1. КІЛЬЦЯ

Почнемо із загального означення кільця. Надалі, щоправда, доведеться мати справу лише з комутативними кільцями.

Означення 1.1. Нехай R – довільна непорожня множина, а "$*$" та "$\circ$" – бінарні алгебраїчні операції на R. Тоді трійка $(R, *, \circ)$, якщо виконані такі аксіоми:

1°. $(R, *)$ – абелева група;

2°. $a \circ (b * c) = (a \circ b) * (a \circ c)$,
$(b * c) \circ a = (b \circ a) * (c \circ a)$, $\forall a, b, c \in R$.

Означення 1.2. Якщо операція "$\circ$" на R асоціативна, то кільце називається *асоціативним*; якщо вона ж ще і комутативна, то кільце називається *комутативним*; якщо містить нейтральний елемент по цій операції, то говорять про *кільце з одиницею*.

В силу традиції операцію "$*$" називають *додаванням* та позначають "+", а другу операцію називають *множенням* і позначають точкою або зовсім не пишуть. Тому, переходячи до традиційного запису операцій, опускаємо запис про них в позначенні кільця і говорити просто про кільце R. Нейтральні елементи тоді отримують також традиційні позначення та назви «нуль» і «одиниця». Група $(R, +)$ називається *адитивною групою кільця*.

Означення 1.3. Два ненульові елементи кільця, добуток яких дорівнює нулю (нейтральному елементу по додаванню), називаються *дільниками нуля* в цьому кільці.

Означення 1.4. Комутативне кільце с одиницею $(1 \neq 0)$ без дільників нуля називається *цілісним кільцем*.

Означення 1.5. Цілісне кільце, в якому кожен ненульовий елемент оборотний, називається *полем*.

Приклад 1.1. Кільцями є $(Z, +, \cdot)$ и $(R, +, \cdot)$. Це цілісні кільця.

Приклад 1.2. Нехай $R = \{x \in R \mid x = a + b\sqrt{2}, \quad a, b \in Q\}$. Це цілісне кільце відносно додавання та множення дійсних чисел. Його позначають як $R = Q[\sqrt{2}]$.

Приклад 1.3. Нехай $R = \{a\}$ і задані операції на R: $a + a = a, \quad a \cdot a = a$. Тоді R буде кільцем. До речі, замість a можна взяти число 0.

Приклад 1.4. Нехай $(R, +)$ – адитивна абелєва група. Визначимо операцію множення на R наступним чином: $\forall a, b \in R \quad a \cdot b = 0$. Отримаємо кільце. Яке?

Приклад 1.5. Нехай $R = R[x]$ – множина дійсних многочленів із звичайними операціями додавання та множення. Тоді перед нами комутативне кільце з одиницею та без дільників нуля, тобто цілісне кільце.

Приклад 1.6. Нехай R є множина неперервних дійсних функцій, визначених на відрізку $[-1, 1]$. Позначимо його через $C_{[-1,1]}$. Тоді відносно поточкового додавання та множення отримаємо комутативне кільце з одиницею та дільниками нуля. Дільники нуля можна легко задати наступним чином:

$$f_1(x) = \begin{cases} 0, & -1 \le x < 0, \\ x, & 0 \le x \le 1; \end{cases} \quad \text{и} \quad f_2(x) = \begin{cases} -x, & -1 \le x < 0, \\ 0, & 0 \le x \le 1; \end{cases}$$

З умов на функції видно, що $f_1(x) \cdot f_2(x) \equiv 0$.

Приклад 1.7. $R = M_n(C)$ – множина квадратних комплексних матриць відносно множення та додавання таких матриць. Це асоціативне кільце з дільниками нуля при $n > 1$.

Приклад 1.8. $R = Z[i] = \{z \in C \mid z = a + bi,\ a, b \in Z\}$ – кільце цілих гаусових чисел – цілісне кільце.

Враховуючи сказане, можна легко уявити найпростіші властивості кільця, які можна безпосередньо отримати із аксіом. Саме:

1°. $a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in R$;

2°. $a \cdot (-b) = (-a) \cdot b = -(ab) \quad \forall a, b \in R$;

3°. $a \cdot (-1) = (-1) \cdot a = -a \quad \forall a \in R$, якщо кільце має одиницю 1;

4°. $a \cdot (b - c) = ab - ac \quad \forall a, b, c \in R$. Тут різниця трактується як: $(b - c) = b + (-c)$;

5°. $(b - c) \cdot a = ba - ca \quad \forall a, b, c \in R$.

Якщо кільце не має дільників нуля, то справедливі закони скорочення на ненульовий множник:

6°. $(ac = ad \quad \wedge \quad a \neq 0) \Rightarrow c = d$;

7°. $(ca = da \quad \wedge \quad a \neq 0) \Rightarrow c = d$.

Означення 1.6. Нехай R – кільце и $J \subseteq R$, $J \neq \varnothing$. Тоді J називається *підкільцем* в R, якщо само утворює кільце відносно звуження операцій визначених на R.

Приклад 1.9. $Z \subset Q, \quad Q \subset R, \quad Q[\sqrt{2}] \subset R$.

Приклад 1.10. $\{0\} \subset Z$ – нульове (тривіальне) підкільце. Тривіальним назвемо також випадок $R \subseteq R$.

Приклад 1.11. Нехай $R = C_{[-1,1]}$, $\quad J = \{f(x) \in C_{[-1,1]} \mid f(0) = 0\}$ –підкільце в R.

Приклад 1.12. Нехай $R = Z$, тоді $J = \{x \in Z \mid x \vdots 2\}$ – підкільце в R.

Останній приклад, зокрема, показує, що підкільце може не зберігати всі властивості вихідного кільця. В даному випадку бачимо, що підкільце не має одиниці.

Теорема 1.1. (*критерій підкільця*)

Непуста підмножина J кільця R є його підкільцем тоді і лише тоді, коли

1) $\forall a, b \in J \quad a - b \in J$;

2) $\forall a, b \in J \quad ab \in J$.

Доведення. Перша умова задається критерієм підгрупи, а друге - очевидне.

Означення 1.7. Нехай R – комутативне кільце. Підкільце $J \subseteq R$ називається і*деалом кільця* R, якщо воно замкнуте по множенню на елементи кільця, тобто $\forall a \in J \quad \forall r \in R \quad ar \in J$.

Тривіальними ідеалами, очевидно, будуть само R та $0 = \{0\}$. Але можна привести менш очевидні приклади:

Приклад 1.13. Підкільця із прикладів 1.11, 1.12.

Приклад 1.14. Нехай R – комутативне кільце і $a \in R$, тоді найменшим ідеалом в R, що містить елемент *a, є* $J = < a > = \{x \in R \mid x = ar + na, \quad \forall r \in R, \quad \forall n \in Z\}$.

Приклад 1.15. Нехай R – комутативне кільце та $a \in R$, тоді ідеалом буде підкільце $J = < a > = \{x \in R \mid x = ar, \quad \forall r \in R\}$. Якщо кільце має одиницю, то приклади 1.14 і 1.15 збігаються.

Означення 1.8. Нехай R – комутативне кільце і $J \subseteq R$ ідеал в кільці, тоді J називається *головним ідеалом* в R, якщо в R існує такий елемент *a*, що $J =< a >$. При цьому *a* називається *породжувальним елементом* ідеалу.

Означення 1.9. Цілісне кільце, в якому кожен ідеал є головним, називається *кільцем головних ідеалів*.

Лема 1.1. Кільце Z – кільце головних ідеалів.

