Лекції з загальної алгебри, 2 курс, 4 семестр, математика, частина 1

Анна Вишнякова

Харківський національний університет ім. В.Н.Каразіна

Харків, 2020

Прямий добуток груп

Теорема. Нехай G, H, K – групи. Тоді група G ізоморфна прямому добутку груп H і K, тобто $G \approx H \otimes K$, тоді і тільки тоді, коли виконуються три умови:
1. Існують нормальні підгрупи $\widetilde{H} \triangleleft G$, $\widetilde{K} \triangleleft G$, такі що $\widetilde{H} \approx H, \widetilde{K} \approx K$.

2. $\widetilde{H} \cap \widetilde{K} = \{e\}$.

3. $\widetilde{H}\widetilde{K} = \{hk | h \in \widetilde{H}, k \in \widetilde{K}\} = G$.

Ця теорема може бути узагальненою на довільну кількість прямих множників.

Теорема. Нехай $G, H_1, H_2, \ldots, H_n$ – групи $(n \in \mathbb{N}, n \geq 2)$. Тоді група G ізоморфна прямому добутку груп $H_1, H_2, \ldots, H_n$, тобто $G \approx H_1 \otimes H_2 \otimes \ldots \otimes H_n$, тоді і тільки тоді, коли виконуються три умови:

1. Існують нормальні підгрупи $\widetilde{H}_1 \triangleleft G$, $\widetilde{H}_2 \triangleleft G$, $\ldots$ $\widetilde{H}_n \triangleleft G$, такі що $\widetilde{H}_1 \approx H_1, \widetilde{H}_2 \approx H_2, \ldots, \widetilde{H}_n \approx H_n$.

2. Для кожного $j = 1, 2, \ldots, n$ виконується

$$\widetilde{H}_j \cap \left(\widetilde{H}_1 \cdot \ldots \cdot \widetilde{H}_{j-1} \widetilde{H}_{j+1} \cdot \ldots \cdot \widetilde{H}_n\right) = \{e\}.$$

3. $\widetilde{H}_1 \widetilde{H}_2 \cdot \ldots \cdot \widetilde{H}_n = G.$

В цьому розділі ми будемо вивчати абелеві групи. Зазвичай операцію в довільній абелевій групі позначають знаком $+$ і називають додаванням.

У випадку набору абелевих груп замість прямого добутку кажуть про пряму суму. Якщо G_1, G_2 – дві абелеві групи, операції в обох позначаються знаком $+$, то пряма сума цих груп

$$G_1 \oplus G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\},$$

де операція вводиться "покоординатно"

$$(a, b) + (c, d) = (a + c, b + d), \ a, c \in G_1, \ b, d \in G_2.$$

Циклічні групи

Теорема. Нехай $G = \langle a \rangle$ – циклічна група, $|G| = k \cdot l$, де $k, l \in \mathbb{N} \setminus \{1\}$, НСД$(k, l) = 1$. Тоді ця група є розкладною, а саме, існують підгрупи $K < G, L < G$, $|K| = k$, $|L| = l$, такі що $G \approx K \oplus L$.

Доведення. Розглянемо елементи $b = la \in G$ і $c = ka \in G$. Очевидно, що $|b| = k$, $|c| = l$. Позначимо $K = \langle b \rangle < G$, $L = \langle c \rangle < G$, тобто $|K| = k$, $|L| = l$. Перевіримо, що $G \approx K \oplus L$.

Нехай $d \in K \cap L$, $|d| = s \in \mathbb{N}$. Оскільки $d \in K$, $s|k$, а оскільки $d \in L$, $s|l$, тому з НСД$(k, l) = 1$ отримуємо $s = 1$, тобто $d = 0$. Ми довели, що $K \cap L = \{0\}$.

Перевіримо тепер, що $K + L = G$. З НСД$(k, l) = 1$ маємо: існують цілі числа $m, n \in \mathbb{Z} : ml + nk = 1$. Розглянемо елементи $f = mla = m(la) = mb \in K < G$, $g = nka = n(ka) = nc \in L < G$. Звідки отримуємо

$$a = (ml + nk)a = mla + nka = mb + nc \in K + L,$$

$$ja = jmb + jnc \in K + L, \ \forall j \in \mathbb{Z}.$$

Тобто $K + L = G$. $\square$

Простим наслідком цієї теореми є наступне твердження.

Теорема. Нехай $G = \langle a \rangle$ – циклічна група, $|G| = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$, $p_1, p_2, \ldots, p_m$ – попарно різні прості числа, $m \in \mathbb{N}, m \geq 2$. Тоді ця група є розкладною, а саме, існують підгрупи $H_1 < G, H_2 < G, \ldots, H_m < G$, $|H_j| = p_j^{k_j}$ для $\forall j = 1, 2, \ldots, m$, такі що $G \approx H_1 \oplus H_2 \oplus \ldots \oplus H_m$.

