяти $\frac{1}{2} \in \mathbb{Q}$ та $3 \in \imath(J)$, тоді звідси $\frac{1}{2} \cdot 3 \notin \imath(J)$.

Lemma 3.7.11 Задано $\langle R, +, \cdot\rangle$ – комутативне кільце з одиницею, $a \in R$.
Тоді aR – ідеал для цього кільця. Його ще називають **головним ідеалом, породженим елементом** $a \in R$.
Позначення: $(a) = aR$.

Proof.
$$x_1, x_2 \in aR \implies \begin{cases} x_1 = ar_1 \\ x_2 = ar_2 \end{cases}, \text{ де } r_1, r_2 \in R \implies x_1 - x_2 = a(r_1 - r_2) \implies x_1 - x_2 \in aR.$$
Цим показали, що aR – підгрупа групи $\langle R, +\rangle$.
$x \in aR, r_0 \in R \implies x = ar, r \in R \implies r_0 x = x r_0 = a r r_0 \in aR$.
А цим показали другу умову для ідеала. ■

Proposition 3.7.12 Задано $\langle R, +, \cdot\rangle$ – комутативне кільце з одиницею, $a \in R$. Тоді (a) – найменший ідеал, що містить елемент a.

Proof.
!Припустимо, що існує якийсь інший ідеал $J \ni a$, який менший, тобто $J \subset (a)$. Тоді доведемо, що $J = (a)$.
Нехай $x \in (a)$, тобто $x = ar_0, r_0 \in R$. Оскільки J - ідеал, то звідси $\forall j \in J : \forall r \in R : jr \in J$.
Зокрема для $j = a$, $r = r_0$ ми маємо $ar_0 = x \in J$.
Отже, $(a) \subset J$, а тому звідси $J = (a)$. Суперечність! ■

Remark 3.7.13 Ми знаємо, що $(a) = \{ar \mid r \in \mathbb{R}\}$. Ми можемо узагальнити означення та написати ідеал, породжений кількома елементами:

$$(a_1, \dots, a_n) = \{r_1 a_1 + \dots + r_n a_n \mid r_1, \dots, r_n \in R\}$$

Те, що це дійсно ідеал, неважко переконатися. Причому найменший, що містить $a_1, \dots, a_n$.

Example 3.7.14 Розглянемо кільце $\langle \mathbb{Z}, +, \cdot \rangle$ - комутативне з одиницею. Тоді $(n) = (-n) = n\mathbb{Z}$.

Example 3.7.15 Розглянемо кільце $\langle \mathbb{R}[x], +, \cdot \rangle$ - комутативне з одиничним многочленом. Тоді
$(p(x)) = \{s \in \mathbb{R}[x] : s(x) = p(x)q(x), q \in \mathbb{R}[x]\}$
тобто головний ідеал $(p(x))$ містить многочлени, що діляться націло на многочлен p. Випливає з прямого визначення головного ідеала.
$(x - a) = \{s \in \mathbb{R}[x] : s(x) = (x - a)q(x), q \in \mathbb{R}[x]\}$
тобто головний ідеал $(x - a)$ містить многочлени, що мають корень a.

Remark 3.7.16 $\{0\}$. R – головні ідеали комутативного кільця $\langle R, +, \cdot \rangle$ з одиницею, тому що $\{0\} = 0R = (0)$ та $R = 1R = (1)$.

Definition 3.7.17 Областю (або **кільцем**) **головних ідеалів** називаємо область цілісности, що містить лише головні ідеали.
Англійською це називається **principle ideal domain (PID)**.

Example 3.7.18 Зокрема $\langle \mathbb{Z}, +, \cdot \rangle$ - що є областю цілісності - буде областю головних ідеалів.
!Припустимо, що J - деякий ненульовий ідеал, але не можна розписати його як головний ідеал. Щоб прийти до суперечності, ми покажемо, що $J = (m)$ для числа $m = \min\limits_{\substack{n \in \mathbb{N} \\ n \in J}} n$.
Цей мінімум завжди існує, тому що коли є якесь від'ємне число $-m \in J$, то зокрема $m = (-1) \cdot (-m) \in J$ в силу означення ідеала.
Маємо $m \in J$ та $k \in \mathbb{Z}$, тоді звідси $mk \in J$, а тому $(m) \subset J$.
Маємо $n, m \in J$, застосуємо алгоритм Евкліда - отримаємо
$n = km + r \implies r = n - km \in J$.
Також $0 \leq r < m$. А оскільки m - найменше додатне число, то в силу того, що $r \in J$ маємо $r \geq m$. Тому єдиний варіант - це вимагати $r = 0$.
Отже, $n \in J$, причому $n = km$, звідси $n \in (m)$. Отже, $J \subset (m)$.
Таким чином, $J = (m)$. Суперечність!

Example 3.7.19 Зокрема $\langle \mathbb{R}[x], +, \cdot \rangle$ - що є областю цілісності - буде областю головних ідеалів.
!Припустимо, що J - деякий ненульовий ідеал, але не можна розписати його як головний ідеал. Щоб прийти до суперечності, ми покажемо, що $J = (p(x))$, де p - многочлен, для якого $\deg p = m$, а число $m = \min\limits_{f \in J} \deg f$, де $m > 0$.
Маємо $p(x) \in J$ - многочлен степені m. Тоді $\forall q(x) \in \mathbb{R}[x]$ маємо $r(x) = p(x)q(x) \in J$ за означенням ідеала. Отже, $r(x) \in (p(x))$.
Таким чином, $(p(x)) \subset J$.
Маємо $s(x), p(x) \in J$, застосуємо алгоритм Евкліда - отримаємо
$s(x) = p(x)q(x) + r(x) \implies r(x) = s(x) - p(x)q(x) \in J$.
Також $\deg r < m$ або $r \equiv 0$. А оскільки m - найменше додатне число, то в силу того, що $r(x) \in J$ ми маємо $\deg r \geq m$. Єдиний варіант - це $r = 0$, тоді звідси $s(x) = p(x)q(x) \implies s(x) \in (p(x))$. І звідси $J = (p(x))$. Суперечність!

І взагалі, якщо ми маємо $k[x]$, де k - деяке поле (див. нижче), то ми все одно будемо мати область головних ідеалів.

Example 3.7.20 А от $\langle \mathbb{R}[x_1, \dots, x_n], +, \dots \rangle$ уже не буде областю головних ідеалів.
Поки без доведення.

Theorem 3.7.21 Задано $\langle F, +, \cdot \rangle$ – ненульове комутативне кільце з 1.
$\langle F, +, \cdot \rangle$ – поле $\iff$ містить лише тривіальні ідеали.

Proof.
$\boxed{\Rightarrow}$ Дано: $\langle F, +, \cdot, \rangle$.
!Припустимо, що існує якийсь інший ідеал $J \neq \{0\}$ та $J \neq F$. Тоді

$\forall j \in J : \forall f \in F : jf \in J$.
Зокрема якщо $j \in J$ такий, що $j \neq 0$, то по-перше, $j \in F$, а по-друге, $\exists j^{-1} \in F$. Звідси випливає, що $j \cdot j^{-1} = 1 \in J$. За попереднім твердженням, $J = F$. Суперечність!

$\boxed{\Leftarrow}$ Дано: існують лише тривіальні ідеали.
Нехай $a \in F$, де $a \neq 0$, розглянемо головний ідеал (a). Тоді звідси $(a) = R$. Зокрема оскільки $1 \in R$, то звідси $\exists \tilde{a} \in (a) = R : a\tilde{a} = 1$. Отже, всі ненульові елементи – оборотні, а тому F – поле. ■

Example 3.7.22 Зокрема поле $\langle \mathbb{R}, +, \cdot \rangle$ має лише ідеали $\{0\}$ та $\mathbb{R}$.

3.8 Сума, перетин та добуток ідеалів

Definition 3.8.1 Задано $\langle R, +, \cdot \rangle$ – кільце та I, J – ідеали R.
Перетином ідеалів I, J називають ідеал $I \cap J$.
Сумою ідеалів I, J називають такий ідеал

$$I + J \stackrel{\text{def.}}{=} \{a + b \mid a \in I, b \in J\}$$

Добутком ідеалів I, J називають такий ідеал

$$IJ \stackrel{\text{def.}}{=} \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I, b_i \in J\}$$

Proposition 3.8.2 $I \cap J, I + J, IJ$ – дійсно є ідеалами кільця R.

Proof.
1. $I \cap J$
Спочатку доводимо, що $I \cap J$ – підгрупа $\langle R, + \rangle$.
Нехай $u, v \in I \cap J$. Розглянемо елемент $u - v$.
За умовою, I – підгрупа $\langle R, + \rangle$, тому $u - v \in I$;
За умовою, J – підгрупа $\langle R, + \rangle$, тому $u - v \in J$.
Разом отримали $u - v \in I \cap J$.
Нехай $u \in I \cap J$ та $r \in R$. Тоді оскільки $u \in I$, то тоді $ru, ur \in I$; оскільки $u \in J$, то тоді $ru, ur \in J$. Отримали, що $ru, ur \in I \cap J$.

2. $I + J$
Спочатку доводимо, що $I + J$ – підгрупа $\langle R, + \rangle$.
Нехай $u, v \in I + J$, тобто $u = a_1 + b_1$ та $v = a_2 + b_2$, елементи $a_1, a_2 \in I,\ b_1, b_2 \in J$. Тоді
$u - v = (a_1 - a_2) + (b_1 - b_2)$, причому оскільки I, J – підгрупи $\langle R, + \rangle$, то тоді $a_1 - a_2 \in I,\ b_1 - b_2 \in J$. Отже, $u - v \in I + J$.
Нехай $u \in I + J$, тобто $u = a + b$ при $a \in I, b \in J$, та нехай $r \in R$. Тоді звідси $ur = ar + br$, причому звідси $ar \in I, br \in J$ в силу властивості ідеалу. Отже, $ur \in I + J$. Аналогічним чином доводиться $ru \in I + J$.

3. IJ
Нехай $u, v \in IJ$, тобто
$u = a_1^1 b_1^1 + \cdots + a_n^1 b_n^1$
$v = a_1^2 b_1^2 + \cdots + a_m^2 b_m^2$.
Кожний $a_i^j \in I,\ b_i^j \in J$. Тоді маємо
$u - v = a_1^1 b_1^1 + \cdots + a_n^1 b_n^1 - a_1^2 b_1^2 - \cdots - a_m^2 b_m^2$. Ясно, що звідси $u - v \in IJ$.
Нехай $u \in IJ$, тобто $u = a_1 b_1 + \cdots + a_n b_n$ при $a_i \in I, b_i \in J$, та нехай $r \in R$. Тоді звідси $ur = a_1 b_1 r + \cdots + a_n b_n r$. Зауважимо, що в цьому випадку $b_i r \in J$ і досі $a_i \in I$ тоді звідси $ur \in IJ$. Тепер з іншого боку, $ru = ra_1 b_1 + \cdots + ra_n b_n$. А тут вже $ra_i \in I$ і досі $b_i \in J$, тоді звідси $ru \in IJ$. ■

Remark 3.8.3 Ми визначили IJ тіпа як скалярний добуток елементів з I та з J. Виникає питання, чому ми не позначили $IJ = \{ab \mid a \in I, b \in J\}$. Тому що якщо розписати доведення, то виникнуть проблеми з формуванням підгрупи групи $\langle R, + \rangle$.

Example 3.8.4 Розглянемо кільце $\mathbb{Z}[x]$ та ідеали $I = (2, x),\ J = (3, x)$. Зауважимо, що $IJ = (6, x)$. Справді, $6 = 2 \cdot 3$, де $2 \in I, 3 \in J$, тож звідси $6 \in IJ$. Також $x = 3x - 2x$, де $3x \in J,\ 2x \in I$, тож звідси $x \in IJ$. Отже, $(6, x) \subset IJ$. Те, що $IJ \subset (6, x)$, довести неважко.
При цьому $IJ \neq \{ab \mid a \in I, b \in J\}$. Тому що $x \in IJ$, а елемент x не розписується як добуток елементів з I та J.

Example 3.8.5 Маємо $\mathbb{Z}$ – кільце цілих чисел, маємо $(a), (b)$ – головні ідеали. Тоді:
1) $(a) + (b) = (\gcd(a, b))$
Дійсно, нехай $d = \gcd(a, b)$, тоді звідси $a \in (d), b \in (d)$, а тому отримаємо $(a) + (b) \subset (d)$. Із іншого боку, за рівністю Безу, $d = \alpha a + \beta b$, тож $b \in (a) + (b)$, а звідси $(d) \subset (a) + (b)$.

2) $(a) \cap (b) = (\mathrm{lcm}(a, b))$
Дійсно, нехай $u = \mathrm{lcm}(a, b)$, тоді звідси $u \in (a), u \in (b)$, а тому отримаємо $(u) \subset (a) \cap (b)$. Із іншого боку, якщо $w \in (a) \cap (b)$, то тоді $a \mid w, b \mid w$, тобто $u \mid w$. Значить, $(a) \cap (b) \subset (u)$.

3) $(a) \cdot (b) = (ab)$.

Proposition 3.8.6 Задано R – кільце та I, J – ідеали R. Тоді:
1) $I + J$ – найменший ідеал, що містить I, J;
2) $I \cap J$ – найбільший ідеал, що міститься в I, J;
3) $IJ \subset I \cap J$.

Proof.
1) Припустимо, що існує $S \subset I+J$ – менший ідеал, що містить I, J. Необхідно довести, що $S \supset I+J$. Маємо $u \in I + J$, тобто $u = a + b,\ a \in I, b \in J$. Оскільки S є ідеалом та сам містить ідеали I, J, то з цього випливає, що $u = a + b \in S$.

2) Припустимо, що існує $S \supset I \cap J$ – більший ідеал, що міститься в I, J. Необіхдно довести, що $S \subset I \cap J$.
Маємо $u \in S$. Оскільки S міститься в I, J, то звідси $s \in I, s \in J \implies u \in I \cap J$.

3) Нехай $u \in IJ$, тобто $u = a_1b_1 + \cdots + a_nb_n$. Оскільки $a_i \in I, b_i \in R$ та I – ідеал, то $a_ib_i \in I \implies u \in I$. Оскільки $a_i \in R, b_i \in J$ та J – ідеал, то $a_ib_i \in J \implies u \in J$. Отже, $IJ \subset I \cap J$. ■

Remark 3.8.7 Загалом $IJ \not\supset I \cap J$.
Зокрема в кільці $\mathbb{Z}[x]$ маємо ідеали $I = J = (x)$, тоді $IJ = I^2 = (x^2)$. Але тут $IJ \not\supset I \cap J$, оскільки $x \in I \cap J$, але $x \notin IJ$.

Але дану ситуацію можна виправити.

Proposition 3.8.8 Задано R – комутативне кільце з 1 та I, J – ідеали R, причому $I + J = R$. Тоді $I \cap J = IJ$.

Proof.
Уже знаємо, що $IJ \subset I \cap J$.
Оскільки $I + J = R$, то звідси існують $\alpha \in I$ та $\beta \in J$, для яких $\alpha + \beta = 1$. Якщо $r \in I \cap J$, то тоді $r = r \cdot 1 = r(\alpha + \beta) = r\alpha + r\beta = \alpha r + r\beta$. Ця рівність каже, що $r \in IJ$. Отже, $IJ \supset I \cap J$. ■

3.9 Суміжні класи кілець та факторкільце

Маємо $\langle R, +, \cdot \rangle$, $\langle S, \oplus, \odot \rangle$ – кільця та $f\colon R \to S$ – гомоморфізм. Установимо відношення еквівалентності:
$r_1 \sim r_2 \iff f(r_1) = f(r_2)$.
Окремо пропишемо праву частину еквівалентних чином:
$f(r_1 - r_2) = 0_S \iff r_1 - r_2 \in \ker f$.
Таким чином, ми отримали $r_1 \sim r_2 \iff r_1 - r_2 \in \ker f$.
Але $\ker f$ – це один із ідеалів R. Насправді, ми можемо ці міркування повторити для кожного ідеалу.

Нехай I – ідеал R, встановимо схоже відношення еквівалентності:
$r_1 \sim r_2 \iff r_1 - r_2 \in I$.
Вправа: довести, що це дійсно відношення еквівалентності.
Після цього ми можемо розбити R на класи еквівалентності.

Definition 3.9.1 Суміжним класом r за ідеалом I назвемо клас еквівалентності

$$r + I \overset{\text{def.}}{=} [r]$$

Proposition 3.9.2 $r + I = \{r + i \mid i \in I\}$.
Тому ми зробили відповідне позначення суміжного класа.

Фактормножина $R/_{\sim} \overset{\text{позн.}}{=} R/_I$ буде містити всі суміжні класи.

Цього разу не виникне проблем із діленням на ліві та праві суміжні класи, як це було з групами. Чому ми саме працюємо з ідеалами, а не підгрупами, мотивація краще описує додатковий розділ про кільця в кінці.

Theorem 3.9.3 Задано $\langle R, +, \cdot\rangle$ – кільце та I – ідеал R. На множині $R/_I$ визначимо операцію $+, \cdot$ таким чином:
$(a + I) + (b + I) \overset{\text{def.}}{=} (a + b) + I$.
$(a + I) \cdot (b + I) \overset{\text{def.}}{=} (a \cdot b) + I$.
Тоді структура $\langle R/_I, +, \cdot\rangle$ формує кільце.

Спочатку прокоментую наступну лему:

Lemma 3.9.4 Операції $+, \cdot$ на множині $R/_I$ визначені коректно, тобто якщо $a_1 + I = a_2 + I$ та $b_1 + I = b_2 + I$, то звідси
$(a_1 + b_1) + I = (a_2 + b_2) + I$;
$(a_1 \cdot b_1) + I = (a_2 \cdot b_2) + I$.

Насправді, операція $+$ уже визначена коректно, якщо розглянути $R/_I$ як групу $\langle R/_I, +\rangle$ – це вже утворює абелеву факторгрупу (у нас $I \triangleleft R$ як групи). Залишилося довести коректність множення. А в теоремі залишиться тільки довести останні два аксіоми (що неважко). Тому я залишу лише доведення леми.

Proof.
$a_1b_1 - a_2b_2 = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2 = b_1(a_1 - a_2) + a_2(b_1 - b_2)$.
Оскільки $a_1 + I = a_2 + I$, то звідси маємо $a_1 - a_2 \in I$.
Оскільки $b_1 + I = b_2 + I$, то звідси маємо $b_1 - b_2 \in I$.
Отже, звідси $a_1b_1 - a_2b_2 \in I \implies (a_1 \cdot b_1) + I = (a_2 \cdot b_2) + I$. ■

Definition 3.9.5 Кільце $\langle R/_I, +, \cdot\rangle$ називають **факторкільцем** кільця $\langle R, +, \cdot\rangle$ за ідеалом I, де операції $+, \cdot$ визначені:

$$(a_1 + b_1) + I = (a_2 + b_2) + I;$$
$$(a_1 \cdot b_1) + I = (a_2 \cdot b_2) + I.$$

Remark 3.9.6 Нулем факторкільця буде $0 + I = I$.
Якщо додати умову, що $\langle R, +, \cdot\rangle$ – кільце з одиницею, то $\langle R/_I, +, \cdot\rangle$ – також кільце з одиницею, причому ця одиниця дорівнює $1 + I$.
Якщо додати умову, що $\langle R, +, \cdot\rangle$ – комутативне кільце, то $\langle R/_I, +, \cdot\rangle$ – також комутативне кільце.

Example 3.9.7 Маємо кільце $\langle R, +, \cdot\rangle$, візьмемо ідеал $I = R$. Тоді $a + R = R$ для кожного $a \in R$, при цьому $R/_R = \{R\}$. Ми отримали тривіальне кільце.

Example 3.9.8 Маємо кільце $\langle R, +, \cdot\rangle$, візьмемо ідеал $I = (0)$. Розглянемо гомоморфізм $f\colon R \to R/_{(0)}$ як $a \mapsto a+(0)$. Зрозумілим чином, це сюр'єктивне відображення. Ін'єктивне, тому що $a+(0) = b+(0) \implies a - b \in (0) \implies a = b$. Отже, звідси $R \cong R/_{(0)}$.

Example 3.9.9 Маємо $\langle \mathbb{Z}, +, \cdot\rangle$ – кільце та головний ідеал (n). Тоді $\mathbb{Z}/_{(n)} = \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$.

Example 3.9.10 Маємо $\langle \mathbb{R}[x], +, \cdot\rangle$. Знайдемо $\mathbb{R}[x]/_{(x)}$.
Нехай $f, g \in \mathbb{R}[x]$, тоді звідси
$f \sim g \iff f - g \in (x) \iff f(x) - g(x) = xq(x), q(x) \in \mathbb{R}[x] \iff f(0) = g(0)$.
Таким чином, маємо такі класи еквівалетності:
$\mathcal{P}_\alpha = \{f \in \mathbb{R}[x] : f(0) = \alpha, \alpha \in \mathbb{R}\}$.
А тому $\mathbb{R}[x]/_{(x)} = \{\mathcal{P}_\alpha \mid \alpha \in \mathbb{R}\}$.

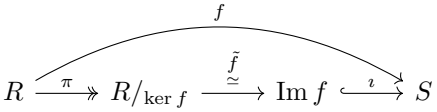
3.10 Основні теореми про ізоморфізми (кілець)

Наша мета розкласти відображення в канонічному вигляді, але цього разу ми маємо справу з гомоморфізмом кілець.

Lemma 3.10.1 Маємо $\langle R, +, \cdot \rangle$ – кільце та I – ідеал. Розглянемо ось таке факторвідображення $\pi \colon R \to R/_I$, тобто $\pi(r) = r + I$. Тоді π – гомоморфізм кілець. Крім того, $\ker \pi = I$.
Відображення π називають **проєкцією** (або **природний гомоморфізм**).
Вправа: довести.

Lemma 3.10.2 Маємо $\langle R, +, \cdot \rangle$ – кільце та $S \subset R$ – підкільце. Розглянемо вкладення $\imath \colon S \to R$. Тоді $\imath$ – гомоморфізм кілець.
Відображення $\imath$ називають **гомоморфізмом вкладень.**
Вправа: довести.

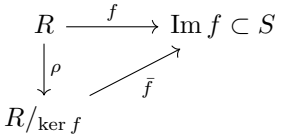
Theorem 3.10.3 Задано R, S – кільця та $f \colon R \to S$ – гомоморфізм. Тоді існує єдиний ізоморфізм $\tilde{f} \colon R/_{\ker f} \to \operatorname{Im} f$, для якого $\imath \circ \tilde{f} \circ \rho = f$.



Тут π – проєкція та $\imath$ – вкладення.
Більш детально, відображення $\tilde{f}(r + \ker f) = f(r)$.
Все аналогічно, як це було з групами. Для гомоморфізма кілець єдине треба довести, що виконується збереження операції множення.

3.10.1 Перша теорема про ізоморфізм

Theorem 3.10.4 Перша теорема про ізоморфізм
Задані R, S – кільця та $f \colon R \to S$ – гомоморфізм. Тоді $R/_{\ker f} \cong \operatorname{Im} f$. Ізоморфізм задається діаграмою нижче.



Тут $\bar{f}(g + \ker f) = f(g)$.
Тут нічого нового не написано, тупо попередня теорема.

3.10.2 Друга теорема про ізоморфізм

Lemma 3.10.5 Задано R – кільце, S – підкільце R та I – ідеал R. Тоді $S \cap I$ – ідеал S.

Proof.
Зауважимо, що $\langle S \cap I, + \rangle$ задає підгрупу $\langle S, + \rangle$ – це вже було неодноразово доведено в теорії груп. Нехай $s \in S$ та $u \in I \cap S$. По-перше, $su, us \in S$ в силу умови підкільця. По-друге, $s \in R, u \in I \implies su, us \in I$. Разом $su, us \in I \cap S$. ■

Lemma 3.10.6 Задано R – кільце, S – підкільце R та I – ідеал R. Тоді I – ідеал $I + S$.

Proof.
Спочатку варто довести, що $\langle S + I, +, \cdot \rangle$ – підкільце. Дійсно, нехай $u, v \in S+I$, тобто $u = a_1 + b_1,\ v = a_2 + b_2$, причому $a_1, a_2 \in S,\ b_1, b_2 \in I$. Тоді
$u - v = (a_1 - a_2) + (b_1 - b_2) = \tilde{a} + \tilde{b}$, де $\tilde{a} \in S,\ \tilde{b} \in I$, звідси $u - v \in S + I$;
$uv = (a_1 + b_1)(a_2 + b_2) = a_1 a_2 + (b_1 a_2 + a_1 b_2 + b_1 b_2) = \tilde{\tilde{a}} + \tilde{\tilde{b}}$, де $\tilde{\tilde{a}} \in S,\ \tilde{\tilde{b}} \in I$, звідси $uv \in S + I$.
Тепер легко довести, що I – ідеал $I + S$. Маючи $I \in I,\ v \in S + I$, буде $uv = u(a + b) = ua + ub \in I$ та $vu = (a + b)u = au + bu \in I$. ■

Theorem 3.10.7 Друга теорема про ізоморфізм
Задано R – кільце, S – підкільце R та I – ідеал R. Тоді
$S/_{S\cap I} \cong (S+I)/_I$.
Вказівка: розглянути $\varphi\colon S \to (S+I)/_I$ таким чином: $s \mapsto s+I$. Далі провести (майже) такі самі доведення, що було раніше.

3.10.3 Третя теорема про ізоморфізм

Lemma 3.10.8 Задано R – кільце та I, J – ідеали R, причому $I \subset J \subset R$. Тоді $J/_I$ – ідеал $R/_I$.

Proof.
Розглянемо відображення $\varphi\colon R/_I \to R/_J$, що задається
$\varphi(a+I) = a+J$.
Якщо $a+I = b+I$, то звідси $a-b \in I \subset J$, а тому $a+J = b+J$, тобто $\varphi(a+I) = \varphi(b+J)$. Значить, відображення коректно визначене.
Зрозуміло, що φ – сюр'єктивний гомоморфізм.
Відомо, що $\ker\varphi$ – ідеал $R/_I$, але
$\ker\varphi = \{a+I \in R/_I \mid \varphi(a+I) = 0+J\} =$
$= \{a+I \in R/_I \mid a+J = 0+J\} = \{a+I \in R/_I \mid a \in J\} = J/_I$. ■

Theorem 3.10.9 Третя теорема про ізоморфізм
Задано R – кільце та I, J – ідеали R, причому $I \subset J \subset R$.
$R/_I/_{J/_I} \cong R/_J$.

Proof.
Із попередньої леми, маючи відображення, ми можемо застосувати першу теорему про ізоморфізм, що миттєво дає цей результат. ■

3.10.4 Четверта теорема про ізоморфізм

Theorem 3.10.10 Четверта теорема про ізоморфізм
Задано R – кільце та I – ідеал. Тоді існує бієкція $F\colon U_1 \to U_2$, де окремо $U_1 = \{S$ – підкільце $R \mid S \supset I\}$, а також $U_2 = \{K$ – підкільце $G/_I\}$.

3.11 Прямі добутки

Definition 3.11.1 Задані $\langle R, +_R, \cdot_R\rangle$ та $\langle S, +_R, \cdot_R\rangle$ – кільця.
(Зовнішнім) прямим добутком двох кілець називають множину

$$R \times S = \{(r,s) \mid r \in R, s \in S\},$$

на якій визначені операції $+, \cdot$ таким чином:

$$(r_1,s_1) + (r_2,s_2) = (r_1 +_R r_2, s_1 +_S s_2)$$
$$(r_1,s_1) \cdot (r_2,s_2) = (r_1 \cdot_R r_2, s_1 \cdot_S s_2)$$

Proposition 3.11.2 За умовами означення, $\langle R\times S, +, \cdot\rangle$ – кільце.
Вправа: довести.

Remark 3.11.3 Можна означення розширити до $R_1 \times R_2 \times \cdots \times R_n$ або навіть до $R_1 \times R_2 \times \ldots$

Remark 3.11.4 Якщо R, S – комутативні та/або кільця з одиницями, то $R \times S$ – також.

Remark 3.11.5 Проте якщо R, S – область цілісності, то не обов'язково взагалі, що $R \times S$ стане областю цілісності. Це питання взагалі особливе для такого випадку.
Зокрема маємо поле $\langle \mathbb{R}, +, \cdot\rangle$ та добуток $\mathbb{R}\times\mathbb{R}$. Добуток не формує область ціліності, бо $(0,1)\cdot(1,0) = (0,0)$ при двох ненульових елементах.
До речі, тим самим множина $\mathbb{C}$ та $\mathbb{R}\times\mathbb{R}$ як кільця відрізняються.

Proposition 3.11.6 Задані $\langle R, +, \cdot\rangle$ та $\langle S, +, \cdot\rangle$ (не буду символьно відрізняти операції, уже все ясно) – кільця. Тоді $(R\times S)^\times = R^\times \times S^\times$.

Proof.
Нехай $(u,v) \in (R \times S)^\times$, тобто $(u,v) \in (R \times S)$, який є оборотним. Тоді існує $(a,b) \in (R \times S)$, для яких $(u,v) \cdot (a,b) = (1,1)$. Тобто $(u \cdot a, v \cdot b) = (1,1)$. Звідси $\begin{cases} u \cdot a = 1 \\ v \cdot b = 1 \end{cases}$. Оскільки $u \in R$ та існує $a \in R$, для якого $u \cdot a = 1$, то тоді $u \in R^\times$. Аналогічно $v \in S^\times$. Отже, $(u,v) \in R^\times \times S^\times$.
Нехай $(u,v) \in R^\times \times S^\times$, тобто $u \in R^\times,\ v \in S^\times$, тобто $u \in R, v \in S$ - оборотні в своїх кільцях. Тож існують $a \in R, b \in S$, для яких $\begin{cases} u \cdot a = 1 \\ v \cdot b = 1 \end{cases}$, тоді звідси вилпиває, що $(u,v)\cdot(a,b) = (u\cdot a, v\cdot b) = (1,1)$, тобто $(u,v) \in (R \times S)$ та є оборотним. Отже, $(u,v) \in (R \times S)^\times$.
Висновок: $(R \times S)^\times = R^\times \times S^\times$. ■

3.12 Китайська теорема про остачі в кільцях

Нехай R – кільце та I, J – ідеали R. Маємо дві проєкції π_I, π_J. Розглянемо відображення $\rho\colon R \to (R/_I) \times (R/_J)$ таким чином:
$\rho(r) = (\pi_I(r), \pi_J(r))$.
Вправа: довести, що ρ – гомоморфізм кілець.
Обчислимо його ядро:
$\ker \rho = \{r \in R \mid \pi_I(r) = 0, \pi_J(r) = 0\} =$
$= \{r \in R \mid r + I = 0 + I, r + J = 0 + J\} = \{r \in R \mid r \in I, r \in J\} = I \cap J$.
За першою теоремою про ізоморфізм, $\operatorname{Im}\rho \cong R/_{I\cap J}$.

Proposition 3.12.1 Задані I, J – ідеали кільця R з 1, причому $I + J = R$. Тоді гомоморфізм ρ – сюр'єктивний.

Proof.
Оскільки $I + J = R = (1)$, то звідси існують $\alpha \in I, \beta \in J$, для яких $\alpha + \beta = 1$. Маємо $a + I \in R/_I, b + J \in R/_J$. Знайдемо такий елемент $r \in R$, що $\rho(r) = (a + I, b + J)$.
Оберемо $r = b\alpha + a\beta$.
$\pi_I(r) = r + I = (b\alpha + a\beta) + I = a\beta + I$, тому що $b\alpha \in I$.
$a\beta + I = a(1 - \alpha) + I = a - a\alpha + I = a + i$, тому що $a\alpha \in I$.
Таким чином, $\pi_I(r) = a + I$. Аналогічно $\pi_J(r) = b + J$. ■

Corollary 3.12.2 Якщо $I + J = R$, то звідси $R/_{I\cap J} \cong (R/_I) \times (R/_J)$.

Theorem 3.12.3 Китайська теорема про остачі
Задано R – комутативне кільце з 1 та I, J – ідеали, причому $I + J = R$. Тоді $R/_{IJ} \cong (R/_I) \times (R/_J)$.
Ізоморфізм $\rho\colon R/_{IJ} \to (R/_I) \times (R/_J)$ задається таким чином:
$\rho(r + IJ) = (a + I, b + J)$, де $r = \beta a + \alpha b$.

Example 3.12.4 Китайська теорема про остачі з теорії чисел
Розглянемо кільце $\mathbb{Z}$ та ідеали $I = m\mathbb{Z},\ J = n\mathbb{Z}$, причому $\gcd(m,n) = 1$. Уже відомо, що $IJ = (mn)\mathbb{Z}$, а за китайською теоремою про остачі,
$\mathbb{Z}/_{mn\mathbb{Z}} \cong (\mathbb{Z}/_{m\mathbb{Z}}) \times (\mathbb{Z}/_{n\mathbb{Z}})$.

Ще раз, маємо m, n – взаємно прості. Оберемо довільні $a_1, a_2 \in \mathbb{Z}$, отримаємо $\overline{a}_1 \in \mathbb{Z}/_{m\mathbb{Z}}, \overline{a}_2 \in \mathbb{Z}/_{n\mathbb{Z}}$. Звідси випливає, що існує $\overline{x} \in \mathbb{Z}/_{mn\mathbb{Z}}$, для якого $\rho(\overline{x}) = (\overline{a}_1, \overline{a}_2)$. Ця рівність означає, що $(\overline{x} + \mathbb{Z}/_{m\mathbb{Z}}, \overline{y} + \mathbb{Z}/_{n\mathbb{Z}}) = (\overline{a}_1, \overline{a}_2)$. Звідси отримаємо $\overline{x - a_1} \in \mathbb{Z}/_{n\mathbb{Z}}$ та $\overline{x - a_2} \in \mathbb{Z}/_{m\mathbb{Z}}$. Більш розгорнуто отримаємо:
$$\begin{cases} x \equiv a_1 \pmod m \\ x \equiv a_2 \pmod n \end{cases}.$$
Розв'язок є, а в силу ізоморфності, такий розв'язок єдиний за $\pmod{mn}$.
Також $x = \alpha_2 a_1 + \alpha_1 a_2$, де відомо, що $\alpha_1 + \alpha_2 = 1$ (за теоремою). Знаючи, що $\alpha_1 \in m\mathbb{Z},\ \alpha_2 \in n\mathbb{Z}$, отримаємо $mu + nv = 1$. Тобто маємо умови $\begin{cases} nv \equiv 1 \pmod m \\ mu \equiv 1 \pmod n \end{cases}$ на розв'язок $x = nva_1 + mua_2$.
Отримали ту саму китайську теорему про остачі.

