1 Групповые алгебры

Примеры из прошлой лекции: **группа Гейзенберга**, **группа аффинных преобразований**.

Группа $\mathrm{Aff} = \{\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}\}$,

Группа
$$\widetilde{\mathrm{Aff}} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \right\}$$

Лемма 1. *существует изоморфизм* $\mathrm{Aff} \to \widetilde{\mathrm{Aff}}$.

1.1 Действия групп на множестве

Пусть G группа и X множество. Рассмотрим $f : G \times X \to X$. Если f ясно из контекста, будем писать просто gx. Такое отображение будем называть действием, если выполнены следующие условия.

1) $f(g_1g_2, x) = F(g_1, f(g_2, x))$ или, проще
$$(g_1g_2)x = g_1(g_2x).$$

2) $f(e, x) = x$.

Пример 1. Пусть $\mathbb{T}$ — группа точек единичной окружности на комплексной плоскости. Пусть $X = \mathbb{C}$. Тогда $f(g, x) = gx$ (в правой части подразумевается комплексное умножение.

Замечание 1. В некоммутативных группах различают *правые* и *левые* действия.

Лемма 2. *Действие определеяет отношение эквивалентности:* $x_1 \sim x_2$.

Док-во. ...

Определение 1. Классы эквивалентности в этом случае называются **орбитами** (действия).

Пример 2. $X = \mathbb{F}_2^5$, $G = \mathbb{Z}_5$.
$$f(z, \vec{x}) = f(z, (x_0, \dots, x_4)) = (x_{0-z}, x_{1-z}, \dots x_{4-z}).$$

Разность в координатах берётся по модулю 5.

Найдём орбиту точки $(1, 1, 0, 0, 0)$ для действия из последнего примера.

- $0(11000) = 11000$,
- $1(11000) = 01100$,
- $2(11000) = 00110$,
- $3(11000) = 00110$,
- ...

Хотелось бы, чтобы размер орбиты всегда совпадал с размером группы. В действительности, размеры орбит будут делителями группы. Например, орбита точки 11111 из последнего примера.

Пример 3. $X = \mathbb{F}_2^4$, $G = \mathbb{Z}_4$. Запишем размеры орбит каждого элемента.

- 0000 — 1
- 0001 — 4
- 0101 — 2
- ...

Пример 4. $X = \mathbb{F}_2^4$, $G = S_4$.

- 0000 — 1,
- $1000 - 4 = C_4^1$,
- $1100 - 6 = C_4^2$,
- ...

Вес Хэмминга здесь однозначно определяет орбиту.

Лемма 3. *Рассмотрим* ***стабилизатор*** *элемента* x*:*
$$\mathrm{St}_G(x) = \{g \in G \mid gx = x\}.$$
Стабилизатор является подгруппой.

Пример 5. $X = \mathbb{F}_2^4$, $G = \mathbb{Z}_4$.

- $\mathrm{St}(0000) = \mathbb{Z}_4$,
- $\mathrm{St}(0001) = 0$,
- ...
- $|\,\mathrm{St}(0101)| = 2$,
- ...

Гипотеза.
$$\forall x \in G\colon |G| = |\,\mathrm{St}(x)| * |\text{орбита } x|.$$

Определение 2. Действие группы называется **эффективным**, если орбита каждой точки совпадает с X.

1.2 Определение и примеры групповых алгебр.

Будем предполагать группу G конечной. Рассмотрим формальные выражения вида:
$$\sum_{g \in G} a_g g, \qquad a \in \mathbb{F}.$$

Такие выражения можно рассматривать как функции, определённые на группе со значениями в поле. На этих объектах мы введём две внутренних ($+$, $\times$) и одну внешнюю («умножение на скаляр») операцию.

1. Операция $+$ выполняется поточечно:
$$\sum_{g\in G} a_g g + \sum_{g\in G} a_g g = \sum_{g\in G} (a_g + b_g).$$
2. Операция умножения на скаляр выполняется поточечно:
$$\lambda \sum_{g\in G} a_g g = \sum_{g\in G} (\lambda a_g) g.$$
3. Операция $\times$ выполняется «как в многочленах» («свёрткой»).

$$\begin{aligned}&\sum_{g\in G} a_g g \times \sum_{g\in G} a_g g = \\ &\qquad \sum_{g\in G}\left(\sum_{q,w\in G, qw=g} a_q b_w\right) g = \\ &\qquad \sum_{g\in G}\left(\sum_{w\in G} a_{gw^{-1}} b_w\right) g.\end{aligned}$$

Примеры.

- $\bar{j}_g = 1$,
- $\hat{1}_x = 0$ для $x \neq 0$ и $\bar{1}_x = 0$,
- $\hat{0}_x = 0$.

Замечание 2. В групповой алгебре элементы $\hat{0}$ и $\hat{1}$ являются нулём и единицей алгебры.

Обозначения. Групповая алгебра обозначается $\mathbb{F}G$. Слагаемые с нулевыми коэффициентами не пишем. Коэффициенты, равные 1 не пишем. Например: $1g$.

Приведём ещё один пример.

- $\delta_g = 1g$.

Упражнение. Пусть G группа, а G_0 её подгруппа. Имеется естественный мономорфизм $\mathbb{F}G_0$ в $\mathbb{F}G$.

Пример 6. $\mathbb{F} = \mathbb{F}_2$, $G = \mathbb{Z}_4$. Попробуем провести умножение двух элементов.

$$\begin{aligned}(1,1,0,0)\times(1,0,1,0) = (&\\ &1\cdot 1 + 0\cdot 0 + 0\cdot 1 + 1\cdot 0,\\ &1\cdot 1 + 1\cdot 0 + 0\cdot 1 + 0\cdot 0,\\ &\ldots,\\ &\ldots\\ &).\end{aligned}$$

Определение 3. Рассмотрим идеал J алгебры $\mathbb{F}G$. Пусть J^t это подалгебра алгебры $\mathbb{F}G$, порождённая элементами вида
$$x_1 \ldots x_t, \qquad x_i \in J.$$

Напомним, что алгебра порождённая элементами множества M, это в точности:
$$\sum_i \alpha_i \prod_j m_{i,j}, \qquad m_{i,j} \in M$$

Лемма 4. *Если J — правый (левый, двусторонний) идеал, то J^t — также правый (левый, двусторонний) идеал.*

Рассмотрим ещё один специальный вид идеалов в $\mathbb{F}G$. Обозначим:
$$\kappa\colon \mathbb{F}G \to \mathbb{F}, \qquad \kappa(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$$

Лемма 5. *Имеют место следующие утверждения относительно κ.*

1. *κ — эпиморфизм.*
2. *$\ker(\kappa)$ — максимальный идеал.*