Доведення. Нехай J – довільний ідеал в Z і $J \neq \{0\}$. Нехай *a* – найменший додатний елемент в J. Тоді для будь-якого елемента $b \in J$ маємо по теоремі про ділення з остачею, що $b = aq + t$, де $0 \le t < a$. Звідси $t = b - aq \in J$, що суперечить вибору *a*,, якщо $t > 0$. Тому, $t = 0$, отже, $b = aq$ з деяким $q \in Z$. Тоді зрозуміло, що $J =< a >$, тобто головний ідеал.

Слідство. Всі ідеали кільця Z вичерпуються кільцями виду $nZ = \{x \in Z \mid x \vdots n,\ n \in N\}$.

Наведена лема легко доводиться, тому що в кільце цілих чисел справедлива теорема про ділення з остачею. Наявність останньої призводить до наступного означення.

Означення 1.10. Цілісне кільце R називається *евклідовим*, якщо є якась функція λ, $\lambda : R^* \to N_0$, що має наступну властивість: для будь-яких $a, b \in R$, $b \neq 0$, знайдуться такі $c, d \in R$, що $a = bc + d$ і або $d = 0$, або $\lambda(d) < \lambda(b)$.

Таким чином, видно, що кільце цілих чисел є евклідовим. Так само є і кільце многочленів над полем, бо в ньому також справедлива теорема про ділення з остачею, а роль функції λ грає ступінь многочлена $\deg$. Звідси виходить результат:

Лема 1.2. Кільце многочленів над полем є кільце головних ідеалів.

Доведення протікає як і в лемі 1.1.

Нарешті, розглянемо кільце цілих гаусових чисел $R = Z[i]$. Виберемо в якості функції λ норму числа, а саме: $\lambda(a + bi) = a^2 + b^2$. Легко бачити, що в цьому випадку $\lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta) \quad \forall \alpha, \beta \in Z[i]$.

Лема 1.3. Кільце цілих гаусових чисел евклідове.

Доведення. Нехай $\alpha = a + bi$, $\gamma = c + di$ і $\gamma \neq 0$. Тоді $\alpha/\gamma = r + si$, де $r, s \in Q$. Виберемо цілі $m, n \in Z$ такі, що $|r - m| \le 1/2$, $|s - n| \le 1/2$. І положимо $\delta = m + ni \in Z[i]$.

$$\lambda((\alpha/\gamma) - \delta) = (r - m)^2 + (s - n)^2 \le 1/4 + 1/4 = 1/2.$$

Нехай $\rho = \alpha - \gamma\delta$. Тоді $\rho \in Z[i]$ і або $\rho = 0$, або

$$\lambda(\rho) = \lambda(\gamma(\alpha/\gamma) - \delta) = \lambda(\gamma)\lambda(\alpha/\gamma - \delta) \le 1/2\,\lambda(\gamma) < \lambda(\gamma).$$

Таким чином, λ перетворює $Z[i]$ в евклідове кільце.

Лема 1.4. Кільце $Z[i]$ – кільце головних ідеалів.

Доведення легко повторює міркування леми 1.1 с $\lambda(\alpha)$ в якості норми.

Означення 1.11. Нехай R – комутативне кільце з одиницею, $J \subset R$ – ідеал в R і $\alpha, \beta \in R$. Тоді кажуть, що α *порівнюване* з β за ідеалом J і пишуть $\alpha \equiv \beta (\bmod J)$, якщо $\alpha - \beta \in J$.

Це бінарне відношення, очевидно, є відношенням еквівалентності і розбиває кільце R на класи елементів, що попарно не перетинаються, порівнюваних по ідеалу. Легко бачити, що зазначені класи є класами суміжності групи R по підгрупі J. Таким чином, отримуємо адитивну факторгруппу R/J, елементи якої мають вигляд: $\forall \alpha \in R \quad \overline{\alpha} = \alpha + J$. Операція над класами визначається співвідношенням:
$\overline{\alpha} + \overline{\beta} = (\alpha + J) + (\beta + J) = (\alpha + \beta) + J = \overline{\alpha + \beta}, \quad \forall \alpha, \beta \in R$. Визначимо тепер операцію множення класів, спираючись на наступні властивості порівнянності по ідеалу. А саме:

1°. Якщо $\alpha \equiv \beta (\bmod J)$ і $\gamma \equiv \delta (\bmod J)$, то $\alpha + \gamma \equiv \beta + \delta (\bmod J)$;

2°. Якщо $\alpha \equiv \beta (\bmod J)$ і $\gamma \equiv \delta (\bmod J)$, то $\alpha \cdot \gamma \equiv \beta \cdot \delta (\bmod J)$;

3°. Якщо $\alpha \equiv \beta (\bmod J)$, то $\alpha^n \equiv \beta^n (\bmod J) \ \ \forall n \in N_0$;

4°. Якщо $\alpha \equiv \beta (\bmod J)$, то $k\alpha \equiv k\beta (\bmod J) \ \ \forall k \in Z$;

5°. Якщо $\alpha \equiv \beta (\bmod J)$, то $\alpha + \gamma \equiv \beta + \gamma (\bmod J) \ \ \forall \gamma \in R$;

6°. Якщо $\alpha \equiv \beta (\bmod J)$, то $\alpha \cdot \gamma \equiv \beta \cdot \gamma (\bmod J) \ \ \forall \gamma \in R$.

Всі ці властивості елементарно доводяться, виходячи із означення порівнянності. Тоді операція множення класів може бути представлена співвідношенням:

$$\overline{\alpha} \times \overline{\beta} = (\alpha + J) \times (\beta + J) = \alpha\beta + J = \overline{\alpha\beta}.$$

Операція, описана таким чином, виявляється коректною, тобто не залежить від вибору представників в класах. Дійсно, якщо $\alpha_1 \in \overline{\alpha}$ и $\beta_1 \in \overline{\beta}$, то $\alpha_1 \equiv \alpha (\bmod J)$ і $\beta_1 \equiv \beta (\bmod J)$. Тому $\alpha_1\beta_1 \equiv \alpha\beta (\bmod J)$, отже $\overline{\alpha_1\beta_1} = \overline{\alpha\beta}$. Тоді факторгруппа R/J перетворюється в комутативне кільце з одиницею $1 + J$. Дистрибутивність множення відносно додавання перевіряється елементарно. Отримане кільце називається *факторкільцем кільця* R *по ідеалу* J.

Приклад 1.16. Нехай $R = Z$. Як ідеал виберемо головний ідеал, породжений цілим додатним числом $m > 1$, тобто $J = < m >$. Тоді R/J перетворюється в кільце класів відрахувань по модулю m, тобто в Z_m. Таке кільце при складеному m завідомо має дільники нуля, бо, якщо $m = m_1 m_2$, то $\overline{0} = \overline{m} = \overline{m_1 m_2} = \overline{m_1} \times \overline{m_2}$. Але при $m = p$, де p – просте число, Z_m перетворюється в поле класів віідрахувань. Кільце Z_p, вочевидь, цілісне. А оберненість ненульових елементів, тобто породжуваних числами взаємно простими з числом p, випливає з лінійного представлення найбільшого спільного дільника. Саме, якщо $\overline{a} \neq \overline{0}$, то $(a, p) = 1$, звідки отримаємо, що для деяких $u, v \in Z$

$$1 = a \cdot u + p \cdot v.$$

Переходячи до класів, легко видно, що

$$\overline{1} = \overline{a \cdot u + p \cdot v} = \overline{a \cdot u} + \overline{p \cdot v} = \overline{a} \times \overline{u} + \overline{p} \times \overline{v} = \overline{a} \times \overline{u} + \overline{0} \times \overline{v} = \overline{a} \times \overline{u}.$$

Таким чином, $\overline{u} = (\overline{a})^{-1}$. Отримуємо найпростіший варіант кінцевого поля, про яких будемо говорити пізніше. Слід сказати, що в цьому випадку можна представити поле з двох елементів, тобто мінімальне із можливих по порядку.