Залишилося розглянути циклічні групи порядків p^m, де p – просте число, $m \in \mathbb{N}$. Такі групи називають примарними.

Нерозкладність примарних циклічних груп

Теорема. Нехай $G = \langle a \rangle$ – циклічна група, $|G| = p^m$, де p – просте число, $m \in \mathbb{N}$. Тоді група G є нерозкладною.

Доведення. Якщо група G є розкладною, то в ній існують дві ненульові підгрупи, перетин яких складається з нейтрального елемента (нуля групи). Ми покажемо, що кожна ненульова підгрупа групи G містить елемент $p^{m-1}a \neq 0$.

Нехай $H < G, H \neq \{0\}$. Розглянемо довільний ненульовий елемент підгрупи $b = ka \in H, k \in \mathbb{N},\ 1 \leq k \leq p^m - 1$. Запишемо число k у вигляді $k = p^l t, 0 \leq l \leq m-1$, НСД$(p, t) = 1$ (p – просте число). Тобто, існують цілі числа $u, v \in \mathbb{Z}$ такі що

$$up + vt = 1.$$

Елемент $p^{m-l-1}vb \in H$, і ми маємо

$$p^{m-l-1}vb = p^{m-l-1}vka = \left(p^{m-l-1}vk\right)a = \left(p^{m-l-1}vp^{l}t\right)a =$$

$$\left(p^{m-1}vt\right)a = \left(p^{m-1}(1-up)\right)a = p^{m-1}a - up^{m}a = p^{m-1}a \in H.$$

Тобто, довільна ненульова підгрупа групи G містить елемент $p^{m-1}a \neq 0$.

$\square$

Скінчені абелеві групи

Теорема. Нехай G – абелева група, $|G| = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$, $p_1, p_2, \ldots, p_m$ – попарно різні прості числа, $m \in \mathbb{N}, m \geq 2$. Тоді існує єдиний набір підгруп $H_1 < G, H_2 < G, \ldots, H_m < G$, такий що для цього набору підгруп виконується

$$G \approx H_1 \oplus H_2 \oplus \ldots \oplus H_m,$$

а кожна з цих підгруп має наступну властивість: $x \in H_j \Rightarrow |x| = p_j^n,\ 0 \leq n \leq k_j \quad (j = 1, 2, \ldots, m)$.

Доведення. Розглянемо довільний ненульовий елемент групи $a \in G, a \neq 0$, тоді порядок цього елемента $|a| \mid |G|$, $|a| = p_1^{l_1} p_2^{l_2} \cdot \ldots \cdot p_m^{l_m}$, $0 \leq l_j \leq k_j$, $\forall j = 1, 2, \ldots, m$. Оскільки $|a| \neq 1$, існує $s = 1, 2, \ldots, m$, такий що $l_s \neq 0$. Розглянемо тоді елемент

$$b = p_1^{l_1} p_2^{l_2} \cdot \ldots \cdot p_{s-1}^{l_{s-1}} p_{s+1}^{l_{s+1}} \cdot \ldots \cdot p_m^{l_m}\ a \in G,$$

очевидно, що $|b| = p_s^{l_s}$.

Тобто в групі G існують елементи, порядки яких є степенями простих чисел, при цьому ці прості числа належать множині $p_1, p_2, \ldots, p_m$ (поки що ми не знаємо, чи для кожного простого числа з набору $p_1, p_2, \ldots, p_m$ є елемент групи, порядок якого є степенем саме цього простого числа).

Введемо наступні позначення

$$H_j = \{x \in G \mid |x| = p_j^l,\ 0 \le l \le k_j\} \subset G,\ j = 1, 2, \ldots, m.$$

Нескладно перевірити, що $H_j < G,\ j = 1, 2, \ldots, m$ (наразі ми не виключаємо випадку, що деякі з цих підгруп складаються тільки з нульового елемента). Дійсно, якщо $a, b \in H_j$, $|a| = p_j^{r_1},\ |b| = p_j^{r_2},\ r_1, r_2 \in \mathbb{N} \cup \{0\}$, $0 \le r_1 \le k_j$, $0 \le r_2 \le k_j$, то

$$p_j^{\max(r_1,r_2)}(a+b) = p_j^{\max(r_1,r_2)-r_1}(p_j^{r_1}a) + p_j^{\max(r_1,r_2)-r_2}(p_j^{r_2}b)$$
$$= 0 + 0 = 0,$$

звідки $|a+b| = p_j^r,\ 0 \le r \le \max(r_1, r_2) \le k_j \ \Rightarrow\ (a+b) \in H_j$. Крім того, $|0| = 1 \ \Rightarrow\ 0 \in H_j$. І, на останок, $|a| = |-a|$, звідки $a \in H_j \ \Rightarrow\ (-a) \in H_j$. Тобто, ми довели, що $H_j < G,\ j = 1, 2, \ldots, m$.

