Абелевы p-группы и целые числа

В последний раз было рассказано некоторое количество соображений про устройство абелевых p-групп (p-примарных групп).

Попробую прояснить то, что происходило на паре. А так же нарисовать много картинок.

Первое очевидное соображение состоит в том, что порядок p-группы есть степень p, то есть p^n. Количество неизоморфных p-групп порядка p^n , как следует из теоремы о классификации конечных абелевых групп, равно количеству разбиений числа n на слагаемые (порядок, естественно неважен).

Любое разбиение числа n на слагаемые можно (единственным образом) представить в виде следующей картинки:

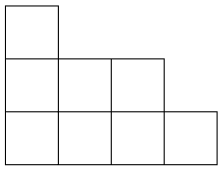

Рис. 1. $n = 8 = 3 + 2 + 2 + 1$, соответствующая группа изоморфна $\mathbb{Z}/p^3 \oplus \mathbb{Z}/p^2 \oplus \mathbb{Z}/p^2 \oplus \mathbb{Z}/p$

Такие картинки (или перевёрнутые) называются диаграммами Юнга (Young diagram), довольно активно используются в комбинаторике.

Пусть теперь дана некоторая p-примарная абелева группа G, порядка p^n, которой соответствует некоторая диаграмма Юнга. А именно число столбцов высоты ровно k есть число прямых слагаемых вида $\mathbb{Z}/p^k$ при разложении группы в прямую сумму примарных циклических (число всех клеток в диаграмме равно $\log_p(|G|)$). Для удобства можно считать $G = \bigoplus_{i=1}^l \mathbb{Z}/p^{k_i}$.

Мы установили, что количество элементов порядка $\leq p^k$ в точности равно $p^{\text{количество квадратиков на высоте не более } k}$. Из этого несложно получить формулу для числа элементов порядка p^k. Так же нам было удобно ввести

Определение 1. *Пусть G абелева группа. Тогда обозначим за $G_{\leq p^k} = \{x \in G \,|\, p^k x = 0\}$ подгруппу p-примарных элементов порядка меньше или равного p^k.*

В диаграмме подгруппе $G_{\leq p^k}$ соответствуют все клетки на высоте не более k. Отметим красным на картинке группу $G_{\leq p}$

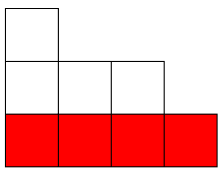

Рис. 2. $8 = 3 + 2 + 2 + 1$, $G_{\leq p}$

Такой рисунок даёт ответ на вопрос, какой диаграмме соответствует $G_{\leq p^k}$. Например $G_{\leq p} \cong \bigoplus_{\substack{\text{количество} \\ \text{слагаемых в } G}} \mathbb{Z}/p$, что мы отмечали на занятиях. Проверьте, что картинка даёт правильный ответ и для больших степеней p.

Вообще говоря группа G может быть по разному отождествлена с $\bigoplus_{i=1}^l \mathbb{Z}/p^{k_i}$. В частности существует много различных изоморфизмов из $\bigoplus_{i=1}^l \mathbb{Z}/p^{k_i}$ в себя. Наша ближайшая задача — научиться считать их число, а так же число различных наборов подгрупп, которые задают разложение G в прямую сумму.

Для того, чтобы задать изоморфизм из $\bigoplus_{i=1}^l \mathbb{Z}/p^{k_i}$ необходимо задать его значение на образующих (элементах $(0, \ldots, 1, \ldots, 0)$). Чтобы получился изоморфизм образы элементов порядка p^k должны быть элементами порядка p^k.

Так же, можно заметить, что образы подгрупп вида $\{0\}\oplus\dots\oplus\{0\}\oplus\mathbb{Z}/p^{k_i}\oplus\{0\}\oplus\dots\oplus\{0\}$ должны задавать разложение образа в прямую сумму (вообще говоря, отличным от исходного способом).