Якщо для простого p задати множину $F_p = \{0, 1, \ldots, p-1\}$ та визначити на цій множині операції додавання та множення за модулем p, то ця множина наділяється структурою поля Z_p. При очевидному ізоморфізмі $F_p \cong Z_p$ отримуємо абстрактний варіант кінцевого поля із p елементів.

Означення 1.12. Нехай R – довільне кільце. Якщо існує таке натуральне число n, що для будь-якого $r \in R$ виконується рівність $nr = 0$, то найменше із таких чисел n

називається *характеристикою* кільця R, а само кільце R називається кільцем додатної характеристики n. Якщо такого числа n не існує, то говорять, що кільце R має *нульову характеристику*. Позначення: $CharR$.

Лема 1.5. Якщо ненульове кільце R з одиницею і без дільників нуля має позитивну характеристику, то n – просте число.

Доведення. Так як кільце R містить ненульові елементи, то $n = CharR \geq 2$. Якщо n – складене число, то знайдуться такі $k, m \in N$, $1 < k < m < n$, що $n = km$. Тоді

$$0 = n1 = (km)1 = (k1)(m1).$$

Звідки або $k1 = 0$ або $m1 = 0$ (бо в кільці немає дільників нуля). Тому, або $kr = (k1)r = 0$, або $mr = (m1)r = 0$ для будь-якого $r \in R$, що входить в суперечність з означенням характеристики.

Слідство. Характеристика кінцевого поля завжди просте число. Зокрема, $CharF_p = p$.

Теорема 1.2. *Нехай* R *– комутативне кільце простої характеристики* p. *Тоді*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad и \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

для всіх $a, b \in R$ *і* $n \in N$.

Доведення. Скористаємося тим, що для $k \in N$, $1 \leq k \leq p-1$, біноміальний коефіцієнт

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} \equiv 0 \pmod{p}.$$

Це випливає з того, що коефіцієнт є цілим числом і множник p не може скоротитися. Тому у відповідність до формули бінома Ньютона маємо:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p.$$

А далі індукцією по n встановлюється основна і похідна тотожності.

Розглянемо на закінчення питання про те, яким має бути ідеал J комутативного кільця R з одиницею, щоб факторкільце R/J було цілісним або полем. Будуть потрібні нові означення.

Означення 1.13. Нехай R – комутативне кільце зс одиницею. Елемент $a \in R$ називається *дільником* елемента $b \in R$, якщо знайдеться такий елемент $c \in R$, що $ac = b$.

Означення 1.14. Дільники одиниці називаються *оберненими елементами* кільця.

Означення 1.15. Елементи a і b із R називаються *асоційованими*, якщо існує елемент $\varepsilon \in R$ такий, що $a = b\varepsilon$.

Означення 1.16. Елемент $c \in R$ називається *простим елементом* в R, якщо він не є оберненим елементом та не має інших дільників, крім асоційованих з ним елементів або оберненим елементів.

Означення 1.17. Ідеал $P \neq R$ кільця R називається *простим ідеалом*, якщо для $a, b \in R$ включення $ab \in P$ має місце лише в тому випадку, коли або $a \in P$, або $b \in P$.

Означення 1.18. Ідеал $M \neq R$ кільця R називається *максимальним ідеалом*, якщо для будь-якого ідеалу J кільця R включення $M \subseteq J$ тягне за собою $J = M$, або $J = R$.

Теорема 1.3. *Нехай* R *– комутативне кільце з одиницею. Тоді*

1°. Ідеал M кільця R є максимальним тоді й тільки тоді, коли факторкільце R/M є полем.

2°. Ідеал P кільця R є простим тоді й тільки тоді, коли факторкільце R/P є цілісним кільцем.

3°. Кожен максимальний ідеал кільця R є простим.

4°. Якщо R – кільце головних ідеалів, то факторкільце $R/<c>$ є полем в тому і тільки в тому випадку, коли c – простий елемент кільця R.

Доведення. 1°. Нехай M – максимальний ідеал кільця R. Тоді для $a \in R$, $a \notin M$, множина $J = \{ar + m \mid r \in R, m \in M\}$ є ідеалом кільця R, що містить M і відмінним від M. Тоді $J = R$. Зокрема, існують такі $r \in R$ і $m \in M$, що $ar + m = 1$. Це значить, що якщо $a + M \neq 0 + M$, тобто клас $a + M$ ненульовий в R/M, то він має мультиплікативне обернене, так як $(a+M)(r+M) = (1-m) + M = 1 + M$. Отже, R/M – поле. Зворотно, нехай R/M – поле, і нехай J – такий ідеал кільця R, що $J \supseteq M$, $J \neq M$. Тоді для $a \in J$, $a \notin M$, клас відрахувань $a + M$ має мультиплікативний зворотний, так що $(a+M)(r+M) = 1 + M$ для деякого $r \in R$. Це означає, що $ar + m = 1$ для деякого $m \in M$. Оскільки J – ідеал, $1 \in J$, а отже, $(1) = R \subseteq J$. Звідки $J = R$. Таким чином, M – максимальний ідеал кільця R.

2°. Нехай P – простий ідеал кільця R. Тоді факторкільце R/P є комутативним кільцем з одиницею $1 + P \neq 0 + P$. Нехай $(a+P)(b+P) = 0 + P$. Тоді $ab \in P$. Оскільки P – простий ідеал, то або $a \in P$, або $b \in P$, тобто або $a + P = 0 + P$, або $b + P = 0 + P$. Таким чином, факторкільце R/P не має дільників нуля, а тому є цілісним кільцем. Проводячи міркування в зворотному порядку встановлюємо достатність твердження.

3°. Це твердження випливає з двох попередніх, бо кожне поле є цілісне кільце.

4°. Нехай тепер $c \in R$ и $R/<c>$ – поле. Якщо c – обернений елемент, то $<c> = R$ і факторкільце $R/<c>$ складається з єдиного елемента і, таким чином, не може бути полем. Якщо c не обернений і не простий елемент, то c має деякий дільник $a \in R$, який не є асоційованим з c і не є оберненим елементом. При цьому $a \neq 0$, так як якщо $a = 0$, то і $c = 0$ і a було б асоційованим з c. Нехай $c = ab$, де $b \in R$. Можна стверджувати, що $a \notin <c>$. Дійсно, у противному випадку $a = cd = abd$, де $d \in R$. Таким чином, $a(1 - bd) = 0$. Оскільки $a \neq 0$, то $bd = 1$. Звідки b – обернений елемент, а це суперечить тому, що a не асоційований з c. Отже, $<c> \subset <a> \subset R$, де всі включення власні, так що факторкільце $R/<c>$ не може бути полем через 1°. Отже, залишається останній варіант, за якого c є простий елемент кільця R.

Якщо c – простий елемент R, то покажемо, що $R/<c>$ – поле. Маємо, $<c> \neq R$, тому що c не є оберненим елементом. Нехай далі $J \supseteq <c>$ – ідеал кільця R. Тоді $J = <a>$ для деякого $a \in R$, бо R – кільце головних ідеалів. Отже, $c \in <a>$, так що a є дільником елемента c. Тому a – або обернений елемент, або асоційований з c. Звідки або $J = R$, або $J = <c>$. Це значить, що $<c>$ – максимальний ідеал кільця R. І за першою частиною теореми отримуємо, що $R/<c>$ – поле.