Corollary 3.12.5 Задані числа $n_1, \dots, n_k > 1$ – попарно взаємно прості числа. Тоді $\mathbb{Z}/_N \cong (\mathbb{Z}/_{n_1\mathbb{Z}}) \times \cdots \times (\mathbb{Z}/_{n_k\mathbb{Z}})$, де $N = n_1 \dots n_k$.
Більш того, якщо $N = p_1^{\alpha_1} \dots p_q^{\alpha_q}$, то $\mathbb{Z}/_N \cong (\mathbb{Z}/_{p_1^{\alpha_1}\mathbb{Z}}) \times \cdots \times (\mathbb{Z}/_{p_q^{\alpha_q}\mathbb{Z}})$.

Знову повернімося до теорії чисел. Виявляється, що по-інакшому можна довести мультиплікативність функції Ейлера.

Proposition 3.12.6 Функція φ – мультиплікативна.

Proof.
$\varphi(1) = 1$ – так і залишається.
Уже знаємо, що $\varphi(n)$ – це кількість оборотних елементів в $\mathbb{Z}/_{n\mathbb{Z}}$. Значить, $\varphi(n) = \text{card}((\mathbb{Z}/_{n\mathbb{Z}})^\times)$. За китайською теоремою про остачі, маємо $\mathbb{Z}/_{(ab)\mathbb{Z}} \cong (\mathbb{Z}/_{a\mathbb{Z}}) \times (\mathbb{Z}/_{b\mathbb{Z}})$. Але звідси $(\mathbb{Z}/_{(ab)\mathbb{Z}})^\times \cong (\mathbb{Z}/_{a\mathbb{Z}})^\times \times (\mathbb{Z}/_{b\mathbb{Z}})^\times$.
$\varphi(ab) = \text{card}((\mathbb{Z}/_{(ab)\mathbb{Z}})^\times) = \text{card}((\mathbb{Z}/_{a\mathbb{Z}})^\times)\,\text{card}((\mathbb{Z}/_{b\mathbb{Z}})^\times) = \varphi(a)\varphi(b)$. ■

3.13 Прості та максимальні ідеали

Definition 3.13.1 Задано $\langle R, +, \cdot\rangle$ – комутативне кільце з 1 та I – ідеал.
Ідеал I називається **простим**, якщо

$$\forall a, b \in R : (ab \in I) \implies (a \in I) \vee (b \in I)$$

Definition 3.13.2 Задано $\langle R, +, \cdot\rangle$ - комутативне кільце з 1 та $I \neq R$ - ідеал.
Він називається **максимальним**, якщо більше не знайдеться якийсь інший нетривіальний ідеал I^*, для якого

$$I \subsetneq I^*$$

Theorem 3.13.3 Задано $\langle R, +, \cdot\rangle$ – комутативне кільце з 1 та I – ідеал.
I – простий ідеал $\iff$ $R/_I$ – область цілісності.

Proof.
$\boxed{\Rightarrow}$ Дано: I – простий ідеал. Попередньо ми знаємо, що $R/_I$ кільце, яке ще й комутативне з одиницею (бо R комутативне кільце з 1).
Нехай $(a + I)(b + I) = 0 + I$, тобто $ab + I = 0 + I$, а це означає, що $ab \in I$. Оскільки I – простий ідеал, то $a \in I$ і тоді $a + I = 0$, або $b \in I$ і тоді $b + I = 0$.

$\boxed{\Leftarrow}$ Дано: $R/_I$ – область цілісності. Нехай $a, b \in R$ так, що $ab \in I$. Тоді звідси $ab + I = 0 + I$. Або інакше, $(a + I)(b + I) = 0 + I$. Оскільки $R/_I$ є областю цілісності, то звідси $a + I = 0 + I$ або $b + I = 0 + I$, тобто $a \in I$ або $b \in I$. ■

Remark 3.13.4 Деякі автори вимагають в означенні простого ідеала, щоб $I \neq R$. Якщо це вимагати, то в теоремі вище в сторону $\boxed{\Leftarrow}$ треба довести окремо, що $I \neq R$. Але це дійсно так, адже якби $I = R$, то звідси $R/_I = \{0 + R\}$, що неправда в силу того, що $R/_I$ - область цілісності.

Theorem 3.13.5 Задано $\langle R, +, \cdot\rangle$ – комутативне кільце з 1 та I – ідеал.
I – максимальний ідеал $\iff$ $R/_I$ – поле.

Proof.
$\boxed{\Rightarrow}$ Дано: I – максимальний ідеал. Тоді оскільки $I \neq R$, то звідси $R/_I$ уже нетривіальне кільце.
!Припустимо, що $R/_I$ не буде полем, тоді існує $\bar{J}$ – ідеал $R/_I$ такий, що $(0) \subsetneq \bar{J} \subsetneq (1)$. За четвертою теоремою про ізоморфізм, йому ставиться в відповідність ідеал $I \subsetneq J \subsetneq R$. Суперечність!

$\boxed{\Leftarrow}$ Дано: $R/_I$ – поле, а тому нетривіальне кільце. Це означає, що $I \neq R$.
!Припустимо, що існує J – ідеал R, для якого $I \subsetneq J \subsetneq R$. Тоді $J/_I$ – ідеал $R/_I$, причому за четвертою теоремою про ізоморфізм, $(0) \subsetneq J/_I \subsetneq (1)$. Ми знайшли нетривіальний ідеал, а тому $R/_I$ не може бути полем – суперечність! ■

Proposition 3.13.6 Задано $\langle R, +, \cdot\rangle$ - комутативне кільце з 1 та I – максимальний ідеал. Тоді I – простий ідеал.
Випливає з того факту, що будь-яке поле – область цілісності.

Example 3.13.7 Розглянемо кілька прикладів:
1. $\langle \mathbb{Z}, +, \cdot \rangle$, яка взагалі є областю головних ідеалів. Тут $n\mathbb{Z}$ - максимальний $\iff$ n - просте число.
Зокрема $n\mathbb{Z}$ - простий ідеал $\iff$ n - просте число.
Тобто $11\mathbb{Z}$ - максимальний, а от $6\mathbb{Z}$ - ні, тому що $6\mathbb{Z} \subset 2\mathbb{Z}$.

2. $\langle \mathbb{R}[x], +, \cdot \rangle$, яка взагалі є областю головних ідеалів. Тут $(p(x))$ - максимальний тоді й тільки тоді, коли $p(x)$ не можна розкласти в добуток многочленів ненульового степеня.
Тобто $(x^2 + x + 1)$ - максимальний, а от $(x^2 - 1)$ - ні, тому що $(x^2 - 1) \subset (x - 1)$.
Важливе зауваження на прикладі: $(2x^2 + 2x + 2) = (x^2 + x + 1)$, тобто для запису максимального ідеалу можна взяти многочлен з одиничним старшим коефіцієнтом.

Example 3.13.8 $\mathbb{Z}/_{p\mathbb{Z}}$, а також $\mathbb{R}[x]/_{(x-a)}, \mathbb{R}[x]/_{\substack{(ax^2+bx+c) \\ D<0}}$ - всі вони поля.

3.14 Найбільший спільний дільник

Definition 3.14.1 Задано $\langle R, +, \cdot \rangle$ – комутативне кільце з 1 та $a, b \in R$.
Елемент b **ділить** a, якщо

$$\exists c \in R : a = bc$$

По суті кажучи, це теж саме, що $a \in (b)$.
Позначення: $b \mid a$.

Definition 3.14.2 Задано $\langle R, +, \cdot \rangle$ – область цілісності та $a, b \in R$.
Елемент $d \in R$ назвемо **найбільшим спільним дільником** a, b, якщо

$$d \mid a, d \mid b \text{ (тобто } d - \text{ спільний дільник } a, b)$$
$$d' \text{ - інший спільний дільник } a, b \implies d' \mid d$$

Позначення: $d = \gcd(a, b)$.

Remark 3.14.3 В області цілісності $\gcd(a, b)$ не завжди існує.
До прикладу $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$. Зауважимо, що 2 та $1 + \sqrt{-3}$ - вони спільні дільники чисел $4, 2 + 2\sqrt{-3}$. Але між цими двома числами нема найбільшого.
!Припустимо, що $\gcd(4, 2 + 2\sqrt{-3}) = g$. Важливо зауважити:
$g \neq 2$ або $g \neq 1 + \sqrt{-3}$. Бо в першому випадку $1 + \sqrt{-3} \mid 2$ як два спільних дільника, але насправді, $1 + \sqrt{-3} \nmid 2$. Аналогічно другий.
$g \neq 4$ або $g \neq 2 + 2\sqrt{-3}$. Бо в першому випадку $4 \mid 2 + 2\sqrt{-3}$, але насправді, $4 \nmid 2 + 2\sqrt{-3}$. Аналогічно другий.
Ми розглянемо функцію $N(x + y\sqrt{-3}) = x^2 + 3y^2$ (вона не задає евклідовість). Можна легко показати, що $N(ab) = N(a)N(b)$. А як наслідок, $a \mid b \implies N(a) \mid N(b)$.
У цьому випадку $2 \mid g \mid 4 \implies N(2) \mid N(g) \mid N(4) \implies 4 \mid N(g) \mid 16$.
Враховуючи результати вище, ми отримаємо $N(g) = 8$.
Оскільки $g \mid 4$, то звідси $4 = gu \implies N(u) = 2 = x^2 + 3y^2$. Дана рівність в цілих числах неможлива - суперечність!
Отже, $\nexists \gcd(4, +2\sqrt{-3})$.

Remark 3.14.4 Навіть якщо $\gcd(a, b)$ існує, то його не завжди можна записати в вигляді лінійної комбінації a, b.
Зокрема в кільці $\langle \mathbb{Z}[x], +, \cdot \rangle$ у нас $\gcd(2, x) = 1$. Проте не існують такі $f, g \in \mathbb{Z}[x]$, щоб $f \cdot 2 + g \cdot x = 1$.

Proposition 3.14.5 Задано R – область головних ідеалів (!), нехай $a, b \in R$. Тоді існує $\gcd(a, b) = d$.
На мові ідеалів виконано $(a, b) = (d)$.

Proof.
Маємо ідеал (a, b) (те, що він ідеал – довести неважко). Оскільки R - область головних ідеалів, то має знайтись елемент $d \in R$, для якого $(d) = (a, b)$. А тепер доведемо, що d – дійсно НСД елементів a, b.
Ясно, що $(a) \subset (a, b) = (d)$, тоді звідси $a \in (d)$, тобто $d \mid a$.
Аналогічно $(b) \subset (a, b) = (d)$, тоді звідси $b \in (d)$, тобто $d \mid b$.
Отже, d - спільний дільник. Переконаємось, що – найбільший.

Припустимо, що d' - будь-який інший спільний дільник, тобто $d' \mid a$, $d' \mid b$. Треба довести, що $d' \mid d$. А це теж саме, що довести, що $d \in (d')$.
Оскільки $d \in (a,b)$, то звідси $d = xa + yb = xq'd' + yr'd' = (xq + yr)d'$, тобто маємо $d \in (d')$. Отже, $d' \mid d$, причому для будь-якого спільного дільника d'. А тому d буде найбільшим спільним дільником. ■

Corollary 3.14.6 Якщо раптом $\gcd(a,b) = 1$, то тоді $(a,b) = R$.

Definition 3.14.7 Задано $\langle R, +, \cdot \rangle$ - область цілісності та $x \in R$.
Елемент $y \in R$ назвемо **асоційованим** з елементом x, якщо

$$y = x \cdot u, u \in R^\times$$

Proposition 3.14.8 "Єдиність"
Задано $\langle R, +, \cdot \rangle$ - область цілісності та $d = \gcd(a,b)$. Тоді будь-який інший $d' = \gcd(a,b)$ буде асоційовним з d.

Proof.
Маємо d, d' - два НСД. Тоді за означенням, $d' \mid d$ та $d \mid d'$, тобто
$d = d' \cdot u$ та $d' = d \cdot v$. Тоді
$d = d \cdot u \cdot v \implies d(1 - uv) = 0$.
За умовою, $d \neq 0$, а також не забуваймо, що ми працюємо в області цілісноті. Тому для рівності треба вимагати, щоб $1 - uv = 0 \implies uv = 1$.
Таким чином, ми довели, що u - оборотний елемент, а тому $u \in R^\times$.
Отже, d - асоційований з d', тому що $d = d' \cdot u$, де $u \in R^\times$. ■

Example 3.14.9 Розглянемо три приклади:
1. Для області головних ідеалів $\mathbb{Z}$ ми маємо $\mathbb{Z}^\times = \{-1, 1\}$. За попередніми міркуваннями, якщо маємо x_1, x_2 - два якісь НСД, то
$x_1 = x_2$ або $x_1 = -x_2$.
Тобто НСД в цілих числах - єдиний з точністю до знаку.

2. Для області головних ідеалів $k[x]$ ми маємо $(k[x])^\times = k^\times = k \setminus \{0\}$. Знову за попередніми міркуваннями, x_1, x_2 - два якісь НСД - тоді
$x_1 = cx_2$, де $c \in k \setminus \{0\}$.
Тобто НСД в многочленах - єдиний з точністю до ненульової константи.

3. Для гаусових чисел $\mathbb{Z}[i]$ маємо $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$. Тоді якщо x_1, x_2 - два якісь НСД, то
$x_1 = \pm x_2$ або $x_1 = \pm i x_2$.
Тобто НСД гаусових чисел - єдиний з точністю до знаку та уявної одиниці.

Remark 3.14.10 Можна визначити $d = \gcd(x_1, \ldots, x_n)$, тобто НСД для кількох елементів. А всі решта міркувань повністю аналогічні.

3.15 Прості та незвідні елементи

Definition 3.15.1 Задано $\langle R, +, \cdot \rangle$ – область цілісності.
Елемент $p \in R$ називається **простим**, якщо

$$p \mid ab \implies p \mid a \text{ або } p \mid b$$

По суті кажучи, це теж саме, що сказати, що (p) – простий ідеал.

Definition 3.15.2 Задано $\langle R, +, \cdot \rangle$ – область цілісності.
Елемент $q \in R$ називається **незвідним**, якщо

$$q = ab \implies a \in R^\times \text{ або } b \in R^\times$$

Remark 3.15.3 Якщо q – незвідний, то автоматично $q \neq 0$.
Бо якби $q = 0$, то тоді $0 = 0 \cdot 0$, але жодний з цих елементів не є оборотним.

Remark 3.15.4 Більшість авторів вимагають додаткову умову: щоб $q \notin R^\times$, хоча це не принципово. Зокрема в $\mathbb{Z}$ маємо $1 = ab$, тоді звідси $a = \pm 1, b = \pm 1$, тобто звідси $a, b \in \mathbb{Z}^\times$. Число 1 – незвідне, хоча $1 \in \mathbb{Z}^\times$.

Як і решта означень, хочеться переписати мовою головних ідеалів. Маємо таку лему:

Lemma 3.15.5 Задано $\langle R, +, \cdot \rangle$ - область цілісності. Тоді
1. $r_1 = r_2 a$ для деякого $a \in R \iff (r_1) \subset (r_2)$;
2. $r_1 = r_2 a$ для деякого $a \in R^\times \iff (r_1) = (r_2)$.
Вправа: довести.

Таким чином, означення 'q - незвідний' перепишеться таким чином:

$$q = ab \implies (q) = (b) \text{ або } (q) = (a)$$

Proposition 3.15.6 Задано $\langle R, +, \cdot \rangle$ – область цілісності та $p \in R$ – простий. Тоді p – незвідний.

Proof.
Нехай $p = ab$, із цього випливає $p \mid ab$. Оскільки p – простий, то тоді $p \mid a$ або $p \mid b$.
Якщо $p \mid a$, то тоді $a = qp$. Підставимо в найперше рівняння – отримаємо $p = qbp \implies qb = 1$. А це означає, що $b \in R^\times$.
Якщо $p \mid b$, то аналогічно доведемо, що $a \in R^\times$.
Разом отримаємо, що p – незвідний. ■

Remark 3.15.7 Якщо p – незвідний, то в області цілісності $\langle R, +, \cdot \rangle$ не завжди з цього випливає, що p – простий.

Example 3.15.8 Маємо $R = \left(x^2, y^2, xy\right) \subset \mathbb{Q}[x, y]$. Одразу зауважу, що $R^\times = \mathbb{Q}^\times$ - тобто многочлени вигляді константи.
Многочлен xy - незвідний.
Припустимо, що xy - звідний, тобто $xy = f(x, y)g(x, y)$, де многочлени $f, g \notin R^\times$. $\deg(xy) = 2$. А тому звідси $\deg f(x, y) = \deg g(x, y) = 1$. Але суперечність, бо вони, $f, g \in \langle x^2, y^2, xy \rangle$.
Але многочлен xy - не простий, тому що $xy \mid x^2y^2$, але $xy \nmid x^2$ та $xy \nmid y^2$. Останні два дуже легко показуються.

Proposition 3.15.9 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів (!) та $\in R$ – невіздний. Тоді – простий.

Proof.
Нехай r – незвідний. Припустимо, що $r \mid ab$. Якщо $r \mid a$, то кінець доведення.
Тож нехай $r \nmid a$, тобто треба показати, що $r \mid b$.
$r \nmid a \implies \gcd(r, a) = 1$.
!Припустимо, що $\gcd(r, a) = d$, тобто $d \mid r, d \mid a$ або $r = dx, a = dy$.
Оскільки r - незвідний, то звідси два випадки:
$x \in R^\times$, тоді $d = rx^{-1} \implies a = rx^{-1}y \implies r \mid a$. Суперечність!
$d \in R^\times$, тоді d буде асоційовним з 1, а НСД однаковий з точністю до асоційовності. Отже, все одно прийдемо до $\gcd(r, a) = 1$.
Тоді за одним наслідком, $(r, a) = R$.
Тоді $(rb, ab) = (b)$ - в принципі, неважко показати.
Але оскільки $r \mid ab$, то тоді $(rb, ab) = (b) \subset (r)$ - теж відносно неважко показати. Таким чином, $b \in (r)$, а значить, $r \mid b$. ■

3.16 Евклідова область

Definition 3.16.1 Задано $\langle R, +, \cdot \rangle$ – область цілісності.
Вона називається **евклідовою областю**, якщо

$$\exists \lambda \colon R \setminus \{0\} \to \{1, 2, 3, \dots\},$$

яка називається **евклідовою нормою**, для якої виконується ділення з остачею, тобто

$$\forall a, b \in R, a \neq 0 : \exists q, r \in R : b = qa + r$$
$$\lambda(r) < \lambda(a) \text{ або } r = 0$$

Example 3.16.2 Зокрема маємо:
$\langle \mathbb{Z}, +, \cdot \rangle$ – евклідова область, якщо взяти $\lambda(n) = |n|$;
$\langle k[x], +, \cdot \rangle$ – евклідова область, якщо взяти $\lambda(f) = \deg f$.

Example 3.16.3 Розглянемо кільце гаусових чисел $\langle \mathbb{Z}[i], +, \cdot \rangle$, де
$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. Це область цілісноті, неважко показати.
Задамо норму $\lambda(m + in) = m^2 + n^2$ та покажемо, що утвориться евклідова область цілісності.
Маємо $a, b \in \mathbb{Z}[i]$, де $b \neq 0$.
$a = m_1 + in_1$
$b = m_2 + in_2$
$$\frac{a}{b} = \frac{m_1 + in_1}{m_2 + in_2} = \frac{m_1 m_2 + n_1 n_2}{m_2^2 + n_2^2} - i\frac{m_1 n_2 - m_2 n_1}{m_2^2 + n_2^2}.$$
Можемо поділити в кожному дробі два числа з остачею:
$m_1 m_2 + n_1 n_2 = q_1(m_2^2 + n_2^2) + r_1$
$m_1 n_2 - m_2 n_1 = q_2(m_2^2 + n_2^2) + r_2$
Причому $-\frac{1}{2}(m_2^2 + n_2^2) < r_1, r_2 \leq \frac{1}{2}(m_2^2 + n_2^2)$. Тоді
$$\frac{a}{b} = q_1 + \frac{r_1}{m_2^2 + n_2^2} - i\left(q_2 + \frac{r_2}{m_2^2 + n_2^2}\right) = (q_1 - iq_2) + \frac{1}{\lambda(b)}(r_1 - ir_2).$$
Звідси $a = b(q_1 - iq_2) + \frac{b}{\lambda(b)}(r_1 - ir_2) = bq + r$.
Зазначимо, що $q = q_1 - iq_2 \in \mathbb{Z}[i]$, а також $r = \frac{b}{\lambda(b)}(r_1 - ir_2) \in \mathbb{Z}[i]$.
Залишилось довести, що $\lambda(r) < \lambda(b)$. Дійсно,
$$r = \frac{1}{\lambda(b}(m_2 + in_2)(r_1 - ir_2) = \frac{1}{\lambda(b)}(m_2 r_1 + n_2 r_2 + i(n_2 r_1 - m_2 r_2))$$
$$\lambda(r) = \frac{1}{\lambda^2(b)}((m_2 r_1 + n_2 r_2)^2 + (n_2 r_1 - m_2 r_2)^2) =$$
$$= \frac{1}{\lambda^2(b)}(m_2^2(r_1^2 + r_2^2) + n_2^2(r_1^2 + r_2^2)) = \frac{1}{\lambda^2(b)}(r_1^2 + r_2^2)\lambda(b) \leq$$
$$\leq \frac{1}{\lambda^2(b)}\left(\frac{1}{4}\lambda^2(b) + \frac{1}{4}\lambda^2(b)\right)\lambda(b) = \frac{1}{2}\lambda(b) < \lambda(b).$$

Example 3.16.4 Будь-яке поле $\langle F, +, \cdot \rangle$ буде евклідовою областю, якщо визначити норму $\lambda(a) = 1$ при $a \neq 0$. Тоді $\forall a, b \in F$, причому $a \neq 0$, маємо $b = b \cdot (b^{-1} \cdot a) + 0$.

Theorem 3.16.5 Задано $\langle R, +, \cdot \rangle$ - евклідова область. Тоді $\langle R, +, \cdot \rangle$ – область головних ідеалів.

Proof.
За означенням евклідової області, R - область цілісності.
Залишилось довести, що кожний ідеал має структуру головного ідеалу.
!Припустимо, що J - деякий ідеал, але не головний. Для суперечності ми доведемо, що $J = (x)$, де $x \in J$, такий, що $\lambda(x) = \min\limits_{y \in J \setminus \{0\}} \lambda(y)$.
Нехай $z \in (x)$, тоді звідси $z = xr$, де $x \in J$ та $r \in R$. Тоді автоматично $z \in J$ за визначенням ідеала. Отже, $(x) \subset J$.
Нехай $z \in J$. Застосуємо узагальнений алгоритм Евкліда для елементів x, z - маємо:
$z = xq + r$, причому $r = 0$ або $\lambda(r) < \lambda(x)$. Виразимо остачу - отримаємо
$r = z - xq \in J$ за визначенням ідеала. Тоді звідси $\lambda(r) \geq \lambda(x)$ за визначенням $\lambda(x)$. І тому єдиний можливий варіант для остачі - це стати $r = 0$.
Отже, $z = xq \implies z \in (x)$, тобто звідси $J \subset (x)$.
Нарешті, довели $J = (x)$. Суперечність! ■

Example 3.16.6 Зокрема оскільки $\mathbb{Z}, k[x], \mathbb{Z}[i]$ - евклідові області, то вони ж - області головних ідеалів.

Example 3.16.7 Ось тут $\mathbb{Z}[x]$ не буде областю головних ідеалів, тому що для ідеалу $(2, x)$ не можна знайти головний ідеал. А значить, $\mathbb{Z}[x]$ – не евклідова область.

3.17 Область однозначної факторизації

Lemma 3.17.1 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів. Розглянемо ланцюг ідеалів $I_1 \subset I_2 \subset \ldots$. Тоді знайдеться $m \in \mathbb{N}$, для якого $I_m = I_{m+1} = \ldots$

Proof.
Розглянемо множину $I = \bigcup\limits_{j=1}^{\infty} I_j$, яка є ідеалом – це зрозуміло. Оскільки R – область головних ідеалів, то звідси $I = (s)$. А тому звідси $\exists m > 0 : s \in I_m$. Внаслідок цього отримаємо:
$I = (s) \subset I_m \subset I_{m+1} \subset \cdots \subset I$. Звідси $I_m = I_{m+1} = \ldots$ ■

Lemma 3.17.2 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів. Розглянемо $a \in R$ такий, що $a \neq 0$ та $a \notin R^{\times}$. Тоді a ділиться на деякий незвідний елемент.

Proof.
Якщо a вже незвідний, то нема про що говорити (тому що $a \mid a$).
Тому нехай a – звідний, тобто $a = a_1 b_1$, де $a_1, b_1 \notin R^{\times}$. Із цієї рівності випливає, що $(a) \subset (a_1)$. Якщо a_1 – незвідний, то тоді $a_1 \mid a$ - закінчили.
Інакше $a_1 = a_2 b_2$, $a_2, b_2 \notin R^{\times}$. Із цієї рівності випливає, що $(a_1) \subset (a_2)$. Якщо a_2 – незвідний, то тоді $a_2 \mid a_1 \mid a$ закінчили.
$\vdots$
Продовжуючи, отримаємо ланцюг $(a) \subset (a_1) \subset (a_2) \subset \ldots$ За попередньою лемою, $(a_k) = (a_{k+1}) = \ldots$ для деякого $k \in \mathbb{N}$. Значить, $a_k = a_{k+1} b_{k+1}$, де обов'язково $b_{k+1} \in R^{\times}$. А тому a_k – останній незвідний, для якого $a_k \mid a$. ■

Lemma 3.17.3 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів. Розглянемо $a \in R$ такий, що $a \neq 0$ та $a \notin R^{\times}$. Тоді a можна розкласти на добуток незвідних елементів, тобто
$a = p_1 \ldots p_r$, де $p_1, \ldots, p_r$ – всі незвідні.

Proof.
Якщо a - незвідний, то нема про що говорити ($a = a$).
Інакше існує незвідний елемент p_1, для якого $p_1 \mid a$. Тоді $a = p_1 q_1$. Зауважимо, що $(a) \subset (q_1)$. Якщо $q_1 \in R^{\times}$, то тоді маємо асоційований незвідний елемент $p_1^* = p_1 q_1$, звідси $a = p_1^*$ – закінчили.
Інакше для числа q_1 знайдеться якийсь незвідний елемент p_2, для якого $p_2 \mid q_1$, тоді $q_1 = p_2 q_2$. Зауважимо, що $(q_1) \subset (q_2)$. Якщо $q_2 \in R^{\times}$, то тоді маємо асоційований незвідний елемент $p_2^* = p_2 q_2$, звідси $a = p_1 \cdot p_2^*$ – закінчили.
$\vdots$
Продовжуючи, отримаємо ланцюг $(a) \subset (q_1) \subset (q_2) \subset \ldots$ За позапопередньою лемою, $(q_m) = (q_{m+1}) = \ldots$ для деякого $m \in \mathbb{N}$. Значить, $q_m = q_{m+1} p_{m+1}$, де обов'язково $p_{m+1} \in R^{\times}$. А тому $q_{m+1} p_{m+1} = p_{m+1}^*$ буде асоційованим незвідним елементом. Звідси випливає, що $a = p_1 p_2 \ldots p_m q_m = p_1 p_2 \ldots p_m p_{m+1}^*$. ■

Lemma 3.17.4 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів. Розглянемо $a \in R$ такий, що $a \neq 0$ та $a \notin R^{\times}$. Ми вже знаємо, що a можна розкласти на добуток незвідних елементів. Тоді цей розклад розписується єдиним чином з точністю до перестановки та асоціативності незвідних елементів.

Proof.
!Припустимо, що існують два різні розклади, тобто
$a = p_1 \ldots p_r$
$a = q_1 \ldots q_s$.
Ми припускаємо, що $r < s$. Маємо $p_1 \mid a$, тобто $p_1 \mid q_1 \ldots q_s$. Але в області головних ідеалів незвідний елемент точно простий. Тому, не втрачаючи загальності, $p_1 \mid q_1$, тобто $q_1 = p_1 u_1$, де $u_1 \in R^{\times}$. Підставимо отримане:
$p_1(p_2 \ldots p_r) = p_1(u_1 q_2 \ldots q_s)$
$p_2 \ldots p_r = u_1 q_2 \ldots q_s$.
Далі все теж саме робиться. Продовжуючи, отримаємо
$1 = u_1 \ldots u_r q_{r+1} \ldots q_s$.
Із цієї рівності випливає, що $q_{r+1}, \ldots, q_s = (u_1 \ldots u_r)^{-1} = u_r^{-1} \ldots u_1^{-1}$. Підставимо в другий розклад: $a = q_1 \ldots q_r u_r^{-1} \ldots u_1^{-1} = p_1^* \ldots p_r^*$. Отримали, що $p_1, \ldots, p_r$ є відповідно асоційованим з $p_1^*, \ldots, p_r^*$ – отримали суперечність! ■

Definition 3.17.5 Задано $\langle R, +, \cdot \rangle$ – область цілісності.
Вона називається **областю однозначної факторизації**, якщо будь-який ненульовий оборотний елемент розкладається на добуток незвідних елементів єдиним чином з точністю до перестановки.

Theorem 3.17.6 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів. Тоді $\langle R, +, \cdot \rangle$ – область однозначної факторизації.

Example 3.17.7 Тоді $\mathbb{Z}, k[x], \mathbb{Z}[i]$ – області однозначної факторизації.

Remark 3.17.8 Не кожна область однозначної факторизації буде областю головних ідеалів. Наприклад, $\mathbb{Z}[x]$.

Теорему про розклад елемента на добуток незвідних елементів можна записати мовою ідеалів:

Theorem 3.17.9 Задано $\langle R, +, \cdot \rangle$ – область головних ідеалів, $(a) \neq (0)$ – власний ідеал. Тоді існують прості ідеали (q_i), для яких $(a) = (q_1) \dots (q_r)$. Даний розклад буде єдиним з точністю до перестановки ідеалів.
Зокрема якщо (a) такий, що a – оборотний, то тоді $(a) = (1)$.

Theorem 3.17.10 Узагальнення розкладу елемента
Задано R - область головних ідеалів. Позначимо P - множина простих елементів, так, що:
- кожен простий елемент в R асоційований з деяким елементом з P;
- жодні два елементи в P не є асоційованими.
Тоді будь-який елемент $r \neq 0 \in R$ можна розкласти єдиним чином як добуток простих елементів. Тобто
$r = u \prod_{p \in P} p^{e_p}$,
де $e_p \in \mathbb{N} \cup \{0\}$; $e_p = 0$ для майже всіх p, також $u \in R^{\times}$.

Фінал

Позначимо:
R – комутативне кільце з одиницею;
ID – область цілісності;
UFD – область однозначної факторизації;
PID – область головних ідеалів;
ED – евклідова область;
F – поле.
Тоді буде справедливе ось таке вкладення:

$$R \supset ID \supset UFD \supset PID \supset ED \supset F$$

Сучасний підхід до означення кілець

Часто коли автори кажуть про кільця, вони вважають автоматично, що там є одиниця. Якщо притримуватися такої філософії, то кілька тверджень можуть змінитися. І зараз про них ми поговоримо. А поки оновимо означення.

Definition. Задано R – деяку множину та дві бінарні операції $+, \cdot$.
Кільцем назвемо трійку $\langle R, +, \cdot \rangle$, для якої виконуються властивості:
I. $\forall a, b \in R : a + b \in R$ – замкненість відносно $+$;
II. $\forall a, b \in R : a \cdot b \in R$ – замкненість відносно $\cdot$;
III. Підпорядкована такими аксіомами:

1) $\forall a, b, c \in R : a + (b + c) = (a + b) + c$ – асоціативність додавання
2) $\forall a, b, c \in R : a + b = b + a$ – комутативність додавання
3) $\exists 0 \in R : a + 0 = a$ – існування нейтрального елементу за додаванням
4) $\forall a \in R : \exists (-a) \in R : a + (-a) = 0$ – існування оберненого елементу за додаванням
5) $\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ – асоціативність множення
6) $\forall a, b, c \in R : (a + b) \cdot c = (a \cdot c) + (b \cdot c)$ та $c \cdot (a + b) = (c \cdot a) + c \cdot b)$ – дистрибутивність множення відносно додавання
7) $\exists 1 \in R : a \cdot 1 = 1 \cdot a = a$

У рамках цього окремого розділу, коли задається кільце, то там вже є одиниця!

Миттєво з цього означення випливає зміна поняття підкільця.

Definition. Задано $\langle R, +, \cdot \rangle$ – кільце та множину $R_1 \subset R$.
Воно називається **підкільцем**, якщо

$$\langle R_1, +, \cdot \rangle \text{ – кільце,}$$

де операцію $+$ ми успадкували з R. Також вимагається $1_R = 1_{R_1}$.

Remark. У R та R_1 уже нулі точно збігаються. Щодо одиниць: якщо припустити, що $1' \in R_1$ – одиниця кільця, то тоді $1 = 1' \cdot 1 = 1'$.

Для визначення підкільця є абсолютно ідентичний критерій, що з теорії груп, просто буде додаткова та схожа умова.

Theorem 3.17.11 Критерій підкільця
Задано $\langle R, +, \cdot \rangle$ – кільце та множину $R_1 \subset R$.

$$R_1 \text{ – підкільце } \iff \begin{cases} \forall a, b \in R_1 : a + b \in R_1 \\ \forall a, b \in R_1 : a \cdot b \in R_1 \\ \forall a \in R_1 : -a \in R_1 \end{cases} \quad \text{та } 0_R, 1_R \in R_1.$$

Вправа: довести.

Corollary 3.17.12 Переписаний критерій

$$R_1 \text{ – підкільце } \iff \begin{cases} \forall a, b \in R_1 : a - b \in R_1 \\ a \cdot b \in R_1 \end{cases} \quad \text{та } 0_R, 1_R \in R_1.$$

Маючи оновлений критерій підкільця, один приклад зміниться.

Example. Маємо $\langle \mathbb{Z}_6, +, \cdot \rangle$ - кільце. Якщо раніше $S = \{\overline{0}, \overline{3}\} \subset \mathbb{Z}_6$ можна сприймати було як підкільце, то в оновлених домовленностях S більше не буде підкільцем. Хоча само по собі кільцем є. А все тому що $1_S = \overline{3}$, коли водночас $1_{\mathbb{Z}_6} = \overline{1}$ – не збігаються одиниці.

Definition. Задано $\langle R, +, \cdot \rangle$ та $\langle S, +, \cdot \rangle$ – кільця.
Гомоморфізмом кілець називають відображення $f \colon R \to S$, де

$$\forall a, b \in R : f(a + b) = f(a) + f(b)$$
$$\forall a, b \in R : f(a \cdot b) = f(a) \cdot f(b)$$
$$f(1_R) = 1_S$$

Example. Якщо раніше можна було задати гомоморфізм $f\colon \mathbb{Z}_n \to \mathbb{Z}$ (і це лише $f(\overline{a}) = 0$), то зараз між цими множинами просто не існує гомоморфізма.