Ми хочемо довести, що $G \approx H_1 \oplus H_2 \oplus \ldots \oplus H_m$. Розглянемо довільний елемент групи $x \in G$ і його циклічну підгрупу $\langle x \rangle < G$. $|x| = |\langle x \rangle| = p_1^{l_1} p_2^{l_2} \cdot \ldots \cdot p_m^{l_m}$, $0 \le l_j \le k_j,\ \forall j = 1, 2, \ldots, m$. Як ми вже довели, циклічна група елемента x є прямою сумою своїх примарних циклічних підгруп. Тобто, існують циклічні підгрупи

$$C_j < \langle x \rangle < G,\ |C_j| = p_j^{l_j},\ j = 1, 2, \ldots, m :$$

$$\langle x \rangle \approx C_1 \oplus C_2 \oplus \ldots \oplus C_m.$$

Зокрема, $x = c_1 + c_2 + \ldots + c_m,\ c_j \in C_j,\ j = 1, 2, \ldots, m.$

З того, що $|C_j| = p_j^{l_j}$ випливає, що $|c_j| = p_j^{t_j}$, $0 \leq t_j \leq l_j$, тобто $c_j \in H_j$, $j = 1, 2, \ldots, m$. Ми перевірили, що

$$\forall x \in G \quad x \in H_1 + H_2 + \ldots + H_m,$$

тобто

$$G = H_1 + H_2 + \ldots + H_m.$$

Для завершення доведення нам необхідно показати, що

$$\forall j = 1, 2, \ldots, m \quad H_j \cap \big(H_1 + \ldots + H_{j-1} + H_{j+1} + \ldots + H_m\big) = \{0\}.$$

Нехай $y \in H_j \cap \left(H_1 + \ldots + H_{j-1} + H_{j+1} + \ldots + H_m\right)$. З того, що $y \in H_j$ маємо $|y| = p_j^t$, $t = 0, 1, \ldots$

З того, що $y \in H_1 + \ldots + H_{j-1} + H_{j+1} + \ldots + H_m$, маємо $y = d_1 + \ldots + d_{j-1} + d_{j+1} + \ldots + d_m$, $d_i \in H_i$. Тому $|y|$ є дільником найменшого спільного кратного порядків елементів $d_1, \ldots, d_{j-1}, d_{j+1}, \ldots, d_m$, тобто $|y| = p_1^{t_1} \cdot \ldots \cdot p_{j-1}^{t_{j-1}} p_{j+1}^{t_{j+1}} \cdot \ldots \cdot p_m^{t_m}$. З того, що $p_1, p_2, \ldots, p_m$ – попарно різні прості числа, маємо $|y| = 1$, або $y = 0$. Ми довели, що

$$\forall j = 1, 2, \ldots, m \quad H_j \cap \big(H_1 + \ldots + H_{j-1} + H_{j+1} + \ldots + H_m\big) = \{0\}.$$

Ми довели, що

$$G \approx H_1 \oplus H_2 \oplus \ldots \oplus H_m.$$

(Єдиність набору підгруп випливає з методу їх побудови) $\square$

Залишилося дослідити групи із наступною властивістю: порядок кожного елемента групи є степенем одного і того ж простого числа.

Теорема. Нехай p – просте число, G – скінчена абелева група із наступною властивістю: для кожного $g \in G$ існує $s \in \mathbb{N} \cup \{0\}$, таке що $|g| = p^s$. Тоді існують $b_1, b_2, \ldots, b_n \in G$, такі що $G \approx \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \ldots \oplus \langle b_n \rangle$, тобто група G ізоморфна прямій сумі своїх циклічних підгруп (зокрема, $|G| = p^m$, $m \in \mathbb{N} \cup \{0\}$).

Доведення. Нехай b_1 – один із елементів групи, який має найбільший порядок. Можливі два випадки:

1. Для кожного елемента групи G виконується:

$$\forall x \in G : \quad \langle b_1 \rangle \cap \langle x \rangle \neq \{0\}.$$

Тоді побудову закінчено, і в подальшому ми покажемо, що $G = \langle b_1 \rangle$.

2. Існують елементи групи G, такі що

$$\exists y \in G : \quad \langle b_1 \rangle \cap \langle y \rangle = \{0\}.$$

Тоді з усіх елементів з такою властивістю ми виберемо елемент найвищого порядку (один з таких) і позначимо його b_2.
Тобто $\forall y \in G : \quad \langle b_1 \rangle \cap \langle y \rangle = \{0\} \ \Rightarrow |y| \leq |b_2|$.
Ми маємо $|b_1| \geq |b_2|$ (пояснення!)