Як додаток, помітимо, що можна одержати інший доказ того, що $Z/<p> = Z_p$ – поле для будь-якого простого числа p. За аналогією можна будувати поля як факторкільця кільця многочленів над полем за ідеалом, породженим неприведеним над даним полем многочленом тощо.

2. РОЗШИРЕННЯ ПОЛІВ

В цьому розділі розглянемо деякі конструкції, пов'язані з полями. Зокрема, можливості побудови нових полів на основі наявних. Оскільки кожне поле є цілісне кільце, то все сказане вище про них виявляється справедливим і для полів. Але все ж дамо кілька необхідних визначень

Означення 2.1. Непорожня підмножина S поля P називається його *підполем,* якщо сама є полем відносно звуження операцій, визначених для P. Поле P при цьому називається *розширенням* поля S.

Лема 2.1. Перетин будь-якої сукупності підполів даного поля є підполе цього поля.

Доведення тривіальне.

Означення 2.2. Поле, що не має власних підполів, крім себе самого, називається *простим* полем.

Означення 2.3. Перетин всіх підполів даного поля називається *простим підполем* цього поля.

Просте підполе, очевидно, є простим. Наведемо кілька прикладів. По-перше, приклади полій.

Приклад 2.1. Поле раціональних чисел Q.

Приклад 2.2. Поле дійсних чисел R.

Приклад 2.3. Поле комплексних чисел C.

Приклад 2.4. Поле $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$.

Приклад 2.5. Поле $Q(i) = \{a + bi \mid a, b \in Q\}$ гаусових чисел.

Приклад 2.6. Поле $F_p \cong Z_p$. Останнє є поле класів відрахувань по модулю простого p.

Приклад 2.7. Поле $R(x) = \left\{ \dfrac{f(x)}{g(x)} \mid f(x), g(x) \in R[x], g(x) \neq 0 \right\}$ – це поле дійсних раціональних функцій відносно звичайних операцій додавання та множення.

Приклад 2.8. Поле F_4 з чотирьох елементів, операції в якому задаються наступними таблицями Келі: $F_4 = \{0, 1, a, b\}$,

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Легко бачити, що мають місце наступні включення:

$$Q \subset Q(\sqrt{2}) \subset R \subset C, \quad Q \subset Q(i) \subset C \text{ и } F_2 \subset F_4.$$

В останньому випадку $F_2 = \{0, 1\}$ має тривіальні таблиці Келі, де $1 + 1 = 0$.

Поля із прикладів 2.6 і 2.8 мають характеристику 2, всі інші мають характеристику 0. Поле F_p очевидно просте. А простоту поля Q можна довести, як невелику вправу. Тут доречно сформулювати нескладну теорему.

Теорема 2.1. *Просте підполе поля P ізоморфно або полю F_p при деякому простому числі p, або полю Q. Відповідно до цього характеристика поля P дорівнює p або 0.*

Доведення видається тривіальним.

Надалі, якщо не зазначено протилежне, дослідження проводяться для полів *нульової* характеристики.

Означення 2.4. Нехай K є розширення поля P. Елемент $\alpha \in K$ називається *алгебраїчним елементом над* P, якщо існує ненульовий многочлен $f(x) \in P[x]$, коренем якого є α, тобто $f(\alpha) = 0$. Якщо такого многочлена не існує, то елемент α називається *трансцендентним над* P.

Приклад 2.9. Число $\sqrt{2}$ є алгебраїчним над полем Q, бо є коренем многочлена $x^2 - 2 \in Q[x]$.

Приклад 2.10. Кожен елемент із P алгебраїчний над P.

Приклад 2.11. В курсах теорії чисел доводиться трансцендентність чисел e і π над полем Q. Доведення ці зовсім не прості.

Важливо усвідомити, що поняття алгебраїчності і трансцендентності є відносними. Тут вирішальне значення має те поле, над яким розглядається елемент. Так число $e \in R$ і $\pi \in R$ алгебраїчні над R.

Означення 2.5. Поле K називається *алгебраїчним розширенням* поля P, якщо кожен його елемент алгебраїчний над P.

Виходячи з цього означення можна сказати, що поле комплексних чисел є алгебраїчним розширенням поля R, бо кожне суттєво комплексне число є коренем дійсного квадратичного многочлена. Поле $Q(\sqrt{2})$ є алгебраїчне розширення поля Q. З іншого боку, поле R не є алгебраїчним розширенням поля Q.

Означення 2.6. Розширення K поля P називається *трансцендентним*, якщо воно не є алгебраїчним розширенням.

Означення 2.7. Розширення K поля P називається *скінченим*, якщо в полі K існують такі елементи $\alpha_1, \alpha_2, \ldots, \alpha_n$, що будь-який елемент $\beta \in K$ єдиним чином записується у вигляді лінійної комбінації з коефіцієнтами із поля P:

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n,\ a_i \in P,\ i = 1, 2, \ldots, n.$$

При цьому система елементів $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ називається *базисом* поля K над полем P.

Очевидно, що таке означення дає змогу розглядати кінцеве розширення як лінійний простір над полем P скінченної розмірності n. Базис поля перетворюється в базис лінійного простору, а оскільки всі базиси скінченовимірного простору складаються з однакової кількості векторів (розмірність простору), то й усі базиси поля K над P зобов'язані складатися з n елементів.

Означення 2.8. Кількість елементів базису поля К над полем P називається *ступенем розширення* K над P і позначається $[K : P]$.

Приклад 2.12. Легко показати, що $[K : P] = 1 \Leftrightarrow K = P$.

Приклад 2.13. Розглянемо пару (вежу полів) $Q \subset Q(\sqrt{2})$. Ясно, що базисом поля $Q(\sqrt{2})$ над Q є лінійно незалежна над Q система $\langle 1, \sqrt{2} \rangle$, через яку лінійно виражається кожен елемент із $Q(\sqrt{2})$. Тому це і буде базисом $Q(\sqrt{2})$ над Q. А тоді $[Q(\sqrt{2}) : Q] = 2$.

Теорема 2.2. *Кожне скінченне розширення є алгебраїчним.*

Доведення. Нехай K – скінченне розширення поля P и $[K:P]=n$. Тоді для будь-якого $\beta \in K$ система елементів $\langle 1, \beta, \beta^2, \ldots, \beta^n \rangle$ виявляється лінійно залежною над P як система із $n+1$ елемента. Тому існують елементи $c_0, c_1, c_2, \ldots, c_n \in P$, не всі рівні нулю, такі, що

$$c_0 \cdot 1 + c_1 \cdot \beta + c_2 \cdot \beta^2 + \cdots + c_n \cdot \beta^n = 0.$$

Отже, елемент β є коренем ненульового многочлена $g(x) \in P[x]$,

$$g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n.$$

А тоді β виявляється алгебраїчним над полем P, а отже і K алгебраїчно над P.

Означення 2.9. Нехай P – довільне поле, M – деяка множина елементів така, що існує поле T, що містить поле P і множину M, причому операції в полях P і T узгоджені. Тоді мінімальне підполе поля T, що містить поле P і множину M, називається полем, отриманим із P *приєднанням елементів* із M і позначається $P(M)$.

Зрозуміло, що $P(M)$ є перетин всіх підполів із T, що містять P і множину M. Зазвичай M містить кінцеве число елементів, тобто $M = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Тоді пишуть $P(M) = P(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Означення 2.10. Якщо M – скінченна множина, то $P(M) = P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ називають *скінчено породженим* розширенням поля P. Якщо $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ алгебраїчні над P, то говорять про *алгебраїчно породжене* розширення; якщо $n=1$ – то про *просте алгебраїчне розширення*.

