Базис бесконечнопорожденного пространства

На прошлом занятии мы научились строить базисы для конечнопорожденных, проделаем же это и для бесконечнопорожденных.

Пусть у нас пространство над полем $V(K)$, расммотрим частично-упорядоченное отношением "подмножество" множество

$$P = \{L \subset V : L - \text{ЛНЗ}\}$$

Если мы покажем, что существует максимум L_0, то его линейная оболочка совпадет со всем пространством V и базис будет получен.

Для того, чтобы доказать совпадение выше, достаточно рассмотреть $x \in V \setminus L_0$, который разложится через L_0 или ... не разложится и сделает противоречие.

То есть теперь наша задача – лемма Цорна:

Теорема (Лемма Цорна)

Если задано $\langle M, (\preceq)\rangle$ и для всякого линейно-упорядоченного $S \subseteq M$ выполнено $upb_M S \neq \varnothing$, то в M существует максимальный элемент.

Привет матлогу! И да, это опять философский разговор про добавление в ZF аксиомы выбора и эквивалентные ей утверждения.

Конечные поля

Сначала рассмотрим такие 2 поля: $K \subset K'$ и попробуем задать векторное пространство $K'(K)$: $K \times K' \to K' : (k, a) \mapsto ka$, где умножение из K'. Ну и нетрудно проверить, что все мы удовлетворяем все аксиомы. (Кажется, это верно и для колец)

Так, ну мы можем найти базис, а значит $\forall x \in K' : \exists\{c_i\} : x = \sum c_i e_i$ – запомним, это и будет полезно в конечных полях.

Конечное поле единиц – определяется своей характеристикой

$$\operatorname{char}(K) = \min\left\{n : \underbrace{1 + ... + 1}_{n} = 0\right\}$$

А вообще сложить n раз единичку – полезное занятие: пусть дано поле $K : \operatorname{char}(K) = p \in \mathbb{P}$, $\mathbb{Z}/p\mathbb{Z}$ тоже имеет характеристику p. Рассмотрим

$$\varphi : \mathbb{Z}/p\mathbb{Z} \to K : [m] \mapsto \underbrace{1 + ... + 1}_{m}$$

где $[m]$ – класс вычетов. Ну, это корректная инъекция-вложение гомоморфизм. А следовательно K – векторное пространство над $\mathbb{Z}/p\mathbb{Z}$, и еще раз следовательно $|K| = p^m : p \in \mathbb{P}$ – одно из домашних упражнений решено!

Последнее равенство может быть неочевидно – предлагается попытться разложить K в прямую сумму чего? Смотреть предыдущую заметку.

Упражнения

1. Вспомним групповые кольца. Что такое KG? Когда это будет полем? На занятии сказали – как минимум не должно быть кручений.
2. $\forall p : \exists! K : |K| = p^m$ (такие поля обозначают $\mathbb{F}_{p^m}$).

Порядок группы обратимых матриц

Как мы уже знаем, $GL_n(K)$ – группа обратимых матриц над полем K. Давайте сразу представим $K = \mathbb{F}_{p^m} : GL_n\left(\mathbb{F}_{p^m}\right)$ и посчитаем ее порядок.

Выше мы обсуждали базисы – и не просто так. Их количество считать проще, поэтому напрашивается построить какую-нибудь биекцию в них.

А какие преобразования над базисами мы знаем? Матрица перехода.

$\mathbb{F}_{p^m} = K$ – векторное пространство над полем $\mathbb{Z}/p\mathbb{Z}$, у него есть базис $\{e_i\}$. Для любого другого базиса существует единственная матрица перехода – она обратима. С другой стороны любая обратимая матрица может стать матрицей перехода. Тем самым множество базисов $\mathbb{F}_{p^m}$ биективно $GL_n(K)$.

А базисы мы посчитаем просто комбинаторно.

Выбираем базисный вектор	Количество способов это сделать
e_1	$p^{mn} - 1$
e_2	$p^{mn} - p^m$
e_3	$p^{mn} - p^m p^m$
...	...

Ответ – произведение значений из правого столбца. В качестве упражнений можно разобрать частные случаи (например, $m = 1$).

Копредставление группы перестановок

Перед тем как находить его для общего случая, разберем пару базовых.

$$S_2 = \langle a \mid a^2 = 1 \rangle \cong \mathbb{Z}_2$$

$$S_3 = \langle \text{транспозиции } \sigma_i(i, i+1) = (i+1, i) : \sigma_1, \sigma_2 \mid \sigma_i^2 = 1, \left(\sigma_1\sigma_2\right)^3 = 1 \rangle$$

С двойкой все понятно, с тройкой: ну $\langle ... \rangle \to S_3$ – сюръекция понятно почему, мы перечислили все элементы:

$$\left\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \left(\sigma_1\sigma_2\right)^2, \sigma_1\sigma_2\sigma_1\right\}$$

Как получить инъекцию? Сделать обратное преобразование. Можно заметить интуицию – формула для n выглядит как-то так:

$$\langle \sigma_1, \sigma_2, ..., \sigma_{n-1} \mid \sigma_i^2 = 1, \left(\sigma_i\sigma_{i+1}\right)^3 = 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \sigma_i\sigma_{j>i+1} = \sigma_{j>i+1}\sigma_i \rangle$$

Последнее – *условие дальней абелевости*. В качестве упражнения нужно осознать конструкцию на *полноту* и *ЛНЗ*, а также доказать ее индуктивным переходом.

Теория кос

Если убрать из формулы выше убрать 1 и 2 условие, то получатся группы кос (перестановки с историей) – en.wikipedia (это ссылка).

На следующем занятии

Начнем обсуждать ключевой результат – для произвольных уравнений степени хотя бы 5 невозможно указать явную формулу для решений.