!Припустимо, що оновлений гомоморфізм $f\colon \mathbb{Z}_n \to \mathbb{Z}$ існує. Якщо $n = 1$, то тоді $\mathbb{Z}_1 = \{\overline{0}\}$ – нульове кільце. Значить, $f(\overline{0}) = 0$, а також $f(\overline{0}) = 1$ (тому що в нульововму кільці одиниця та нулі збігаються). Разом $0 = 1$.
Тож далі нехай $n > 1$. Відомо, що $f(\overline{1}) = 1$. Тоді звідси
$f(\underbrace{\overline{1} + \cdots + \overline{1}}_{n \text{ разів}}) = nf(\overline{1}) = n.$
Із іншого боку, $f(\underbrace{\overline{1} + \cdots + \overline{1}}_{n \text{ разів}}) = f(\overline{0}) = 0.$
Разом отримали $n = 0$ – суперечність!

Можна, до речі, це узагальнити, а доведення буде аналогічним.

Proposition. Задані R, S – кільця, причому $\operatorname{char} S = 0$.
Якщо $\operatorname{char} R > 0$, то не існує гомоморфізму кілець $f\colon R \to S$.

Example. Задано $\langle R, +, \cdot\rangle$ – кільце. Розглянемо відображення $\sigma\colon \mathbb{Z} \to R$, що задається таким чином:
$\sigma(n) = \underbrace{1_R + \cdots + 1_R}_{n \text{ разів}},\ n > 0$
$\sigma(n) = -\sigma(n),\ n < 0$
$\sigma(0) = 0.$
Тоді це утворює гомоморфізм кілець. Причому серед всіх гомоморфізмів кілець $\mathbb{Z} \to R$ гомоморфізм σ – єдиний.
При $m, n > 0$ маємо наступне:
$\sigma(n+m) = \underbrace{1_R + \cdots + 1_R}_{n+m \text{ разів}} = \underbrace{1_R + \cdots + 1_R}_{n \text{ разів}} + \underbrace{1_R + \cdots + 1_R}_{m \text{ разів}} = \sigma(n) + \sigma(m).$
$\sigma(nm) = \underbrace{1_R + \cdots + 1_R}_{nm \text{ разів}} = \underbrace{\underbrace{1_R + \cdots + 1_R}_{n \text{ разів}} + \cdots + \underbrace{1_R + \cdots + 1_R}_{n \text{ разів}}}_{m \text{ разів}} =$
$= (\underbrace{1_R + \cdots + 1_R}_{n \text{ разів}})(\underbrace{1_R + \cdots + 1_R}_{m \text{ разів}}) = \sigma(n)\sigma(m).$
$\sigma(1) = 1_R.$
Для всіх інших випадків m, n легко довести.
!Припустимо, що існує інший гомоморфізм $\tau\colon \mathbb{Z} \to R$. Тоді звідси $\tau(1) = 1_R$, а також при $n > 0$ маємо
$\tau(n) = \tau(\underbrace{1 + \cdots + 1}_{n \text{ разів}}) = \underbrace{\tau(1) + \cdots + \tau(1)}_{n \text{ разів}} = \underbrace{1_R + \cdots + 1_R}_{n \text{ разів}} = \sigma(n).$
$\tau(0) = 0_R = \sigma(0).$
$\tau(-n) = -\tau(n) = -\sigma(n) = \sigma(n).$
Тобто довели $\tau \equiv \sigma$ – суперечність!

До властивостей ізоморфізму кілець в цьому випадку додається ще одна властивість:

Proposition. Маємо $f\colon R \to S$ – гомоморфізм кілець. Тоді $a \in R^\times \iff f(a) \in S^\times$.

Proof.
Дійсно, нехай $a \in R^\times$, тобто звідси $a \cdot a^{-1} = 1_R$. Подіявши гомоморфізмом f, отримаємо $f(a) \cdot f(a^{-1}) = 1_S$. Звідси $(f(a))^{-1} = f(a^{-1})$, а також $f(a) \in S^\times$.
Навпаки аналогічно. ■

Означення ідеала не зміниться жодним чином. Але раніше було зауваження: J – ідеал кільця $R \implies J$ – підкільце R. Зараз це вже – неправда.

Example 3.17.13 Зокрема $\langle \mathbb{Z}_6, +, \cdot\rangle$ – кільце та $J = \{\overline{0}, \overline{3}\}$ – ідеал. Воно кільцем само по собі є, але не є підкільцем $\mathbb{Z}_6$ (ми вже це з'ясовували).

У нас змінюється формулювання четвертої теореми про ізоморфізм.

Theorem 3.17.14 Четверта теорема про ізоморфізм
Задано R – кільце та I – ідеал. Тоді існує бієкція $F\colon U_1 \to U_2$, де окремо $U_1 = \{S$ – ідеал $R \mid S \supset I\}$, а також $U_2 = \{K$ – ідеал $G/_I\}$.

Proof.

■

4 Многочлени

По-перше, дивись підрозділ 3.6., щоб згадати про кільце многочленів.
По-друге, уже щось про многочлени обговорювали на лінійній алгебрі, але це було лише в $\mathbb{R}[x]$ та $\mathbb{C}[x]$. Ми тут ще раз це обговоримо, у будь-якому випадку, проте цього разу необхідно зробити певне узагальнення. Зробимо певні означення:

Definition 4.0.1 Маємо $\langle R, +, \cdot \rangle$ – кільце з одиницею. Розглянемо ненульовий многочлен $f \in R[x]$, тобто $f(x) = a_0 + a_1 x + \cdots + a_d x^d$, де $a_d \neq 0$.
Степенем многочлена f назвемо число $\deg f = d$.
Нормованим многочленом назвемо тоді, коли $a_d = 1_R$.

Remark 4.0.2 Якщо $f(x) = 0$, то він не має степені та старшного коефіцієнта.

Proposition 4.0.3 Задано $\langle R, +, \cdot \rangle$ – область цілісності та $f, g \in R[x]$. Тоді $\deg(fg) = \deg f + \deg g$.

Proof.
Позначимо $\deg f = m,\ \deg g = n$. Маємо два многочлени:
$f(x) = a_0 + a_1 x + \cdots + a_m x^m$
$g(x) = b_0 + b_1 x + \cdots + b_n x^n$.
Перемножуючи многочлени, отримаємо:
$f(x)g(x) = a_m b_n x^{m+n} + \cdots + a_0 b_0$.
Зауважимо, що $a_m b_n \neq 0$, просто тому що R – область цілісності за умовою. Таким чином, $\deg(fg) = n + m$. ■

Remark 4.0.4 Область цілісності – принципова умова.
Зокрема на $\mathbb{Z}/_{4\mathbb{Z}}$ розглянемо многочлени $f(x) = 2x + 1$ та $g(x) = 2x$. Тоді отримаємо $f(x)g(x) = 2x$. У цьому випадку $\deg(fg) \neq \deg f + \deg g$.

4.1 Ділення з остачею. Корені многочлена

У нас вже було ділення з остачею в $\mathbb{R}[x]$ та $\mathbb{C}[x]$. Виявляється, що для довільного кільця це теж виконується.

Proposition 4.1.1 Задано $\langle R, +, \cdot \rangle$ – кільце з одиницею. Нехай $f, g \in R[x]$, причому $f \not\equiv 0$. Також нехай старший коефіцієнт f оборотний. Тоді існують такі $q, r \in R[x]$, для яких $g(x) = q(x)f(x) + r(x)$, де $r \equiv 0$ або $\deg r < \deg f$.

Proof.
Якщо $g \equiv 0$ або $\deg g < \deg f$, то тоді оберемо $q \equiv 0$ та $r \equiv g$. Тоді звідси $g(x) = 0 \cdot f(x) + g(x)$.

Тепер нехай $\deg g \geq \deg f$. Позначимо $\deg g = n,\ \deg f = m$.
!Припустимо, що існують f, g, для яких твердження не виконується. Ми можемо обрати многочлен g, де $\deg g$ є настільки малим, наскільки можливо.
$f(x) = a_0 + a_1 x + \cdots + a_m x^m \quad g(x) = b_0 + b_1 x + \cdots + b_n x^n$
У нас $a_m \in R^\times$. Значить, існує елемент $u \in R$, для якого $a_m u = 1$.
Розглянемо ось такий многочлен:
$g_1(x) = g(x) - b_n u f(x) x^{n-m} =$
$= (b_0 + \cdots + b_n x^n) - (b_n u a_0 x^{n-m} + \cdots + b_n u a_m x^n)$.
Зауважимо, що $b_n - b_n u a_m = 0$, тобто x^n зникає. А це означає, що $\deg g_1 < n$ або $g_1 \equiv 0$. Тоді $\deg g_1 < \deg f$ в силу мінімальності $\deg g$, а тому звідси існують многочлени q_1, r_1, для яких $g_1(x) = q_1(x)f(x) + r_1(x)$, причому $r_1 \equiv 0$ або $\deg r_1 < \deg f$. Звідси випливає, що
$g(x) = (q_1(x) + b_n u x^{n-m}) f(x) + r_1(x)$.
Тобто g поділили на f з остачею, де $\deg r_1 < \deg f$ або $r_1 \equiv 0$ – суперечність! Тому що ми підібрали так g, що цього робити не можна. ■

Corollary 4.1.2 Якщо додатково $\langle R, +, \cdot \rangle$ – область цілісності, то ділення з остачею визначається єдиним чином.
Зокрема, як в $\mathbb{R}[x], \mathbb{C}[x]$, ділення з остачею єдине.

Proof.
!Припустимо, що можна двома способами поділити:
$g(x) = q_1(x)f(x) + r_1(x)$;
$g(x) = q_2(x)f(x) + r_2(x)$.
$\deg r_1 < \deg f$ або $r_1 \equiv 0$, також $\deg r_2 < \deg f$ або $r_2 \equiv 0$.
$(q_1(x) - q_2(x))f(x) = r_2(x) - r_1(x)$.
Якщо $q_1 \equiv q_2$, то тоді $r_2 \equiv r_1$, що автоматично суперечить. Тож нехай $q_1 \not\equiv q_2$. Тоді звідси $\deg(q_1 - q_2)f \geq \deg f$ в силу того, що $R[x]$ – область цілісності та $f \not\equiv 0$. Але з іншого боку, $\deg(r_2 - r_1) \leq \max\{\deg r_1, \deg r_2\} < \deg f$. Суперечність! ■

Definition 4.1.3 Задано $\langle R, +, \cdot\rangle$ – кільце з одиницею та $g \in R[x]$.
Елемент $a \in R$ називається **коренем** $g(x)$, якщо

$$g(a) = 0_R$$

Proposition 4.1.4 Задано $\langle R, +, \cdot\rangle$ – кільце з одиницею та $g \in R[x]$.
a – корінь $g(x) \iff (x - a) \mid g(x)$.

Proof.
$\boxed{\Rightarrow}$ Дано: a – корінь g, тобто $g(a) = 0$. Поділимо g на $(x - a)$:
$g(x) = q(x)(x - a) + r(x)$.
Зокрема $\deg r < \deg(x - a) = 1$, а тому звідси $r(x) \equiv R$. Якщо підставити $x = a$, то ми отримаємо $R = 0$. Отже, $q(x) = q(x)(x - a)$.

$\boxed{\Leftarrow}$ Дано: $(x - a) \mid g(x)$, тобто
$g(x) = f(x)(x - a) \implies g(a) = f(a) \cdot 0 = 0$. ■

Theorem 4.1.5 Нехай k – поле. Тоді $k[x]$ – евклідове кільце.

Proof.
По-перше, ясно, що $k[x]$ – область цілісності. А по-друге, ми встановимо евклідову норму $\lambda(f) = \deg f$. А далі можна для кожного $f, g \in k[x]$ застосувати ділення з остачею. Принаймні тому що для $g \not\equiv 0$ старший коефіцієнт завжди оборотний. Якщо $g \equiv 0$, то тоді $0 = 0 \cdot f(x) + 0$. ■

Corollary 4.1.6 $k[x]$ – область головних ідеалів. Як черговий наслідок, $k[x]$ – область однозначної факторизації.

Запишемо ділення з остачею мовою ідеалів.

Corollary 4.1.7 Задано $\langle R, +, \cdot\rangle$ – область цілісності та $f, g \in R[x]$, причому $f \not\equiv 0$. Також нехай старший коефіцієнт f оборотний. Тоді будь-який суміжний клас $R[x]/_{(f(x))}$ має єдиного представника вигляду $r(x) + (f(x))$, де $r(x) = 0$ або $\deg r < \deg f$.

Proof.
Маємо $g(x) + (f(x)) \in R[x]/_{(f(x))}$. Відомо, що існують, причому єдині $q, r \in R[x]$, для яких $g(x) = q(x)f(x) + r(x)$. Тут $r \equiv 0$ або $\deg r < \deg f$.
Тоді $g(x) + (f(x)) = r(x) + (f(x))$.
!Припустимо, що $g(x)+(f(x)) = r_1(x)+(f(x))$, тобто інший представник. Але тоді $g(x) = q_1(x)f(x)+ r_1(x)$. Із єдиності, $q_1 \equiv q, r_1 \equiv r$ – суперечність! ■

Theorem 4.1.8 Задано k – поле та $f \in k[x]$, причому $f \not\equiv 0$. Позначимо $\deg f = d$. Тоді $k[x]/_{(f(x))}$ – векторний простір над полем k, причому $\dim k[x]/_{(f(x))} = d$.

Proof.
Розглянемо відображення $A\colon k^d \to k[x]/_{(f(x))}$ таким чином:
$(a_0, a_1, \ldots, a_{d-1}) \mapsto (a_0 + a_1x + \cdots + a_{d-1}x^{d-1}) + (f(x))$.
Кожному елементу $g(x)+(f(x)) \in k[x]/_{(f(x))}$ ставиться в відповідність єдиний представник формату $r(x) + (f(x))$, де $\deg r < d$. Звідси $r(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$, йому ставиться у відповідність $(a_0, a_1, \ldots, a_{d-1})$, тобто відображення бієктивне.
Те, що відображення – лінійне, неважко довести. ■

Example 4.1.9 Зокрема маємо $\mathbb{Z}/_{5\mathbb{Z}}$ – поле з 5 елементів. Тоді кільце
$(\mathbb{Z}/_{5\mathbb{Z}})[x]/_{(x^3+1)} \cong (\mathbb{Z}/_{5\mathbb{Z}})^3$ – ізоморфність векторних просторів, а тому містить 125 елементів.

4.2 Незвідність многочлена

Proposition 4.2.1 Задано k – поле. Тоді будь-який многочлен $k[x]$ степені 1 – невіздний.

Proof.
Маємо $f(x) = a + bx$. Розпишемо $f(x) = g(x)h(x)$. Оскільки $\deg f = 1$, то звідси $\deg(gh) = 1$, а тому $\deg g + \deg h = 1$. Звідси або $\deg g = 0$ та $\deg h = 1$, або $\deg g = 1$ та $\deg h = 0$. Тобто або $g = c_0 \in (k[x])^\times$, або $h = d_0 \in (k[x])^\times$. ■

Remark 4.2.2 Принципово мати поле. У області цілісності вже не прокатить. Зокрема в $\mathbb{Z}$ маємо многочлен $2x$, що не є незвідним, бо $2, x \notin (\mathbb{Z}[x])^\times$.

Proposition 4.2.3 Задано k – поле. Нехай $f \in k[x]$, причому $\deg f \geq 2$ та має корінь. Тоді f – звідний.

Proof.
Дійсно, нехай x_0 – корінь многочлена. Тоді $f(x) = (x - x_0)g(x)$. Із цього випливає, що $\deg g \geq 1$, а це автоматично означає, що $g \notin (k[x])^\times$. Також ясно, що $x - x_0 \notin (k[x])^\times$. ■

Proposition 4.2.4 Задано k – поле. Нехай $f \in k[x]$, причому $\deg f = 2$ або 3. Тоді f – незвідний $\iff$ f не має коренів.

Proof.
$\boxed{\Rightarrow}$ Дано: f – незвідний. Тоді звідси за попереднім твердженням, f не має коренів.

$\boxed{\Leftarrow}$ Дано: f не має коренів.
!Припустимо, що $f(x) = g(x)h(x)$, де $g, h \notin (k[x])^\times$. Звідси $\deg g + \deg h = 2$ або 3. У першому випадку $\deg g = \deg h = 1$. А в другому випадку або $\deg g = 1$, або $\deg h = 1$. Коли $\deg g = 1$, то звідси $g(x) = (a + bx)$. Тоді
$f(x) = (a + bx)h(x) = (ab^{-1} + x) \cdot b \cdot h(x)$.
Ми для f знайшли корінь $x = -ab^{-1}$ – суперечність! ■

Remark 4.2.5 Маємо $(2x - 1)^2 \in \mathbb{Z}[x]$, який звідний. Водночас в $\mathbb{Z}$ коренів нема. Значить, $\boxed{\Leftarrow}$ не завжди працює в області цілісності.

Remark 4.2.6 Маємо $x^4 - 4 \in \mathbb{Q}[x]$, який звідний, тому що $x^4 - 4 = (x^2 - 2)(x^2 + 2)$. Водночас коренів нема в $\mathbb{Q}$. Значить, умова $\deg f \in \{2, 3\}$ є необхідною.

4.3 Незвідність на $\mathbb{C}[x]$ та $\mathbb{R}[x]$

Theorem 4.3.1 Основна теорема алгебри
Будь-який неконстантний многочлен $f \in \mathbb{C}[x]$ має корінь в $\mathbb{C}$.
Без доведення: теорема доволі важка.

Corollary 4.3.2 $f \in \mathbb{C}[x]$ незвідний $\iff$ $\deg f = 1$.

Proof.
$\boxed{\Rightarrow}$ Ми припустимо краще, що $\deg f \neq 1$. Кілька випадків:
$\deg f > 1$. За основною теоремою алгебри, $f(x) = (x - x_0)g(x)$, де x_0 – корінь. Значить, $\deg g > 0$, а тому ми розклали f на необоротні. Отже, f – звідний.
$\deg f = 0$. Тоді $f(x) = c_0$, причому c_0 – оборотний елемент, а тому не є незвідним.
Тобто f – незвідний $\implies$ $\deg f = 1$.

$\boxed{\Leftarrow}$ **Prp. 4.2.1** ■

Corollary 4.3.3 Будь-який многочлен $f \in \mathbb{C}[x]$, де $d = \deg f$, розкладається на d множників степені 1 з точністю до оборотного елементу.
Зрозуміло.

Тобто якщо $f \in \mathbb{C}[x]$, де $\deg f = d$, то звідси $f(x) = c_0(x - x_1) \dots (x - x_d)$, де x_i – корені.

Proposition 4.3.4 Задано многочлен $f \in \mathbb{R}[x]$. Тоді f – незвідний $\iff$
(i) $\deg f(x) = 1$
(ii) $\deg f(x) = 2$ та для многочлена $f(x) = ax^2 + bx + c$ дискримінант від'ємний.

Proof.
$\boxed{\Rightarrow}$ Спочатку якщо $\deg f(x) = 2$, але дискримінант невід'ємний, то тоді існує хоча б один корніь, а тому є звідним уже.
Якщо $\deg f = 0$, то тоді отримаємо оборотний елемент, що звідний.
Якщо $\deg f > 2$, то тоді треба розглянути f на полі комплексних чисел. Якщо α – якийсь комплексний корінь, то $\bar{\alpha}$ – теж комплексний корінь (якщо коефіцієнти многочлена дійсні!). А тому $(x-\alpha)(x-\bar{\alpha}) \mid f(x)$. Але $(x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha} = x^2 + 2\operatorname{Re}\alpha + |\alpha|^2$ – многочлен з дійсними коефіцієнтами. Тобто f буде звідним.

$\boxed{\Leftarrow}$ **Prp. 4.2.1** та **Prp. 4.2.4**. ■

Example 4.3.5 Многочлен $x^4 + 4$ зобов'язаний бути звідним над $\mathbb{R}$ (хоча дійсних коренів нема). Дійсно, $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$.

4.4 Незвідність на $\mathbb{Q}[x]$ та $\mathbb{Z}[x]$

Lemma 4.4.1 Задані многочлени $\alpha, \beta \in \mathbb{Z}[x]$. Припустимо, що існує просте число p, що ділить всі коефіцієнти многочлена $\alpha \cdot \beta$. Тоді або p ділить всі коефіцієнти α, або p ділить всі коефіцієнти β.

Proof.
Розглянемо ідеал $p\mathbb{Z}$. За одним твердженням, $(\mathbb{Z}/_{p\mathbb{Z}})[x] \cong \mathbb{Z}[x]/_{p\mathbb{Z}[x]}$. Звідси випливає, що $p\mathbb{Z}[x]$ – простий ідеал.
Справді, $p\mathbb{Z}$ – простий ідеал за умовою, тобто $\mathbb{Z}/_{p\mathbb{Z}}$ – область цілісності, а тому $\mathbb{Z}/_{p\mathbb{Z}}[x]$ – область цілісності теж. Водночас в силу ізоморфізму, $\mathbb{Z}[x]/_{p\mathbb{Z}[x]}$ теж область цілісності. Отже, $p\mathbb{Z}[x]$ – простий.
Але $p\mathbb{Z}[x]$ – многочлени, коефіцієнти якого діляться на p. Зокрема $\alpha\beta \in p\mathbb{Z}[x]$ за умовою, а значить, $\alpha \in p\mathbb{Z}[x]$ або $\beta \in p\mathbb{Z}$. ■

Lemma 4.4.2 Лема Гауса
Задані $f \in \mathbb{Z}[x]$ та $g, h \in \mathbb{Q}[x]$ такі функції, що $f(x) = g(x)h(x)$. Тоді існує раціональне число $a, b \in \mathbb{Q}$, для якого $ag, bh \in \mathbb{Z}[x]$, а також $f(x) = ag(x) \cdot bh(x)$.

Proof.
Оберемо $a, b \in \mathbb{Q}$, для яких $ag, bg \in \mathbb{Z}[x]$. Тоді звідси $ag(x)bh(x) = abf(x)$. Ми хочемо підібрати так a, b, щоб $ab = 1$.
Розглянемо множину $S = \{ab \mid a, b \in \mathbb{Q}, ag, bh \in \mathbb{Z}[x], ab \in \mathbb{N}\}$.
$S \neq \emptyset$. Дійсно, нехай $\alpha \in \mathbb{Q}[x]$.
Якщо $\alpha \equiv 0$, то $1 \cdot \alpha(x) = 0 \in \mathbb{Z}[x]$.
Якщо $\alpha \not\equiv 0$, то тоді $\alpha(x) = \dfrac{a_0}{b_0} + \cdots + \dfrac{a_m}{b_m}x^m$. Позначимо $u = b_0 \dots b_m \in \mathbb{N}$, а тоді звідси $u\alpha \in \mathbb{Z}[x]$.
Ці міркування допомагають зробити висновок, що $S \neq \emptyset$. У нас $S \subset \mathbb{N}$, тому оберемо $d = \min\limits_{c \in S} c$. Тоді існують $a, b \in \mathbb{Q}$, для яких $d = ab$, а також $ag, bg \in \mathbb{Z}[x]$. Причому $df(x) = abf(x) = (ag(x))(bh(x))$.
!Припустимо, що $d > 1$, тоді існує просте число $p \mid d$. Ясно, що p ділить всі коефіцієнти $df(x)$. Тому за попередньою лемою (не втрачаючи загальності), p ділить всі коефіцієнти многочлена $ag(x)$. Тобто $\dfrac{a}{p}g \in \mathbb{Z}[x]$. Тому звідси $\dfrac{a}{p} \cdot b = \dfrac{d}{p} \in S$, але тут $\dfrac{d}{p} < d$ – суперечність!
Отже, $d = 1$ – єдиниц варіант. Тобто $f(x) = (ag(x))(bh(x))$. ■

Definition 4.4.3 Задано многочлен $f \in \mathbb{Z}[x], f \not\equiv 0$.
НСД між всіма коефіцієнтами назвемо **контентом** многочлена.
Многочлен назвемо **примітивним**, якщо контент дорівнює 1.

Тоді кожний ненульовий многочлен $f \in \mathbb{Z}[x]$ можна записати таким чином:
$f(x) = df_1(x)$, де d – контент многочлена f та f_1 – примітивний.

Corollary 4.4.4 Задано $f \in \mathbb{Z}[x]$ такий, що примітивний.
f – незвідний в $\mathbb{Z}[x] \iff f$ – незвідний в $\mathbb{Q}[x]$.

Ми будемо доводити, що f – звідний в $\mathbb{Q}[x] \iff f$ – звідний в $\mathbb{Z}[x]$.

Proof.
$\boxed{\Rightarrow}$ Дано: f – звідний в $\mathbb{Q}[x]$, тоді $f(x) = g(x)h(x)$, де многочлени $g, h \notin (\mathbb{Q}[x])^\times = \mathbb{Q} \setminus \{0\}$. За лемою Гауса, існують числа $a, b \in \mathbb{Q}$, для яких $f(x) = (a \cdot g(x)) \cdot (b \cdot h(x))$, де в цьому випадку $a \cdot g, b \cdot h \notin (\mathbb{Z}[x])^\times$. Тоді ми довели, що f – звідний в $\mathbb{Z}[x]$.

$\boxed{\Leftarrow}$ Дано: f – звідний в $\mathbb{Z}[x]$. Маємо $f(x) = g(x)h(x)$, причому $g, h \notin (\mathbb{Z}[x])^\times$. Оскільки контент многочлена f одиничний, за умовою примітивності, то ані g, ані h не можуть бути сталими. Значить, $\deg f, \deg g > 0$, а це каже про $g, h \notin (\mathbb{Q}[x])^\times$. Значить, f – звідний в $\mathbb{Q}[x]$. ■

Corollary 4.4.5 $\mathbb{Z}[x]$ – область однозначної факторизації.

Proof.
Маємо $f \in \mathbb{Z}[x]$, причому $f \not\equiv 0$. Розпишемо як $f(x) = d \cdot f_1(x)$, де d – контент f та f_1 – примітивний. Оскільки $d \in \mathbb{Z},\ d \neq 0$, то за основною теоремою арифметики, ми можемо розписати d на добуток незвідних елементів, які будуть одночасно незвідними в $\mathbb{Z}[x]$ (це неважко довести).
Далі f_1 сприймаємо як многочлен з $\mathbb{Q}[x]$, а ми вже знаємо, що $\mathbb{Q}[x]$ – область однозначної факторизації. Тож f_1 розписується на добуток незвідних елементів $g_i \in \mathbb{Q}[x]$. За лемою Гауса, f_1 розпишеться на добуток елементів $a_i \cdot g_i \in \mathbb{Z}[x]$, причому всі вони будуть примітивними (теж неважко довести). А звідси $a_i \cdot g_i$ – незвідні в $\mathbb{Z}[x]$ за щойно доведеним наслідком. ■

Тести на незвідність в $\mathbb{Z}[x]$

Proposition 4.4.6 Задано $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}[x]$. Припустимо, що $c = \dfrac{p}{q} \in \mathbb{Q}$ (дріб нескоротимий) є коренем многочлена f. Тоді $p \mid a_0,\ q \mid a_d$.

Proof.
За умовою, $f(c) = 0$. Розписавши детально, отримаємо:
$a_0 + a_1 \dfrac{p}{q} + \cdots + a_d \dfrac{p^d}{q^d} = 0$
$a_0 q^d + a_1 p q^{d-1} + \cdots + a_d p^d = 0.$
Із цього отримаємо два рівняння:
$a_0 q^d = -(a_1 q^{d-1} + \cdots + a_d p^{d-1}) \cdot p$
$a_d p^d = -(a_0 q^{d-1} + \cdots + a_{d-1} p^{d-1}) \cdot q$
Звідси отримаємо $p \mid a_0 q^d$ та $q \mid a_d p^d$. Оскільки числа p, q уже взаємно прості, то тоді $p \mid a_0$ та $q \mid a_d$. ■

Remark 4.4.7 Тобто це твердження дозволяє знайти всі раціональні корені многочлена з цілими коефіцієнтами.

Example 4.4.8 З'ясувати, чи буде многочлен $f(x) = 4x^3 + 2x^2 - 5x + 3$ незвідним в $\mathbb{Z}[x]$.
Зауважимо, що f – уже примітивний многочлен. Тому ми покажемо, що f буде незвідним в $\mathbb{Q}[x]$. Оскільки $\deg f = 3$, то нам залишилося показати, що f не має коренів.
Нехай $c = \dfrac{p}{q} \in \mathbb{Q}$ – корінь, тоді звідси $p \mid 3$ та $q \mid 4$. Можливі значення c наступні:
$\pm 1,\ \pm 3,\ \pm\dfrac{1}{2},\ \pm\dfrac{3}{2},\ \pm\dfrac{1}{4},\ \pm\dfrac{3}{4}.$
Підставивши їх, отримаємо, що жодний з них – не корінь.
Отже, f – незвідний в $\mathbb{Q}[x]$, а тому й $\mathbb{Z}[x]$.

Example 4.4.9 Маємно многочлен $g(x) = 4x^3 + 2x^2 - 4x + 3$ – знову примітивний. Аналогічними міркуваннями отримаємо, що лише $-\dfrac{3}{2}$ буде коренем рівняння. Оскільки $\deg g \geq 2$, то g уже буде звідним в $\mathbb{Q}[x]$. Тоді звідси g буде звідним в $\mathbb{Z}[x]$ (попри відсутності цілих розв'язків). Дійсно, $g(x) = (2x + 3)(2x^2 - 2x + 1)$.

Example 4.4.10 Маємо многочлен $h(x) = x^4 - 3x^2 + 1$ – знову примітивний. Аналогічними міркуваннями ми доведемо, що h не має коренів в $\mathbb{Q}[x]$. Але попри це, не можна стверджувати, що h – незвідний в $\mathbb{Q}[x]$, бо вже $\deg h > 3$. Насправді, $h(x) = (x^2 + x - 1)(x^2 - x - 1)$. Тому звідси h – звідний в $\mathbb{Z}[x]$.

Proposition 4.4.11 Задано $f \in \mathbb{Z}[x]$ та p – просте число, причому воно не ділить старший коефіцієнт f. Нехай $\underline{f}$ – многочлен, що отриманий був з f взяттями конгруенціями за $(\mathrm{mod}\ p)$ – незвідний в $(\mathbb{Z}/_{p\mathbb{Z}})[x]$. Тоді f не можна розписати в добуток многочленів із $\mathbb{Z}[x]$ з додатними степенями.

Proof.
Припустимо, що f все ж таки розкладається, як зазначено. Тобто
$f(x) = g(x)h(x)$, причому $\deg g = m,\ \deg h = n$ – обидва додатні.
Старший коефіцієнт f не ділиться на p. Із рівності випливає, що старші коефіцієнти g, h також не діляться на p. Це означає, що $\deg \underline{g} = \deg g,\ \deg \underline{h} = \deg h$. Зрозуміло, що виконується рівність
$\underline{f}(x) = \underline{g}(x)\underline{h}(x)$, обидва многочлени не оборотні.
Отже, ми довели, що $\underline{f}$ – звідний в $(\mathbb{Z}/_{p\mathbb{Z}})[x]$. ■

Corollary 4.4.12 Якщо виконано твердження, то f – незвідний в $\mathbb{Q}[x]$.

Proof.
Уже знаємо, що $f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ не можна розписати як $f(x) = g(x)h(x)$, де $\deg g > 0, \deg h > 0$, також $g, h \in \mathbb{Z}$. Але ще невідомо, чи можна так само зробити для многочленів з раціональними коефіцієнтами.
!Припустимо, що $f(x) = g(x)h(x),\ \deg g > 0, \deg h > 0$, але цього разу $g, h \in \mathbb{Q}[x]$. За лемою Гауса, $f(x) = (ag(x))(bh(x)),\ \deg(ag) > 0,\ \deg(bh) > 0$, а також $ag, bh \in \mathbb{Z}[x]$ – суперечність!
Із цього випливає, що f – незвідний в $\mathbb{Q}[x]$. ■

Example 4.4.13 З'ясувати, чи буде многочлен $f(x) = 675x^3 - 23129x + 1573$ незвідним в $\mathbb{Z}[x]$.
Оберемо просте число $p = 2$ та маємо многочлен $\underline{f}(x) = x^3 - x + 1$. Зауважимо, що $\deg \underline{f} = 3$ та в полі $\mathbb{Z}/_{2\mathbb{Z}}$ нема коренів. Отже, $\underline{f}$ – незвідний в $(\mathbb{Z}/_{2\mathbb{Z}})[x]$. Звідси, за наслідком доведеного твердження, f – незвідний в $\mathbb{Q}[x]$. Далі кялькулятором можна побачити, що f – примітивний многочлен, тож f – незвідний в $\mathbb{Z}[x]$.

Lemma 4.4.14 Задано $\langle R, +, \cdot\rangle$ – область цілісності та $g, h \in R[x]$. Припустимо, що $g \cdot h$ – одночлен. Тоді g, h – одночасно одночлени.

Proof.
Маємо многочлени
$g(x) = b_0 + b_1x + \cdots + b_mx^m$
$h(x) = c_0 + c_1x + \cdots + c_nx^n$.
Позначимо $r \le m$ як найменший степінь многочлена g із ненульовими коефіцієнтами. Аналогічно позначимо $s \le n$ для h. Після цього отримаємо наступне:
$g(x)h(x) = b_rc_sx^{r+s} + \cdots + b_mc_nx^{m+n}$.
Припустимо, що g – не одночлен, тоді звідси $r < m$. Але тоді $r + s < m + n$. Оскільки R – область цілісності, то $b_rc_s, b_mc_n \neq 0$. Отже, $g \cdot h$ має два ненульові коефіцієнти, тому $g \cdot h$ не може бути одночленом.
Якщо h – не одночлен, то аналогічно $g \cdot h$ не може бути одночленом. ■

Remark 4.4.15 Розглянемо $\mathbb{Z}/_{4\mathbb{Z}}$, що не є областю цілісності та многочлени $g(x) = 2,\ h(x) = x + 2$. Попри те, що $g(x)h(x) = 2x + 4 = 2x$ є одночленом, із цього не випливає, що g, h – одночасно одночлени.

Theorem 4.4.16 Критерій Айзенштайна
Задано $f \in \mathbb{Z}$, запишемо $f(x) = a_0 + a_1x + \cdots + a_dx^d$. Також нехай p – таке, просте число, для якого
1) $p \nmid a_d$;
2) $p \mid a_0, a_1, \ldots, a_{d-1}$;
3) $p^2 \nmid a_0$.
Тоді f не можна розписати в добуток многочленів із $\mathbb{Z}[x]$ з додатними степенями.