Будемо проводити таку побудову далі. Нехай ми вже побудували елементи $b_1, b_2, \ldots, b_s$, $s \geq 2$. Розглянемо підгрупу групи G, яка породжена цими елементами:

$$H_s = \{k_1 b_1 + k_2 b_2 + \ldots + k_s b_s \mid k_1, k_2, \ldots, k_s \in \mathbb{Z}\} \subset G.$$

Легко перевірити, що $H_s < G$. Дійсно, нехай $c, d \in H_s$, $c = m_1 b_1 + m_2 b_2 + \ldots + m_s b_s$, $d = r_1 b_1 + r_2 b_2 + \ldots + r_s b_s$, $m_1, m_2, \ldots, m_s$, $r_1, r_2, \ldots, r_s \in \mathbb{Z}$. Тоді $c + d = (m_1 + r_1) b_1 + (m_2 + r_2) b_2 + \ldots + (m_s + r_s) b_s \in H_s$. Крім того, $0 = 0 \cdot b_1 + 0 \cdot b_2 + \ldots + 0 \cdot b_s \in H_s$ і $-c = -m_1 b_1 - m_2 b_2 - \ldots - m_s b_s \in H_s$. Ми довели, що $H_s < G$.

Можливі два випадки:

1. Для кожного елемента групи G виконується:

$$\forall x \in G: \quad H_s \cap \langle x \rangle \neq \{0\}.$$

Тоді побудову закінчено, і в подальшому ми покажемо, що $G \approx \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \ldots \oplus \langle b_s \rangle$.

2. Існують елементи групи G, такі що

$$\exists y \in G: \quad H_s \cap \langle y \rangle = \{0\}.$$

Тоді з усіх елементів з такою властивістю ми виберемо елемент найвищого порядку (один з таких) і позначимо його b_{s+1}.
Тобто $\forall y \in G: \quad H_s \cap \langle y \rangle = \{0\} \;\Rightarrow |y| \leq |b_{s+1}|$.
Ми маємо $|b_1| \geq |b_2| \geq |b_3| \geq \ldots \geq |b_s| \geq |b_{s+1}|$. (пояснення!)

Оскільки група G є скінченою, то за скінчену кількість кроків нашу побудову буде закінчено. Тобто, ми побудуємо елементи $b_1, b_2, \ldots, b_n \in G$ такі що

$$1.\ |b_1| = \max_{x \in G} |x|.$$

$$2.\ \forall j = 2, 3, \ldots, n \quad H_{j-1} \cap \langle b_j \rangle = \{0\},$$

$$(H_{j-1} = \{k_1 b_1 + k_2 b_2 + \ldots + k_{j-1} b_{j-1} \mid k_1, k_2, \ldots, k_{j-1} \in \mathbb{Z}\}).$$

$$3.\ \forall y \in G, \forall j = 2, 3, \ldots, n: \quad H_{j-1} \cap \langle y \rangle = \{0\} \ \Rightarrow |y| \leq |b_j|.$$

$$4.\ |b_1| \geq |b_2| \geq \ldots \geq |b_n|.$$

$$5.\ \forall x \in G \quad H_n \cap \langle x \rangle \neq \{0\}.$$

Ми хочемо довести, що $G \approx \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \ldots \oplus \langle b_n \rangle$.

Перевіримо спочатку, що $G = \langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle$. Розглянемо довільний елемент $x \in G$. Оскільки $x \in G$, маємо $|x| = p^s,\ s \in \mathbb{N} \cup \{0\}$. Якщо $s = 0$, то $|x| = 1$, тобто $x = 0$. $0 = 0 + 0 + \ldots + 0 \in \langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle$. Будемо розглядати випадок $|x| = p^s, s \in \mathbb{N}$. Ми будемо доводити той факт, що $x \in \langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle$ індукцією за s.

База індукції $s = 1$, $|x| = p$. Нам відомо, що $\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle \cap \langle x \rangle \neq \{0\}$.

Ми також знаємо, що $H_n = \langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle < G$, $\langle x \rangle < G$, тому ми отримуємо $H_n \cap \langle x \rangle < G$.
Отже $H_n \cap \langle x \rangle < G$, і $H_n \cap \langle x \rangle \subset \langle x \rangle$, тобто $H_n \cap \langle x \rangle < \langle x \rangle$. І ми знаємо, що $H_n \cap \langle x \rangle \neq \{0\}$. Оскільки$|\langle x \rangle| = |x| = p$, а p – просте число, ми приходимо до висновку, що $H_n \cap \langle x \rangle = \langle x \rangle$. Зокрема, $x \in H_n$. Базу індукції доведено.

Індуктивний перехід $\leq m \rightsquigarrow (m+1)$. Припустимо, що ми довели, що кожен елемент групи G, порядок якого не перевищує p^m, належить до $\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle$. Нехай $x \in G$, $|x| = p^{m+1}$. З того, що $|b_1| \geq |b_2| \geq \ldots \geq |b_n|$, ми отримуємо:

$$\exists k \in \{1, 2, \ldots, n\} \quad \forall j = 1, 2, \ldots k : \ |x| \leq |b_j| \wedge \forall j > k : \ |x| > |b_j|.$$

За побудовою елементів $b_1, b_2, \ldots, b_n$, це означає, що

$$\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_k \rangle \cap \langle x \rangle \neq \{0\}.$$

Як ми вже відмічали, $\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_k \rangle \cap \langle x \rangle < G$, звідки $\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_k \rangle \cap \langle x \rangle < \langle x \rangle$. В попередньому розділі ми відмітили, що кожна ненульова підгрупа циклічної групи $\langle x \rangle$ порядку $|\langle x \rangle| = |x| = p^{m+1}$ містить елемент $p^m x$. Тобто, $y = p^m x \in \langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_k \rangle$.