Означення 2.11. Розширення K поля P називається *складеним алгебраїчним розширенням*, якщо існує вежа полів

$$P = L_0 \subset L_1 \subset \ldots \subset L_{s-1} \subset L_s = K$$

така, що для будь-якого $i = 1, 2, \ldots, s$ поле L_i є простим алгебраїчним розширенням поля L_{i-1}. Якщо $L_i = L_{i-1}(\alpha_i)$, $i = 1, 2, \ldots, s$, то поле K позначається через $K = P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$.

Зазначимо так, що алгебраїчність $\alpha_2, \ldots, \alpha_s$ над P не передбачається.

Лема 2.2. Поле $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ є множина дробово-раціональних функцій від $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Доведення. Многочлени над полем P, очевидно, будуть елементами цього поля. А оскільки потрібна ще й оборотність ненульових елементів, то приходимо до дробово-раціональних функцій.

Нехай тепер P – деяке поле і α – алгебраїчний над P елемент. Це означає, що α є корінь ненульового многочлена із $P[x]$.

Означення 2.12. Многочлен найменшого ступеня із $P[x]$, коренем якого є алгебраїчний над P елемент α, називається *мінімальним многочленом* цього елемента.

Лема 2.3. За умов означення 2.12 мінімальний многочлен неприводимий над P.

Доведення. Якщо припустити протилежне, то елемент α виявиться коренем якого-небудь власного дільника цього многочлена, тобто коренем многочлена меншого ступеня, що суперечить визначенню.

Припустимо, що у даного елемента є два мінімальні многочлени, що задовольняють визначенню 2.12. Тоді внаслідок того, що вони не є взаємно прості й обидва неприводимі, вони мають ділитися один на одного. Це означає, що ці многочлени відрізняються один від одного лише постійним множником. Таким чином, із множини мінімальних многочленів завжди можна виділити один *нормований* многочлен. Він уже визначений однозначно, і його будемо вважати мінімальним многочленом елемента α.

Означення 2.13. Ступінь мінімального многочлена елемента α над полем P називається *ступенем алгебраїчного елемента* α над полем P.

З теореми 2.2 випливає, що ступінь будь-якого елемента скінченного розширення K поля P не перевершує ступені розширення $[K:P]$.

Задача. Показати, що ступінь α дорівнює одиниці тоді й тільки тоді, коли $\alpha \in P$.

Розглянемо будову простих алгебраїчних розширень $P(\alpha)$. Як уже говорилося, лема 2.2, поле $P(\alpha)$ є множина дробово-раціональних функцій від елемента α. Тепер доведемо більш сильне твердження.

Теорема 2.3. *Будь-який елемент простого алгебраїчного розширення* $P(\alpha)$ *може бути представлений у вигляді многочлена від* α *над полем* P.

Доведення. Нехай $f(x)$ буде мінімальним многочленом елемента α над P ступеню n. Розглянемо множину K тих елементів $\beta \in P(\alpha)$, для яких існує многочлен $g(x) \in P[x]$ такий, що $\beta = g(\alpha)$. Ясно, що $K \subset P(\alpha)$. Доведемо, що K є поле. Операції додавання та множення таких елементів, очевидно, алгебраїчні. Тому слід лише довести оборотність ненульових елементів. Нехай $\beta \neq 0$, $\beta \in K$, покажемо, що $\beta^{-1} \in K$. За умовою $\beta = g(\alpha)$, де $g(x) \in P[x]$. При цьому α не є коренем $g(x)$. За властивістю не приведених многочленів, тому що $f(x)$ не ділить $g(x)$, тому взаємно простий з ним. Тоді по теоремі про лінійне представлення найбільшого спільного дільника існують такі многочлени $u(x), v(x) \in P[x]$, що

$$f(x)u(x) + g(x)v(x) = 1.$$

Припускаючи в цій рівності $x = \alpha$, отримаємо

$$g(\alpha)v(\alpha) = 1,$$

або

$$\beta \cdot v(\alpha) = 1.$$

Таким чином,

$$\beta^{-1} = v(\alpha), \quad \text{а} \quad v(\alpha) \in K.$$

Отже, K є полем. Оскільки $P \subset K$ за означенням і $\alpha \in K$, то K є розширенням поля P, що містить α. Тоді в силу мінімальності $P(\alpha)$ маємо:
$P(\alpha) \subset K$, т.е. $P(\alpha) = K$. Теорему доведено.

Многочлен $g(x)$ для елемента β визначений неоднозначно. Дійсно, до нього можна додати будь-який многочлен, що ділиться на $f(x)$. Іншими словами, з кожним β можна зв'язати клас суміжності по ідеалу $(f(x))$. Справедлива теорема:

Теорема 2.4. $g(\alpha) = g_1(\alpha) \Leftrightarrow g(x) \equiv g_1(x) (\mathrm{mod}\, f(x))$.

Доведення. *Необхідність*. Розглянемо різницю $g(x) - g_1(x)$ і розділимо її на $f(x)$ з остачею. Маємо

$$g(x) - g_1(x) = f(x)q(x) + r(x), \text{ де } \deg r(x) < \deg f(x) \text{ або } r(x) = 0.$$

Вважаючи $x=\alpha$, одержимо

$$0=g(\alpha)-g_1(\alpha)=f(\alpha)q(\alpha)+r(\alpha)=r(\alpha).$$

Звідси видно, що через мінімальність $f(x)$ многочлен $r(x)=0$, а значить

$$g(x)\equiv g_1(x)(\mathrm{mod}\, f(x)).$$

Достатність. Якщо $g(x)-g_1(x)=f(x)q(x)$, то очевидно, що $g(\alpha)-g_1(\alpha)=0$, звідки одержуємо потрібне.

Отже, у кожному класі суміжності можна вибрати многочлен в вигляді залишку $r(x)$ від ділення на $f(x)$. Цей залишок буде мати ступень, що не перевищує $n-1$. Саме:

$$r(x)=b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}\in P[x].$$

Тоді

$$\beta=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_{n-1}\alpha^{n-1}.$$

Причому це представлення єдине, що випливає з теореми 2.4. У підсумку отримуємо наступну теорему:

Теорема 2.5. *Елементи* $\langle 1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\rangle$ *утворюють базис поля* $P(\alpha)$ *над* P, *тобто просте алгебраїчне розширення* $P(\alpha)$ *є скінченним і його ступінь* $[P(\alpha):P]$ *дорівнює ступеню елемента* α *над* P.

Займімося тепер складеними розширеннями. Нехай $K=P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$ – складене алгебраїчне розширення поля P. Виявляється, що будь-який елемент такого розширення є многочлен над полем P от $\alpha_1,\alpha_2,\ldots,\alpha_s$.

Теорема 2.6. *Для будь-якого елемента* $\beta\in P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$ *існує над полем* P *многочлен* $g(x_1,x_2,\ldots,x_s)$ *від невідомих* $x_1,x_2,\ldots,x_s$, *що*

$$\beta=g(\alpha_1,\alpha_2,\ldots,\alpha_s).$$

Доведення. Доведемо це твердження індукцією по s. Для $s=1$ теорема справедлива через теорему 2.3. Нехай теорема вже доведена для поля $L=P(\alpha_1)(\alpha_2)\ldots(\alpha_{s-1})$. Розглянемо довільний елемент $\beta\in K$. Так як $K=L_{s-1}(\alpha_s)$, то над полем L_{s-1} існує такий многочлен $h(x)$, що $\beta=h(\alpha_s)$. Нехай

$$h(x)=\gamma_0+\gamma_1x+\cdots+\gamma_nx^n,\quad \text{де}\quad \gamma_0,\gamma_1,\ldots,\gamma_n\in L_{s-1}.$$

За припущенням індукції для будь-якого $i=0,1,\ldots,n$ знайдеться такий многочлен

$$h_i(x_1,x_2,\ldots,x_{s-1})$$

від $s-1$ невідомих, що

$$\gamma_i=h_i(\alpha_1,\alpha_2,\ldots,\alpha_{s-1}).$$

Отже, вважаючи

$$g(x_1,x_2,\ldots,x_s)=h_0(x_1,x_2,\ldots,x_{s-1})+h_1(x_1,x_2,\ldots,x_{s-1})x_s+\cdots+h_n(x_1,x_2,\ldots,x_{s-1})x_s^n,$$

отримаємо, що

$$\beta=g(\alpha_1,\alpha_2,\ldots,\alpha_s).$$

Теорему доведено.