Remark 4.4.17 Звідси аналогічно випливає, що f – незвідний в $\mathbb{Q}[x]$.

Proof.
!Припустимо, що f розписується як добуток многочленів із $\mathbb{Z}[x]$ з додатними степенями. Тобто
$f(x) = g(x)h(x)$, де $g, h \in \mathbb{Z}[x]$,
$g(x) = b_0 + b_1x + \cdots + b_mx^m$
$h(x) = c_0 + c_1x + \cdots + c_nx^n$.
У нашому випадку припускається $m, n > 0$. Також зауважимо, що $m + n = d$. Перейшовши на $\mathbb{Z}/_{p\mathbb{Z}}$, маємо наступне:
$\underline{f}(x) = \underline{g}(x)\underline{h}(x)$.
За 1), $\underline{a_d} \neq 0$.

За 2), $\underline{f}(x) = \underline{a_d}x^d$, тобто $\underline{f}$ буде одночленом. За лемою, оскільки $\mathbb{Z}/_{p\mathbb{Z}}$ є областю цілісності, то $\underline{g}(x) = \underline{b_m}x^m$, $\underline{h}(x) = \underline{c_n}x^n$, тобто вони теж одночлени. Але оскільки $m, n > 0$, то тоді $\underline{b_0} = \underline{c_0} = 0$, тобто тоді $p \mid b_0,\ p \mid c_0$. Проте звідси $p^2 \mid b_0c_0 = a_0$ – порушується 3) – суперечність! ■

Example 4.4.18 З'ясувати, чи буде многочлен $f(x) = 7x^3 + 6x^2 + 4x + 6$ незвідним в $\mathbb{Z}[x]$.
Нехай $p = 2$, старший коефіцієнт $a_3 = 7$ та вільний коефіцієнт $a_0 = 6$. Решта коефіцієнтів $a_2 = 6, a_1 = 4$. Маємо:
1) $p \nmid a_d$;
2) $p \mid a_0, a_1, \ldots, a_{d-1}$;
3) $p^2 \nmid a_0$.
За критерієм Айзенштайна, f – незвідний в $\mathbb{Q}[x]$, а тому й в $\mathbb{Z}[x]$ в силу примітивності многочлена.

Example 4.4.19 Розглянемо многочлен $f(x) = x^2 - p$, де p – просте число. Він підпорядковується критерію Айзенштайна, тому f – незвідний в $\mathbb{Q}[x]$. Значить, за **Th. 4.2.3**, f не має коренів в $\mathbb{Q}$, тобто $\sqrt{p} \notin \mathbb{Q}$.
Аналогічні міркування проводяться для многочлена $f(x) = x^n - p$, а тому отримаємо $\sqrt[n]{p} \notin \mathbb{Q}$. Отримали класний наслідок:

Corollary 4.4.20 В кільці $\mathbb{Q}[x]$ існують незвідні многочлени будь-якого високого степеня.

5 Теорія модулів

Надалі всюди, де буде кільце $\langle R, +, \cdot \rangle$, вона буде містити одиницю. Лише в окремих випадках (де це буде) виникне окремий коментар. Також множення $\cdot$ я писати явно не буду, тобто замість $r \cdot s$ писатиму rs.

Оскільки ми беремо в увагу кільця з одиницями, то варто дещо сказати.

Proposition 5.0.1 Задано R, S – кільця з двома одиницями та $f\colon R \to S$ – гомомрфізм кілець. Тоді $f(1_R) = 1_S$.

Proof.
$f(1_R) = f(aa^{-1}) = f(a)f(a^{-1}) = f(a)(f(a))^{-1} = 1_S$. ■

5.1 Основа

Definition 5.1.1 Задано $\langle R, +, \cdot \rangle$ – кільце. Маємо множину $M \neq \emptyset$.
Структура $(M, +, \cdot)$ називається **(лівим) модулем над кільцем** R, яка має операції $+$ (додавання) та $r\cdot$ (множення на скаляр):

$$\forall a, b \in M : a + b \in M$$
$$\forall r \in R, \forall a \in M : r \cdot a \in M$$

Вони підпорядковують таким аксіомам:

1) $\forall a, b, c \in M : a + (b + c) + (a + b) + c$
2) $\exists 0_M \in M : \forall a \in M : a + 0_M = 0_M + a = a$
3) $\forall a \in M : \exists \tilde{a} \in M : a + \tilde{a} = 0_M$
4) $\forall a, b \in M : a + b = b + a$
5) $\forall a \in M : 1_R \cdot a = a$
6) $\forall r, s \in R, \forall a \in M : (rs) \cdot a = r \cdot (s \cdot a)$
7) $\forall r, s \in R, \forall a \in M : (r + s) \cdot a = r \cdot a + s \cdot a$
8) $\forall r \in R, \forall a, b \in M : r \cdot (a + b) = r \cdot a + r \cdot b$

(Правим) модулем над кільцем R буде вже, якщо операція множення на скаляр визначено справа, тобто $\forall r \in R, \forall a \in M : a \cdot r \in M$.

Example 5.1.2 Будь-який векторний простір L над полем k – це вже модуль над цим кільцем.
Тобто модуль над кільцем – це певне узагальнення.

Example 5.1.3 Одноточкова множина $\{x\}$ буде R-модулем, якщо визначити множення на скаляр як $r \cdot x = x$, для всіх $r \in R$. Це називають **тривіальним модулем**, а позначають за $\{0\}$.

Remark 5.1.4 Кільце $\langle R, +, \cdot \rangle$ можна сприймати як модуль над самим ж кільцем R.

Example 5.1.5 Задамо $\langle R, +_R, \cdot_R \rangle, \langle S, +_S, \cdot_S \rangle$ – два кільця та $f\colon R \to S$ – гомоморфізм. Розглянемо таке множення елемента S на скаляр f:
$r \cdot s \overset{\text{def.}}{=} f(r) \cdot_S s$ (множення варто розрізняти тут).
Тоді $(S, +_S, \cdot)$ – модуль над кільцем R.
Умови 1)–4) уже виконані. Залишилося перевірити 5)–8):
5) $1_R \cdot a \overset{\text{def.}}{=} f(1_R)a = 1_S a = a$;
6) $(r_1 r_2) \cdot a \overset{\text{def.}}{=} f(r_1 r_2)a = f(r_1)(f(r_2)a) \overset{\text{def.}}{=} r_1 \cdot (f(r_2)a) \overset{\text{def.}}{=} r_1 \cdot (r_2 \cdot a)$;
7) $(r_1 + r_2) \cdot a \overset{\text{def.}}{=} f(r_1 + r_2)a = (f(r_1) + f(r_2))a = f(r_1)a + f(r_2)a \overset{\text{def.}}{=} r_1 \cdot a + r_2 \cdot a$;
8) $r \cdot (a + b) \overset{\text{def.}}{=} f(r)(a + b) = f(r)a + f(r)b \overset{\text{def.}}{=} r \cdot a + r \cdot b$.

Example 5.1.6 Із минулого цього прикладу випливає наступне. Якщо R – кільце та I – ідеал, то $R/_I$ – модуль над R, взявши множення вище.

Corollary 5.1.7 Інше означення ідеалу
Задано $\langle R, +, \cdot \rangle$ – кільце та $I \subset R$.
I – (лівий) ідеал над $R \iff (I, +, \cdot)$ – (лівий) модуль над R.
(для правих ідеалів та модулів це теж виконується)

Proposition 5.1.8 Властивості модуля
Задано $(M,+,\cdot)$ – R-модуль. Тоді
1) 0_M – єдиний елемент;
2) $\forall a \in M : \tilde{a} \in M$ існує, причому єдиним чином;
3) $\forall m \in M : 0_R \cdot m = 0_M$;
4) $\forall a \in M : \tilde{a} = (-1)_R \cdot a = -a$.

Proof.
Дійсно, маємо наступне:

1) Припускаючи, що в нас $0_M, \tilde{0}_M$ – два нульових елементи, маємо
$0_M = 0_M + \tilde{0}_M = \tilde{0}_M$.

2) Припускаючи, що для $a \in M$ у нас є два протилежних $\tilde{a}_1, \tilde{a}_2 \in M$,
$\tilde{a}_1 = \tilde{a}_1 + 0_M = \tilde{a}_1 + (a + \tilde{a}_2) = (\tilde{a}_1 + a) + \tilde{a}_2 = 0_M + \tilde{a}_2 = \tilde{a}_2$

3) $0_R \cdot m = (0_R + 0_R) \cdot m = 0_R \cdot m + 0_R \cdot m$.
Тобто звідси в нас $0_M = 0_R \cdot m$ як нульовий елемент (в силу єдиності).

4) $a + (-1)_R \cdot a = (1_R + (-1)_R)a = 0_R \cdot a = 0_M$.
Отже, в силу єдиності $\tilde{a} = (-1)_R \cdot a = -a$.

Всі властивості доведені. ■

Proposition 5.1.9 Задано $\langle M,+\rangle$ – абелева група. Тоді $(M,+,\cdot)$ задаватиме однозначно $\mathbb{Z}$-модуль, якщо визначити множення на скаляр:
$n \cdot a \overset{\text{def.}}{=} \underbrace{a + \cdots + a}_{n \text{ разів}}$
$(-n) \cdot a \overset{\text{def.}}{=} \underbrace{-a - \cdots - a}_{n \text{ разів}}$
$0 \cdot a = 0_M$.
У всіх випадках ми маємо $n \in \mathbb{N}$.

Proof.
Оскільки $\langle M,+\rangle$ – абелева група, то 1)–4) уже є.
5) $1_{\mathbb{Z}} \cdot a = \underset{1 \text{ раз}}{a} = a$.
6) $(nm) \cdot a = \underset{nm \text{ разів}}{a + \cdots + a} = \underbrace{\underbrace{(a + \cdots + a)}_{n \text{ разів}} + \cdots + \underbrace{(a + \cdots + a)}_{n \text{ разів}}}_{m \text{ разів}} =$
$= \underset{n \text{ разів}}{m \cdot (a + \cdots + a)} = m \cdot (na)$.
7) $(m+n) \cdot a = \underset{m+n \text{ разів}}{a + \cdots + a} = \underbrace{a + \cdots + a}_{m \text{ разів}} + \underbrace{a + \cdots + a}_{n \text{ разів}} = m \cdot a + n \cdot a$.
8) $m \cdot (a+b) = \underset{m \text{ разів}}{((a+b) + \cdots + (a+b))} \overset{1),4)}{=}$
$= \underset{m \text{ разів}}{a + \cdots + a} + \underset{m \text{ разів}}{b + \cdots + b} = m \cdot a + m \cdot b$.

Тепер нехай заданий інший $\mathbb{Z}$-модуль $(M,+,\odot)$ (тобто інше множення на скаляр). Тоді за аксіомою 5), маємо $1_{\mathbb{Z}} \odot a = a$. Далі
$n \odot a = \underbrace{(1 + \cdots + 1)}_{n \text{ разів}} \odot a \overset{7)}{=} \underbrace{1 \odot a + \cdots + 1 \odot a}_{n \text{ разів}} = \underbrace{a + \cdots + a}_{n \text{ разів}} = n \cdot a$.
$0 \odot a = 0_M = 0 \cdot a$.
$(-n) \odot a = (-n) \cdot a$ аналогічним чином.
Тобто дві різні операції множення співпали взагалі. ■

Remark 5.1.10 Із одного боку, із R-модуля $(M,+,\cdot)$ випливає, що $\langle M,+\rangle$ – абелева група. Із іншого боку, із абелевої групи $\langle M,+\rangle$ випливає $(M,+,\cdot)$ – $\mathbb{Z}$-модуль вище.

Підкреслю: абелева група $\langle M,+\rangle$ дорівнює $\mathbb{Z}$-модулю $(M,+,\cdot)$.

5.2 Категорія модулів

Definition 5.2.1 Задано $\langle R, +, \cdot \rangle$ – кільце та M, N – R-модулі.
Відображення $f\colon M \to N$ називають **гомоморфізмом модулів над кільцями** R, якщо

$$\forall a, b \in M : f(a+b) = f(a) + f(b)$$
$$\forall r \in R, \forall a \in M : f(r \cdot a) = r \cdot f(a)$$

Ще це називають **лінійним відображенням над** R.

Example 5.2.2 Зокрема між двома векторними просторами L, M над полем k розглядали лінійні оператори $A\colon L \to M$ – це й є лінійне відображення над кільцем k між двома модулями L, M.

Example 5.2.3 Маємо $f\colon R \to S$ – гомоморфізм над кільцями R, S. Ми вже знаємо, що R, S можна сприймати як модулі над кільцем R. Тоді f буде R-лінійним відображенням. Дійсно,
$f(a+b) = f(a) + f(b)$ (просто з означення гомоморфізма кілець);
$f(r \cdot a) = f(ra) = f(r)f(a) = r \cdot f(a)$ (в кінці множення на скаляр в S).

Example 5.2.4 Відображення $f_n\colon \mathbb{Z} \to \mathbb{Z}$, що задається як $f_n(a) = n \cdot a$, буде $\mathbb{Z}$-лінійним відображенням (неважко довести). Між іншим, серед f_n лише єдиний f_1 буде гомоморфізмом кілець. У інших $f_n, n \neq 1$, не виконується друга властивість гомомрфізма кілець.

Example 5.2.5 Відображення $0\colon M \to N$, що задається як $0(m) = 0_N$, буде **тривіальним гомоморфізмом модулів над** R.

Example 5.2.6 Якщо R – кільце та M – модуль над R, то для визначення R-лінійного відображення $f\colon R \to M$ досить знати, чому дорівнює $f(1)$. Дійсно, позначимо $m = f(1)$. Звідси $f(r) = f(r \cdot 1) = r \cdot f(1) = r \cdot m$.

Навпаки теж: якщо $f(r) = r \cdot m$, то це задає R-лінійне відображення.

Proposition 5.2.7 Категорія гомоморфізмів модулів
Задані M, L, K – модулі над кільцем R. Тоді виконуються наступне:
1) $\mathrm{id}\colon M \to M$ – R-лінійне відображення;
2) Якщо $\varphi\colon M \to L, \psi\colon L \to K$ – R-лінійні відображення, то $\psi \circ \varphi\colon M \to K$ – також R-лінійне відображення;
3) Операція композиції гомоморфізми модулів – асоціативна.
Вправа: довести.

Proposition 5.2.8 Маємо $f\colon M \to N$ – гомоморфізм над R-модулями. Тоді $f(0_M) = 0_N$.
Вправа: довести.

Definition 5.2.9 Задано $f\colon M \to N$ – гомоморфізм над R-модулями.
Ми будемо це називати **ізоморфізмом над** R**-модулями**, якщо

$$f \text{ – бієктивне відображення}$$

У свою чергу R-модулі M, N називатимуться **ізоморфними**.
Позначення: $M \cong N$.

Remark 5.2.10 Аналогічно можна отримати еквівалентні означення. Також неважко переконатися, що якщо f – гомоморфізм, то f^{-1} – теж гомоморфізм.

Remark 5.2.11 Між довільними двома R-модулями можна знайти хоча б один гомоморфізм – і це тривіальний.
Між довільними кільцями не завжди можна знайти гомоморфізм. Наприклад, $\mathbb{Z}_3 \to \mathbb{Z}_2$ нема.

Example 5.2.12 $\mathbb{Z} \cong \mathbb{Z}$ як модулі, бо існує або ізоморфізм $f(n) = n$, або ізоморфізм $f(n) = n$.
Також $\mathbb{Z} \cong \mathbb{Z}$ як кільця, але там єдиний ізоморфізм $f(n) = n$.

Example 5.2.13 $\mathbb{R} \times \mathbb{R} \cong \mathbb{C}$ як модулі над $\mathbb{Z}$.
Водночас зазначимо, що $\mathbb{R} \times \mathbb{R} \ncong \mathbb{C}$ як кільця (перше кільце не область цілісності, а друге навпаки).

5.3 Підмодулі

Definition 5.3.1 Задано $(M, +, \cdot)$ – R-модуль та $N \subset M$.
Підмножина N називається **підмодулем модуля** M, якщо

$$(N, +, \cdot) \text{ – } R\text{-модуль},$$

де операції $+$, $\cdot r$ ми успадкували з модуля M.

Proposition 5.3.2 Задані $(M, +, \cdot)$ – R-модуль та $N \subset M$. Нехай $(N, +, \cdot)$ – R-модуль (поки що ми вважаємо, що тут якісь інші операції).
N – підмодуль $M \iff \imath\colon N \hookrightarrow M$ задає R-лінійне відображення.
Аналогічне доведення, як це було з групами або кільцями.

Theorem 5.3.3 Критерій підмодуля
Задані $(M, +, \cdot)$ – R-модуль та множина $N \subset M$.

$$N \text{ – підмодуль } \iff \begin{cases} \forall a, b \in N : a + b \in N \\ \forall r \in R, \forall a \in N : r \cdot a \in N \end{cases} \quad \text{та } N \neq \emptyset.$$

Proof.
$\boxed{\Rightarrow}$ Дано: N – підмодуль. Тоді операція $+|_N, (\cdot r)|_N$ успадковується з модуля M, тому замкненість відносно цих операцій автоматично є. Також $N \neq \emptyset$, тому що $0_N \in N$ за другою аксіомою.

$\boxed{\Leftarrow}$ Дано: замкненість відносно $+$, $(\cdot r)$ та $N \neq \emptyset$.
Всі (поки крім 2), 3)) виконані, тому що вони виконані в M і підмножина N замкнена відносно цих операцій.
Зауважимо, що при $n \in N$ маємо $0_R \cdot n \in N$. Але $0_R \cdot n = 0_M \in M$, при цьому $0_M + n = n$. Отже, існує $0_N = 0_M$, для якого $0_N + n = n + 0_N = n$.
Зауважимо, що при $n \in N$ маємо $-n \in N$. Але $-n \in M$, при цьому $n - n = 0_M$. Отже, існує $\tilde{n} = -n$, для якого $n + \tilde{n} = 0_N$.
Звідси 2) та 3) виконані. Тому $(N, +|_N, \cdot|_N)$ задає R-модуль. Тож N – підмодуль. ■

Proposition 5.3.4 Задано M – модуль та N_1, N_2 – два підмодуля. Визначимо множину $N_1 + N_2 \overset{\text{def.}}{=} \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}$.
Тоді $N_1 + N_2$ – підмодуль модуля M.
Вправа: довести.

Proposition 5.3.5 Задано M – модуль та N_1, N_2 – два підмодуля.
Тоді $N_1 \cap N_2$ – підмодуль модуля M.
(підмодулем також може бути перетин якоїсь сім'ї підмодулів).
Вправа: довести.

Definition 5.3.6 Задано M – R-модуль.
Підмодуль, породжений $m_1, \ldots, m_k \in M$, називають таку множину:

$$\langle m_1, \ldots, m_k \rangle = \{r_1 \cdot m_1 + \cdots + r_k \cdot m_k \mid r_1, \ldots, r_k \in R\}$$

Модуль M називатиметься **скінченно породженим**, якщо існують $m_1, \ldots, m_k \in M$, для яких

$$M = \langle m_1, \ldots, m_k \rangle$$

Модуль M називатиметься **циклічним**, якщо існує $m \in M$, для якого

$$M = \langle m \rangle$$

Proposition 5.3.7 Задано M – R-модуль. Тоді $\langle m_1, \ldots, m_k \rangle$ – дійсно підмодуль M, причому найменший підмодуль, що містить $m_1, \ldots, m_k$.

Proof.
Дійсно, нехай $u, v \in \langle m_1, \ldots, m_k \rangle$, тоді звідси
$u = r_1 m_1 + \cdots + r_k m_k$
$s = s_1 m_1 + \cdots + s_k m_k$.

$u + s = (r_1 + s_1)m_1 + \cdots + (r_k + s_k)m_k$, причому $r_i + s_i \in R$, а тому звідси $u + s \in \langle m_1, \ldots, m_k \rangle$.
$t \cdot u = (tr_1)m_1 + \cdots + (tr_k)m_k$, причому $tr_i \in R$, а тому звідси $t \cdot u \in \langle m_1, \ldots, m_k \rangle$.

Припустимо, що існує N – ще менший підмодуль модуля M, що містить $m_1, \ldots, m_k$. Тобто $N \subset \langle m_1, \ldots, m_k \rangle$. Але якщо $u \in \langle m_1, \ldots, m_k \rangle$, тоді $u = r_1 m_1 + \cdots + r_k m_k$. Оскільки $m_1, \ldots, m_k \in N$, то звідси $u \in N$. Отримали $N \supset \langle m_1, \ldots, m_k \rangle$. Отже, $N = \langle m_1, \ldots, m_k \rangle$. ■

Example 5.3.8 Маємо R – кільце та I – ідеал. Тоді ми вже знаємо, що це модуль над R. Оскільки $\pi \colon R \to R/_I$ – гомоморфізм кілець, то звідси визначено вже операція множення на скаляр. Більш того, $R/_I = \langle 1 + I \rangle$.

Proposition 5.3.9 Задано $f \colon M \to N$ – R-лінійне відображення. Тоді:
1) якщо M' – підмодуль M, тоді $f(M')$ – підмодуль N;
2) якщо N' – підмодуль N, тоді $f^{-1}(N')$ – підмодуль M.
Вправа: довести.

5.4 Фактормодулі

Ми тут давали суміжні класи груп та кілець одним способом, а зараз підемо трошки здалеку для різноманіття.

Definition 5.4.1 Задано $f \colon M \to N$ – R-лінійне відображення між модулями.
Ядром R-лінійного відображення f назвемо множину

$$\ker f = \{m \in M : f(m) = 0_N\}$$

Образом R-лінійного відображення f назвемо множину

$$\operatorname{Im} f = \{n \in N \mid \exists m \in M : n = f(m)\}$$

Remark 5.4.2 Зауважимо, що $\ker f = f^{-1}(\{0_N\})$ та $\operatorname{Im} f = f(M)$.
Оскільки $\{0_N\}$ – підмодуль N, то звідси $f^{-1}(\{0_N\})$ – підмодуль M.
Оскільки M – модуль, то $f(M)$ – підмодуль N.

Remark 5.4.3 Більш того, поставимо відношення еквівалентності на M таким чином:
$m_1 \sim m_2 \iff f(m_1) = f(m_2)$.
За властивостями гомоморфізма, $f(m_1 - m_2) = 0$. Тобто ми отримали:
$m_1 \sim m_2 \iff m_1 - m_2 \in \ker f$.

І така еквівалентність працює лише для підмодуля $\ker f$. Ми можемо це узагальнити для будь-якого підмодуля K модуля M. На множині M встановимо відношення еквівалентності
$m_1 \sim m_2 \iff m_1 - m_2 \in K$.
Тоді ми отримаємо класи еквівалентності $[m] = \{k \in M \mid m - k \in K\}$ та фактормножину $M/_\sim$.

Definition 5.4.4 Суміжним класом елемента m за модулем K назвемо клас еквівалентності множини m, тобто

$$m + K \overset{\text{def.}}{=} [m]$$

Remark 5.4.5 Неважко буде переконатися, що цю множину можна записати в більш зручному вигляді (як це було в групах та кільцях):
$m + K = \{m + k \mid k \in K\}$.

Враховуючи, чому тепер дорівнює суміжний клас, можна переписати відношення еквівалентності також в більш зручному вигляді:
$m_1 \sim m_2 \iff m_1 + K = m_2 + K$.

Definition 5.4.6 R-фактормодулем модуля $(M, +, \cdot)$ за підмодулем K назвемо множину $M/_\sim \overset{\text{позн.}}{=} M/_K$, для якій визначені наступні операції:

$$(m_1 + K) + (m_2 + K) = (m_1 + m_2) + K$$
$$r \cdot (m_1 + K) = r \cdot m_1 + K$$

Lemma 5.4.7 Операції вище – коректно визначені.
Вправа: довести.

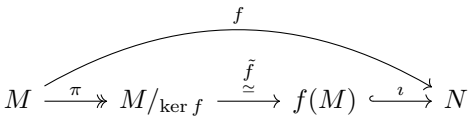
Theorem 5.4.8 $(M/_K, +, \cdot)$, де операції зазначені вище, – R-модуль.
Вправа: довести.

5.5 Основі теореми про ізоморфізм

Lemma 5.5.1 Задані M – модуль над кільцем R та K – підмодуль M. Тоді $\pi\colon M \to M/_K$ – сюр'єктивний гомоморфізм модулів.
Вправа: довести.

Lemma 5.5.2 Задані M – модулі над кільцем R. Тоді $\imath\colon f(M) \to M$ – ін'єктивний гомоморфізм модулів.
Вправа: довести.

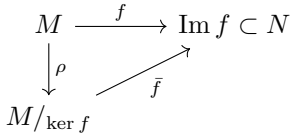
Theorem 5.5.3 Канонічний розклад гомомрфізму модулів
Задано $f\colon M \to N$ – гомоморфізм модулів над кільцем R. Тоді існує єдиний гомоморфізм $\tilde{f}\colon M/_{\ker f} \to f(M)$, для якого $\imath \circ \tilde{f} \circ \pi = f$.



Тут $\pi\colon M \to M/_{\ker f}$ – проєкторний гомоморфізм: $\pi(m) = m + \ker f$. Також $\imath\colon f(M) \to N$ – гомоморфізм вкладень.

Насправді, єдине, що треба довести, – так це $\tilde{f}(m + \ker f) = f(m)$ – гомоморфізм модулів. Решта уже виконано.
Вправа: довести.

Theorem 5.5.4 Перша теорема про ізоморфізм
Задано M та N – R-модулі та $f\colon M \to N$ – R-лінійне відображення. Тоді $M_{\cdot\ker f} \cong \operatorname{Im} f$. Ізоморфізм задається діаграмою нижче.



Тут нічого нового не написано, тупо попередня теорема.

Theorem 5.5.5 Друга теорема про ізоморфізм
Задано M – R-модуль та K, L – підмодулі. Тоді $L/_{K\cap L} \cong (K + L)/_K$.

Remark 5.5.6 До речі, $K \cap L$ справді є підмодулем модуля L. Також неважко пересвідчитися, що K буде підмодулем модуля $K + L$. Тож запис ізоморфності двох множин коректний.

Proof.
Установимо відображення $\varphi\colon L \to (K + L)/_K$ таким чином:
$\varphi(l) = l + K$.
Зауважимо, що це сюр'єктивне відображення. Справді, нехай $(k + l) + K \in (K + L)/_K$. Можна показати, що $(k+l)+K = l+K$, оскільки $(k+l)-l = k \in K$. Тому ми знайшли елемент $l \in L$, для якого $\varphi(l) = l + K = (k + l) + L$.
Дане відображення задає R-лінійне відображення (доводиться аналогічно, як доводили той факт, що проєкція $\pi\colon M \to M/_K$ задає R-лінійне відображення).
Нарешті, нехай $l \in \ker\varphi$, тобто $\varphi(l) = l+K = K$, а це означає, що $l \in K$. Тобто отримали $l \in K \cap L$.
Звідси $\ker f = K \cap L$.
За І теоремою про ізоморфім, $L/_{K\cap L} \cong (K + L)/_K$. ■

Theorem 5.5.7 Маємо M – R-модуль та K – підмодуль. Тоді існує бієкція $U_1 = \{L$ – підмодуль $M : L \supset K\} \to \{L/_K$ – підмодуль $M/_K\} = U_2$.

Proof.
Розглянемо проєкцію $\pi\colon M \to M/_K$ (що вже гомоморфізм).
Нехай L – підмодуль M, причому $L \supset K$. Тоді звідси $\pi(L) = L/_K$ – підмодуль $M/_K$ як образ.

Нехай $\bar{L}$ – підмодуль $M/_K$. Тоді звідси $\pi^{-1}(\bar{L}) = L$ – підмодуль M, причому $L = \pi^{-1}(\bar{L}) \supset \pi^{-1}(\{0_{M/_K}\}) = K$.

Тобто ми довели, що U – підмодуль $M/_K \iff U = L/_K$.
Перевіримо, що відображення $F\colon U_1 \to U_2$, що задається як $F(L) = \pi(L)$, буде бієктивним.
Нехай $\pi(L_1) = \pi(L_2)$, тобто $L_1/_K = L_2/_K$. Нам треба показати, що $L_1 = L_2$. Справді, $l \in L_1 \implies l + K \in L_1/_K = L_2/_K \implies l \in L_2$. Аналогічно $l \in L_2 \implies l \in L_1$.
Сюр'єктивність була доведена вище. ■

Theorem 5.5.8 Третя теорема про ізоморфізм
Задано M – R-модуль та K – підмодуль. Також L буде підмодулем, причому $L \supset K$.
Тоді $(M/_K)/_{L/_K} \cong M/_L$.

Remark 5.5.9 Ми вже довели, що в цьому випадку $L/_K$ буде підмодулем $M/_K$, а значить, $(M/_K)/_{L/_K}$ – коректна штука.

Proof.
Установимо відображення $\varphi\colon M \to (M/_K)/_{L/_K}$ таким чином:
$\varphi(m) = (m + K) + L/_K$.
Насправді, треба зазначити, що $\varphi = \pi_{M/_K \to (M/_K)/_{L/_K}} \circ \pi_{M \to M/_K}$ – композиція двох проєкцій. За безкоштовно довели: φ – сюр'єктивне R-лінійне відображення як композиція таких. Щодо ядра: $m \in \ker\varphi$, тож $\varphi(m) = (m + K) + L/_K = L/_K$, тобто $m + K \in L/_K$, а це означає $m \in \pi^{-1}(L/_K)$, але в силу бієктивності $m \in L$. Отже, $\ker f = L$.
За I теоремою про ізоморфізм, $M/_L \cong (M/_K)/_{L/_K}$. ■

5.6 Пряма сума модулів

Definition 5.6.1 Задано $(M, +_M, \cdot_M)$, $(N, +_N, \cdot_N)$ – два R-модуля.
Прямою сумою M, N назвемо модуль $(M \times N, +, \cdot)$, із таким операціями:

$$(m_1, n_1) + (m_2, n_2) \stackrel{\text{def.}}{=} (m_1 +_M m_2, n_1 +_N n_2)$$
$$r \cdot (m, n) \stackrel{\text{def.}}{=} (r \cdot_M m, r \cdot_N n)$$

Позначення: $M \oplus N$.
Така структура дійсно задає модуль – неважко довести.

Remark 5.6.2 Ясно, що пряму суму можна записати для іншої скінченної кількості модулів над одним кільцем.

Definition 5.6.3 Задано R – кільце.
Вільним R-модулем рангу n називатимемо таку пряму суму:

$$R^{\oplus n} = \underbrace{R \oplus \cdots \oplus R}_{n \text{ разів}}$$

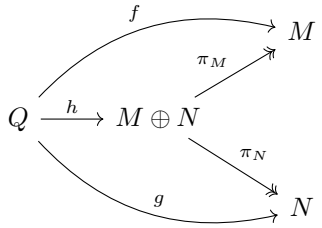
Із прямою сумою пов'язані деякі відображення:
проєкції $\pi_M\colon M \oplus N \twoheadrightarrow M$, $\pi_M(m, n) = m$ $\quad$ $\pi_N\colon M \oplus N \twoheadrightarrow N$, $\pi_N(m, n) = n$

ін'єкції $\imath_M\colon M \hookrightarrow M \oplus N$, $\imath_M(m) = (m, 0_N)$ $\quad$ $\imath_N\colon N \hookrightarrow M \oplus N$, $\imath_N(n) = (0_M, n)$
Всі вони задають R-лінійне відображення – неважко показати.

Remark 5.6.4 Якщо задати ін'єкції подібного характеру на кільці з одиницею, то вони не будуть визначати гомоморфізм (ще одна відмінність).

До речі, завдяки цим ін'єкціям, ми можемо M, N сприймати як підмодулі модуля $M \oplus N$ абсолютно легально.

Proposition 5.6.5 Задані M, N, Q – R-модулі, а також $f\colon Q \to M$, $g\colon Q \to N$ – R-лінійні відображення. Тоді існує єдиний $h\colon Q \to M \oplus N$ – R-лінійне відображення, для якого $f = \pi_M \circ h$ та $g = \pi_N \circ h$.



Proof.
Визначимо відображення $h\colon Q \to M \oplus N$ таким чином:
$h(q) = (f(q), g(q))$.
Зауважимо, що $(\pi_M \circ h)(q) = \pi_M((f(q), g(q)) = f(q)$. Аналогічно $(\pi_N \circ h)(q) = \pi_N((f(q), g(q)) = g(q)$.
Доведемо, що h – R-лінійне відображення.
$h(q_1 + q_2) = (f(q_1 + q_2), g(q_1 + q_2)) = (f(q_1) + f(q_2), g(q_1) + g(q_2)) = (f(q_1), g(q_1)) + (f(q_2), g(q_2)) = h(q_1) + h(q_2)$.
$h(r \cdot q) = (f(r \cdot q), g(r \cdot q)) = (r \cdot f(q), r \cdot g(q)) = r \cdot (f(q), g(q)) = r \cdot h(q)$.

Нехай $\tilde{h}\colon Q \to M \oplus N$ – якесь інше відображення (не обов'язково навіть R-лінійне), для якого $f = \pi_M \circ \tilde{h}$ та $g = \pi_N \circ \tilde{h}$. Отримаємо наступне:
$\tilde{h}(q) = (f(q), n)$, де $n \in N$ та не залежить від q.
$\tilde{h}(q) = (m, g(q))$, де $m \in M$ та не залежить від q.
Об'єднуючи, отримаємо $\tilde{h}(q) = (f(q), g(q)) = h(q)$. ■

Proposition 5.6.6 Задані M_1, M_2 – R-модулі та $L_1 \subset M_1, L_2 \subset M_2$ – відповідні підмодулі. Тоді $L_1 \oplus L_2$ – підмодуль $M_1 \oplus M_2$, причому
$(M_1 \oplus M_2)/_{L_1 \oplus L_2} \cong (M_1/_{L_1}) \oplus (M_2/_{L_2})$.

Proof.
Розглянемо таке відображення $f\colon M_1 \oplus M_2 \to (M_1/_{L_1}) \oplus (M_2/_{L_2})$:
$f(m_1, m_2) = (m_1 + L_1, m_2 + L_2)$.
Неважко буде довести, що це – R-лінійне відображення.
Також неважко довести, що воно – сюр'єктивне. Знайдемо ядро:
$\ker f = \{(m_1, m_2) \mid f(m_1, m_2) = (0 + L_1, 0 + L_2)\} =$
$= \{(m_1, m_2) \mid (m_1 + L_1, m_2 + L_2) = (L_1, L_2)\} =$
$= \{(m_1, m_2) \mid m_1 \in L_1, m_2 \in L_2\} = L_1 \oplus L_2$.
Оскільки $\ker f$ є підмодулем, то довели, що $L_1 \oplus L_2$ – підмодуль.
Нарешті, $(M_1 \oplus M_2)/_{L_1 \oplus L_2} \cong (M_1/_{L_1}) \oplus (M_2/_{L_2})$ – випливає із I теореми про ізоморфізм. ■

5.7 Модулі над областями цілісноті

Усюди вважатимемо в даному розділі, що $\langle R, +, \cdot \rangle$ – область цілісності.