Тобто, існують цілі числа $t_1, t_2, \ldots, t_k \in \mathbb{Z}$, такі що

$$y = p^m x = t_1 b_1 + t_2 b_2 + \ldots + t_k b_k.$$

Оскільки $|x| = p^{m+1}$, то $|y| = |p^m x| = p$, отже

$$py = p^{m+1}x = pt_1b_1 + pt_2b_2 + \ldots + pt_kb_k = 0.$$

Ми доведемо, що з побудови елементів $b_1, b_2, \ldots, b_k \in G$ випливає, що

$$r_1b_1 + r_2b_2 + \ldots + r_kb_k = 0, \quad r_1, r_2, \ldots, r_k \in \mathbb{Z} \ \Rightarrow$$

$$r_1b_1 = 0 \ \wedge \ r_2b_2 = 0 \ \wedge \ \ldots \ r_kb_k = 0.$$

Дійсно,

$$r_1b_1 + r_2b_2 + \ldots + r_kb_k = 0 \ \Rightarrow \ r_1b_1 + r_2b_2 + \ldots + r_{k-1}b_{k-1} = -r_kb_k$$

Ліва частина рівності є елементом підгрупи H_{k-1}, а права частина – елементом підгрупи $\langle b_k \rangle$. Тобто, цей елемент належить $H_{k-1} \cap \langle b_k \rangle$, але за побудовою $H_{k-1} \cap \langle b_k \rangle = \{0\}$. Ми маємо

$$-r_k b_k = 0 \ \wedge \ r_1 b_1 + r_2 b_2 + \ldots + r_{k-1} b_{k-1} = 0.$$

Із останньої рівності маємо

$$r_1 b_1 + r_2 b_2 + \ldots + r_{k-2} b_{k-2} = -r_{k-1} b_{k-1}.$$

Ліва частина рівності є елементом підгрупи H_{k-2}, а права частина – елементом підгрупи $\langle b_{k-1} \rangle$. Тобто, цей елемент належить $H_{k-2} \cap \langle b_{k-1} \rangle$, але за побудовою $H_{k-2} \cap \langle b_{k-1} \rangle = \{0\}$. Ми маємо

$$-r_{k-1} b_{k-1} = 0 \ \wedge \ r_1 b_1 + r_2 b_2 + \ldots + r_{k-2} b_{k-2} = 0.$$

Міркуючи аналогічно, отримуємо

$$r_1 b_1 = 0 \ \wedge \ r_2 b_2 = 0 \ \wedge \ \ldots \ r_k b_k = 0.$$

Ми зупинилися на тому, що

$$y = p^m x = t_1 b_1 + t_2 b_2 + \ldots + t_k b_k,$$

звідки

$$py = p^{m+1} x = pt_1 b_1 + pt_2 b_2 + \ldots + pt_k b_k = 0.$$

Як ми щойно довели, з цього випливає, що

$$pt_1 b_1 = 0 \ \wedge \ pt_2 b_2 = 0 \ \wedge \ \ldots \ \wedge \ pt_k b_k = 0,$$

звідки

$$|b_1| \;\Big|\; pt_1 \;\wedge\; |b_2| \;\Big|\; pt_2 \;\wedge\; \dots \;\wedge\; |b_k| \;\Big|\; pt_k.$$

Ми знаємо, що

$$\forall j = 1, 2, \dots k : \; |b_j| \geq |x| = p^{m+1},$$

крім того, $|b_j|$, $j = 1, 2, \dots k$, є степенем простого числа p (це властивість порядків усіх елементів групи), тобто

$$p^{m+1} \;\Big|\; pt_1 \;\wedge\; p^{m+1} \;\Big|\; pt_2 \;\wedge\; \dots \;\wedge\; p^{m+1} \;\Big|\; pt_k \;\Rightarrow$$

$$p^{m} \;\Big|\; t_1 \;\wedge\; p^{m} \;\Big|\; t_2 \;\wedge\; \dots \;\wedge\; p^{m} \;\Big|\; t_k.$$

Ми маємо

$$t_1 = p^m l_1, t_2 = p^m l_2, \ldots, t_k = p^m l_k, \quad l_1, l_2, \ldots, l_k \in \mathbb{Z}.$$

Нагадуємо, що $y = p^m x = t_1 b_1 + t_2 b_2 + \ldots + t_k b_k$, тобто

$$y = p^m x = p^m l_1 b_1 + p^m l_2 b_2 + \ldots + p^m l_k b_k \in H_k.$$

Покладемо

$$z := l_1 b_1 + l_2 b_2 + \ldots + l_k b_k \in H_k.$$

Ми маємо

$$y = p^m x \ \wedge \ y = p^m z \ \Rightarrow p^m(x - z) = 0,$$

отже, елемент групи $x - z \in G$ має порядок, менший або рівний p^m.