Для того, чтобы это проверить необходимо и достаточно понять, что подгруппа, порождённая образами первых $i-1$ образующих, не содержит никакое кратное образа i-го (кроме 0). Таким образом, для того, чтобы задать изоморфизм из $G \to G$ надо найти элементы $g_1, \dots, g_l \in G$, такие, что порядок $\operatorname{ord} g_i = p^{k_i}$ и $\langle g_1, \dots, g_{i-1}\rangle \cap \langle g_i\rangle = \{0\}$.

Первое условие в частности значит, что $g_i \in G_{\le p^{k_i}}$, тогда второе можно пересказать так — образ g_i имеет порядок p^{k_i} в группе $G_{\le p^{k_i}}/(\langle g_1, \dots, g_{i-1}\rangle \cap G_{\le p^{k_i}})$. Так как прибавление элемента порядка p^{k_i-1} порядка образа g_i не меняет, то последнее условие эквивалентно тому, что образ g_i не равен 0 в группе $G/((\langle g_1, \dots, g_{i-1}\rangle \cap G_{\le p^{k_i}}) + G_{\le p^{k_i-1}})$.

Допустим теперь, что у нас уже есть набор g_i. Давайте заполним с их помощью клетки диаграммы Юнга. А именно в верхней клетке i-го столбца поставим g_i, ниже на одну ступеньку поставим pg_i, затем p^2g_i и так далее.

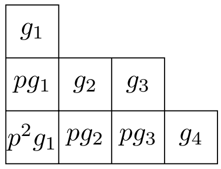

Рис. 3. $8 = 3 + 2 + 2 + 1$, расставляем образующие каждого уровня

Чем хороша эта картинка, что она говорит? Например, можно утверждать, что любой элемент из $G_{\le p^k}$ есть сумма элементиков из клеток высоты, меньшей или равной k.

Или, например, всегда можно сказать, чему изоморфна подгруппа порождённая элементами из клеток диаграммы Юнга. Например, на картинке подгруппа порождённая p^2g_1 и g_3 изоморфна $\mathbb{Z}/p \oplus \mathbb{Z}/p^2$.

А ещё на картинке элемент стоящий под каким-то всегда является его кратным. Но больше всего нас будет интересовать, как считать факторгруппу G по подгруппе, которая порождена элементами из диаграммы. Например $G/\langle p^2g_1, g_3\rangle$. Получиться

$$G/\langle p^2g_1, g_3\rangle \cong \mathbb{Z}/p^2 \oplus \mathbb{Z}/p^2 \oplus \{0\} \oplus \mathbb{Z}/p.$$

На картинке делаем следующее — надо убрать те ячейки, которые соответствуют порождающим и всё под ними. Потом можно переставить столбики так, чтобы сначала шли большие, чтобы привести диаграмму к каноническому виду. Даже образующие в таком факторе понятно какие (образы g_1 — порядка p^2, g_2 – порядка p^2, g_4 – порядка p).

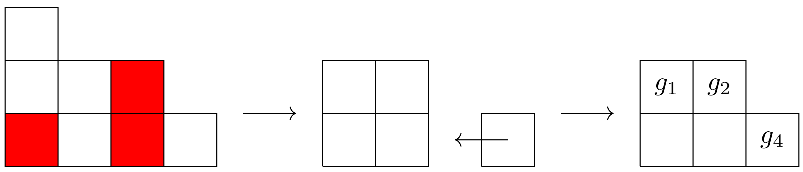

Рис. 4. $8 = 3 + 2 + 2 + 1$, подгруппа $\langle p^2g_1, g_3\rangle$ и фактор по ней

Начнём с элементов наибольшего порядка. Действительно, доказательство теоремы о классификации говорит, что подгруппа, порождённая элементом наибольшего порядка всегда выделяется как прямое слагаемое. Таким образом, на первом шаге надо выбрать элемент g_1 порядка p^3. Их $p^8 - p^7$.

На следующем шаге надо выбрать элемент g_2 порядка p^2 с дополнительными условиями. У нас уже выбран g_1 и поэтому мы можем изобразить соответствующую ему подгруппу на картинке. Точнее изобразим её пересечение с $G_{\le p^2}$, которое нам интереснее.