Definition 5.7.1 Маємо $m \in \mathbb{N} \cup \{0\}$.
R-модуль F називається **вільним**, якщо даний модуль ізоморфіний деякому вільному R-модулю деякого рангу, тобто

$$F \cong R^{\oplus m}$$

Definition 5.7.2 Задано M – R-модуль та $\{x_1, \ldots, x_m\}$.
Система елементів називається **лінійно незалежною**, якщо

$$r_1 x_1 + \cdots + r_m x_m = 0 \implies r_1 = \cdots = r_m = 0$$

Definition 5.7.3 Задано M – R-модуль та $\{x_1, \dots, x_m\}$.
Система називається **базисом**, якщо

$$\{x_1, \dots, x_m\} \text{ – лінійно незалежна;}$$
$$(x_1, \dots, x_m) = M$$

Останнє означає, що будь-який елемент $a \in M$ записується як лінійна комбінація з л.н.з. елементів.

Definition 5.7.4 Кільце R називають **IBN-кільцем** (invariant basis number), якщо для кожного (скінченно породженого) вільного R-модуля F кількість елементів у базисі модуля F не залежить від вибору базису.

Definition 5.7.5 Задано R – IBN-кільце та F – вільний R-модуль та $\{x_1, \dots, x_m\}$ – базис F.
Число m називається **рангом** F.

Remark 5.7.6 Всі комутативні кільця з одиницею, крім $\{0\}$, будуть IBN-кільцями. Тобто це так, чисто формальне означення.

Proposition 5.7.7 Задано F – R-модуль.
F – вільний рангу $m \in \mathbb{N} \iff F$ має базис $\{x_1, \dots, x_m\}$.

Proof.
$\boxed{\Rightarrow}$ Дано: $F \cong R^{\oplus m}$.
На $R^{\oplus}$ ми встановимо елементи $\underline{e}_i = (0, \dots, \underset{i\text{-та позиція}}{1}, \dots 0)$, тут $1 = \overline{1, m}$. Неважко довести, що $\{\underline{e}_1, \dots, \underline{e}_m\}$ - л.н.з. система. Також якщо $r \in F$, тобто $r = (r_1, \dots, r_m)$, то це можемо розписати так:
$r = r_1\underline{e}_1 + \dots + r_m\underline{e}_m$.
Отже, $\{\underline{e}_1, \dots, \underline{e}_m\}$ утворює базис в $R^{\oplus m}$. У силу ізоморфності, F матиме базис $\{\varphi(\underline{e}_1), \dots, \varphi(\underline{e}_m)\}$ – це неважко показати.

$\boxed{\Leftarrow}$ Дано: F має базис $\{x_1, \dots, x_m\}$.
Розглянемо відображення $\varphi\colon R^{\oplus m} \to F$ таким чином:
$\varphi(r_1, \dots, r_m) = r_1x_1 + \dots + r_mx_m$.
Неважко переконатися, що φ – гомоморфізм R-модулів.
Якщо $r \in F$, то тоді r розписується як лінійна комбінація з $\{x_1, \dots, x_m\}$. Отже, φ – сюр'єктивне відображення.
Нехай $\varphi(r_1, \dots, r_m) = \varphi(s_1, \dots, s_m)$, тобто $(r_1 - s_1)x_1 + \dots + (r_m - s_m)x_m = 0$. Оскільки $\{x_1, \dots, x_m\}$ – л.н.з., то звідси $r_1 - s_1 = 0, \dots r_m - s_m = 0 \implies r_1 = s_1, \dots, r_m = s_m$. Отже, φ – ін'єктивне відображення.
Остаточно φ – ізоморфізм, тобто $F \cong R^{\oplus m}$. ■

Example 5.7.8 Абелева група $\mathbb{Z}/_{2\mathbb{Z}}$ не буде вільним $\mathbb{Z}$-модулем.
!Припустимо, що $\mathbb{Z}/_{2\mathbb{Z}}$ має базис. Якщо базис містить два елементи, то там обов'язково існує $\overline{0}$, але це вже автоматично л.з. Тому єдиний кандидат – це базис $\{\overline{1}\}$. Але така система є також л.з., оскільки $2 \cdot \overline{1} = \overline{0}$. Суперечність!

Proposition 5.7.9 Задано $f\colon R^{\oplus m} \to M$ – гомоморфізм R-модулів. Тоді існують елементи $a_1, \dots, a_m \in M$, що $f(r_1, \dots, r_m) = a_1r_1 + \dots + a_mr_m$ (*). У цьому випадку $f(\underline{e}_i) = a_i, i = \overline{1, m}$.
І навпаки, для кожної системи $\{a_1, \dots, a_m\}$ із M існує гомоморфізм $f\colon R^{\oplus m} \to M$, що задовольняє рівності (*).

Proof.
$\boxed{\Rightarrow}$ Дано: $f\colon R^{\oplus m} \to M$ – гомоморфізм R-модулів. Позначимо $a_i = f(\underline{e}_i)$.
$$f(r_1, \dots, r_m) = f(r_1\underline{e}_1 + \dots + r_m\underline{e}_m) = \sum_{i=1}^{m} r_i f(\underline{e}_i) = \sum_{i=1}^{m} r_i a_i.$$

$\boxed{\Leftarrow}$ Дано: $\{a_1, \dots, a_m\}$ – система з M. Визначимо $f\colon R^{\oplus m} \to M$ так, щоб $a_i = f(\underline{e}_i)$. Продовжимо f на лінійні комбінації $\underline{e}_1, \dots, \underline{e}_m$ 'по лінійності', тобто
$f(r_1, \dots, r_m) \overset{\text{def.}}{=} r_1a_1 + \dots + r_ma_m$.
Дане відображення коректне, бо $\{\underline{e}_1, \dots, \underline{e}_m\}$ – базис $R^{\oplus m}$. Неважко переконатися, що f задає R-гомоморфізм. ■

Remark 5.7.10 Твердження вище працює лише для вільних модулів.

Example 5.7.11 Маємо $f\colon \mathbb{Z}/_{2\mathbb{Z}} \to M$ – якийсь гомоморфізм $\mathbb{Z}$-модулів. Звідси $f(\overline{0}) = 0$, залишається визначити $f(\overline{1})$. Але нам відомо, що $0 = f(\overline{1} + \overline{1}) = f(2 \cdot \overline{1}) = 2f(\overline{1})$. Значить, із цього обов'язково випливає, що $f(\overline{1}) = 0$. Тобто $f(\overline{1})$ ми не можемо вибрати довільним чином, щоб задати гомоморфізм.

Corollary 5.7.12 Задано $f\colon R^{\oplus n} \to R^{\oplus m}$ – гомоморфізм вільних R-модулів. Тоді існує матриця $A \in \mathrm{Mat}_{m\times n}(R)$, для якої $f(\underline{r}) = A \cdot \underline{r}$ (**). Для матриці A j-ому стовпчику відповідає $f(\underline{e}_j)$.
І навпаки, кожна матриця $A \in \mathrm{Mat}_{m\times n}(R)$ визначає якийсь гомоморфізм $f\colon R^{\oplus n} \to R^{\oplus m}$ рівністю (**).

Proof.
Нехай задано $f\colon R^{\oplus n} \to R^{\oplus m}$ – гомоморфізм вільних R-модулів. Оберемо $\{\underline{e}_1, \dots, \underline{e}_n\}$ – канонічний базис $R^{\oplus n}$. Тоді звідси $f(\underline{e}_j) = (a_{1j}, \dots, a_{mj})$. Запишемо ці образи в вигляді стовпчиків, тобто $f(\underline{e}_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$. У результати, зберемо всі стовпчики, щоб утворити матрицю

$$A = \begin{pmatrix} f(\underline{e}_1) & \dots & \underline{e}_m \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

Звідси й отримаємо рівність $f(\underline{r}) = A \cdot \underline{r}$.

Навпаки, якщо маємо матрицю $A \in \mathrm{Mat}_{m\times n}(R)$, то система стовпчиків матриці A з $R^{\oplus m}$ утворює гомоморфізм $f\colon R^{\oplus n} \to R^{\oplus m}$, що задовольняє $f(\underline{r}) = A \cdot \underline{r}$. ■

Example 5.7.13 Розглянемо матрицю $A \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$ таким чином:
$A = \begin{pmatrix} -4 & 1 & 7 \\ -2 & 0 & 4 \end{pmatrix}$.
Вона відповідає гомоморфізму $\mathbb{Z}$-модулів $f\colon \mathbb{Z}^{\oplus 3} \to \mathbb{Z}^{\oplus 2}$ такому, що

$$f\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -4 \\ -2 \end{pmatrix},\ f\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ f\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}.$$

Proposition 5.7.14 Задані $f\colon R^{\oplus n} \to R^{\oplus m}$ та $g\colon R^{\oplus m} \to R^{\oplus l}$ – R-лінійні відображення. Скажімо, f відповідає матриця $A \in \mathrm{Mat}_{m\times n}(R)$ та g відповідає матриця $B \in \mathrm{Mat}_{l\times m}(R)$. Тоді $g \circ f$ (що теж R-лінійне) відповідає матриця $BA \in \mathrm{Mat}_{l\times n}(R)$.

Proof.
Дійсно, $(g \circ f)(\underline{r}) = g(f(\underline{r})) = g(A\underline{r}) = B \cdot (A\underline{r}) \overset{!}{=} (BA) \cdot \underline{r}$. ■

Remark 5.7.15 Я тут неявно скористався $\overset{!}{=}$ – асоціативністю з елементом $\underline{r} \in R^{\oplus n}$. Це спокійно можна довести окремо.

У нас у лінійній алгебрі були такі матриці, що відповідали елементарним перетворенням. Таку саму штуку можна зробити для модулів.
Маємо $h\colon R^{\oplus m} \to R^{\oplus m}$, якій відповідає матриця $H \in \mathrm{Mat}_{m\times m}(R)$.
I. H отримана з одиничної матриці I заміною i-го елемента на головній діагоналлі на оборотний елемент $u \in R$. Тобто $H = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & u & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 \end{pmatrix}$. Тоді $H \cdot A$ (та $A \cdot H$) – це матриця A, де до i-го рядка (стовпчика) домножуються елементи $u \in R$.

II. H отримана з одиничної матриці I додаванням i-го стовпчика, що помножений на $r \in R$.
Тоді $H \cdot A$ (та $A \cdot H$) – це матриця A, де до i-го рядка (стовпчика), що помножений на $r \in R$, додається j-ий рядок (стовпчик).

III. H отримана з одиничної матриці I перестановкою i-го та j-го рядків.
Тоді $H \cdot A$ (та $A \cdot H$) – це матриця A, де i-ий та j-ий рядки (стовпчики) помінялися місцями.

Definition 5.7.16 Дві матриці $A, A' \in \mathrm{Mat}_{m\times n}(R)$ називаються **подібними**, якщо

$$\exists P \in GL_m(R), \exists Q \in GL_n(R) : A' = PAQ$$

Remark 5.7.17 Подібність двох матриць задає відношення еквівалентності.

Елементарні перетворення матриці

Маємо матрицю $A \in \mathrm{Mat}_{m\times m}(R)$. Аналогічно, як було в лінійній алгебрі, у нас будуть три основних елементарних перетворення, що описується матрицею $H \in \mathrm{Mat}_{m\times m}(R)$.
1. Матриця H, що була отримана з одиничної матриці I перестановкою стовпчиків (або рядків, не суть).
На прикладі маємо матрицю $H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, переставили другий та третій стовпчики (або рядки). У результаті матриця A зміниться таким чином:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{13} & a_{12} \\ a_{21} & a_{23} & a_{22} \\ a_{31} & a_{33} & a_{32} \end{pmatrix}$$

2. Матриця H, що була отримана з одиничної матриці I заміною i-го елемента головній діагоналлі на елемент $u \in R^\times$.
На прикладі маємо матрицю $H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & 1 \end{pmatrix}$, де $u \in R^\times$. У результаті матриця A зміниться таким чином:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ u\cdot a_{21} & u\cdot a_{22} & u\cdot a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & u\cdot a_{12} & a_{13} \\ a_{21} & u\cdot a_{22} & a_{23} \\ a_{31} & u\cdot a_{32} & a_{33} \end{pmatrix}$$

Ми вимагаємо оборотність, щоб можна було скоротити рядок на елемент.

3. Матриця H, що була отримана з одиничної матриці I додаванням одного стовпчика (або рядка) на інший, що помножений на ненульовий елемент $u \in R$.
На прикладі маємо матрицю $H = \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, до третього стовпчика додали перший, що помножений на $u \in R$. У результаті матриця A зміниться таким чином:

$$\begin{pmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11}+u\cdot a_{31} & a_{12}+u\cdot a_{32} & a_{13}+u\cdot a_{33} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & u\cdot a_{11}+a_{13} \\ a_{21} & a_{22} & u\cdot a_{21}+a_{23} \\ a_{31} & a_{32} & u\cdot a_{31}+a_{33} \end{pmatrix}$$

Всі елементарні перетворення є оборотними матрицями.

1. $H^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ 2. $H^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ 3. $H^{-1} = \begin{pmatrix} 1 & 0 & -u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

5.8 Скінченно породжені (ще раз) та скінченно представлені модулі

Definition 5.8.1 Послідовність з R-модулів та R-лінійних відображень

$$\ldots \xrightarrow{f_{i+2}} M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \ldots$$

називається **точною в члені** M_i, якщо $\operatorname{Im} f_{i+1} = \ker f_i$.
Послідовність називається **точною**, якщо вона точною в кожному члені, для якого це має сенс (у який входить одна зі стрілок і з якого виходить одна зі стрілок).

Example 5.8.2 Ланцюг $M \xrightarrow{f} N \xrightarrow{p} \{0\}$ буде точним $\iff$ f – сюр'єктивне відображення.
Випливає з того, що $\ker p = N$.

Example 5.8.3 Ланцюг $\{0\} \xrightarrow{p} L \xrightarrow{g} M$ буде точним $\iff$ g – ін'єктивне відображення.
Вказівка: відомо, що g *– ін'єктивне* $\iff \ker g = \{0\}$.

Example 5.8.4 Короткою точною послідовністю називають точну послідовність такої форми:

$$\{0\} \xrightarrow{p_1} L \xrightarrow{g} M \xrightarrow{f} N \xrightarrow{p_2} \{0\}$$

Ми тіпа зараз склеїли два ланцюги з попередніх прикладів. Особливість тут така, що $N \cong M/_L$. Дійсно, g – ін'єктивне відображення, тож $L \cong L/_{\ker g} = L/_{\{0\}} \cong \operatorname{Im} g$. Також f – сюр'єктивне, тому $N \cong M/_{\ker f}$. Але $N \cong M/_{\ker f} = M/_{\operatorname{Im} g} \cong M/_L$.

Якщо гомоморфізм R-модулів $f\colon M \to N$ – сюр'єктивний, маємо коротку точну послідовність
$\{0\} \longrightarrow \ker f \xhookrightarrow{\imath} M \xrightarrow{f} N \longrightarrow \{0\}$

Definition 5.8.5 Задано $f\colon M \to N$ – гомоморфізм R-модулів.
Коядром f називається фактормодуль:

$$\operatorname{coker} f \stackrel{\text{def.}}{=} N/_{\operatorname{Im} f}$$

Тоді наступна послідовність буде також точною:
$\{0\} \longrightarrow \ker f \xhookrightarrow{\imath} M \xrightarrow{f} N \xrightarrow{\pi} \operatorname{coker} f \longrightarrow \{0\}$
У цьому випадку $\imath$ – вкладення, π – проєкція.
Тобто коядро дозволяє побудувати точну послідовність для несюр'єктивних відображень.

Definition 5.8.6 Задано M – модуль над R.
Модуль називається **скінченно породженим**, якщо існують вільний R-модуль $R^{\oplus m}$ скінченного рангу та точна послідовність

$$R^{\oplus m} \longrightarrow M \longrightarrow \{0\}$$

Remark 5.8.7 Це друге означення скінченно породженого модуля, але в термінах ланцюгів. Переконаємось, що це еквівалентні.

Proof.
$\boxed{\Rightarrow}$ Дано: M – скінченно породжений (перше означення), тобто $M = \langle r_1, \dots, r_m \rangle$. Із цих елементів, за **Prp. 5.7.9**, існує гомоморфізм $f\colon R^{\oplus m} \to M$, причому це буде сюр'єктивний. Далі, за **Ex. 5.8.2**, приходимо до другого означення.

$\boxed{\Leftarrow}$ Дано: M – скінченно породжений (друге означення), тобто маємо ланцюг $R^{\oplus m} \longrightarrow M \longrightarrow \{0\}$.
Звідси випливає, що $f\colon R^{\oplus m} \to M$ – сюр'єктивний гомоморфізм за **Ex. 5.8.2**. А за **Prp. 5.7.9**, існують елементи $a_1, \dots, a_m \in M$, для яких $f(r_1, \dots, r_m) = a_1 r_1 + \dots + a_m r_m$ для всіх $(r_1, \dots, r_m) \in R^{\oplus m}$. Але $\langle a_1, \dots, a_m \rangle = M$ – отримали ми перше означення. ■

Definition 5.8.8 Задано M – модуль над R.
Модуль називається **скінченно представленим**, якщо існують вільні R-модулі $R^{\oplus m}$ та $R^{\oplus n}$ скінченного рангу і точна послідовність

$$R^{\oplus n} \longrightarrow R^{\oplus m} \longrightarrow M \longrightarrow \{0\}$$

Remark 5.8.9 Скінченно представлені модулі автоматично скінченно породжені. Навпаки – ні, але про це пізніше.

Proposition 5.8.10 Задано M – модуль над R.
M – скінченно представлений $\iff M \cong \operatorname{coker} f$,
де $f\colon R^{\oplus n} \to R^{\oplus m}$ – гомоморфізм.

Proof.

$\boxed{\Rightarrow}$ Дано: M – скінченно представлений R-модуль, тобто існує ланцюг $R^{\oplus n} \xrightarrow{f} R^{\oplus m} \xrightarrow{\pi} M \longrightarrow \{0\}$.
Відображення π – сюр'єктивне (див. **Prp. 5.7.9**), тож за I теоремою про ізоморфізм,
$M \cong R^{\oplus m}/_{\ker \pi} = R^{\oplus m}/_{\operatorname{Im} f} = \operatorname{coker} f$.

$\boxed{\Leftarrow}$ Дано: $M \cong \operatorname{coker} f$, де $f\colon R^{\oplus n} \to R^{\oplus m}$ – гомоморфізм. Тобто маємо $M \cong R^{\oplus m}/_{\operatorname{Im} f}$, а звідти ізоморфізм g. Можемо побудувати гомоморфізм $g \circ \pi\colon R^{\oplus m} \to M$, що є сюр'єктивним. Тоді в нас є ланцюг $R^{\oplus n} \xrightarrow{f} R^{\oplus m} \xrightarrow{g\circ\pi} M \longrightarrow \{0\}$, причому $\operatorname{Im} f = \ker(g \circ \pi)$.
Щоб переконатися в рівності, треба просто розписати $\ker(g \circ \pi)$. ■

Remark 5.8.11 За наслідком **Crl. 5.7.12**, гомоморфізм f визначається матрицею $A \in \operatorname{Mat}_{m\times n}(R)$. Виявляється, знаючи матрицю A, можна підрахувати скінченно представлений модуль M (тобто визначити такий модуль).

Example 5.8.12 Маємо $A = \begin{pmatrix} 4 & 1 & 7 \\ -2 & 0 & 4 \end{pmatrix}$ з минулого прикладу. Вона визначає повний скінченно представлений $\mathbb{Z}$-модуль, що є коядром відповідного гомоморфізму $\mathbb{Z}$-модулів $f\colon \mathbb{Z}^{\oplus 3} \to \mathbb{Z}^{\oplus 2}$.

Proposition 5.8.13 Задані $f\colon M \to N$ та $f'\colon M' \to N'$ – гомоморфізми R-модулів. Нехай існують $\varphi\colon M' \to M$ та $\psi\colon N \to N'$ – ізоморфізми R-модулів, щоб $f' = \psi \circ f \circ \varphi$.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\varphi}\uparrow{\scriptstyle\simeq} & & \downarrow{\scriptstyle\simeq}{\scriptstyle\psi} \\ M' & \xrightarrow{f'} & N' \end{array}$$

Тоді $\operatorname{coker} f \cong \operatorname{coker} f'$.

Proof.
Перепишемо (точніше розширимо) діаграму інакшим чином:

$$\begin{array}{ccccccc} M & \xrightarrow{f} & N & \xrightarrow{\pi} & \operatorname{coker} f & \longrightarrow & \{0\} \\ \downarrow{\scriptstyle\simeq}{\scriptstyle\varphi^{-1}} & & \downarrow{\scriptstyle\simeq}{\scriptstyle\psi} & & & & \\ M' & \xrightarrow{f'} & N' & \xrightarrow{\pi'} & \operatorname{coker} f' & \longrightarrow & \{0\} \end{array}$$

Зауважимо, що $\pi' \circ \psi$ – сюр'єктивний гомоморфізм (як композиція). Знайдемо ядро:
$\ker(\pi' \circ \psi) = (\pi' \circ \psi)^{-1}(\{0\}) = \psi^{-1}(\pi'^{-1}(\{0\})) = \psi^{-1}(\ker \pi') = \psi^{-1}(f'(M')) = \psi^{-1}(f'(\varphi^{-1}(M))) = (\psi^{-1} \circ f' \circ \varphi^{-1}) = f(M) = \ker \pi$.
За I теореою про ізоморфізм, отримаємо бажане:
$\operatorname{coker} f' \cong N/_{\ker(\pi'\circ\psi)} = N/_{\ker \pi} = N/_{\operatorname{Im} f} = \operatorname{coker} f$. ■

Corollary 5.8.14 Задано M – R-модуль, що визначається матрицею $A \in \operatorname{Mat}_{m\times n}(R)$. Нехай A' – подібна до матриці A та M' – R-модуль, що визначена цією матрицею. Тоді $M' \cong M$.

Proof.
Маємо $A' = PAQ$, де $P \in GL_m(R), Q \in GL_n(R)$. Нехай f, f', ϕ, ψ – гомоморфізми вільних R-модулів, які визначаються відповідно матрицями A, A', P, Q. Маємо таку діаграму:

$$\begin{array}{ccc} R^{\oplus n} & \xrightarrow{f} & R^{\oplus n} \\ {\scriptstyle\varphi}\uparrow{\scriptstyle\simeq} & & \downarrow{\scriptstyle\simeq}{\scriptstyle\psi} \\ R^{\oplus m} & \xrightarrow{f'} & R^{\oplus m} \end{array}$$

Тоді $M \cong \operatorname{coker} f$ та $M' \cong \operatorname{coker} f'$ за умовою. Але
$M \cong \operatorname{coker} f \cong \operatorname{coker} f' \cong M'$. ■

Remark 5.8.15 Отже, ми можемо над матрицею застосовувати елементарні перетворення щоб отримати якийсь інший ізоморфний скінченно представлений модуль.

Example 5.8.16 Розглянемо матрицю $A = \begin{pmatrix} -4 & 1 & 7 \\ -2 & 0 & 4 \end{pmatrix}$, що визначає $\mathbb{Z}$.

Застосовуючи до A елементарні перетворення рядків та стовпчиків, зведемо її до найбільш простого виду. Отримана матриця – подібна до A.

$A = \begin{pmatrix} -4 & 1 & 7 \\ -2 & 0 & 4 \end{pmatrix} \overset{(\vec{1})-2(\vec{2})}{\sim} \begin{pmatrix} 0 & 1 & -1 \\ -2 & 0 & 4 \end{pmatrix} \overset{\downarrow}{(3)}+2\overset{\downarrow}{(1)} \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 0 \end{pmatrix} \overset{\downarrow}{(3)}+\overset{\downarrow}{(2)}$

$\sim \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix} \overset{\downarrow}{(1)} \leftrightarrow \overset{\downarrow}{(2)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = A'.$

Матриця A' визначає гомоморфізм $f' \colon \mathbb{Z}^{\oplus 3} \to \mathbb{Z}^{\oplus 2}$. Знайдемо коядро.

Зауважимо, що $f'(\underline{e}_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $f'(\underline{e}_2) = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$. Звідси неважко переконатися, що $\operatorname{Im} f' = (f'(\underline{e}_1)) + (f'(\underline{e}_2))$.

Але $(f'(\underline{e}_1)) = \mathbb{Z}$, також $(f'(\underline{e}_2)) = 2\mathbb{Z}$.

Отже, $\operatorname{coker} f' = (\mathbb{Z} \oplus \mathbb{Z})/_{\mathbb{Z} \oplus 2\mathbb{Z}} \cong \mathbb{Z}/_{\mathbb{Z}} \oplus \mathbb{Z}/_{2\mathbb{Z}} \cong \mathbb{Z}/_{2\mathbb{Z}}$.

Якщо M є R-модулем, що визначається матрицею A, то тоді $M \cong \mathbb{Z}/_{2\mathbb{Z}}$.

Definition 5.8.17 Кільце R називається **ньотеровим**, якщо для кожної зростаючої послідовності ідеалів

$$I_1 \subset I_2 \subset \dots$$

існує $n > 0$, для якого $I_n = I_{n+1} = \dots$ (походить назва від математикині Еммі Ньотер).

Example 5.8.18 Зокрема будь-яка ОГІ – ньотерове кільце.

Proposition 5.8.19 Кільце R – ньотерове $\iff$ кожний ідеал кільця R – скінченно породжений.

Proof.

$\boxed{\Rightarrow}$ Дано: R – ньотерове та нехай I – ідеал R.

!Припустимо, що I – не є скінченно породженим. Позначимо $I_0 = (0)$ та $I_n = I_{n-1} + (r_n)$ для $n > 0$, де елемент $r_n \in I \setminus I_{n-1}$. Зауважимо, що $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ Ніде не виконується рівність, бо на $I_n \subset I_{n+1} = I_n + (r_{n+1})$ елемент r_{n+1} лежить в I_{n+1}, але ми обирали $r_{n+1} \in I \setminus I_n$, тобто $r_{n+1} \notin I_n$. Зауважимо також, що $I \setminus I_n = I \setminus (r_1, \dots, r_n) \neq \emptyset$ при всіх $n \geq 1$ (тому вище міркування легітимні), бо якби так, то було б $I \subset (r_1, \dots, r_n)$, а також в силу того, що $r_1, \dots, r_n \in I$, мали б $(r_1, \dots, r_n) \subset I$ – тобто це суперечило б припущенню.

Висновок: отримали строго зростаючий ланцюг – суперечність за ньотеровістю!

$\boxed{\Leftarrow}$ Дано: кожний ідеал кільця R – скінченно породжений. Нехай $I_1 \subset I_2 \subset \dots$ – зростаюча послідовність ідеалів. Розглянемо ідеал $I = \bigcup_{i=1}^{\infty} I_i$ (уже доводилось, що це ідеал), який також скінченно породжений. Тобто $I = (r_1, \dots, r_k)$. Значить, $x \in (r_1, \dots, r_k) \implies x \in I \implies \exists m_0 : x \in I_{m_0}$. Тобто $(r_1, \dots, r_k) \subset I_{m_0} \subset I_{m_0+1} \subset \dots \subset I = (r_1, \dots, r_k)$. Отже, $I_{m_0} = I_{m_0+1} = \dots$

Тим самим, R – ньотерове кільце

(схоже доведення з цим, що ОГІ – ньотерове кільце). ■

Theorem 5.8.20 Маємо R – ньотерове кільце. Тоді кожен скінченно породжений R-модуль буде скінченно представленим.

Доведення даної теореми розіб'ємо на кілька важливих лем.

Lemma 5.8.21 Маємо $\{0\} \longrightarrow L \xrightarrow{j} M \xrightarrow{\pi} N \longrightarrow \{0\}$ – точна послідовність R-модулів. Відомо, що L, N – скінченно породжені. Тоді M – також скінченно породжена.

Proof.

Маємо $L = \langle l_1, \dots, l_s \rangle$ та $N = \langle n_1, \dots, n_t \rangle$. Із ланцюга видно, що π – сюр'єктивне, то звідси для кожного n_i існує $m_i \in M : \pi(m_i) = n_i$. Також j – ін'єктивне, тому ми можемо L ототожнити з $j(L)$, що є підмодулем M, та вважати, що $l_1, \dots, l_s \in M$.

Хочемо довести, що $M = \langle l_1, \dots, l_s, m_1, \dots, m_t \rangle$.
Нехай $m \in M$, тоді $\pi(m) \in N$, а тому звідси
$\pi(m) = r_1 n_1 + \dots + r_t n_t$.
Розглянемо елемент $m - r_1 m_1 - \dots - r_t n_t \in M$. Тоді
$\pi(m - r_1 m_1 - \dots - r_t n_t) = \pi(m) - r_1 n_1 - \dots - r_t n_t = 0$.
Значить, $m - r_1 m_1 - \dots - r_t n_t \in \ker \pi$. Але з ланцюга відомо, що $\ker \pi = \operatorname{Im} j = L$. Із цього випливає
$m - r_1 m_1 - \dots - r_t n_t = r'_1 l_1 + \dots + r'_s l_s$.
$m = r_1 m_1 + \dots + r_t n_t + r'_1 l_1 + \dots + r'_s l_s$.
Це схоже на доведення твердження з лінійної алгебри, що для лінійного оператора A маємо $\dim \ker A + \dim \operatorname{Im} A = \dim L$. ■

Lemma 5.8.22 Маємо R – ньотерове кільце. Тоді для кожного $m \geq 0$ кожен підмодуль модуля $R^{\oplus m}$ – скінченно породжений.

Proof.
База індукції: $m = 0$ – тривіально виконується, при $m = 1$ випливає з означення ньотерових кілець. Просто тому що якщо $F \subset R$ – підмодуль, то F уже є ідеалом. За еквівалентним означенням ньотерового кільця, даний ідеал – скінченно породжений.
Припущення індукції: нехай для всіх $k < m$ лема виконується. Тобто всі підмодулі модуля $R^{\oplus k}$ скінченно породжені.
Крок індукції: ми розглянемо $R^{\oplus m}$ під кутом множини $R^{\oplus(m-1)} \oplus R$. Визначимо два гомоморфізми:
$j \colon R^{\oplus(m-1)} \to R^{\oplus m} \qquad j(r_1, \dots, r_{m-1}) = (r_1, \dots, r_{m-1}, 0)$ – ін'єктивний;
$\pi \colon R^{\oplus m} \to R \qquad \pi(r_1, \dots, r_m) = r_m$ – сюр'єктивний.
Ми використовуємо j, щоб $R^{\oplus(m-1)}$ ототожнити з підмодулем $j(R^{\oplus(m-1)}) = R^{\oplus(m-1)} \times \{0\} = F$ модуля $R^{\oplus m}$. Більш того, π – проєкція, яка сюр'єктивна, а звідси $R^{\oplus m}/_F \cong R$ за першою теоремою про ізоморфізм.
Нехай M – підмодуль $R^{\oplus m}$. Маємо точну коротку послідовність:

$$\{0\} \longrightarrow M \cap F \longrightarrow M \longrightarrow M/_{M \cap F} \longrightarrow \{0\}$$

(тут $M \cap F \to M$ між ними вкладення та $M \to M/_{M \cap F}$ – проєкція, а тому тут ін'єктивність та сюр'єктивність відповідно). $M \cap F$ є скінченно породженим, тому що це підмодуль $F \cong R^{\oplus(m-1)}$ та всі підмодулі $R^{\oplus(m-1)}$ скінченно породжені за припущенням. Але з іншого боку, за II теоремою про ізоморфізм, $M/_{M \cap F} \cong (M + F)/_F$. Зауважимо, що $M + F$ – це підмодуль $R^{\oplus m}$, тому на $(M + F)/_F$ можна дивитися як на підмодуль модуля $R^{\oplus m}/_F \cong R$ (за відповідністю). Цей модуль скінченно породжений, бо R – ньотерове кільце за припущенням. Далі застосовуємо попередню лему, доводячи M – скінченно породжений. ■

Тепер доведемо теорему, яка була вище.

Proof.
Нехай M – скінченно породжений R-модуль. Тобто існує сюр'єктивний гомоморфізм $f \colon R^{\oplus m} \to M$. Зауважимо, що $\ker f$ – підмодуль $R^{\oplus m}$. Значить, за другою лемою, $\ker f$ – скінченно породжений модуль. Отже, існує сюр'єктивний гомоморфізм $g_0 \colon R^{\oplus n} \to \ker f$. Установимо вкладення $\imath \colon \ker f \to R^{\oplus m}$. Тоді $g \overset{\text{def.}}{=} \imath \circ g_0 \colon R^{\oplus n} \to R^{\oplus m}$ – гомоморфізм модулів, де $\operatorname{Im} g = \ker f$. Внаслідок сказаного маємо точну послідовність модулів:

$$R^{\oplus n} \xrightarrow{\ g\ } R^{\oplus m} \xrightarrow{\ f\ } M \longrightarrow \{0\}$$

А це в точності означає, що M – скінченно представлений. ■

5.9 Зв'язок із векторними просторами

Theorem 5.9.1 Скінченно породжені векторні простори над полем k – вільні k-модулі.
Тобто якщо V – скінченний векторний простір над k, тоді $V \cong k^{\oplus d}$.
У цьому контексті, $d = \dim V$.

Remark 5.9.2 Також, насправді, дана теорема пацює для нескінченно вимірних векторних просторів

Доведення цієї теореми буде після однієї леми.

Lemma 5.9.3 Маємо k – поле та $A \in \mathrm{Mat}_{m\times n}(k)$ – матриця. Тоді, завдяки елементарним перетворенням рядків та стовпчиків, матрицю можна звести до такого вигляду: $\left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array}\right)$. Тут $I_r \in \mathrm{Mat}_{r\times r}(k)$ – одинична матриця, де $0 \le r \le \min(m,n)$. Це число ніщо інше, як ранг матриці A.