За індуктивним припущенням, $w = x - z \in H_k < H_n$. Крім того, за побудовою $z \in H_k < H_n$, отже $x = w + z = (x - z) + z \in H_k < H_n$.

Отже,ми довели методом математичної індукції, що $G = \langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_n \rangle$.

Залишилося довести, що для усіх $j = 1, 2, \ldots, n$ виконується

$$\langle b_j \rangle \cap (\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_{j-1} \rangle + \langle b_{j+1} \rangle + \ldots + \langle b_n \rangle) = \{0\}.$$

Нехай

$$x \in \langle b_j \rangle \cap (\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_{j-1} \rangle + \langle b_{j+1} \rangle + \ldots + \langle b_n \rangle).$$

Це означає, що

$$x \in \langle b_j \rangle \ \wedge \ x \in (\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_{j-1} \rangle + \langle b_{j+1} \rangle + \ldots + \langle b_n \rangle).$$

Тобто ми маємо

$$x = t_j b_j \ \wedge \ x = t_1 b_1 + t_2 b_2 + \ldots + t_{j-1} b_{j-1} + t_{j+1} b_{j+1} + \ldots + t_n b_n,$$

де $t_1, t_2, \ldots, t_n \in \mathbb{Z}$. Прирівняємо ці вирази і отримуємо

$$t_1 b_1 + t_2 b_2 + \ldots + t_{j-1} b_{j-1} - t_j b_j + t_{j+1} b_{j+1} + \ldots + t_n b_n = 0.$$

Вище ми вже доводили, що з цієї рівності випливає, що

$$t_1 b_1 = 0 \ \wedge \ t_2 b_2 = 0 \ \wedge \ \ldots \ \wedge \ t_j b_j = 0 \ \wedge \ \ldots \ \wedge \ t_n b_n = 0,$$

отже $x = 0$. Тобто для усіх $j = 1, 2, \ldots, n$ виконується

$$\langle b_j \rangle \cap (\langle b_1 \rangle + \langle b_2 \rangle + \ldots + \langle b_{j-1} \rangle + \langle b_{j+1} \rangle + \ldots + \langle b_n \rangle) = \{0\}.$$

Отже, ми довели, що $G \approx \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \ldots \oplus \langle b_n \rangle$. $\square$

Наслідок. Нехай p – просте число, G – скінчена абелева група із наступною властивістю: для кожного $g \in G$ існує $s \in \mathbb{N} \cup \{0\}$, таке що $|g| = p^s$. Тоді існує таке $m \in \mathbb{N} \cup \{0\}$, що $|G| = p^m$.

Доведення. Ми довели, що існують такі елементи $b_1, \ldots, b_n \in G$, що

$$G \approx \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \ldots \oplus \langle b_n \rangle.$$

Тоді

$$|G| = |\langle b_1 \rangle| \cdot |\langle b_2 \rangle| \cdot \ldots \cdot |\langle b_n \rangle| = |b_1| \cdot |b_2| \cdot \ldots \cdot |b_n| = p^m.$$

$\square$

Теорема. Нехай p – просте число, G – скінчена абелева група із наступною властивістю: для кожного $g \in G$ існує $s \in \mathbb{N} \cup \{0\}$, таке що $|g| = p^s$. Нехай знайшлися $b_1, b_2, \dots, b_n \in G \setminus \{0\}$, такі що $G \approx \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \dots \oplus \langle b_n \rangle$, і, крім того, знайшлися $c_1, c_2, \dots, c_m \in G \setminus \{0\}$, такі що $G \approx \langle c_1 \rangle \oplus \langle c_2 \rangle \oplus \dots \oplus \langle c_m \rangle$. Тоді $n = m$, і існує така перестановка $\sigma \in S_n$, що для довільного $j = 1, 2, \dots, n$ виконується $|\langle b_j \rangle| = |\langle c_{\sigma(j)} \rangle|$.

Кажуть, що розкладання групи порядку $|G| = p^m$, де p – просте число, в пряму суму примарних циклічних груп є однозначним з точністю до порядку прямих доданків.

Доведення. Не зменшуючи загальності, ми можемо вважати, що $|b_1| \geq |b_2| \geq \ldots \geq |b_n|$ і $|c_1| \geq |c_2| \geq \ldots \geq |c_m|$. Позначимо через

$$|b_1| = p^{k_1}, |b_2| = p^{k_2}, \ldots, |b_n| = p^{k_n},$$

$$k_1 \geq k_2 \geq \ldots \geq k_n,$$

і

$$|c_1| = p^{l_1}, |c_2| = p^{l_2}, \ldots, |c_m| = p^{l_m},$$

$$l_1 \geq l_2 \geq \ldots \geq l_m.$$

Якщо твердження нашої теореми не виконується, то знайдеться таке $j \in \mathbb{N}$, що виконується

$$k_1 = l_1, k_2 = l_2, \ldots, k_{j-1} = l_{j-1}, k_j \neq l_j.$$

(пояснення!)