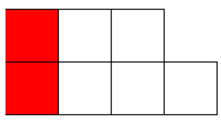

Рис. 5. $G_{\le p^2}$ и её подгруппа $\langle g_1\rangle \cap G_{\le p^2}$

Если ещё прибавить к $\langle g_1\rangle \cap G_{\le p^2}$ подгруппу $G_{\le p}$, то получится подгруппа, занимающая 5 клеток (порядка p^5), а в факторе останется две клеточки, то есть будет подгруппа порядка p^2. В ней меня устраивает любой элемент кроме 0 — их $p^2 - 1$. Итого получаем $(p^2 - 1)p^5$ элементов на роль g_2.

Третий шаг. Рисуем $(\langle g_1, g_2\rangle \cap G_{\le p^2}) + G_{\le p}$.

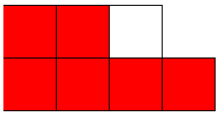

Рис. 6. $G_{\le p^2}$ и её подгруппа $(\langle g_1, g_2\rangle \cap G_{\le p^2}) + G_{\le p}$

Клетка одна, получаем $(p-1)p^6$ элементов. Четвёртый шаг даёт $(p-1)p^3$, так как выбирается кандидат в одну клетку на нижнем уровне, а остальные три уже заняты.

Итого число подходящих g_1, g_2, g_3, g_4, то есть число изоморфизмов, то есть число отождествлений равно

$$(p-1)p^7(p^2-1)p^5(p-1)p^6(p-1)p^3 = (p+1)(p-1)^4p^{21}.$$

Если нам теперь хочется понять, какое число наборов подгрупп у нас получилось, то надо вспомнить, что ровно $p^2(p-1)$ элементов g_1 задают одну и ту же подгруппу, $p(p-1)$ элементов g_2 задают одну и ту же подгруппу, $p(p-1)$ элементов g_3 задают одну и ту же подгруппу и $(p-1)$ элементов g_4 задают одну ту же подгруппу (и изменение g_i на эквивалентные не затрагивает последующие). Плюс, если нас не интересует порядок подгрупп в наборе, то g_2 можно менять с g_3. Получаем ответ

$$\frac{(p+1)(p-1)^4p^{21}}{p^2(p-1)p(p-1)p(p-1)(p-1)2} = \frac{p+1}{2}p^{17}$$

Допустим теперь мы хотим посчитать $G/\langle x\rangle$ для некоторого элемента x. Основная идея состоит в том, что можно так выбрать набор образующих g_i, что $x = p^s g_t$, для некоторых s и t. Такие факторы мы уже умеем считать. Осталось понять, как эти s и t найти. Для этого рассмотрим все такие y, что $p^k y = x$. Рассмотрим какой-нибудь y наибольшего порядка среди таких — его и можно взять в качестве образующей на каком-то шаге (проверьте).

Задания про p-группы

Определение 2. *Пусть G группа. Число $d \in \mathbb{N}$ называется экспонентой группы G, если d наименьшее такое число, что $g^d = 1$ для всех $g \in G$.*

Задание 1. Пусть A — p-примарная конечная абелева группа, а H её подгруппа. Покажите, что экспонента H и экспонента A/H являются степенями p и меньше, чем экспонента A.

Задание 2. Пусть A конечная абелева группа, а H её подгруппа. Пусть d_1 — экспонента H и d_2 экспонента A/H являются степенями простого числа p.
а) Покажите, что A — p-примарная и d — экспонента A удовлетворяет неравенствам $\max(d_1, d_2) \le d \le d_1 + d_2$.
б) Предъявите примеры, когда каждое из неравенств на d обращается в равенство.