Proof.
Якщо $A = O$, то тоді матриця A задовольняє лему. Вважатимемо надалі, що $A \neq O$. Доведення буде за MI по $\min(m,n)$.
База індукції: $\min(m,n) = 1$, тоді A – або рядок, або стовпчик. Оберемо перший варіант (другий аналогічно). Оскільки A ненульова, то ми переставимо елементи так, щоб на a_{11} був ненульовий елемент. А далі домножимо рядок на a_{11}^{-1} – уже буде рядок $\begin{pmatrix}1 & a_{12} & \dots & a_{1n}\end{pmatrix}$. Далі там, де ненульові елементи, беремо i-ий стовпчик додаємо до 1-го стовпчика помножений на $-a_{1i}$. Виникне $\begin{pmatrix}1 & 0 & \dots & 0\end{pmatrix}$.
Припущення індукції: нехай для $\min(m,n) < s$ лема виконується.
Крок індукції: маємо $\min(m,n) = s$. Оскільки A ненульова, то тоді існує $a_{ij} \neq 0$. Переставимо так рядки та стовпчики, щоб цей елемент був $a_{11} \neq 0$. Домножимо перший рядок на a_{11}^{-1} – і буде $a_{11} = 1$. Далі аналогічно, як в базі, добиваємось того, щоб перший рядок та стовпчик були нулями в інших місцях. Отримаємо матрицю:

$$\tilde{A} = \left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \dots & a_{mn} \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right).$$

Матриця B представляється вже до вигляду $\left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array}\right)$, за припущенням MIm тому що $\min(m-1, n-1) < \min(m,n) = s$. Зауважимо, що елементарні операції над $\tilde{A}$, де беруть участь лише рядки та стопчики, що перетинають матрицю B, не міняють перший рядок та стовпчик матриці $\tilde{A}$. Тому ми зможемо привести до такого ж вигляду, що в лемі. ■

Тепер доведемо нашу теорему.

Proof.
Зауважимо, що V – скінченно представлений векторний простір, тому що поля – ньотерові кільця автоматично. Звідси існують гомоморфізми $g\colon k^n \to k^m$ та $f\colon k^m \to V$, такі, що послідовність

$$k^n \xrightarrow{\ g\ } k^m \xrightarrow{\ f\ } V \longrightarrow \{0\}$$

буде точною. При цьому ще відомо, що $V \cong \operatorname{coker} g = k^m/_{\operatorname{Im} g}$.
Нехай гомоморфізму g відповідає матриця $A \in \mathrm{Mat}\, m \times n(k)$. За лемою вище, матриця A подібна до матриці A' вигляду з леми, що має ранг $0 \le s \le \min(m,n)$.
Нехай $g'\colon k^n \to k^m$ – гомоморфізм, якому відповідає матриця A'. Значить, $V \cong \operatorname{coker} g'$. Підрахуємо це коядро.
$\operatorname{Im} g' = \underbrace{k \oplus \dots \oplus k}_{s \text{ разів}} \oplus \underbrace{0 \oplus \dots \oplus 0}_{m-s \text{ разів}} \subset k^m$.
$\operatorname{coker} g' = k^m/_{\operatorname{Im} g'} = \underbrace{k/_k \oplus \dots \oplus k/_k}_{s \text{ разів}} \oplus \underbrace{k/_0 \oplus \dots \oplus k/_0}_{m-s \text{ разів}} \cong \underbrace{0 \oplus \dots \oplus 0}_{s \text{ разів}} \oplus \underbrace{k \oplus \dots \oplus k}_{m-s \text{ разів}} \cong k^{\oplus(m-s)}$.
Для завершення доведення зауваижмо, що $d = m - s \ge 0$. ■

Example 5.9.4 Нехай скінченно представлений $\mathbb{Q}$-модуль M буде коядром гомоморфізму $g\colon \mathbb{Q}^{\oplus 3} \to \mathbb{Q}^{\oplus 2}$, що задається матрицею $A = \begin{pmatrix}-4 & 1 & 7\\ -2 & 0 & 4\end{pmatrix}$. Підрахуємо M.

$$\begin{pmatrix}-4 & 1 & 7\\ -2 & 0 & 4\end{pmatrix} \overset{-\frac14(\vec1)}{\sim} \begin{pmatrix}1 & -\frac14 & -\frac74\\ -2 & 0 & 4\end{pmatrix} \overset{(\vec2)+2(\vec1)}{\sim} \begin{pmatrix}1 & -\frac14 & -\frac74\\ 0 & -\frac12 & \frac12\end{pmatrix} \overset{\downarrow}{\underset{\downarrow}{(\vec2)+\frac14(\vec1)}} \begin{pmatrix}1 & 0 & -\frac74\\ 0 & -\frac12 & \frac12\end{pmatrix}$$

$$\overset{\downarrow}{\underset{\downarrow}{(\vec3)+\frac74(\vec1)}} \begin{pmatrix}1 & 0 & 0\\ 0 & -\frac12 & \frac12\end{pmatrix} \overset{-2\cdot(\vec2)}{\overset{\downarrow}{\underset{\downarrow}{(\vec3)+(\vec2)}}} \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} = A'.$$

Отже, $M \cong (k \oplus k)/_{k\oplus k} \cong 0$.

5.10 Зв'язок із евклідовими областями

Theorem 5.10.1 Задано M – скінченно породжений модуль над R – евклідова область. Тоді M ізоморфна прямій сумі циклічних модулів. Тобто існують елементи $d_1, \dots, d_s \in R$, де $d_1 \mid d_2 \mid \dots \mid d_s$

та $d_1 \notin R^\times$, а також існує $r \geq 0$, для якого:
$M \cong R^{\oplus r} \oplus (R/_{(d_1)}) \oplus (R/_{(d_2)}) \oplus \cdots \oplus (R/_{(d_s)})$.

Розглянемо дві леми, друга буде дещо схожа з лемою попереднього підрозділу.

Lemma 5.10.2 Маємо $A, A' \in \mathrm{Mat}_{m\times n}(R)$. Нехай A' отримана з A за допомогою елементарних перетворень рядків та стовпчиків. Нехай $\alpha \in R$. Тоді якщо всі елементи матриці A діляться на α, то й всі елементи A' діляться на α.
Вказівка: розглянути основні елементарні перетворення та з'ясувати, чи буде далі ділитися елемент.

Lemma 5.10.3 Задано R – евклідова область та $A \in \mathrm{Mat}_{m\times n}(R)$. Тоді, завдяки елементарним перетворенням рядків та стовпчиків, матрицю можна звести до вигляду: $\left(\begin{array}{cccc|c} d_1 & 0 & \dots & 0 & \\ 0 & d_2 & \dots & 0 & \\ \vdots & \vdots & \ddots & \vdots & O \\ 0 & 0 & \dots & d_s & \\ \hline \multicolumn{4}{c|}{O} & O \end{array}\right)$.

Тут $d_1 \mid d_2 \mid \cdots \mid d_s$. Може бути можливість $s = 0$ – тоді матриця нулева.

Перед доведення леми, хотілося би описати один процес.

Очиста рядка/стовпчика

Мета полягає в тому, щоб $\begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix}$ перетворився елеметарним чином в $\begin{pmatrix} d & 0 & \dots & 0 \end{pmatrix}$. ('очистка' стовпчика має аналогічний процес).
Маємо рядок, причому нехай $a_1 \neq 0$. Розглянемо такі послідовність дій:
I. Всі a_i $(i = \overline{2,n})$ поділимо на a_1 з остачею. Отримаємо $a_i = q_i a_1 + r_i$, причому або $r_i = 0$, або $\mu(r_i) < \mu(a_1)$.
II. До i-го стовпчика додамо 1-ий стовпчик, що помножений на $-q_i a_i$. Тепер буде рядок виглядати як $\begin{pmatrix} a_1 & r_2 \dots & r_n \end{pmatrix}$.
III. Якщо існує $r_i \neq 0$, то міняємо i-ий стовпчик з 1-м стовпчиком. Перепозначимо $r_i = a_1$, а далі повторюємо I.
IV. Якщо маємо $\begin{pmatrix} d & 0 & \dots & 0 \end{pmatrix}$, при $d \neq 0$, очистка завершена.

Даний процес буде скінченним! Число $\nu(a_1) \in \mathbb{N}$ строго зменшується щоразу, коли ми повертаємось від III до I кроку.
Якщо буде матриця, то пілся очистки першого стовпчика можливі дві опції:
- перший стовпчик не змінюється;
- або число $\nu(a_{11})$ зменшується.

Example 5.10.4 Ілюстративно наведемо приклад на $\begin{pmatrix} -4 & 3 & 7 \end{pmatrix}$ в евклідовій області $\mathbb{Z}$.
I. Ділення з остачею:
$1 = 0 \cdot (-4) + 3$
$7 = (-1) \cdot (-4) + 3$
II. Додаємо так, як зазначено на другому кроці – отримаємо $\begin{pmatrix} -4 & 3 & 3 \end{pmatrix}$.
III. Існує елемент $3 \neq 0$, тоді його міняємо з -4 – отримаємо $\begin{pmatrix} 3 & -4 & 3 \end{pmatrix}$.
Повторюючи ті самі кроки I, II, отримаємо $\begin{pmatrix} 3 & -1 & 0 \end{pmatrix}$.
Знову існує $-1 \neq 0$, тому міняємо з 3 місцями – отримаємо $\begin{pmatrix} -1 & 3 & 0 \end{pmatrix}$. Знову через I, II отримаємо $\begin{pmatrix} -1 & 0 & 0 \end{pmatrix}$ – кінець очистки.

Proof.
Якщо $A = O$, то тоді кінець доведення. Тому надалі $A \neq O$. Знову доведення за МІ по $\min(m, n)$.
База індукції: $\min(m, n) = 1$, тоді аналогічно розглянемо рядок матриці A (стовчик так само робиться). Ми переставимо елементи так, щоб $a_{11} \neq 0$. Робимо очистку, як було зазначено вище.
Припущення індукції: нехай для $\min(m, n) < s$ лема виконується.

Крок індукції: маємо $\min(m, n) = s$, знову вважаємо $a_{11} \neq 0$. До матриці A застосуємо таку послідовність перетворень:
(а) очистка 1-го рядка;
(б) очистка 1-го стовпчика;

(в) якщо $a_{1j} \neq 0$ при $j = \overline{2,n}$ (тобто забруднився 1-ий рядок), то повертаємось до (а) (це можливо, просто тому що в алгоритмі очистки стовпчика ми можемо задіяти перший рядок, що поміняється з іншим);
(г) на початку цього кроку $a_{11} \neq 0$, а всі інші елементи 1-го рядка та 1-го стовпчика нулеві. Якщо $\exists a_{ij}$ таке, що $a_{11} \nmid a_{ij}$, то робимо наступне:
- додаємо до 1-го рядка i-ий рядок;
- повертаємось до (а);
(д) на початку цього кроку $a_{11} \neq 0$, всі інші елементи 1-го рядка та 1-го стовпчика нулеві. Якщо $a_{11} \mid a_{ij}$, для всіх $i, j = \overline{2,m}$, то кінець.

Ця послідовність перетворень буде скінченною! Коли ми повертаємось від кроку (в) до (а), це означає, що перед цим на кроці (б) ми змінили 1-й рядок матриці A, тому $\nu(a_{11})$ зменшилося. Якщо ми повернулися від (г) до (а), то маємо в 1-му рядку матриці A елменти a_{ij}, який не ділиться на A. Отже, під час наступного виконання кроку (а) число $\nu(a_{11})$ зменшиться.
Після кроку (д) матриця A матиме вигляд

$$\tilde{A} = \left(\begin{array}{c|ccc} d_1 & 0 & \dots & 0 \\ \hline 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \dots & a_{mn} \end{array}\right) = \left(\begin{array}{c|ccc} d_1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right).$$

Всі елементи матриці B ділться на d_1. За припущенням МІ, B за допомогою елементарних перетворень зводиться до вигляду, як зазначено в лемі. Тоді матриця A звелася до вигляду: $\tilde{\tilde{A}} =$

$$\left(\begin{array}{c|ccc|ccc} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ \hline 0 & d_2 & \dots & 0 & & & \\ \vdots & \vdots & \ddots & \vdots & & O & \\ 0 & 0 & \dots & d_s & & & \\ \hline 0 & & & & & & \\ \vdots & & O & & & O & \\ 0 & & & & & & \end{array}\right).$$

Відомо, що $d_2 \mid d_3 \mid \dots \mid d_s$. Ми знаємо, що всі елементи B діляться на d_1, а тому всі елементи B' (після перетвоорення) діляться на d_1, зокрема $d_1 \mid d_2$. ■

Нарешті, закінчимо цей розділ з доведення основної теореми.

Proof.
Всі евклідові кільця – ОГІ, що є ньотеровими. Тож модуль M буде скінченно представленим, тобто існує точна послідовність

$$R^{\oplus n} \xrightarrow{g} R^{\oplus m} \longrightarrow M \longrightarrow \{0\},$$

у якій g визначається матрицею $A \in \mathrm{Mat}_{m\times n}(R)$. Ми маємо $M \cong \operatorname{coker} g'$, де гомоморфізм $g' \colon R^{\oplus n} \to R^{\oplus m}$ визначається матрицею виду із леми.
$\operatorname{Im} g' = (d_1) \oplus (d_2) \oplus \dots \oplus (d_s) \oplus 0 \oplus \dots \oplus 0 \subset R^{\oplus m}$.
$\operatorname{coker} g' \cong (R/_{(d_1)}) \oplus \dots \oplus (R/_{(d_s)}) + R^{\oplus r}$, причому $d_1 \mid \dots \mid d_s$. Може статися так, що для якогось $k = \overline{1,s}$ елементи d_i оборотні при $i = \overline{1,k}$. Тоді $R/_{(d_i)}$ нульові. Отже, можемо вважати, що d_i необоротний. ■

Definition 5.10.5 Елементи $d_1, \dots, d_s \in R$ із теореми називаються **інваріантними факторами модуля** M. Вони всі визначені з точністю до оборотних елементів.

Абелеві групи як модулі

Ми тепер розглянемо абелеву групу $\langle A, + \rangle$ під призмою модуля над кільцем $\mathbb{Z}$.

Theorem. Задані A, B – абелеві групи та $f\colon A \to B$.
f – гомоморфізм абелевих груп $\iff \forall a, a' \in A : f(a + a') = f(a) + f(a')$.

Proof.
$\boxed{\Rightarrow}$ Дано: f – гомоморфізм абелевих груп, тобто це $\mathbb{Z}$-лінійне відображення між модулями A, B. Тоді автоматично виконується права частина.

$\boxed{\Leftarrow}$ Дано: $\forall a, a' \in A : f(a + a') = f(a) + f(a')$. Доведемо, що це $\mathbb{Z}$-лінійне відображення між модулями A, B.
$f(0a) = f(0) = 0 = 0f(a)$
$f(na) = f(a + \cdots + a) = f(a) + \cdots + f(a) = nf(a),\ n > 0$
$f(-na) = -nf(a),\ n > 0 \implies f(na) = nf(a),\ n < 0.$ ■

Theorem. Задано A – абелева група.
$S \subset A$ – підгрупа $A \iff \forall a_1, a_2 \in S : a_1 - a_2 \in S$ та $S \neq \emptyset$.

Proof.
$\boxed{\Rightarrow}$ Дано: S – підгрупа A, тобто S є підмодулем A над $\mathbb{Z}$. Звідси й випливає замкненість.

$\boxed{\Leftarrow}$ Дано: $\forall a_1, a_2 \in S : a_1 - a_2 \in S$ та $S \neq \emptyset$.
Маємо $a \in S$, тоді звідси $0 = a - a \in S$. Також $\forall b \in S : -b = 0 - b \in S$. Звідси випливає, що $a + b = a - (-b) \in S$. Внаслідок цього $\forall n \in \mathbb{Z} : \forall a \in S : na \in S$. Значить, S – підмодуль A, тому є підгрупою. ■

Theorem. Існує єдина циклічна група нескінченного порядку, яка ізоморфна $\mathbb{Z}$. Також для кожного $n > 0$ існує єдина циклічна група порядку n, яка ізоморфна $\mathbb{Z}/_{n\mathbb{Z}}$.

Proof.
Розглянемо відображення $\varphi\colon \mathbb{Z} \to G$ як $\varphi(n) = ng$. Ми вже показували, що це – $\mathbb{Z}$-лінійне відображення, тож це гомоморфізм абелевих груп. Оскільки $G = [\varphi(1)]$, то відображення φ – сюр'єктивне.
$\ker \varphi = \{0\} \implies G \cong \mathbb{Z}$ (φ – ізоморфізм);
$\ker \varphi \neq \{0\}$, тоді це підмодуль $\mathbb{Z}$-модуля $\mathbb{Z}$, а тому $\ker \varphi$ – ідеал кільця $\mathbb{Z}$. Але $\mathbb{Z}$ – область головних ідеалів, тому $\ker \varphi = n\mathbb{Z}, n > 0$. Значить, $G \cong \mathbb{Z}/_{n\mathbb{Z}}$ за першою теоремою про ізоморфізм. ■

Proposition. Нескінченна циклічна група $\mathbb{Z}$ має твірні $1, -1$. Циклічна група $\mathbb{Z}/_{n\mathbb{Z}}$ має $\varphi(n)$ твірних.
$\overline{a}$ породжує $\mathbb{Z}/_{n\mathbb{Z}} \iff \gcd(a, n) = 1$.

Proof.
Маємо $\mathbb{Z} = [d]$, тобто звідси $1 = kd$. Тому або $d = 1$, або $d = -1$.
Маємо $\mathbb{Z}/_{n\mathbb{Z}} = [\overline{d}]$, тоді звідси $\overline{1} = k\overline{d} = \overline{kd} = \overline{kd}$. Внаслідок цього $\overline{d} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$. У зворотний бік нехай $\overline{d} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$, тоді звідси $\overline{1} = \overline{bd}$. Тоді
$\overline{c} = \overline{c}\overline{1} = \overline{c}\overline{bd} = \overline{cbd} = \overline{(bd)d} = cb\overline{d}$.
Отже, $[\overline{d}] = \mathbb{Z}/_{n\mathbb{Z}}$. ■

Класифікація скінченних абелевих груп

Definition. Нехай A – абелева група та p – просте число.
p-компонентою групи A називається множина

$$A_p = \{a \in A \mid \exists k \in \mathbb{N} : p^k a = 0\}$$

Зрозуміло, що A_p задає підгрупу A.

Theorem. Задано A – скінченна абелева група. Тоді існують цілі числа $1 < d_1, d_2, \ldots, d_s$, для яких $d_1 \mid d_2 \mid \cdots \mid d_s$, а також $A \cong C_{d_1} \oplus \cdots \oplus C_{d_s}$.
Еквівалентно кажучи, існують прості числа $p_1, \ldots, p_r$ та цілі $\alpha_{ij} > 0$ такі, що $A \cong \bigoplus\limits_{i,j} \left(\mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}\right)$

Числа $d_1, \dots, d_s$ в цьому випадку називаються **інваріантними множниками групи** A.
Числа $p_i^{\alpha_{ij}}$ в цьому випадку називаються **елементарними дільниками групи** A

Proof.
Оскільки скінченна абелева група – скінченно породжений модуль над евклідовим кільцем $\mathbb{Z}$, то звідси $A \cong C_{d_1} \oplus \dots \oplus C_{d_s}$ із теорії модулів.
Друге представлення випливає з наслідка, також з теорії модулів (це дозволило із першого перейти в другу репрезентацію).

Доведемо, що з другого представлення випливає перше представлення.
При фіксованому $i = \overline{1,r}$ маємо $\bigoplus\limits_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$, кількість α може відрізнятися в залежності від i. Спочатку переставимо ці групи в сумі так, щоб $\alpha_{ij} \le \alpha_{i,j+1}$. Оберемо s – найбільша кількість α серед всіх i.
Для кожного $i = \overline{1,r}$ доповнимо послідовність (α_{ij}) зліва нулями стільки, щоб довжина послідовності була s. Отримаємо послідовність $\alpha_i = (0, \dots, 0, \alpha_{i1}, \alpha_{12}, \dots) \overset{\text{позн.}}{=} (a_{i1}, \dots, a_{is})$.
Всі ці рядки запишемо в матрицю

$$D = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rs} \end{pmatrix}.$$

Позначимо $d_j = p_1^{a_{1j}} p_2^{a_{2j}} \dots p_r^{a_{rj}}$, а також $A_j = \bigoplus\limits_{i=1}^{r} \mathbb{Z}/_{p_i^{a_{ij}}\mathbb{Z}}$. Оскільки всі числа p_k попарно взаємно прості (за умовою), то $A_j \cong \mathbb{Z}/_{d_j\mathbb{Z}} \cong C_{d_j}$. Зауважимо, що

$$\bigoplus_{j=1}^{s} \mathbb{Z}/_{p_i^{a_{ij}}\mathbb{Z}} = 0 \oplus \dots \oplus 0 \oplus \bigoplus_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}} = \bigoplus_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}.$$

Нульові доданки відповідають тим нулям, які ми додали до рядків.

$$A \cong \bigoplus_i \bigoplus_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}} = \bigoplus_{i=1}^{r} \bigoplus_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}} = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} \mathbb{Z}/_{p_i^{a_{ij}}\mathbb{Z}} = \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{r} \mathbb{Z}/_{p_i^{a_{ij}}\mathbb{Z}}$$

$$= \bigoplus_{j=1}^{s} A_j \cong \bigoplus_{j=1}^{s} C_{d_j}.$$

Оскільки $a_{ij} \le a_{i,j+1}$, то маємо $d_1 \mid \dots \mid d_s$. ■

Для єдиності репрезентації треба довести кілька лем:

Lemma. Нехай $A \cong \bigoplus\limits_{i,j} \left(\mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}\right)$. Тоді p-компонента $A_{p_i} = \bigoplus\limits_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$.

Proof.
Зауважимо, що $A_p = \{a \in A \mid |a| = p^k \text{ для деякого } k \ge 0\}$. Тобто цю множину можна подати в іншому вигляді.
Дійсно, $a \in A_p$, тоді існує $k \ge 1$, для якого $p^k \cdot a = 0$, звідси $|a| \mid p^k$. Із іншого боку, якщо p^k поділити на $|a|$, то там обов'язково нульова остача, тож $p^k \mid |a|$.

Зауважимо, що $A_{p_i} \supset \bigoplus\limits_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$. Дійсно, якщо $x \in \bigoplus\limits_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$, то тоді $|x| = \operatorname{lcm}_j(|x_j|)$, де кожний $x_j \in \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$. Кожний $|x_j| \mid p_i^{\alpha_{ij}}$, тож звідси $|x| = p^k$ при деякому k.
Навпаки якщо $x \notin \bigoplus\limits_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$, то $|x|$ має простий дільник q, що відмінний від p_i, але тоді $a \notin A_{p_i}$.
Отже, $A_{p_i} \subset \bigoplus\limits_j \mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}$. ■

Lemma. Припустимо, що маємо дві репрезентації, тобто
$A \cong \bigoplus\limits_{i,j} \left(\mathbb{Z}/_{p_i^{\alpha_{ij}}\mathbb{Z}}\right)$, а також $A \cong \bigoplus\limits_{k,l} \left(\mathbb{Z}/_{q_k^{\alpha_{kl}}\mathbb{Z}}\right)$.
Тут $p_1, \dots, p_r$ та $q_1, \dots, q_s$ – прості. Тоді звідси $r = s$, а після перестановки індексів для всіх i, j отримаємо $p_i = q_i, \alpha_{ij} = \beta_{ij}$.

Proof.
TODO: ■

Example 5.10.6

6 Теорія полів

Вступна лемі, які, насправді, є корисними надалі.

Lemma 6.0.1 Задано R, F – відповідно нетривіальне кільце з одиницею та поле. Тоді нетривіальний гомоморфізм кілець $f\colon F \to R$ – ін'єктивний.

Proof.
Зауважимо, що оскільки F – поле, то всі ідеали – тривіальні. Зокрема або $\ker f = \{0\}$, або $\ker f = F$. Якщо обрати другий варіант, то $f(x) = 0_R$ для всіх $x \in F$. А це тривіальний гомоморфізм – неможливо.
Якщо $\ker f = \{0\}$, то тоді f – ін'єктивне. ■

Значить, кожний гомоморфізм $f\colon k \to F$ між двома полями (а там тривіальних гомоморфізмів нема) – ін'єктивний. Тому ми можемо k сприймати як підполе F. Писатимемо це як $k \subset F$.

Lemma 6.0.2 Задано R, S – поля та $f\colon R \to S$ – гомоморфізм. Тоді $f(1_R) = 1_S$.

Proof.
Маємо $r \in R$, тоді звідси $r \cdot r^{-1} = 1_R$. Отже,
$f(1_R) = f(r \cdot r^{-1}) = f(r)f(r^{-1}) = f(r) \cdot (f(r))^{-1} = 1_S$.
Оскільки $r \neq 0$, то тоді $f(r) \neq 0$ в силу того, що наш гомоморфізм – ін'єктивний. ■

6.1 Поле часток області цілісності

Основна мотивація її полягає в наступному спостереженні. У нас є множина цілих чисел $\mathbb{Z}$ – область цілісності та $\mathbb{Q}$ – поле. Якщо повернутися до визначення, то $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$. Виявляється, що $\mathbb{Q}$ – найменше поле, яке містить область цілісності $\mathbb{Z}$.
Це означає (на прикладі) наступне. Якщо ми маємо інше поле $\mathbb{R}$, що є вкладенням $\mathbb{Z} \hookrightarrow \mathbb{R}$, то ми завжди можемо знайти вкладення $\mathbb{Q} \hookrightarrow \mathbb{R}$, тобто $\mathbb{R}$ буде більшим полем, аніж $\mathbb{Q}$.
Зараз ми хочемо узагальнити це все поняття. Спочатку буде конструкція поля часток, яка є аналогічною до конструкції раціональних чисел.

Маємо $\langle R, +, \cdot \rangle$ – область цілісності (зазвичай це вже автоматично ненульове кільце). Маємо множину $\hat{F} = \{(r, s) \in R \times R \mid s \neq 0\}$ та визначимо на ній відношення еквівалентності (неважко довести)

$$(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$$

Розглянемо фактормножину $F = \tilde{F}/_\sim$, на якій визначаться операції $+, \cdot$ таким чином:

$$[(r_1, s_1)] + [(r_2, s_2)] = [(r_1 \cdot s_2 + r_2 \cdot s_1, s_1 \cdot s_2]$$
$$[(r_1, s_1)] \cdot [(r_2, s_2)] = [(r_1 \cdot r_2, s_1 \cdot s_2])$$

Proposition 6.1.1 Вищеописані операції визначені коректно.

Proof.
Доведу лише коректність операції $+$, бо з множенням простіше.
Нехай $[(r_1, s_1)] = [(r_1', s_1')]$ та $[(r_2, s_2)] = [(r_2', s_2')]$. Хочемо довести, що
$[(r_1 s_1 + r_2 s_1, s_1 s_2)] = [(r_1' s_2' + r_2' s_1', s_1' s_2')]$. Тобто $(r_1 s_2 + r_2 s_1)(s_1' s_2') = (r_1' s_2' + r_2' s_1')(s_1 s_2)$.
За умовою, $r_1 s_1' = r_1' s_1$ та $r_2 s_2' = r_2' s_2$. Тоді отримаємо наступне:
$(r_1 s_2 + r_2 s_1)(s_1' s_2') = r_1 s_2 s_1' s_2' + r_2 s_1 s_1' s_2' = r_1 s_1' s_2 s_2' + r_2 s_2' s_1 s_1' =$
$= r_1' s_1 s_2 s_2' + r_2' s_2 s_1 s_1' = r_1' s_2' s_1 s_2 + r_2' s_1' s_1 s_2 = (r_1' s_2' + r_2' s_1')(s_1 s_2)$. ■

Theorem 6.1.2 $\langle F, +, \cdot \rangle$ – поле.

Proof.
Те, що F – кільце, причому комутативне, це дуже легко перевіряється. Єдине зауважу, що нуль кільця буде $[(0, 1)]$. Також зрозуміло, що кільце має одиницю $[(1, 1)]$.
Окремо покажемо, що F – ненульове кільце. Якби $F = \{[(0, 1)]\}$, то тоді отримали б $[(0, 1)] = [(1, 1)]$ (нуль та одиниця в нулевому кільці збігаються). Власне, звідси би отримали $0 \cdot 1 = 1 \cdot 1 \implies 0 = 1$. Але ми припускали, що R – область цілісності, тому це неможливо.
Нехай $[(r, s)] \neq [(0, 1)]$, тоді звідси $r \cdot 1 \neq 0 \cdot s = 0$. Тоді існує елемент $(s, r) \in \hat{F}$, а згодом розглянемо $[(s, r)] \in F$. Тоді $[(r, s)] \cdot [(s, r)] = [(rs, sr)]$. При цьому $rs \cdot 1 = 1 \cdot sr$, тож звідси $(rs, sr) \sim (1, 1)$. Отже, $[(r, s)] \cdot [(s, r)] = [(1, 1)]$. Це доводить те, що F – поле. ■

Надалі буде звичне позначення: $[(r, s)] = \frac{r}{s}$. Звідси ми отримаємо $\frac{r_1}{s_1} = \frac{r_2}{s_2} \iff r_1 \cdot s_2 = r_2 \cdot s_1$.

Definition 6.1.3 Маємо $\langle R, +, \cdot \rangle$ – область цілісності та $\hat{F} = \{(r, s) \in R \times R \mid s \neq 0\}$.
Полем часток області цілісності R називається фактомножина

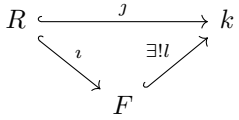
$$F = \hat{F}/_\sim \qquad (r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1,$$

на якій визначаються операції $+, \cdot$ таким чином:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 \cdot r_2}{s_1 \cdot s_2}$$

Remark 6.1.4 Можна визначити ін'єктивний гомоморфізм $\imath \colon R \hookrightarrow F$ як $\imath(r) = \frac{r}{1}$. Значить, R ми можемо сприймати як підкільце поля часток F. (це як кільце $\mathbb{Z}$ сприймати як підкільце $\mathbb{Q}$).

Theorem 6.1.5 Задано R – область цілісності та F – поле часток R. Тоді F – єдине найменше поле, яке містить R.
Математично це звучить так. Нехай k – інше поле, причому існує ін'єктивний гомоморфізм $\jmath\colon R \hookrightarrow k$. Тоді існує єдиний ін'єктивний гомоморфізм $l\colon F \hookrightarrow k$, для якого $\jmath = l \circ \imath$.



Proof.
Побудуємо відображення $l\colon F \to k$ таким чином: $l\left(\frac{r}{s}\right) = \jmath(r)(\jmath(s))^{-1}$.
Оскільки $\jmath$ – ін'єктивне за умовою, то при $s \neq 0 \implies \jmath(s) \neq 0$. Таким чином, $(\jmath(s))^{-1}$ існує, оскільки k – поле. Залишилося переконатися в коректності означення (тут дріб – клас еквівалентності).
Нехай $\frac{r_1}{s_1} = \frac{r_2}{s_2}$, тобто $r_1 s_2 = r_2 s_1$. Тоді отримаємо $\jmath(r_1)\jmath(s_2) = \jmath(r_1 s_2) = \jmath(r_2 s_1) = \jmath(s_2)\jmath(s_1)$. Із цього рівняння випливає $\jmath(r_1)(\jmath(s_1))^{-1} = \jmath(r_2)(\jmath(s_2))^{-1}$. Тобто отримали $l\left(\frac{r_1}{s_1}\right) = l\left(\frac{r_2}{s_2}\right)$.
Доведемо тепер, що l задає гомоморфізм кілець. Дійсно,
$l\left(\frac{r_1}{s_1}\right) + l\left(\frac{r_2}{s_2}\right) = \jmath(r_1)(\jmath(s_1))^{-1} + \jmath(r_2)(\jmath(s_2))^{-1} = \jmath(r_1 s_2)(\jmath(s_1 s_2))^{-1} + \jmath(r_2 s_1)(\jmath(s_1 s_2))^{-1} =$
$= [\jmath(r_1 s_2) + \jmath(r_2 s_1)](\jmath(s_1 s_2))^{-1} = \jmath(r_1 s_2 + r_2 s_1)(\jmath(s_1 s_2))^{-1} = l\left(\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\right) = l\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right)$.
$l\left(\frac{r_1}{s_1}\right) l\left(\frac{r_2}{s_2}\right) = \jmath(r_1)(\jmath(s_1))^{-1}\jmath(r_2)(\jmath(s_2))^{-1} = \jmath(r_1)\jmath(r_2)(\jmath(s_1))^{-1}(\jmath(s_2))^{-1} = \jmath(r_1 r_2)(\jmath(s_1 s_2))^{-1} =$
$= l\left(\frac{r_1 r_2}{s_1 s_2}\right) = l\left(\frac{r_1}{s_1}\frac{r_2}{s_2}\right)$.
l – ін'єктивний, оскільки кожний гомоморфізм із поля в кільце – ін'єктивний. Нарешті,
$l \circ \imath(r) = l\left(\frac{r}{1}\right) = \jmath(r)(\jmath(1))^{-1} = j(r)$ для всіх $r \in R$.
Щодо єдиності. Припустимо, що існує $l\colon F \to k$, що задовольняє умові теореми. Оскільки l – гомоморфізм, то
$l\left(\frac{r}{s}\right) = l\left(\frac{r}{1}\frac{1}{s}\right) = l\left(\frac{r}{1}\right) l\left(\frac{1}{s}\right) = l\left(\frac{r}{1}\right)\left(l\left(\frac{s}{1}\right)\right)^{-1} = l(\imath(r))(l(\imath(s)))^{-1} = \jmath(r)(\jmath(s))^{-1}$.
Тобто якщо такий гомоморфізм існує, то він має вигляд $l\left(\frac{r}{s}\right) = \jmath(r)(\jmath(s))^{-1}$ – інших нема. ■

Example 6.1.6 Маємо $k[x]$ – поле (тому область цілісності). Ми можемо визначити поле часток $k[x]$ – отримаємо елементи вигляду $\frac{f(x)}{g(x)}$. Така множина має особливе позначення: $k(x)$.
Тобто $k(x) = \left\{\frac{f(x)}{g(x)} \mid f, g \in k[x]\right\}$.
Дане поле є найменшим полем, яке може містити поле k.

Більше нічого про поле часток не можу сказати. Але насамкінець цього підрозділу додам цікаве твердження.

Proposition 6.1.7 Задано F – поле. Тоді F містить копію $\mathbb{Q}$ або $\mathbb{Z}/_{p\mathbb{Z}}, p$ – просте число.