Не зменшуючи загальності, $k_j < l_j$. Введемо позначення

$$H := \{x \in G \mid |x| \le p^{k_j}\}.$$

Нескладно перевірити, що $H < G$ (зробіть це). Оскільки G – абелева група, ми маємо $H \lhd G$.

Розглянемо фактор-групу G/H. Відмітимо, що

$$p^{k_1-k_j}b_1 \in H, p^{k_2-k_j}b_2 \in H, \dots, p^{k_{j-1}-k_j}b_{j-1} \in H,$$

$$b_j \in H, b_{j+1} \in H, \dots, b_n \in H.$$

З іншого боку,

$$p^{k_1-k_j-1}b_1 \notin H, p^{k_2-k_j-1}b_2 \notin H, \dots, p^{k_{j-1}-k_j-1}b_{j-1} \notin H,$$

якщо показники степенів не є від'ємними.

Це означає, що клас суміжності елемента b_i по підгрупі H має в фактор-групі G/H порядок $p^{k_i-k_j}$ для усіх $i = 1, 2, \ldots, j-1$ (тобто, найменше $t \in \mathbb{N}$, таке що $t[b_i] = [tb_i] = [0] = H$, дорівнює $p^{k_i-k_j}$).

Доведемо, що група G/H є прямою сумою циклічних підгруп елементів $[b_i] = b_i + H$, $i = 1, 2, \ldots, j-1$:

$$G/H \approx \langle [b_1] \rangle \oplus \langle [b_2] \rangle \oplus \ldots \oplus \langle [b_{j-1}] \rangle,$$

і тому порядок цієї фактор-групи дорівнює

$$|G/H| = p^{(k_1-k_j)+(k_2-k_j)+\ldots+(k_{j-1}-k_j)}.$$

Нехай x – довільний елемент групи G, тоді $x = s_1 b_1 + s_2 b_2 + \ldots + s_n b_n$, де $s_1, \ldots, s_n \in \mathbb{Z}$. Для $i = j, j+1, \ldots, n$ маємо $s_i b_i \in H$, тому $[s_i b_i] = [0]$. Ми довели, що

$[x] = [s_1 b_1] + [s_2 b_2] + \ldots + [s_{j-1} b_{j-1}] \in \langle [b_1] \rangle + \langle [b_2] \rangle + \ldots + \langle [b_{j-1}] \rangle.$

Тобто ми довели, що

$$G/H = \langle [b_1] \rangle + \langle [b_2] \rangle + \ldots + \langle [b_{j-1}] \rangle.$$

Перевіримо тепер, що для довільного $i = 1, 2, \ldots, j-1$ виконується

$$\langle[b_i]\rangle \cap (\langle[b_1]\rangle + \langle[b_2]\rangle + \ldots + \langle[b_{i-1}]\rangle + \langle[b_{i+1}]\rangle + \ldots + \langle[b_{j-1}]\rangle) = \{[0]\}.$$

Нехай виконується

$$[y] \in \langle[b_i]\rangle \cap (\langle[b_1]\rangle + \langle[b_2]\rangle + \ldots + \langle[b_{i-1}]\rangle + \langle[b_{i+1}]\rangle + \ldots + \langle[b_{j-1}]\rangle),$$

тобто

$$[y] \in \langle[b_i]\rangle \wedge [y] \in \langle[b_1]\rangle + \langle[b_2]\rangle + \ldots + \langle[b_{i-1}]\rangle + \langle[b_{i+1}]\rangle + \ldots + \langle[b_{j-1}]\rangle.$$

Ми маємо

$$y = t_i b_i + h_i \wedge y = (t_1 b_1 + h_1) + (t_2 b_2 + h_2) + \ldots + (t_{i-1} b_{i-1} + h_{i-1})$$

$$+ (t_{i+1} b_{i+1} + h_{i+1}) + \ldots + (t_{j-1} b_{j-1} + h_{j-1}),$$

де $t_1, \ldots, t_{j-1} \in \mathbb{Z}$, $h_1, h_2, \ldots, h_{j-1} \in H$. Тоді виконується

$$t_1 b_1 + t_2 b_2 + \ldots + t_{i-1} b_{i-1} - t_i b_i + t_{i+1} b_{i+1} + \ldots + t_{j-1} b_{j-1} = h \in H.$$