Задание 3. Пусть $G \cong \mathbb{Z}/p^3 \oplus \mathbb{Z}/p^3 \oplus \mathbb{Z}/p^2 \oplus \mathbb{Z}/p$.
а) Сколько в G пар не пересекающихся подгрупп порядка p^3?
б) Сколько в G элементов x порядка p^2, что существует y порядка p^3, что $py = x$?
в) Сколько в G элементов x порядка p, что существует y порядка p^3, что $p^2y = x$?
г) Сколько изоморфизмов из $G \to G$?
д) Какая диаграмма соответствует группе $G/\langle(2p, p^2, p, 3)\rangle$ в зависимости от p?

Задания про целые числа и кольца

Задание 4. Найдите линейное разложение НОД$(29, 21)$ и найдите все решения уравнения $21x + 29y = 5$

Задание 5. Числа Фибоначчи удовлетворяют рекуррентному соотношению $u_{n+1} = u_n + u_{n-1}$, и условиям $u_1 = u_2 = 1$. Найдите НОД(u_n, u_{n+1}).

Задание 6. Найдите НОД$(3^n - 1, 3^m - 1)$ в зависимости от n и m.

Определение 3. *Пусть R - ассоциативное кольцо с единицей. Тогда $x \in R$ называется*
а) делителем 0, если $\exists y \in R$, такой что $xy = 0$, а $y \ne 0$
б) нильпотентом, если $\exists n \in N$, такой что $x^n = 0$
в) идемпотентом, если $x^2 = x$.

Определение 4. *Пусть R_1 и R_2 — два кольца. Определим структуру кольца на $R_1 \times R_2$ следующим образом:*

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \quad (r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2).$$

Если R_1 и R_2, были ассоциативными, с единицей, коммутативными, то их произведение будет обладать соответствующими свойствами.

Задание 7. Пусть R_1 и R_2 — два ассоциативных кольца с единицей. Рассмотрим кольцо $R = R_1 \times R_2$. Покажите, что элементы $e_1 = (1, 0)$ и $e_2 = (0, 1)$ являются идемпотентами, а также, что $\forall x \in R$ $e_1x = xe_1$, $e_2x = xe_2$ и $e_1 \cdot e_2 = 0$.

Определение 5. *Пусть R и S — два кольца. Гомоморфизмом из R в S называется отображение $f\colon R \to S$, что*

$$\forall x, y \in R \ \text{ выполнено } f(x + y) = f(x) + f(y) \ \text{ и } f(xy) = f(x)f(y).$$

Если кольца R и S с единицей, то естественно дополнительно потребовать $f(1) = 1$. Сюръективные, инъективные, биективные гомоморфизмы называются эпи-, моно- и изоморфизмами соответственно.

Задание 8. Пусть R — некоторое кольцо с единицей, а e — идемпотент. Покажите, что
а) $1 - e$ тоже идемпотент и $(1 - e)e = e(1 - e) = 0$.
б) Покажите, что $eRe = \{ere \,|\, r \in R\}$ является подкольцом в R. Кроме того, покажите, что в этом кольце роль единицы играет e.
в) Пусть, дополнительно $ex = xe$ $\forall x \in R$. Покажите, что $R \cong eRe \times (1 - e)R(1 - e)$. В частности, для коммутативных колец наличие нетривиального ($\neq 0, 1$) идемпотента эквивалентно тому, что кольцо есть прямое произведение двух других.

Напоследок

В заключение теории групп хочу дать ссылки на некоторые алгоритмы(или утверждения, которые можно переделать в алгоритмы). Прежде всего стоит дать ссылку на лемму, с помощью которой можно явно описать образующие стабилизатора (что мы не делали). Это лемма Шрайера.

Следующий в списке Алгоритм Тода-Коксетера. Берёт группу, заданную образующими и соотношениями, и перечисляет в ней элементы. Если группа конечна, то он даже закончит работу. Узнать заранее по соотношениям, конечна группа или нет, к сожалению, алгоритмически нельзя. Если известна оценка на порядок группы, то нельзя ничего сказать про время работы алгоритма, кроме того, что оно конечное...

Последний алгоритм — Алгоритм Кнута-Бендикса решает примерно ту же задачу, что и предыдущий.