Proof.
Розглянемо відображення $\sigma\colon \mathbb{Z} \to F$ таким чином: $\sigma(1) = 1_F,\ \sigma(n) = \underbrace{1_F + \cdots + 1_F}_{n \text{ разів}}$.
Нехай $\operatorname{char} F = 0$, тоді відображення σ буде ін'єктивним. Але за **Th. 6.1.5**, поле F має містити поле часток $\mathbb{Z}$, а в цьому випадку це $\mathbb{Q}$.
Нехай $\operatorname{char} F = p$. Тоді $\ker\sigma = p\mathbb{Z}$, а за першою теоремою про ізоморфізм, $F \supset \operatorname{Im}\sigma \cong \mathbb{Z}/_{p\mathbb{Z}}$. ■

Дані поля $\mathbb{Q}, \mathbb{Z}/_{p\mathbb{Z}}$ ще називають **простими**. Для другого поля є позначення $\mathbb{Z}/_{p\mathbb{Z}} = \mathbb{F}_p$.

6.2 Розширення поля

Definition 6.2.1 Задано k – поле.
Розширенням поля k називають поле F, для якого

$$k \subset F$$

Інколи можна побачити таке позначення: F/k.

Example 6.2.2 Розглянемо кілька прикладів:
1. $\mathbb{R}$ – розширення поля $\mathbb{Q}$;
2. Нехай $f \in \mathbb{Q}[t]$ – незвідний многочлен. Тоді $\mathbb{Q}[t]/_{(f(t))}$ – поле, тому що в нас $(f(t))$ – максимальний ідеал за умовою. Можна визначити ін'єктивний гомоморфізм $\mathbb{Q} \hookrightarrow \mathbb{Q}[t]/_{(f(t))}$ як $q \mapsto q + (f(t))$, тоді $\mathbb{Q} \subset \mathbb{Q}[t]/_{(f(t))}$. Таким чином, $\mathbb{Q}[t]/_{(f(t))}$ – розширення поля $\mathbb{Q}$;
3. $\mathbb{Q}(t)$ – поле часток многочленів $\mathbb{Q}[t]$ – розширення поля $\mathbb{Q}$;
4. $\bar{\mathbb{Q}}$ – алгебраїчні числа – теж розширення поля $\mathbb{Q}$.

Proposition 6.2.3 Задані поля $k \subset F$. Тоді $\operatorname{char} k = \operatorname{char} F$.

Proof.
Дійно, нехай $\operatorname{char} k = 0$. Тоді $1 + 1 + \ldots \neq 0$. Зокрема оскільки $1 \in k$, то в силу розширення $1 \in F$. Значить, $1 + 1 + \ldots \neq 0$, тому $\operatorname{char} F = 0$.
Нехай $\operatorname{char} k = p$, де p – просте. Ми припустимо, що $\operatorname{char} F = q$, де q – інше просте. Тоді $\underbrace{1 + \cdots + 1}_{q \text{ разів}} =$ 0 в F, а згодом (в силу ін'єктивності гомоморфізма) $\underbrace{1 + \cdots + 1}_{p \text{ разів}} = 0$ в k. Звідси випливає, що $p \mid q$, а це можливо при $p = q$. Отримаємо, що $\operatorname{char} F = p$. ■

Proposition 6.2.4 Задані поля $k \subset F$. Тоді F є векторним простором над полем k.
Це природним чином.

Definition 6.2.5 Степенем розширення поля $k \subset F$ називають розмірність векторного простора F над k. Тобто:

$$[F : k] = \dim_k F$$

Definition 6.2.6 Розширення поля $k \subset F$ називається **скінченним**, якщо

$$[F : K] < \infty$$

У протилежному випадку дане розширення називається **нескінченним**.

Example 6.2.7 Розглянемо кілька прикладів:
1) $[\mathbb{C} : \mathbb{R}] = 2$, можна підібрати базис $\{1, i\}$ над $\mathbb{R}$. Тобто розширення $\mathbb{R} \subset \mathbb{C}$ – скінченне.
2) $[\mathbb{Q}(t) : \mathbb{Q}] = \infty$, оскільки є нескінченна лінійно незалежна система $\{1, t, t^2, \ldots\}$.
3) $[\mathbb{R} : \mathbb{Q}] = \infty$, оскільки є нескіченна лінійно незалежна система $\{1, e, e^2, \ldots\}$. Якби ця система була л.з. на якомусь етапі, то мали би $a_0 + a_1 e + \cdots + a_n e^n = 0$. Тобто число e було б розв'язком деякого многочлена з $\mathbb{Q}[x]$, але це неможливо, оскільки (відомий факт) e – трансцендентне число.

Remark 6.2.8 Розширення поля $k \subset F$ – тривіальне (тобто $k = F$) $\iff [F : k] = 1$.

Proposition 6.2.9 Задані $k \subset E \subset F$ – розширення полів.
$k \subset E$ та $E \subset F$ – скінченні розширення $\iff k \subset F$ – скінченне розширення.
При цьому $[F : k] = [F : E][E : k]$.

Proof.
$\boxed{\Rightarrow}$ Дано: $k \subset E, E \subset F$ – скінченні розширення.
Позначимо $[E : k] = m, [F : E] = n$. Поле E має базис $\{\epsilon_1, \ldots, \epsilon_m\}$ над k; поле F має базис $\{\varphi_1, \ldots, \varphi_n\}$ над E. Хочу довести, що $\{\epsilon_i \varphi_j \mid i = \overline{1, m}, j = \overline{1, n}\}$ формуватиме базис F над k.
$\sum_{j=1}^{n} \sum_{i=1}^{m} k_{ij} \epsilon_i \varphi_j = 0.$
Оскільки система $\{\varphi_i\}$ лінійно незалежна над E, то звідси випливає

$\sum_{i=1}^{m} k_{ij}\epsilon_i = 0$ для всіх $j = \overline{1,n}$.
Оскільки $\{\epsilon_i\}$ лінійно незалежна над k, то звідси $k_{ij} = 0$ для всіх i, j. Отже, $\{\epsilon_i\varphi_j\}$ – л.н.з.

Нехай $x \in F$, тоді єдиним чином має розклад $x = \sum_{j=1}^{n} e_j\varphi_j$. Кожний елемент $e_j \in E$, тоді єдиним чином має розклад $e_j = \sum_{i=1}^{m} k_{ij}\epsilon_i$. Таким чином, $x = \sum_{j=1}^{n}\sum_{i=1}^{m} k_{ij}k_{ij}\epsilon_i\varphi_j$. Тим самим $\{\epsilon_i\varphi_j\}$ – базис.
Звідси маємо, що $[F : k] = nm = [F : E][E : k]$.

$\boxed{\Leftarrow}$ Дано: $k \subset F$ – скінченне розширення.
Маємо $[F : k] = d$. Зауважимо, що F – векторний простір над k, коли водночас E – підпростір F. Таким чином, $\dim_k E \leq \dim_k F = d$, тому вже $k \subset E$ – скінченне розширення.
!Припустимо, що $E \subset F$ є нескінченний розширенням. Маємо $\{f_i \mid i \in I\}$ – базис F над E та $\{e_1, \ldots, e_m\}$ – базис E над k. Тоді, насправді, $\{f_ie_j \mid i \in I, j = \overline{1,m}\}$ буде лінійно незалежною системою F над k (доводиться аналогічно). Але базис F над k містить скінченне число елементів. Суперечність! ■

Definition 6.2.10 Задано $k \subset E \subset F$ – розширення полів. Тоді E називають **проміжним полем** розширення $k \subset F$.

Remark 6.2.11 Якщо маємо скінченне розширення $k \subset F$, при цьому $[F : k]$ – просте число, то єдині проміжні поля даного розширення – це або k, або F.

Example 6.2.12 Доведемо, що $\sqrt{3} \notin \mathbb{Q}[\sqrt[5]{3}]$.
!Припустимо, що $\sqrt{3} \in \mathbb{Q}[\sqrt[5]{3}]$. Тоді маємо ось таке розширення $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}] \subset \mathbb{Q}[\sqrt[5]{3}]$. Тепер зауважимо, що $[\mathbb{Q} : \mathbb{Q}[\sqrt{3}]] = 2$ та $[\mathbb{Q} : \mathbb{Q}[\sqrt[5]{3}]] = 5$. Відомо, що $[\mathbb{Q} : \mathbb{Q}[\sqrt[5]{3}]] = [\mathbb{Q} : \mathbb{Q}[\sqrt{3}]] \cdot [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}[\sqrt[5]{3}]]$, тобто $5 = 2 \cdot [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}[\sqrt[5]{3}]]$. Така рівність неможлива, тому суперечність!

Proposition 6.2.13 Задано k – поле та $f \in k[t]$ – незвідний многочлен. Тоді $k[t]/_{(f(t))}$ буде полем та гомоморфізм $k \to k[t]/_{(f(t))}$, де $a \mapsto a + (f(t))$, визначає розширення $k \subset k[t]/_{(f(t))}$. Таке розширення скінченне, причому $\left[k[t]/_{(f(t))} : k\right] = \deg f$.

Proof.
Оскільки f – незвідний, то $(f(t))$ – максимальний ідеал. Тобто уже $k[t]/_{(f(t))}$ є полем, а також є векторним простором над k розмірності $\deg f$.
Можна зауважити, що $\{1 + (f(t)), t + (f(t)), \ldots, t^{\deg f} + (f(t))\}$ – базис. ■

Example 6.2.14 Розширення $\mathbb{Q} \subset \mathbb{Q}[x]/_{(t^7+2t^2+2)}$ не має проміжного поля, що не збігається з $\mathbb{Q}$ або з $\mathbb{Q}[t]/_{(t^7+2t^2+2)}$.
Зауважимо, що за критерієм Айзенштайна, $t^7 + 2t^2 + 2$ буде незвідним над $\mathbb{Q}$. Отже, $\mathbb{Q}[t]/_{(t^7+2t^2+2)}$ буде справді полем. Причому $\left[\mathbb{Q}[t]/_{(t^7+2t^2+2)} : \mathbb{Q}\right] = 7$. Далі якщо припустити, що є проміжне поле E, то тоді звідси $7 = [E : \mathbb{Q}]\left[\mathbb{Q}[t]/_{(t^7+2t^2+2)} : E\right]$, проте 7 – просте число. Значить, ми прийдемо до того, що E буде збігатися з одним з двом полів – неможливо.

6.3 Прості розширення

Нехай $k \subset F$ – розширення поля та $\alpha_1, \ldots, \alpha_r \in F$. Позначимо $k(\alpha_1, \ldots, \alpha_r)$ – найменше підполе F, що містить k та еллементи α_i.

Definition 6.3.1 Розширення поля $k \subset F$ називається **скінченно породженим**, якщо

$$F = k(\alpha_1, \ldots, \alpha_r) \text{ для деяких } \alpha_1, \ldots, \alpha_r \in F$$

Definition 6.3.2 Розширення поля $k \subset F$ називається **простим**, якщо

$$F = k(\alpha) \text{ для деякого } \alpha \in F$$

Proposition 6.3.3 Структура простого розширення
Нехай $k \subset k(\alpha) = F$ – просте розширення поля. Тоді є два варіанти:
1) $F \cong k[t]/_{(p(t))}$ для незвідного зведеного многочлена $p \in k[t]$, де $p(\alpha) = 0$. Причому $[F : k] = \deg p$;
2) $F \cong k(t)$, де $k(t)$ – поле часток $k[t]$. Причому $[F : k] = \infty$.

Я надалі зведений многочлен буду називати монічним (monic polynomial).

Proof.
Маємо $F = k(\alpha)$. Визначимо гомоморфізм $\varphi\colon k[t] \to F$ таким чином: $\varphi(f(t)) = f(\alpha)$.
Якщо $\ker\varphi \neq (0)$, тоді звідси $\ker\varphi = (p(t))$ для деякого $p \not\equiv 0$, оскільки $k[t]$ – ОГІ. За побудовою гомоморфізма, $p(\alpha) = 0$; а після помноження $p(t)$ на обернений елемент старшого коефіцієнта, ми можемо вважати $p(t)$ за монічним многочленом. За І теоремою про ізоморфізм, існує гомоморфізм $\tilde{\varphi}\colon k[t]/_{(p(t))} \hookrightarrow F$. Зокрема звідси $k[t]/_{(p(t))}$ має бути областю цілісності, тож $(p(t))$ – простий ідеал, а тому й максимальний (це можливо в ОГІ). Отже p стане незвідним многочленом, а $k[t]/_{(p(t))}$ – дійсно буде полем. Зауважимо, що $\operatorname{Im}\tilde{\varphi} \subset F$ – підполе, що містить α (просто тому що, взявши многочлен $t \in k[t]$, отримаємо $\varphi(t) = \alpha$) та поле k. Але тоді $\operatorname{Im}\tilde{\varphi} = F$, оскільки F – найменше поле, що містить k та α. Звідси $\tilde{\varphi}$ – сюр'єктивний гомоморфізм, тож $k[t]/_{(p(t))} \cong F$. Отже, $[F : k] = \deg p$.
Якщо $\ker\varphi = (0)$, то гомоморфізм – ін'єктивний. Оскільки $k[t]$ – область цілісності, то існує поле часток $k(t)$. Значить, існує ін'єктивний гомоморфізм $k(t) \hookrightarrow F$, образ якого буде підполем F, що містить $\varphi(t) = \alpha$. Значить, $k(t) \cong F$, оскільки F породжена α. Розмірність векторного простору $k(t)$ над k нескінченна (беремо лінійно незалежну систему $\{1, t, t^2, \dots\}$), тож $[F : k] = \infty$. ■

Definition 6.3.4 Задано $k \subset F$ – розширення та $\alpha \in F$.
Елемент α називається **алгебраїчним** над полем k, якщо

$$\exists p \in k[t] : p(\alpha) = 0$$

Якщо α не є алгебраїчним, то такий елемент називають **трансцендентним**.

Користуючись щойно доведеним твердженням, можна дане означення переформулювати:

Corollary 6.3.5 Задано $k \subset F$ – розширення та $\alpha \in F$.
α – алгебраїчний елемент над $k \iff [k(\alpha) : k] = d$ – скінченне розширення.

Proof.
$\boxed{\Rightarrow}$ Дано: α – алгебраїчне, тобто $\exists f \in k[t] : f(\alpha) = 0$. Знову розглянемо гомоморфізм $\varphi\colon k[t] \to F$ як $\varphi(f(t)) = f(\alpha)$. У цьому випадку $\ker\varphi \neq (0)$, тоді аналогічними міркуваннями $\ker\varphi = (p(t))$ та за І теоремою про ізоморфізм, $k(\alpha) \cong k[t]/_{\ker\varphi}$. Отже, $k \subset k(\alpha)$ – скінченне розширення.

$\boxed{\Leftarrow}$ Дано: $k \subset k(\alpha)$ – скінченне розширення. Тоді за твердженням вище, нам підійде $F \cong k[t]/_{(p(t))}$, тоді ми знайшли многочлен $p \in k[t]$, для якого $p(\alpha) = 0$. Отже, α – алгебраїчний над k. ■

Corollary 6.3.6 У випадку твердження вище α буде також коренем єдиного незвідного монічного многочлена $p \in k[t]$ із властивістю $p \mid f$ та $k(\alpha) \cong k[t]/_{(p(t))}$.

Proof.
Ми вже знаємо, що $\ker\varphi = (p(t))$, де p – незвідний многочлен. За умовами, що були вище, $f \in \ker\varphi \implies p \mid f$. Ми довели, що $k \subset k(\alpha)$ – скінченне розширення. Але тоді $k(\alpha) \cong k[t]/_{(\tilde{p}(t))}$ – інший незвідий многочлен $\tilde{p} \in k[t]$, для якого $\tilde{p}(\alpha) = 0$. Будемо вважати, що він монічний, тому що старший коефіцієнт можна завжди поділити. Покажемо, що $p \equiv \tilde{p}$.
Дійсно, $\tilde{p} \in \ker\varphi$, тож $p \mid \tilde{p}$, тобто $\tilde{p}(t) = p(t)q(t)$, але в силу незвідності $q \in (k[t])^\times \implies q(t) = c$. Оскільки обидва многочлени – моніки, то $c = 1$. ■

Definition 6.3.7 Задано $k \subset F$ – розширення та $\alpha \in F$ – алгебраїчне надо k.
Многочлен $p \in k[t]$ називається **мінімальним многочленом** α над k, якщо

$$p \text{ – незвідний, монічний, при цьому } p(\alpha) = 0$$

Такий мінімальний многочлен – єдиний, за міркуваннями вище.

Definition 6.3.8 Маємо розширення $\mathbb{Q} \subset \mathbb{C}$ та $\alpha \in \mathbb{C}$.
Якщо α є алгебраїчним елементом над $\mathbb{C}$, то його називають **алгебраїчним числом**. Інакше – **трансцендентним числом**.
Позначення: $\bar{\mathbb{Q}}$.

Example 6.3.9 Наприклад, число $\sqrt[5]{2}$ – алгебраїчне, бо є коренем $t^5 - 2 = 0$.

Proposition 6.3.10 $\bar{\mathbb{Q}}$ – зліченна множина.

Proof.
Спочатку покажемо, що множина $\mathbb{Q}[x]$ буде зліченною.
Розглянемо $\mathbb{Q}_n[x] = \{a_0+a_1x+\cdots+a_nx^n \mid a_i \in \mathbb{Q}\}$. Кожному такому многочлену $a_0+a_1x+\cdots+a_nx^n$ поставимо взаємно однозначним чином пару $(a_0, a_1, \ldots, a_n)$. Заужавимо, що кількість a_i зліченна, тому й декартів добуток – зліченна, що доводить зліченність $\mathbb{Q}_n[x]$. Нарешті, $\mathbb{Q}[x] = \bigcup\limits_{n\geq 0} \mathbb{Q}_n[x]$ – зліченна, як зліченне об'єднання зліченних множин.
Тепер, кожному алгебраїчному числу ставиться у відповідність єдиний мінімальний многочлен $p \in \mathbb{Q}[x]$, кількість яких зліченна. Отже, $\bar{\mathbb{Q}}$ – зліченна. ■

Example 6.3.11 Зауважимо, що i – алгебраїчне над $\mathbb{R}$ з мінімальним многочленом $t^2+1=0$; але алгебраїчне над $\mathbb{C}$ з іншим мінімальним многочленом $t-i=0$.
Число π – трансцендентне над $\mathbb{Q}$ (факт), але є алгебраїчним над $\mathbb{R}$ з мінімальним многочленом $t-\pi=0$.

Proposition 6.3.12 Задано $k \subset E \subset F$ – розширення полів та $\alpha \in F$. Нехай α – алгебраїчне над k з мінімальним многочленом $p_k(t)$. Тоді α – алгебраїчне над E з мінімальним многочленом $p_E(t)$, при цьому $p_E \mid p_k$.

Proof.
Маємо α – алгебраїчне над k, тобто $p_k(\alpha)=0$. Оскільки $k \subset E$ та $p_k \in k[t]$, то звідси $p_k \in E[t]$, при цьому все одно $p_k(\alpha)=0$. Отже, α – алгебраїчне над E. Там існує мінімальний многочлен $p_E \in E[t]$, для якого $p_E \mid p_k$ (за наслідком). ■

Remark 6.3.13 p_k мало б бути незвідним многочленом, а тут має множник p_E. Насправді, p_k – незвідний многочлен як многочлен із $k[t]$. Над більшими полями (як-от E) многочлен p_k може мати уже нетривіальні множники.

Example 6.3.14 Розширення $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ буде простим. Доведемо, що $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
Оскільки $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, то звідси миттєво $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Доведемо, що $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Позначимо $\alpha = \sqrt{2}+\sqrt{3}$. Зауважимо, що $\alpha^3 = 11\sqrt{2}+9\sqrt{3}$. Отримаємо систему рівнянь $\begin{cases} \alpha = \sqrt{2}+\sqrt{3} \\ \alpha^3 = 11\sqrt{2}+9\sqrt{3} \end{cases}$. Звідси $\sqrt{2} = \dfrac{\alpha^3-9\alpha}{2}, \sqrt{3} = \dfrac{11\alpha-\alpha^3}{2}$. Таким чином, $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, а це нам дає $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Example 6.3.15 Маємо $k \subset F$ – скінченне розширення, причому k – скінченне поле. Тоді маємо просте розширення.
Із нашої умови випливає, що F – скінченне поле. Дійсно, маємо $\{f_1, \ldots, f_d\}$ – базис F над k. Тоді $x = k_1f_1 + \cdots + k_df_d$. Оскільки k – скінченне поле, у нас є скінченне число способів побудувати x.
Далі зауважимо, що $\langle F^\times, \cdot \rangle$ – циклічна група, тобто $F^\times = \langle \alpha \rangle$ (TODO: додати твердження, що абелева та скінченна група, для якої $g^n = 1$ до n штук елементів g для всіх n – циклічна). Отже, $F \setminus \{0\} = \langle \alpha \rangle$. Тим самим доводимо, що $F = k(\alpha)$.

Proposition 6.3.16 Задано $k \subset k(t)$ – просте розширення, де t – трансцдендентне число. Тоді розширення $k \subset k(t)$ допускає нескінченну кількість проміжних полів.

Proof.
Маємо $k \subset k(t)$. Розглянемо поля $k(t^2), k(t^3), \ldots$. Відносно зрозуміло, що кожний $k \subset k(t^n) \subset k(t)$, де $n \geq 2$, буде проміжним полем. Зауважимо, що $k(t^n) \neq k(t)$. оскільки, у нас $t \notin k(t^n)$. Приблизно так само $k(t^n) \neq k(t^m)$ (TODO: чіткіше довести). ■

Proposition 6.3.17 Задано $k \subset F = k(\alpha)$ – просте розширення та α – алгебраїчний елемент над k. Тоді розширення $k \subset F$ допускає лише скінченну кількість проміжних полів.

Proof.
Оскільки α – алгебраїчний над k, то маємо $p \in k[t]$ – мінімальний многочлен α над k. Нехай E – проміжне поле $k \subset k(\alpha)$. Тоді можна p сприймати як $p \in E[t]$. Ми вже доводили, що p_E – мінімальний многочлен α над E – ділить p.
Нехай $p_E(t) = e_0 + e_1t + \cdots + e_{d-1}t^{d-1} + t^d$, тож $[k(\alpha) : E] = d$. Хочемо довести, що $E = k(e_0, e_1, \ldots, e_{d-1})$. Для зручності позначимо $k(e_0, e_1, \ldots, e_{d-1}) = E'$, тобто треба $E = E'$.
Зауважимо, що в нас є послідовність $E' \subset E \subset k(\alpha)$. Оскільки E' містить коефіцієнти p_E, то

тоді даний многочлен можна сприймати як $p_E \in E'[t]$. Оскільки p_E – незвідний над E, то тоді p_E – незвідний над E'. Отже, p_E – монічний, незвідний над E', а тому він є мінімальним многочленом α над E'. Звідси випливає, що $[k(\alpha) : E'] = d = [k(\alpha) : E]$. Разом отримаємо $d = [k(\alpha) : E'] = [k(\alpha) : E][E : E'] = d[E : E']$, а тому $[E : E'] = 1$. Отже, $E = E'$.
Ми тільки-но показали, що E визначається коефцієнтами з p_E єдиним чином, а той многочлен p_E є множником p. Але оскільки p має лише скінченне число множників в $F[t]$ ($F[t]$ є ООФ, тому там розклад на скінченне число многочленів), то кількість проміжних полів E – скінченна. ■

Lemma 6.3.18 Задано $k \subset F = k(\alpha_1, \ldots, \alpha_n)$ – скінченно породжене розширення. Нехай α_i – алгебраїчний над $k(\alpha_1, \ldots, \alpha_{i-1})$ при кожному $i = \overline{1, n}$. Тоді $k \subset F$ – скічненне розширення.

Proof.
Оскільки α_i – алгебраїчне над $k(\alpha_1, \ldots, \alpha_{i-1})$, то $[k(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : k(\alpha_1, \ldots, \alpha_{i-1})] = d_i < \infty$.
Зауважимо, що ми маємо такий ланцюг полів:
$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_{n-1}) \subset k(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = F$.
Отже, $[F : k] = [F : k(\alpha_1, \ldots, k(\alpha_{n-1})] \cdots [k(\alpha_1, \alpha_2) : k(\alpha_1)] \cdot [k(\alpha_1) : k] = d_n \ldots d_2 d_1 < \infty$. ■

Proposition 6.3.19 Задано $k \subset F = k(\alpha)$ – просте розширення, що допускає лише скінченну кількість проміжних полів. Тоді α – алгебраїчний елемент над k.

Proof.
Із умови випливає, що $k \subset F$ – скінченно породжене: якби ні, ми би побудували нескінченно зростаючу послідовність $k \subsetneq k(u_1) \subsetneq k(u_1, u_2) \subsetneq \cdots \subset F$, даючи нескінченне число проміжних полів.
Тож маємо $F = k(u_1, \ldots, u_n)$. Ми припускаємо, що кожний u_i – алгебраїчний над $k(u_1, \ldots, u_{i-1})$; бо якщо u_i – трансцендентний, тоді всього нескінченна кількість проміжних полів між $k(u_1, \ldots, u_{i-1})$ та $k(u_1, \ldots, u_i)$ (**Prp. 6.3.16**), а тому й між k та F. Зокрема маємо, що $k \subset F$ – скінченне розширення (за щойно доведеною лемою).
Достатньо буде довести, що $k(u, v) = k(\alpha)$. Якщо k – скінченне поле, тоді $k(u, v)$ теж, а тому розширення – просте – кінець доведення. Тому надалі припускаємо, що k – нескінченне поле.
Оберемо елементи виду $u + cv$, де $c \in k$ та розглянемо проміжне поле $k(u + cv)$. За умовою твердження, всього скінченна кількість проміжних полів, тому точно існують $c' \neq c'' \in k$, для яких $k(c'u + v) = k(c''u + v)$. Стверджується, що $k(u, v) = k(\alpha)$ при $\alpha = u + c'v$.
Покажемо, що $u, v \in k(u + c'v) = k(u + c''v)$. Дійсно, $v = \dfrac{(u + c'v) - (u + c''v)}{c' - c''}$ та $u = (u + c'v) - c'v$.
Також $u + c'v \in k(u, v)$ уже, тому рівність $k(u, v) = k(u + c'v)$ виконано.
Отже, $F = k(\alpha)$. Оскільки $k \subset F$ – скінченне розширення, то α – алгебраїчний.
Але в нас був лише випадок, коли $F = k(u_1, u_2)$, тоді ми довели, що $F = k(\alpha)$. У нас є ще можливий сценарій, коли $F = k(u_1, u_2, \ldots, u_n)$. За МІ доведемо, що $k(u_1, u_2, \ldots, u_n) = k(u, u_n)$ при деякому u.
База: $n = 3$. Тоді $k(u_1, u_2, u_3) = k(u_1, u_2)(u_3) = k(u)(u_3) = k(u, u_3)$.
Припущення: для деякого $n - 1$ твердження виконано.
Крок: при n маємо $k(u_1, u_2, \ldots, u_n) = k(u_1, u_2, \ldots, u_{n-1})(u_n) \overset{\text{МІ}}{=} k(u)(u_n) = k(u, u_n)$.
МІ доведено. Тобто ми звели до $F = k(u, u_1)$, тим самим за вищеотриманими результатами, $F = k(\alpha)$. ■

6.4 Алгебраїчне розширення

Definition 6.4.1 Розширення полів $k \subset F$ називається **алгебраїчним**, якщо

$$\forall \alpha \in F : \alpha \text{ – алгебраїчний елемент над } k$$

Proposition 6.4.2 Задано $k \subset F$ – скінченне розширення. Тоді розширення – алгебраїчне.

Proof.
Нехай $\alpha \in F$, тоді маємо проміжне поле $k \subset k(\alpha) \subset F$ (за визначенням $k(\alpha)$). Оскільки $k \subset F$ – скінченне, то $k \subset k(\alpha)$ – скінченне. Отже, α – алгебраїчний над k. ■

Між іншим, степінь алгебраїчного елемента α, тобто $[k : k(\alpha)]$, ділить $[F : k]$ (це неважко).

Можна було твердження по-іншому довести. Маємо $[F : k] = d$ – скінченне число. Тоді $\{1, \alpha, \ldots, \alpha^d\}$ – лінійно залежна система, тобто є ненульові елементи $\lambda_i \in k$, для яких $\lambda_0 + \lambda_1\alpha + \cdots + \alpha_d\alpha^d = 0$.
Отже, α – алгебраїчний елемент над k, із мінімальним многочленом, що ділить $\lambda_0 + \lambda_1 t + \cdots + \lambda_d t^d$.

Proposition 6.4.3 Задано $k \subset F$ – алгебраїчне та скінченно породжене розширення. Тоді $k \subset F$ – скінченне розширення.
Це майже зворотне твердження до попереднього.

Proof.
Оскільки розширення є скінченно породженим, то $F = k(\alpha_1, \dots, \alpha_r)$. Маємо ланцюг полів:
$k \subset k(\alpha_1) \subset \cdots \subset k(\alpha_1, \dots, \alpha_r) = F$.
Оскільки розширення алгебраїчне, то α_i – алгебраїчні над k, тож $[k(\alpha_i) : k] = d_i$ – скінченні розширення. Але тоді зауважимо, що
$[k(\alpha_1, \dots, \alpha_{i-1}, \alpha_i) : k(\alpha_1, \dots, \alpha_{i-1})] = [k(\alpha_1, \dots, \alpha_{i-1})(\alpha_i) : k(\alpha_1, \dots, \alpha_{i-1})] \leq d_i$.
Дійсно, ми маємо мінімальний многочлен p_k^i алгебраїчного числа α_i над k. Маємо проміжне поле $k \subset k(\alpha_1, \dots, \alpha_{i-1}) \subset k(\alpha_1, \dots, \alpha_{i-1}, \alpha_i)$. Мінімальний многочлен $p^i_{k(\alpha_1,\dots,\alpha_{i-1})} \mid p_k^i$ за **Prp. 6.3.12**.
Значить, $\deg p^i_{k(\alpha_1,\dots,\alpha_{i-1})} \leq d_i$. Отже, $[k(\alpha_1, \dots, \alpha_{i-1}, \alpha_i) : k(\alpha_1, \dots, \alpha_{i-1})] \leq d_i$.
$[F : k] \leq d_1 \dots d_r < \infty$, що доводить скінченність розширення. ■

Corollary 6.4.4 $k \subset k(\alpha_1, \dots, \alpha_r)$ – алгебраїчне розширення $\iff$ $\alpha_i, i = \overline{1, r}$ – алгебраїчні над k.

Зокрема цей наслідок каже наступне: маємо α, β – алгебраїчні з мінімальними многочленами $p_\alpha, p_\beta \in k[t]$. Тоді $\alpha + \beta$ та $\alpha\beta$ – також алгебраїчні. Але як їхні мінімальні многочлени побудувати через p_α, p_β, важке питання.

Proposition 6.4.5 Задано $k \subset F$ – розширення поля та E – множина всіх елементів з F, які є алгебраїчними над k. Тоді E – поле.

Proof.
Нехай $\alpha, \beta \in K$. Тобто це $\alpha, \beta \in F$ та є алгебраїчними над k. Звідси випливає, що розширення $k \subset k(\alpha, \beta)$ буде алгебраїчним. Оскільки $\alpha + \beta, \alpha\beta, \alpha^{-1} \in k(\alpha, \beta)$, то вони є алгебраїчними, тобто $\alpha + \beta, \alpha\beta, \alpha^{-1} \in E$. ■

Example 6.4.6 Зокрема $\bar{\mathbb{Q}}$ утворює поле.
Дійсно, $\mathbb{Q} \subset \mathbb{C}$ – розширення та $\bar{\mathbb{Q}}$ – множина всіх елементів з $\mathbb{C}$, що є алгебраїчними над $\mathbb{Q}$ (в сенсі нашого означення).
При цьому розширення $\mathbb{Q} \subset \bar{\mathbb{Q}}$ не буде скінченним. Ми вже знаємо, що $\mathbb{Q}[t]$ має незвідні многочлени скільки завгодно високого степеня. А там є алгебраїчне число степені скільки завгодно високого.

Proposition 6.4.7 Задано $k \subset E$ та $E \subset F$ – два алгебраїчних розширення. Тоді $k \subset F$ – алгебраїчне розширення.

Proof.
Нехай $\alpha \in F$. Ми вже знаємо, що це – алгебраїчний над E, тоді α є коренем $f(t) = e_0 + e_1 t + \cdots + e_n t^n$.
Але $e_0, e_1, \dots, e_n \in k(e_0, \dots, e_n)$, тобто сприймаємо многочлен $f \in k(e_0, \dots, e_n)[t]$. Звідси α уже буде алгебраїчним елементом над $k(e_0, \dots, e_n)$.
Оскільки $k \subset k(e_0, \dots, e_n)$ алгебраїчне (бо $k \subset E$ алгебраїчне) та скінченно породжене розширення, то це скінченне розширення. Отже, $k \subset k(e_0, \dots, e_n) \subset k(e_0, \dots, e_n, \alpha) = k(e_0, \dots, e_n)(\alpha)$ буде скінченним розширенням, а тому алгебраїчним. Отже, α – алгебраїчний над k. ■

Повернімось до п. 6.3.

Ми зараз розглянемо просте розширення під іншим кутом.
Спочатку нехай k – поле та p – незвідний в $k[x]$ (ми можемо взяти монічний многочлен). Тоді $E = k[t]/_{(p(t))}$ буде розширенням поля k, що містить корінь многочлена $p(x)$ (треба розглянути гомоморфізм $c \mapsto c + (p(t))$). Отже, многочлен $p \in k[x]$ можна сприйняти як многочлен $p \in E[x]$. Якщо позначити $\alpha = t + (p(t))$, то зауважимо, що $p(\alpha) = p(t + (p(t)) = p(t) + (p(t)) = 0_E$. Таким чином, α – це корінь $p(x)$ в E.

Proposition 6.4.8 Задано $k \subset F$ – розширення полів та p – незвідний в $k[x]$. Тоді кожний корінь λ для $p(x)$ в F має вкладення $k[t]/_{(p(t))} \subset F$, яке продовжує вкладення $k \subset F$ та відображає $t + (p(t))$ на корінь λ.

Proof.
Нехай $p(x) = a_0 + a_1 x + \cdots + a_d x^d$, тут коефіцієнти з k. Позначимо $\alpha = t + (p(t))$. Припустимо, що λ – корінь $p(x)$ в F.

Розглянемо гомоморфізм $\hat{j}\colon k[t] \to F$ таким чином: $\hat{j}(f(t)) = f(\lambda)$. Такий гомоморфізм продовжує вкладення $k \subset F$ (тобто $\hat{j}$ є продовженням гомоморфізма $\hat{\hat{j}}\colon k \to F$) та відображає t на λ.
Оскільки λ – корінь $p(x)$ в F, то звідси $\hat{j}(p(t)) = p(\lambda) = 0$, звідси $(p(t)) \subset \ker \hat{j}$. Тоді $\hat{j}$ індукує гомоморфізм $j\colon k[t]/_{(p(t))} \to F$, причому $j(\alpha) = \lambda$. Оскільки $k[t]/_{(p(t))}$ – поле в силу незвідності многочлена, то тоді j – ін'єктивний гомоморфізм, тому отримали вкладення. ■

Proposition 6.4.9 Задано $k \subset F$ – розширення полів та p – незвідний в $k[x]$. Нехай $k[t]/_{(p(t))} \subset F$ – вкладення, яке продовжує $k \subset F$. Тоді образом $t + (p(t))$ буде корінь $p(x)$ в F.