Розглянемо тепер довільне алгебраїчно породжене розширення $P(\alpha_1,\alpha_2,\ldots,\alpha_n)$ поля P і визначимо за індукцією поля $L_0,L_1,\ldots,L_n$, вважаючи

$$L_0=P,\ L_1=L_0(\alpha_1),\ \ldots,\ L_i=L_{i-1}(\alpha_i),\ldots,L_n=L_{n-1}(\alpha_n).$$

Тому що для будь-якого $i = 1, \ldots, n$ елемент α_i алгебраїчний над полем P, то він алгебраїчний і над його розширенням L_{i-1}, тому поле L_i є просте алгебраїчне розширення поля L_{i-1} й, отже, поле L_n виявляється складеним алгебраїчним розширенням $P(\alpha_1)(\alpha_2)\ldots(\alpha_n)$ поля P. Тому, відповідно до щойно доведеного твердження, будь-який елемент поля L_n можна виразити у вигляді многочлена (над P) от $\alpha_1, \alpha_2, \ldots, \alpha_n$ і, отже, належить полю $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Інакше кажучи,

$$L_n \subset P(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

З іншого боку, поле L_n містить всі елементи $\alpha_1, \alpha_2, \ldots, \alpha_n$ і, з огляду на мінімальність розширення $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$,

$$P(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset L_n.$$

Отже,

$$P(\alpha_1, \alpha_2, \ldots, \alpha_n) = P(\alpha_1)(\alpha_2)\ldots(\alpha_n).$$

Отримуємо результат:

Теорема 2.7. *Будь-яке алгебраїчно породжене розширення є складеним алгебраїчним.*

Наслідок. Будь-який елемент алгебраїчно породженого розширення $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *виражаєтьсяу вигляді многочлена над полем* P *від елементів* $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Повернемося до довільних скінчених розширень. Через теорему 2.2, базис такого розширення K поля P $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ є система елементів, алгебраїчних над P. Тому розширення $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ є алгебраїчно породженим. Зважаючи на свою мінімальність

$$P(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset K.$$

З іншого боку, довільний елемент із K має вигляд

$$\beta = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n,\ b_i \in P,\ i = 1, 2, \ldots, n.$$

Отже, $\beta \in P(\alpha_1, \alpha_2, \ldots, \alpha_n)$, а звідси

$$K \subset P(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

І, отже, остаточно

$$K = P(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Тим самим доведено

Теорема 2.8. *Усяке скінченне розширення є алгебраїчно породженим.*

Розглянемо тепер вежу полів

$$P \subset L \subset K.$$

Вона визначає три пари розширень полів і доведемо відносно неї наступну теорему.

Теорема 2.9. *Якщо в вежі полів* $P \subset L \subset K$ *є дві пари скінченних розширень, то й третя пара є скінченним розширенням, причому має місце рівність*

$$[K : P] = [K : L] \cdot [L : P]. \qquad (*)$$

Доведення. Якщо K скінченно над P, то скінченність L над P випливає із того, що L є підпростір скінченновимірного простору K над P. Скінченність K над L випливає з того, що для будь-яких $n+1$ елементів із K (де $[K : P] = n$) існує лінійна комбінація, що дорівнює нулю, з коефіцієнтами із P (а отже і з L) не всі з яких дорівнюють нулю. Таким чином, будь-яка система $n+1$ елемента із K лінійно залежна над L.

Якщо ж K скінченно над L, а L скінченно над P, то скінченність K над P випливає із зазначеної формули (*). Тому доведемо її.

Нехай $\langle \xi_1, \ldots, \xi_l \rangle$ – базис L над P, а $\langle \eta_1, \ldots, \eta_m \rangle$ – базис K над L. Покажемо, що система

$$\langle \xi_i \eta_j \mid i = 1, \ldots, l; \quad j = 1, \ldots, m \rangle \qquad (**)$$

утворює базис K над P.

Справді, система елементів $\xi_i \eta_j$ лінійно незалежна над P, бо якщо

$$\sum_{i=1}^{l} \sum_{j=1}^{m} c_{ij} \xi_i \eta_j = 0, \quad c_{ij} \in P, \quad i = 1, \ldots, l; \quad j = 1, \ldots, m,$$

то

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{l} c_{ij} \xi_i \right) \eta_j = \sum_{j=1}^{m} \alpha_j \eta_j = 0, \qquad \alpha_j = \sum_{i=1}^{l} c_{ij} \xi_i \in L.$$

Оскільки $\langle \eta_1, \ldots, \eta_m \rangle$ – базис K над L, то $\alpha_j = 0$, $j = 1, \ldots, m$. Так що

$$\sum_{i=1}^{l} c_{ij} \xi_i = 0$$

для кожного $j = 1, \ldots, m$. Але $\langle \xi_1, \ldots, \xi_l \rangle$ – базис L над P, тому $c_{ij} = 0$ для всіх $i = 1, \ldots, l; \quad j = 1, \ldots, m$. Крім того, якщо $\gamma \in K$, то

$$\gamma = \sum_{j=1}^{m} \beta_j \eta_j, \text{ де } \beta_j \in L, \quad j = 1, \ldots, m.$$

Представимо β_j, $j = 1, \ldots, m$, у вигляді

$$\beta_j = \sum_{i=1}^{l} a_{ij} \xi_i, \quad a_{ij} \in P, \quad i = 1, \ldots, l; \quad j = 1, \ldots, m.$$

Тоді

$$\gamma = \sum_{i=1}^{l} \sum_{j=1}^{m} a_{ij} \xi_i \eta_j.$$

Таким чином, кожен елемент з K лінійно виражається через систему (**) з коефіцієнтами із P, а тому система (**) є базисом K над P. Так що

$$[K : P] = l \cdot m = [L : P] \cdot [K : L].$$

Наслідок. Ступінь будь-якого елемента α скінченого розширення K поля P ділить ступінь розширення $[K : P]$.

Доведення. Дійсно, якщо розглянути просте алгебраїчне розширення $P(\alpha)$ поля P, то маємо вежу полів

$$P \subset P(\alpha) \subset K,$$

а ступінь розширення $P(\alpha)$ за теоремою 2.5 дорівнює ступеню елемента α над P.

Задача 2.2. Довести, що скінченне розширення ступеня n тоді й тільки тоді є простим алгебраїчним розширенням, коли в ньому існує елемент, що має ступінь n.

Далі, розглянемо результат, аналогічний основній теоремі алгебри комплексних многочленів відомо, вона стверджує наявність, узагалі кажучи, комплексного кореня у будь-якого многочлена з числовими коефіцієнтами додатного ступеня. Схожа ситуація складається і в загальному випадку.