З визначення підгрупи H порядок елемента в лівій частині рівності не перевищує p^{k_j} (і є якимось степенем p), звідки

$$p^{k_j} t_1 b_1 + p^{k_j} t_2 b_2 + \ldots + p^{k_j} t_{i-1} b_{i-1} - p^{k_j} t_i b_i +$$

$$p^{k_j} t_{i+1} b_{i+1} + \ldots + p^{k_j} t_{j-1} b_{j-1} = 0.$$

Оскільки за умовою теореми $G \approx \langle b_1\rangle \oplus \langle b_2\rangle \oplus \ldots \oplus \langle b_n\rangle$ (тобто, ця сума підгруп є прямою), із останньої рівності маємо

$$p^{k_j} t_1 b_1 = 0 \ \wedge \ p^{k_j} t_2 b_2 = 0 \ \wedge \ \ldots \ \wedge \ p^{k_j} t_{j-1} b_{j-1} = 0.$$

Тому маємо

$$|b_1| \mid p^{k_j} t_1 \ \wedge \ |b_2| \mid p^{k_j} t_2 \ \wedge \ \ldots \ \wedge \ |b_{j-1}| \mid p^{k_j} t_{j-1},$$

тобто

$$p^{k_1} \mid p^{k_j} t_1 \ \wedge \ p^{k_2} \mid p^{k_j} t_2 \ \wedge \ \ldots \ \wedge \ p^{k_{j-1}} \mid p^{k_j} t_{j-1},$$

звідки маємо

$$p^{k_1 - k_j} \mid t_1 \ \wedge \ p^{k_2 - k_j} \mid t_2 \ \wedge \ \ldots \ \wedge \ p^{k_{j-1} - k_j} \mid t_{j-1}.$$

Але для усіх $i = 1, 2, \ldots, j-1$ маємо: клас суміжності елемента b_i по підгрупі H має в фактор-групі G/H порядок $p^{k_i - k_j}$, тому з того, що $p^{k_i - k_j} \mid t_i$, випливає $[t_i b_i] = [0]$. Ми довели, що $[y] = [0]$, тобто

$$\langle [b_i] \rangle \cap (\langle [b_1] \rangle + \langle [b_2] \rangle + \ldots + \langle [b_{i-1}] \rangle + \langle [b_{i+1}] \rangle + \ldots + \langle [b_{j-1}] \rangle) = \{[0]\}.$$

Таким чином,

$$G/H \approx \langle [b_1] \rangle \oplus \langle [b_2] \rangle \oplus \ldots \oplus \langle [b_{j-1}] \rangle,$$

і тому порядок цієї фактор-групи дорівнює

$$|G/H| = p^{(k_1 - k_j) + (k_2 - k_j) + \ldots + (k_{j-1} - k_j)}.$$

Аналогічно розглянемо розкладання $G \approx \langle c_1 \rangle \oplus \langle c_2 \rangle \oplus \ldots \oplus \langle c_m \rangle$, і отримаємо, що фактор група G/H має представлення

$$G/H \approx \langle [c_1] \rangle \oplus \langle [c_2] \rangle \oplus \ldots \oplus \langle [c_{j-1}] \rangle \oplus \langle [c_j] \rangle \oplus \ldots$$

(підсумування іде по тих циклічних групах класів $[c_i]$, для яких порядок елемента c_i є більшим або рівним p^{k_j}, а за нашим припущенням $|c_j| = p^{l_j} > p^{k_j}$). Тобто, порядок фактор групи дорівнює

$$|G/H| = p^{(l_1-k_j)+(l_2-k_j)+\ldots+(l_{j-1}-k_j)+(l_j-k_j)+\ldots} =$$

$$p^{(k_1-k_j)+(k_2-k_j)+\ldots+(k_{j-1}-k_j)+(l_j-k_j)+\ldots} >$$

$$p^{(k_1-k_j)+(k_2-k_j)+\ldots+(k_{j-1}-k_j)}.$$

Ми отримали протиріччя, яке і доводить теорему. □
Зведемо в одне твердження все, що ми довели для скінчених абелевих груп.

Теорема (основна теорема про скінчені абелеві групи). Нехай G – абелева група, $|G| = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$, $p_1, p_2, \ldots, p_m$ – попарно різні прості числа, $m \in \mathbb{N}$. Тоді ця група є ізоморфною прямої сумі примарних циклічних груп

$$G \approx \langle g_{11} \rangle \oplus \langle g_{12} \rangle \oplus \ldots \oplus \langle g_{1s_1} \rangle \oplus$$

$$\langle g_{21} \rangle \oplus \langle g_{22} \rangle \oplus \ldots \oplus \langle g_{2s_2} \rangle \oplus \cdots$$

$$\oplus \langle g_{m1} \rangle \oplus \langle g_{m2} \rangle \oplus \ldots \oplus \langle g_{ms_m} \rangle,$$

де для кожного $i = 1, 2, \ldots, m$ маємо

$$|g_{i1}| \cdot |g_{i2}| \cdot \ldots \cdot |g_{is_i}| = p_i^{k_i}.$$

Порядки циклічних груп у вказаному представленні знаходяться однозначно з точністю до порядку доданків в прямій сумі.