Proof.
Нехай $j\colon k[t]/_{(p(t))} \to F$ – ін'єктивний гомоморфізм, яке продовжує $k \subset F$. Маємо $\alpha = t + (p(t))$. Тоді
$p(j(\alpha)) = a_0 + a_1 j(\alpha) + \cdots + a_d (j(\alpha))^d = j(a_0 + a_1\alpha + \cdots + a_d\alpha^d) = j(p(\alpha)) = j(0) = 0.$ ■

Corollary 6.4.10 Існує бієкція між множинами всіх коренів незвідного многочлена p в F та множинами всіх вкладень $k[t]/_{(p(t))} \subset F$, що продовжують $k \subset F$.

Нехай p – незвідний над k та $\lambda_1, \ldots, \lambda_n$ – корені в F (тобто всі алгебраїчні). По-перше, $k(\lambda_i) \cong k[t]/_{(p(t))}$. По-друге, λ_i ставить у відповідність вклдаення $k[t]/_{(p(t))} \cong k(\lambda_i) \subset F$, що продовжує $k \subset F$. Всі ці поля $k(\lambda_1), \ldots, k(\lambda_i)$ між собою ізоморфні, але можуть виглядати зовсім по-різному в F.

Example 6.4.11 Зокрема нехай $p(x) = x^3 - 2$, це незвідний многочлен, $p \in \mathbb{Q}[t]$. Поле $\mathbb{C}$ містить множину коренів $\{\lambda_1, \lambda_2, \lambda_3\}$, де $\lambda_1 = \sqrt[3]{2},\ \lambda_2 = \dfrac{-1 + i\sqrt{3}}{2}\lambda_1,\ \lambda_3 = \dfrac{-1 - i\sqrt{3}}{2}\lambda_1$ – корені p в $\mathbb{C}$. Отже, ми маємо поля $\mathbb{Q}(\lambda_1),\ \mathbb{Q}(\lambda_2),\ \mathbb{Q}(\lambda_3)$, що є вкладеннями $\mathbb{C}$ та продовжують вкладення $\mathbb{Q} \subset \mathbb{C}$. При цьому $\mathbb{Q}(\lambda_1),\ \mathbb{Q}(\lambda_2),\ \mathbb{Q}(\lambda_3)$ ізоморфні між собою, проте одна множина $\mathbb{Q}(\lambda_1) \subset \mathbb{R}$, а решта $\mathbb{Q}(\lambda_2),\ \mathbb{Q}(\lambda_3)$ топологічно щільні в $\mathbb{C}$.

Example 6.4.12 Тепер нехай $p(x) = x^2 - 2$, це незвідний многочлен, $p \in \mathbb{Q}[x]$. Маємо корені $\{\sqrt{2}, -\sqrt{2}\}$, які мапяться на різні вкладення $\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(-\sqrt{2})$. Але два різних вкладення визначають одне й те саме підполе $\mathbb{C}$, тому що $-\sqrt{2} = -1 \cdot \sqrt{2}$.

6.5 Поля розщеплень

Definition 6.5.1 Говорять, що многочлен f **розщеплюється** над полем F, якщо

$$f(x) = c\prod_{i=1}^{d}(x - \alpha_i) \text{ в } F[x]$$

При цьому $c \neq 0$ та $\alpha_1, \ldots, \alpha_d \in F$.

Definition 6.5.2 Маємо $k \subset F$ – розширення полів.
Це буде називатися **полем розщеплень** для многочлена $f \in k[x]$, якщо

$$f(x) = c\prod_{i=1}^{d}(x - \alpha_i) \text{ в } F[x]$$
$$F = k(\alpha_1, \ldots, \alpha_d)$$

Example 6.5.3 Нехай $f \in \mathbb{Q}[x]$. Тоді за основною теоремою алгебри, f розщеплюється над полем $\mathbb{C}$, тобто $f(x) = c\prod_{i=1}^{d}(x - \lambda_i)$, при цьому $\lambda_i \in \mathbb{C}, c \in \mathbb{Q}$. При цьому $\mathbb{Q}(\lambda_1, \ldots, \lambda_d) = \mathbb{C}$. Звідси $\mathbb{Q} \subset \mathbb{C}$ буде полем розщеплень для кожного многочлена.

Definition 6.5.4 Маємо $k \subset F$ – розширення полів. Поле F називається **алгебраїчно замкненим**, якщо

кожний многочлен $f \in F[x]$ має корінь

Theorem 6.5.5 Задано k – поле. Тоді існує алгебраїчне розширення полів $k \subset \bar{k}$, для якого $\bar{k}$ – алгебраїчно замкнено. Дане розширення буде єдиним із точністю до ізоморфізма.
Без доведення. (TODO: зробити).

Таке поле $\bar{k}$ називають **алгебраїчним замиканням** поля k.

Тепер кожний многочлен $f \in k[x]$ матиме корінь уже в $\bar{k}[x]$. Той факт, що $k \subset \bar{k}$ – алгебраїчне, робить $\bar{k}$ найменшим алгебраїчно замкненим полем, що містить k. (TODO: обміркувати). Завдяки цієї теореми, поле розщеплень завжди існує.

Theorem 6.5.6 Задано k – поле та $f \in k[x]$, причому $\deg f = d$. Тоді існує поле розщеплень $k \subset F$ для многочлена f, при цьому $[F : k] \leq d!$.

Proof.
Зауважимо, що $k \subset F$ буде полем розщеплень для $f \iff k \subset F$ буде полем розщеплень для $c^{-1}f$ (який є монічним). Тому надалі припускаю, що f – монічний многочлен. Доведення за МІ по d.
База: $d = 1$. Маємо $f(x) = x - c$, причому $c \in k$. Тоді зауважимо, що $k \subset k(c)$ буде полем розщеплень для f та $[k(c) : c] = 1 = 1!$.
Припущення: теорема виконується для випадків $< d$.
Крок: маємо $f \in k[x]$ при $\deg f = d$. За розкладом в ОГІ, оберемо p – незвідний монічний многочлен, де $p \mid f$. Позначимо $E = k[t]/_{(p(t))}$. Ми вже знаємо, що це містить корінь многочлена p в E за міркуваннями вище, тож $E = k(\alpha_1)$, де α_1 – корінь. Значить, $(x - \alpha_1) \mid p \mid f$ в $E[x]$. Отже, $f(x) = (x - \alpha_1)g(x)$ в $E[x]$.
Оскільки $\deg g = d - 1 < d$, то за припущенням МІ, існує поле розщеплеьн $E \subset F$, де $g(x) = \prod_{i=2}^{d}(x - \alpha_i)$ в $F[x]$ та $F = E(\alpha_2, \ldots, \alpha_d)$. При цьому всьому $[F : E] \leq (d-1)!$.
Але зауважимо, що, по-перше, $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ в F, та по-друге, $F = E(\alpha_2, \ldots, \alpha_d) = k(\alpha_1)(\alpha_2, \ldots, \alpha_d) = k(\alpha_1, \ldots, \alpha_d)$. Отже, ми знайшли $k \subset F$ – поле розщеплень для многочлена f. При цьому
$[F : k] = [F : E][E : k] = [F : E] \deg f = [F : E] \cdot d \leq (d-1)!d = d!$. ■

Example 6.5.7 Заарз побудуємо поле розщеплень для многочлена $f(x) = x^3 - 2$ із $f \in \mathbb{Q}[x]$. Робити будемо за процедурою, яка описана була в теоремі (крок індукції).
Оберемо незвідний многочлен, який є множником f. Оскільки f сам є незвідним, то оберемо його. Позначимо $E = \mathbb{Q}[t]/_{(t^3-2)}$. Ми вже знаємо, що f має корінь. Зауважимо тоді, що можемо записати $x^3 - 2 = (x - \alpha_1)(x^2 + \alpha_1 x + \alpha_1^2)$.
Зосередимося тепер на многочлені $g(x) = x^2 + \alpha_1 x + \alpha_1^2$ із E – це також незвідний многочлен. Покладемо $F = E[u]/_{(u^2+\alpha_1 u+\alpha_1^2)}$. Дане поле можна сприймати як поле $E(\alpha_2)$, де α_2 – корінь g (зокрема й корінь f). Оскільки $\deg g = 2$, а в нього є корінь, то буде ще один корінь та $g(x) = (x - \alpha_2)(x - \alpha_3)$. Два корені $\alpha_2, \alpha_3 \in F$. Таким чином, $x^2 - 2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.
Розширення $\mathbb{Q} \subset F = E[u]/_{(u^2-\alpha_1 u+\alpha_1^2} = E(\alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ буде полем розщеплень. Більш того, $[F : \mathbb{Q}] = 6 = 3!$ (буде саме рівність).

Remark 6.5.8 Конструктивно ми змогли отримати, що $[F : k] = d!$. Чи можна строго менше?
Можна. Якщо $k \subset F$ – поле розщеплень для $f \in k[x]$ та E – будь яке проміжне поле, то $E \subset F$ – також поле розщеплень уже для $f \in E[x]$. При цьому якщо $k \subsetneq E$, то звідси $[F : E] < [F : k] \leq d!$.

Remark 6.5.9 Якщо $k \subset F$ – поле розщеплень для $f \in k[x]$, то зрозуміло, що $F \subset F$ – теж поле розщеплень уже для $f \in F[x]$.

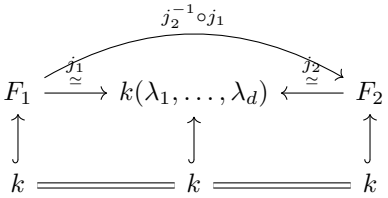
Зараз постає інше питання. Коли будували поле розщеплень, то була залежність від обрання незвідного монічного многочлена p, який брав участь у розкладі f. Насправді, це не має значення, бо скоро отримаємо поле розщеплень, які ізоморфні один одному.

Proposition 6.5.10 Нехай k – поле, $\bar{k}$ – алгебраїчне замикання. Маємо $f \in k[x]$ та $f(x) = c\prod_{i=1}^{d}(x - \lambda_i)$ в $\bar{k}[x]$. Нехай $k \subset F$ буде полем розщеплень для f. Тоді існує гомоморфізм $F \to \bar{k}$, який продовжує розширення $k \subset \bar{k}$, а також його образ дорівнює $k(\lambda_1, \ldots, \lambda_d)$.

Proof.
Доведення буде за індукцією по $\deg f = d$.
База: $d = 1$. Маємо $f(x) = x - c$ для деякого $c \in k$. Тоді поле розщеплень $F = k$ – далі нема що доводити.
Припущення: при $\deg f < d$ твердження виконано.
Крок: маємо $F = k(\alpha_1, \dots, \alpha_d)$ за умовою. Тоді α_1 – алгебраїчний над k, а для мінімального многочлена p для α_1 маємо $p \mid f$. Розглянемо $k(\alpha_1)$ – підполе F, тоді $k(\alpha_1) \cong k[t]/_{(p(t))}$, причому $\alpha_1 \mapsto \alpha_1 + (p(t))$. Оскільки p є множником f, один з коренів f в $\bar{k}$ буде коренем в p. Із точністю до перестановки припустимо, що λ_1 є таким коренем. Тоді за **Prp. 6.4.8**, ми маємо гомоморфізм $k[t]/_{(p(t))} \cong k(\alpha_1) \to \bar{k}$, де $t + (p(t)) \mapsto \alpha_1 \mapsto \lambda_1$. Тобто ми маємо розширення $k(\alpha_1) \subset \bar{k}$. Зауважимо, що $k \subset k(\alpha_1) \subset \bar{k}$, поле $\bar{k}$ є алгебраїчним замиканням k, а тому буде алгебраїчним замиканням $k(\alpha_1)$.
Маємо $f(x) = (x - \alpha_1)g(x)$ в $k(\alpha_1)[x]$. За означенням, $k(\alpha_1) \subset F$ буде полем розщеплень, а $g(x) = \prod_{i=2}^{d}(x - \alpha_i)$. Оскільки $\deg g < d$, то за припущенням МІ, ми маємо гомоморфізм $F \to \bar{k}$, який продовжує розширення $k(\alpha_1) \subset \bar{k}$ та $\alpha_i \mapsto \lambda_i$. (TODO: обдумати ще раз доведення). ■

Corollary 6.5.11 Поля розщеплень для $f \in k[x]$ єдині з точністю до ізоморфізму. Тобто маємо $k \subset F_1$ та $k \subset F_2$ – два поля розщеплень для f. Тоді $F_1 \cong F_2$, причому даний ізоморфізм продовжує тотожність на k.

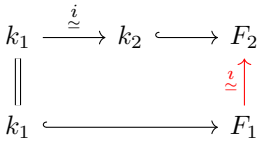
Proof.



Ізоморфізми $j_1 \colon F_1 \to k(\lambda_1, \dots, \lambda_d)$ та $j_2 \colon F_2 \to k(\lambda_1, \dots, \lambda_D)$ взяті з попереднього твердження. ■

Proposition 6.5.12 Задані $i \colon k_1 \to k_2$ – ізоморфізм полів. Нехай $f_1 \in k_1[x], f_1(x) = a_0 + a_1 x + \dots + a_d x^d$ та також $f_2 \in k_2[x], f_2(x) = i(a_0) + i(a_1)x + \dots + i(a_d)x^d$. Припустимо, що $k_1 \subset F_1$ – поле розщеплень f_1 та $k_2 \subset F_2$ – поле розщеплень f_2. Тоді існує ізоморфізм $\imath \colon F_1 \to F_2$, яке продовжує ізоморфізм $i \colon k_1 \to k_2$.

Proof.



Композиція $k_1 \to k_2 \to F_2$ дозволяє розглянути F_2 як розширення поля k_1 (як наслідок, як поле розщеплень f_1). За попереднім наслідком, існує ізоморфізм $\imath \colon F_1 \to F_2$, яке продовжує тотожність на k_1. У свою чергу це продовжує ізоморфізм $i \colon k_1 \to k_2$. ■

6.6 Нормальне розширення

Definition 6.6.1 Задано $k \subset F$ – алгебраїчне розширення. Припустимо, що $p \in k[x]$ – будь-який незвідний многочлен, який містить хоча б один корінь із E.
Тоді дане розширення називається **нормальним**, якщо

$$p \text{ розщеплюється на } F$$

Example 6.6.2 Зокрема алгебраїчне розширення $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ не буде нормальним. Тому що існує невіздний многочлен $p(x) = x^3 - 2$, який містить корінь з $\mathbb{Q}(\sqrt[3]{2})$, але не розщеплюється (оскільки інші два корені є суто комплексними).

Theorem 6.6.3 Задано $k \subset F$ – розширення поля.
$k \subset F$ – поле розщеплень для деякого $f \in k[x] \iff k \subset F$ – скінченне нормальне розширення.

Proof.
$\boxed{\Rightarrow}$ Дано: $k \subset F$ – поле розщеплень для деякого $f \in k[x]$. Зокрема це вже автоматично доводить скінченність даного поля.
Ми вже знаємо, що F можна сприймати як $k(\lambda_1, \dots, \lambda_d)$, який є підполем $\bar{k}$, що породжена коренями f. Тепер нехай $p \in k[x]$ – незвідний многочлен та $\alpha \in F$ – корінь p. Оберемо β – інший корінь p. Наша мета довести, що $\beta \in F$.
Зауважимо, що $k \subset k(\alpha)$ та $k \subset k(\beta)$ (розширення в межах $\bar{k}$) будуть обидва ізоморфними до $k[t]/_{(p(t))}$. Значить, існує ізоморфізм $k(\alpha) \xrightarrow{\sim} k(\beta)$, причому $\alpha \mapsto \beta$ (TODO: чому?). Отже, $[k(\alpha) : k] = [k(\beta) : k]$.
Оскільки F – поле розщеплень f над k $k(\alpha) \subset F$, то F – поле розщеплень f над $k(\alpha)$.
Зауважимо, що $F(\beta) = k(\beta, \lambda_1, \dots, \lambda_d) \subset \bar{k}$ буде полем розщеплень f над $k(\beta)$. По-перше, оскільки f розщеплюється в F, то f розщеплюється в $F(\beta)$. По-друге, корені f над k породжують поле F, а тому корені f над $k(\beta)$ породжують поле $F(\beta)$.
Далі маємо $F \supset k(\alpha), F(\beta) \supset k(\beta)$ – поля розщеплень f. Тоді існує ізоморфізм $F \xrightarrow{\sim} F(\beta)$, який продовжує ізоморфізм $k(\alpha) \xrightarrow{\sim} k(\beta)$. Таким чином, $[F(\beta) : k] = [F : k]$.
Водночас $F = k(\lambda_1, \dots, \lambda_d) \subset k(\beta, \lambda_1, \dots, \lambda_d) = F(\beta)$ в межах $\bar{k}$. Із цього випливатиме, що (оскільки $k \subset F \subset F(\beta)$) $[F(\beta) : k] = [F(\beta) : F][F : k] \implies [F(\beta) : F] = 1$. Єдиний варіант тоді – це $F(\beta) = F$, зокрема $\beta \in F$.
Під час доведення $F(\alpha) = F$, не до кінця зрозумів чому.

$\boxed{\Leftarrow}$ Дано: $k \subset F$ – скінченне нормальне розширення.
$F = k(\alpha_1, \dots, \alpha_r)$. Нехай p_i – мінімальний многочлен α_i. Оскільки розширення нормальне, то p_i розщеплюється. Отже, f також розщеплюється. Таким чином, $k \subset F$ – розщеплення f. ■

6.7 Сепарабельне розширення

Definition 6.7.1 Задано $k \subset F$ – алгебраїчне розширення.
Многочлен $f \in k[x]$ називається **сепарабельним**, якщо

його розклад над його полем розщеплень (над $\bar{k}$) не має кратних множників

Водночас розширення називається **сепарабельним**, якщо

кожний мінімальний многочлен – сепарабельний

Example 6.7.2 Розглянемо поле $\mathbb{F}_2(u)$ – трансцендентне просте розширення $\mathbb{F}_2$. Оберемо $f(x) = x^2 - u$. Даний многочлен є незвідним над $\mathbb{F}_2(u)$, бо не існує раціональних функції, чиї квадрати дорівнюють u.
Полем розщеплень даного многочлена буде поле $F = \mathbb{F}_2(u)[t]/_{(t^2-u)}$. Суміжний клас $\underline{t}$ по t буде коренем $x^2 - u$, тобто $\underline{t}^2 = u$. Але $(x - \underline{t})^2 = x^2 - 2x\underline{t} + \underline{t}^2 = x^2 - u$ (просто тому що $2 = 0$ в F). Отже, f має кратні множники в полі розщеплень та єдиний корінь.
Тобто f – незвідний, але при цьому несепарабельний.
Аналогічно можна провести для $\mathbb{F}_p, p$ – просте та показати, що $x^p - u$ – незвідний та несепарабельний в $\mathbb{F}_p(u)[t]$.

Нехай $f \in k[x]$, розгорнуто $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$. Визначимо "похідну"заданого многочлену
$f'(x) = a_1 + 2a_2 x + \dots + n a_n x^{n-1}$.
(тут нема прив'язки до похідної з мат аналізу, але властивості похідних виконані: додавання та множення похідних).

Example 6.7.3 Похідною $x^3 \in \mathbb{F}_3[x]$ буде 0.

Proposition 6.7.4 Многочлен $f \in k[x]$ – сепарабельний $\iff \gcd(f, f') = 1$.

Proof.
$\boxed{\Leftarrow}$ Дано: f – несепарабельний. Нехай F – поле розщеплень для f. Тоді існує $\alpha \in F$ та $g \in F[x]$, для яких $f(x) = (x-\alpha)^2 g(x)$. Таким чином, $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. Внаслідок цього f, f' мають нетривіальні спільні множники в F, тому $\gcd(f, f') \neq 1$ в F, тому $\gcd(f, f') \neq 1$ в k.

$\boxed{\Rightarrow}$ Дано: $\gcd(f, f') \neq 1$. Якщо p – спільний множник, нехай α буде коренем p; тоді $(x-a) \mid f$ та $(x-a) \mid f'$ в $F[x]$. Маємо $f(x) = (x-\alpha)g(x)$ в F. Отже, $f'(x) = g(x) + (x-\alpha)g'(x)$. Оскільки $(x-\alpha) \mid f'$, обов'язково $(x-\alpha) \mid g$. Отже, $f(x) = (x-\alpha)^2 h(x)$ для деякого $h \in F[x]$. Показали, що f – несепарабельний. ■

Example 6.7.5 Ми покажемо, що $f(x) = x^p - u$ є несепарабельним над $\mathbb{F}_p(u)$ іншим способом.
Маємо похідну $f'(x) = px^{p-1} = 0$. Таким чином, $\gcd(f, f') \neq 1$, що свідчить про несепарабельність.

Proposition 6.7.6 Задано k – поле при $\operatorname{char} k = 0$. Нехай $f \in k[x]$ – незвідний многочлен. Тоді f – сепарабельний. Внаслідок цього, алгебраїчне розширення полів нульової характеристики – сепарабельні.

Proof.
Нехай f – незвідний многочлен (як наслідок, $\deg f \geq 1$).
$f(x) = a_0 + a_1 x + \cdots + a_d x^d$ при $d \geq 1, a_d \neq 0$.
Звідси $f'(x) = a_1 + \cdots + d a_d x^{d-1} \neq 0$, оскільки $d a_d \neq 0$ за умовою характеристики поля.
Оскільки f – незвідний та $\deg f' < \deg f$, то f, f' не мають спільних незвідних множників.
Якби був незвідний p, для якого $p \mid f, p \mid f'$, то було би $f(x) = q(x)p(x)$. У силу незвідності f маємо $q \in (k[x])^\times$, тож $p(x) = q^{-1}(x) f(x)$. Водночас $f'(x) = s(x)p(x) = s(x)q^{-1}(x)f(x)$. У полі $\deg f' = \deg f + \deg s + \deg q^{-1} \geq \deg f$, що неможливо.
Таким чином, $\gcd(f, f') = 1$, а многочлен f – сепарабельний.
Якщо $k \subset F$ – алгебраїчне розширення та $\alpha \in F$, то мінімальний многочлен α – незвідний, а тому сепарабельний при $\operatorname{char} k = 0$. ■

Theorem 6.7.7 Теорема про примітивний елемент
Скінченні сепарабельні розширення – прості. Тобто кожне скінченне сепарабельне розширення $k \subset F$ має примітивний елемент $\alpha \in F$, для якого $F = k(\alpha)$.

Proof.
Нехай $k \subset F$ – скінченне розширення. Якщо k – скінченне, тож за **Ex. 6.3.15**, розширення просте. Надалі k – нескінченне. Оскільки $k \subset F$ скінченне розширення, то $F = k(u_1, \ldots, u_n)$. Покажемо спочатку, що якщо $F = k(u, v)$ буде скінченним сепарабельним розширенням, то воно буде простим. Але ми доведемо, що якщо $k \subset k(u, v)$ – непросте розширення, то розширення – несепарабельне. Для несепарабельності розширення достатньо показати, що мінімальний многочлен для v – несепарабельний.
Нехай f, g – мінімальні многочлени для u, v над k. Розглянемо проміжне поле $k(u + cv), c \in k$.
!Припустимо, що існує $c \in k$, для якого $v \in k(u + cv)$. Тоді $u = (u + cv) - cv \in k(u + cv)$, тож, позначивши $\alpha = u + cv$, отримаємо $k(u, v) = k(\alpha)$. Оскільки ми маємо непросте розширення, то це суперечність!
Таким чином, для кожного $c \in k$, маємо $v \notin k(u + cv)$. Нехай p_c – мінімальний многочлен для v над $k(u + cv)$. Тоді $\deg p_c \geq 2$. Дійсно, $\deg p_c = 0$ не може бути в силу незвідності; $\deg p_c = 1$ не може бути, бо тоді отримали б $v \in k(u + cv)$ із мінімального многочлена. Також нехай K – поле розщеплень для g над $k(u, v)$. Достатньо буде довести, що v – це кратний корінь $g \in K[x]$ – і тоді буде несепарабельність.
Оскільки $g(v) = 0$ та p_c – мінімальний многочлен для v над $k(u+cv)$, то $p_c \mid g$ в $k(u+cv)[x]$, зокрема й в $K[x]$. Оскільки c береться із k (це поле – нескінченне), водночас коли g має скінченну кількість множників в $K[x]$, то для нескінченно багатьох $c \in k$ отримаємо $p_c \equiv p,\ p \mid p$ при фіксованому многочлені $p \in K[x]$. Також $\deg p \geq 2$, тому що всі $\deg p_c \geq 2$, тож p містить хоча би два лінійних множниик в $K[x]$ (які можуть збігатися).
Нехай v' – якийсь корінь p в K, тобто $x - v'$ – лінійний множник. Хочемо довести, що $v' = v$, оскільки після цього $x - v \mid p \mid g$, а це гарантує несепарабельність g через другий корінь v.
Для хотілки розглянемо многочлен $f(u+c(v-x)) \in k(u+cv)[x]$. Оскільки $f(u) = 0$, то $f(u+c(v-x)) = 0$ при $x = v$, тож $p_c \mid f(u + c(v-x)) \implies p \mid f(u + c(v-x))$ для нескінченно багатьох $c \in k$. Звідси випливає, що при $x = v'$ маємо $f(u+c(v-v')) = 0$ для нескінченно багатьох $c \in k$. Отже, многочлен $f(u + y(v-v')) \in K[y]$ має нескінченно багато коренів. Оскільки над полем таке неможливо, то $f(u + y(v-v')) \equiv 0$, що дає $v = v'$. ■

Якщо g матиме корінь в $K[x]$, то g – несепарабельний.

Corollary 6.7.8 Задано $k \subset F$ – скінченне сепарабельне розширення. Тоді всього рівно $[F : k]$ вкладень F в алгебраїчне замикання $\bar{k}$, що продовжує вкладення $k \subset \bar{k}$.

Proof.
За попередньою теоремою, $F = k(\alpha) \cong k[t]/_{(p(t))}$ для деякого α. Мінімальний многочлен α має степінь $d = [F : k]$; раз розширення сепарабельне, то всього d різних коренів в $\bar{k}$. Існує рівно одне вкладення $F = k(\alpha)$ в $\bar{k}$, що продовжує $k \subset \bar{k}$, для кожного кореня за **Prp. 6.4.8**. ■

Definition 6.7.9 Задано $k \subset F$ – алгебраїчне розширення.
Степеню сепарабельності назвемо число різних вкладень F в алгебраїчне замикання $\bar{k}$, що продовжує $k \subset \bar{k}$.
Позначення: $[F : k]_s$.

Example 6.7.10 Маємо $k \subset k(\alpha)$ – просте та алгебраїчне розширення, тоді $[k(\alpha) : k]_s =$ кількість різних коренів в $\bar{k}$ мінімального многочлена α. Зокрема $[k(\alpha) : k]_s \leq [k(\alpha) : k]$ завжди. Рівність виконується $\iff$ мінімальний многочлен α над k – сепарабельний.

Proposition 6.7.11 Задані $k \subset F \subset F$ – алгебраїчні розширення. Тоді $[F : k]_s = [F : E]_s[E : k]_s$.

Proof.
Маємо $[E : k]_s$ вкладень $j \colon E \to \bar{k}$, що продовжує $k \subset \bar{k}$. По кожному з них $\bar{k}$ буде алгебраїчним замиканням E. Отже, всього $[F : E]_s$ вкладень F в $\bar{E} = \bar{k}$, що продовжує кожне з вкладень j. Загалом всього $[F : E]_s[E : k]_s$ способів вкласти F в $\bar{k}$, продовжуючи $k \subset \bar{k}$. ■

6.8 Скінченні поля

Proposition 6.8.1 Задано F – скінченне поле. Тоді $|F| = p^r$ для p – простого числа та $r > 0$.

Proof.
Оскільки F – скінченне поле, то $\operatorname{char} F > 0$, тож звідси поле містить $\mathbb{F}_p$ для деякого простого числа p (якщо бути точнішим, $p = \operatorname{char} F$ за **Prp. 6.1.7**). Ми маємо скінченне розширення $\mathbb{F}_p \subset F$. Припустимо, що $\{f_1, \dots, f_r\}$ – базис для деякого $r > 0$. Тоді $x = u_1 f_1 + \dots + u_r f_r$, де кожний $u_i \in \mathbb{F}_p$ можна обрати p способами. У силу єдиності розкладу, x можна розписати p^r способами. Таким чином, $|F| = p^r$. ■

Theorem 6.8.2 Задано p – просте число та $d \in \mathbb{N}$. Нехай $q = p^d$. Тоді існує єдине (із точністю до ізоморфізмів) поле $\mathbb{F}_q$ порядка q. Зокрема $\mathbb{F}_q$ – поле розщеплень для многочлена $x^q - x \in \mathbb{F}_p[x]$. Також розширення $\mathbb{F} \subset \mathbb{F}_q$ – скінченне, нормальне, сепарабельне.

Перед доведення запишемо одне означення:

Definition 6.8.3 Задано F – поле, причому $\operatorname{char} F = p > 0$.
Гомоморфізмом Фробеніуса називають гомоморфізм $\operatorname{Fr} \colon F \to F$, що задано

$$\operatorname{Fr}(x) = x^p$$

Це дійсно гомоморфізм (ми колись це показували в теорії кілець).

Proof.
Ми доведемо наступне:
F – поле розщеплень для $x^{p^d} - x \implies |F| = p^d$;
F – поле, де $|F| = p^d \implies F$ – поле розщеплень для $x^{p^d} - x$.
Всі поля розщеплень єдині з точністю до ізоморфізму за **Crl. 6.5.11**.
Нехай F – поле розщеплень для $f(x) = x^{p^d} - x \in \mathbb{F}_p[x]$. Многочлен f – сепарабельний, оскільки $f'(x) = -1$. Таким чином, f має $q = p^d$ різних коренів в F. Нехай $E \subset F$ – множина коренів (тобто елементи $u \in F$, для яких $u^q = u$). Стверджується, що E утворює поле, але тоді f розщеплюється в E, а E породжена коренями f. Тож E буде полем розщеплень: $E = F$. Зокрема $|F| = |E| = p^d = q$.
Тепер з'ясуємо, чому E – поле.
$u, v \in E \implies u^q = u, v^q = v \implies (uv)^q = u^q v^q = uv$.
$u \in E, u \neq 0 \implies u^q = u \implies (u^{-1})^q = u^{-q} = (u^q)^{-1} = u^{-1} \implies u^{-1} \in E$.

Залишилося довести замкненість відносно віднімання. Нехай $u, v \in E$, тобто $u^q = u, v^q = v$. Зауважимо, що $(x+y)^q = (\dots((x+y)^p)^p \dots)^p = \underset{d \text{ разів}}{\mathrm{Fr} \circ \dots \circ \mathrm{Fr}}(x+y) = x^q + y^q$.
Отже, $(u-v)^q = u^q + (-1)^q v^q = u - v$. Тобто $u - v \in E$.

Доведемо, що кожне поле F, де $|F| = q$, буде полем розщеплень для $f(x) = x^q - x$. Стверджується, що якщо $|F| = q$, то $f(u) = 0$ для всіх $u \in F$. Тим самим F буде містити q коренів f (тобто f розщеплюється в F), в жодному меншому полі це не можна. Отже, F – дійсно буде полем розщеплень.
Доведемо, що стверджувалося. Зауважимо, що $\langle F^\times, \cdot \rangle$ – група порядка $q-1$, тобто $u^{q-1} = 1$ для всіх $u \neq 0$. Отже, $u^q = q \implies f(u) = 0, u \neq 0$. При $u = 0$ все одно $f(u) = 0$.
Нарешті, поля розщеплень – скінченні, нормальні, а також многочлен $x^{p^d} - x$ – сепарабельний над $\mathbb{F}_p$. ■

Надалі можна спокійно позначати $\mathbb{F}_q,\ q = p^d$ – єдине поле (з точністю до ізоморфізма) з q елементами.

Corollary 6.8.4 Для кожного простого p та $d \in \mathbb{N}$ існують незвідні многочлени степеня d в $\mathbb{F}_p[x]$.

Proof.
Зауважимо, що $\mathbb{F}_p \subset \mathbb{F}_q$ – просте розширення (теорема про примітивний елемент). Тобто $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Оскільки $[\mathbb{F}_q : \mathbb{F}_p] = d$, то мінімальний многочлен для α над $\mathbb{F}_p$ має степінь d, що є незвідним. ■

Proposition 6.8.5 Задано $f \in \mathbb{F}_p[x]$ – монічний незвідний многочлен, де $\deg f = e$.
$f \mid x^{p^d} - x$ в полі $\mathbb{F}_p[x] \iff e \mid d$.

Proof.
$\boxed{\Rightarrow}$ Дано: $f \mid x^{p^d} - x$. Оскільки $x^{p^d} - x$ розщеплюється в $\mathbb{F}_{p^d}$, то звідси й f. Нехай β – корінь f в $\mathbb{F}_{p^d}$, таким чином f – мінімальний многочлен для β над $\mathbb{F}_p$. Підполе $\mathbb{F}_p(\beta)$, породжений β в межах $\mathbb{F}_{p^d}$, буде проміжним та $|\mathbb{F}_p(\beta)| = p^e$. Тоббто $\mathbb{F}_p \subset \mathbb{F}_p(\beta) \subset \mathbb{F}_{p^d}$.
$d = [\mathbb{F}_{p^d} : \mathbb{F}_p] = [\mathbb{F}_{p^d} : \mathbb{F}_p(\beta)] \cdot [\mathbb{F}_p(\beta) : \mathbb{F}_p] = [\mathbb{F}_{p^d} : \mathbb{F}_p(\beta)] \cdot e$.
Отже, $e \mid d$.

$\boxed{\Leftarrow}$ Дано: $e \mid d$. Тоді $\mathbb{F}_p \subset \mathbb{F}_p[x]/_{(f(t))} = \mathbb{F}_p(\beta)$ – просте розширення степеня e. Отже, $\mathbb{F}_p(\beta) \cong \mathbb{F}_{p^e}$ – поле розщеплень для $x^{p^e} - x$ за вищезгаданою теоремою. Зокрема $\beta^{p^e} - \beta = 0$, тож мінімальний многочлен f для β ділить $x^{p^e} - x$. Неважко переконатися, що $x^{p^e} - x \mid x^{p^d} - x$, тому звідси $f \mid x^{p^d} - x$. ■

Corollary 6.8.6 Маємо розширення $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d} \iff e \mid d$.