Теорема 2.10 (Кронекера). *Нехай P – поле і $f(x) \in P[x]$, причому* $\deg f(x) = n \geq 1$. *Тоді існує кінцеве розширення K поля P, в якому містяться всі корені $f(x)$.*

Доведення. Не обмежуючи загальності міркувань можна вважати, що $f(x)$ – неприводимий над P многочлен, тому що будь-який многочлен додатного ступеню

розкладається над полем P в добуток неприводимих над P. Розглянемо факторкільце $P[x]/(f(x))$. Через неприводимість $f(x)$ за теоремою 1.3 одержуємо, що цей фактор є полем, тому що $f(x)$ відіграє роль простого елемента в $P[x]$. Це поле, яке містить поле P як підполе. Позначимо його K. Ненульові елементи із P, як многочлени нульового ступеню, розташовуються в різних суміжних класах, а операції над класами узгоджені з операціями в полі P. Тому $P \subset K$. Клас, в якому міститься елемент b, позначимо через B, а через X позначимо клас в якому міститься многочлен $g(x) = x$. Тоді, якщо $\overline{B}$ – клас, який визначається многочленом

$$b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$$

то

$$\overline{B} = b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 = B_{n-1}X^{n-1} + \cdots + B_1 X + B_0.$$

Із цього видно, що система $\langle 1, X, X^2, \ldots, X^{n-1}\rangle$ утворює базис поля K над P, оскільки вона лінійно незалежна над P. Тут треба врахувати, що відбувається заміна поля P на ізоморфне йому поле класів $\overline{P}$, а потім відбувається ототожнення $P \equiv \overline{P}$. Тоді $[K:P] = n$, а $K = P(X)$. Нарешті, якщо

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

то сума

$$A_n X^n + \cdots + A_1 X + A_0$$

визначає в K клас, в якому міститься $f(x)$, а тому

$$A_n X^n + \cdots + A_1 X + A_0 = \overline{0} = 0.$$

Таким чином, у полі K многочлен $f(x)$ має корінь X. Але тоді

$$f(x) = (x - X) f_1(x),$$

де

$$f_1(x) \in K[x], \quad \deg f_1(x) = n - 1.$$

Застосовуючи наведені міркування до неприводимих многочленів над K, на які розкладається многочлен $f_1(x)$, одержимо розширення K_1, в якому міститься корінь $f_1(x)$, а значить і новий корінь $f(x)$. K_1 скінченно над K, а значить і над P.

Таким чином, через кінцеве число кроків побудуємо скінченне розширення $\overline{K}$ поля P, в якому містяться всі корени $f(x)$. Теорема доведена.

Наступний результат у відомому розумінні підбиває певний підсумок питання про скінченні розширення. Саме:

Теорема 2.11 (про примітивний елемент). *Кожне скінченне розширення є простим алгебраїчним.*

Доведення. Нехай K – скінченне розширення поля P, $[K:P] = n$, і нехай $\langle \alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ – базис K над P. Тоді $P(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset K$ й оскільки кожен елемент із K можна представити лінійною комбінацією елементів $\langle \alpha_1, \alpha_2, \ldots, \alpha_n\rangle$, то й $K \subset P(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Отже, $K = P(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Це результат теореми 2.8. І як уже доводили раніше, останнє розширення можна представити у вигляді складеного:

$$P(\alpha_1, \alpha_2, \ldots, \alpha_n) = P(\alpha_1)(\alpha_2)\ldots(\alpha_n).$$

Твердження теореми буде доведено, якщо покажемо, що для будь-яких алгебраїчних над P елементів α і β знайдеться алгебраїчний над P елемент Θ такий, що $P(\alpha, \beta) = P(\Theta)$. Дійсно, тоді маємо

$$P(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) = P(\alpha_1, \ldots, \alpha_{n-2})(\alpha_{n-1}, \alpha_n) = P(\alpha_1, \ldots, \alpha_{n-2})(\Theta_{n-1}) =$$
$$P(\alpha_1, \ldots, \alpha_{n-2}, \Theta_{n-1}) = P(\alpha_1, \ldots, \alpha_{n-3})(\alpha_{n-2}, \Theta_{n-1}) = P(\alpha_1, \ldots, \alpha_{n-3})(\Theta_{n-2}) =$$
$$P(\alpha_1, \ldots, \alpha_{n-3}, \Theta_{n-2}) = \cdots = P(\alpha_1, \Theta_2) = P(\Theta_1).$$

Отже, нехай $K = P(\alpha, \beta)$, де α і β – алгебраїчні над P. Позначимо через $f_1(x)$ і $f_2(x)$ – мінімальні многочлени відповідно елементів α і β над P.

Нехай

$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ – корені $f_1(x)$ в деякому розширенні поля P,

а

$\beta_1 = \beta, \beta_2, \ldots, \beta_n$ – корені $f_2(x)$ в деякому розширенні поля P.

Всі елементи α_i, $i = 1, \ldots, m$, і всі елементи β_j, $j = 1, \ldots, n$, попарно різні, тому що відповідні многочлени неприводимі над P і тому не мають кратних коренів.

Розглянемо елементи виду

$$\frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j},$$

де $i = 1, \ldots, m$, $j = 2, \ldots, n$. Легко бачити, що кількість таких елементів є $m \cdot (n-1)$, тобто кінцева. Тоді в полі P можна вибрати елемент c, не дорівнює жодному із елементів зазначеного виду. Нехай такий вибір зроблено. Позначимо

$$\Theta = \alpha + c\beta.$$

В силу вибору c можна стверджувати, що

$$\Theta \neq \alpha_i + c\beta_j$$

при $i = 1, \ldots, m$, $j = 2, \ldots, n$.

Елемент Θ, очевидно, належить полю K, але K, будучи скінченним розширенням, є алгебраїчним розширенням, значить і Θ алгебраїчно над P.

Побудуємо просте алгебраїчне розширення $P(\Theta)$. Тоді зрозуміло, що

$$P(\Theta) \subset K.$$

Розглянемо многочлен

$$g(x) = f_1(\Theta - cx).$$

Цей многочлен з кільця $P(\Theta)[x]$ має спільний корень β з многочленом $f_2(x)$, який теж можна розглядати над полем $P(\Theta)$. Ніяких інших спільних коренів з $f_2(x)$ многочлен $g(x)$ не має в силу вибору c, тому що, якби знайшлося j серед чисел $2, \ldots, n$ таке, що

$$\Theta - c\beta_j = \alpha_i,$$

де i – одне з чисел $1, \ldots, m$, то виявилося б

$$c = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}.$$

Тому найбільший спільний дільник многочленів $g(x)$ і $f_2(x)$ є $x - \beta$:

$$\big(g(x), f_2(x)\big) = x - \beta.$$

Як відомо з курсу вищої алгебри, найбільший спільний дільник двох многочленів належить тому кільцю, в якому лежать ці многочлени. В розглядуваному випадку це $P(\Theta)[x]$. Отже,

$$\beta \in P(\Theta).$$

А тоді, оскільки $c \in P$, то й

$$\alpha = \Theta - c\beta \in P(\Theta).$$

Як було показано раніше

$$P(\alpha)(\beta) = P(\alpha, \beta),$$

и тепер ясно, що

$$P(\alpha, \beta) \subset P(\Theta).$$

Згадуючи, що

$$K = P(\alpha, \beta) \supset P(\Theta),$$

отримуємо

$$P(\alpha, \beta) = P(\Theta).$$

Теорему доведено. Елемент Θ називається примітивним елементом поля K.

Наслідок. Кожний елемент α ступеня n скінченного розширення K поля P ступеня $n = [K:P]$ є примітивним елементом поля K, тобто. $K = P(\alpha)$.

До сказаного додамо ще один корисний факт.

Теорема 2.12. *Нехай K – розширення поля P. Якщо існує натуральне $n \geq 1$ таке, що кожний елемент $\alpha \in K$ має ступінь менший або рівний n над P, то K – скінченне розширення P і $[K:P] \leq n$.*

Доведення. Дійсно, нехай m – максимальний ступінь елементів із K над P. Тоді знайдеться елемент $\alpha \in K$, ступінь якого дорівнює m. Маємо вежу полів

$$P \subset P(\alpha) \subseteq K.$$

Можна стверджувати, що $K = P(\alpha)$. В іншому випадку, знайдеться $\beta \in K$, $\beta \notin P(\alpha)$. Розглянемо розширення $P(\alpha, \beta)$. Нехай γ буде примітивним елементом $P(\alpha, \beta)$, тобто $P(\alpha, \beta) = P(\gamma)$. Тоді з вежі полів

$$P \subset P(\alpha) \subset P(\alpha, \beta) = P(\gamma)$$

випливає, що

$$[P(\gamma):P] > m,$$

що суперечить умові.

Нехай тепер K и K' – два розширення поля P, і припустимо, що існує ізоморфізм $\varphi: K \to K'$. Позначимо через P_0 множину елементів із P, що залишаються під впливом φ, тобто $P_0 = \{a \in P \mid \varphi(a) = a\}$. Це множина не порожня, тому що 0 й 1 належать P_0. Більш того, P_0 є підполе поля P, що містить просте підполе поля P. Цей факт залишимо студентам для самостійного доведення.

Означення 2.14. Ізоморфізм $\varphi: K \to K'$ (де K и K' – розширення основного поля P) називається *відносним ізоморфізмом*, якщо він залишає на місці всі елементи поля P.

Вивчимо докладніше ізоморфізми у випадку, коли K (а отже і K') – скінченне розширення поля P. Нехай $[K:P] = n$ і Θ – примітивний елемент поля K. Нехай $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ – мінімальний многочлен для Θ над P. Тоді

$$0 = f(\Theta) = \Theta^n + a_{n-1}\Theta^{n-1} + \cdots + a_1\Theta + a_0. \qquad (***)$$

Коефіцієнти a_i, $i = 0, 1, \ldots, n-1$, належать полю P, тому якщо Θ' – образ Θ в полі K' під дією відносного ізоморфізму φ, то застосовуючи φ до рівності (***) і користуючись тим, що образ суми (і, відповідно, добутку) дорівнює сумі (і, відповідно, добутку) образів, одержуємо

$$0 = (\Theta')^n + a_{n-1}(\Theta')^{n-1} + \cdots + a_1\Theta' + a_0. \qquad (****)$$

З (****) робимо висновок, що Θ' є коренем многочлена $f(x)$, і значить, є алгебраїчним над P ступенем n. Але тоді $K' = P(\Theta')$, бо $[P(\Theta') : P] = n$ і $P(\Theta') \subseteq K'$.

Означення 2.15. Два елемента α и β поля K називаються співпряженими над полем P, якщо вони є коренями одного й того же неприводимого над P многочлена.

Задача 2.3. Довести, що образом елемента $\alpha \in K$ при відносному ізоморфізмі K на K' буде елемент $\alpha' \in K'$, співпряжений з α над полем P.

Теорема 2.13. *Нехай K – скінченне розширення поля P. Тоді існує точно n відносних ізоморфізмів поля K над P, де $n = [K : P]$.*

Доведення. Нехай K' – образ K при деякому відносному ізоморфізмі φ. Нехай Θ – який-небудь примітивний елемент поля K, тобто $K = P(\Theta)$. Раніше було показано, що якщо $\varphi(\Theta) = \Theta'$, то Θ и Θ' – співпряжені над P і $K' = P(\Theta')$.

Якщо $[K : P] = n$, то мінімальний многочлен для Θ над полем P має рівно n різних коренів $\Theta_1 = \Theta, \Theta_2, \ldots, \Theta_n$. Тому теорема буде доведена, якщо показати, що відповідність $\Theta \to \Theta_i$ $(i = 1, 2, \ldots . n)$ породжує відносний ізоморфізм поля K в $K_i = P(\Theta_i)$ і повністю визначає цей ізоморфізм. Але це справді так, бо з однозначності представлення елемента $\alpha \in K$ у вигляді

$$\alpha = c_0 + c_1\Theta + \cdots + c_{n-1}\Theta^{n-1}$$

і відповідності $\Theta \to \Theta'$ випливає, що елемент

$$\alpha' = c_0 + c_1\Theta' + \cdots + c_{n-1}(\Theta')^{n-1}$$

взаємно однозначно відповідає елементу α та лежить в полі $K' = P(\Theta')$. Це взаємно однозначна відповідність зберігається при операціях додавання та множення, віднімання та ділення. Покажемо, наприклад, для операції ділення.

Нехай

$$\alpha = c_0 + c_1\Theta + \cdots + c_{n-1}\Theta^{n-1},$$
$$\beta = d_0 + d_1\Theta + \cdots + d_{n-1}\Theta^{n-1}, \quad \beta \neq 0.$$

Якщо $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ – мінімальний многочлен для Θ над P, то многочлен $f(x)$ и $g(x) = d_0 + d_1x + \cdots + d_{n-1}x^{n-1}$ – взаємно прості. За теоремою про лінійне представлення НОД двох многочленів маємо

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1,$$

де $u(x), v(x) \in P[x]$. Але тоді

$$f(\Theta) \cdot u(\Theta) + g(\Theta) \cdot v(\Theta) = 1,$$
$$f(\Theta') \cdot u(\Theta') + g(\Theta') \cdot v(\Theta') = 1,$$

тобто $g(\Theta) \cdot v(\Theta) = 1, \quad g(\Theta') \cdot v(\Theta') = 1$.

Тому

$$\frac{\alpha}{\beta} = \frac{c_0 + c_1\Theta + \cdots + c_{n-1}\Theta^{n-1}}{d_0 + d_1\Theta + \cdots + d_{n-1}\Theta^{n-1}} = \frac{h(\Theta)}{g(\Theta)} = \frac{h(\Theta) \cdot v(\Theta)}{g(\Theta) \cdot v(\Theta)} = h(\Theta) \cdot v(\Theta),$$

$$\frac{\alpha'}{\beta'} = \frac{c_0 + c_1\Theta' + \cdots + c_{n-1}(\Theta')^{n-1}}{d_0 + d_1\Theta' + \cdots + d_{n-1}(\Theta')^{n-1}} = \frac{h(\Theta')}{g(\Theta')} = \frac{h(\Theta') \cdot v(\Theta')}{g(\Theta') \cdot v(\Theta')} = h(\Theta') \cdot v(\Theta').$$

Тепер у силу

$$h(x) \cdot v(x) = f(x) \cdot q(x) + r(x), \qquad \deg r(x) \leq n - 1,$$

випливає

$$\frac{\alpha'}{\beta'} = r(\Theta') = \left(\frac{\alpha}{\beta}\right)' .$$

Наслідок. Елементи із P *і тільки вони лишаються на місці під дією всіх відносних ізоморфізмів поля* K *над* P *.*

Доведення. Справді, елементи з K, що залишаються на місці під дією кожного відносного ізоморфізму $\sigma_1, \sigma_2, \ldots, \sigma_n$, утворюють підполе поля K, що містить поле P. Це легко перевіряється з використанням критерія підгрупи для адитивного та мультиплікативного випадків. Позначимо це поле через L. Тоді, розглядаючи K як розширення L, одержимо, що є, принаймні, n відносних ізоморфізмів K над L. Але тоді за доведеною теоремою $[K:L] \geq n$. І тепер для вежі

$$P \subset L \subset K$$

з рівності

$$n = [K:P] = [K:L] \cdot [L:P]$$

Робимо висновок, що $[K:L] = n$, $[L:P] = 1$, а тому $L = P$.