Алгебра 2
18.09.97

Векторные пространства и расширения полей

Часть 1. Векторные пространства над полями.

Примеры полей: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Q}(i)$, $\mathbb{Q}(t)$, $\mathbf{k}(t)$.

Важным полем является поле формальных рядов:

$$\mathbb{C}((z)) = \{\, a_N z^N + a_{N+1} z^{N+1} + \dots \,\}, \qquad N \in \mathbb{Z}.$$

Элементы из этого поля можно складывать, умножать и делить:

$$\frac{1+z}{z-z^2} \;=\; (1+z)(z^{-1}+1+z+z^2+\dots) \;=\; z^{-1}+2+2z+2z^2+\dots$$

Аналогично определению векторного пространства над $\mathbb{R}$ можно определить векторные пространства над любым полем. Примерами векторных пространств над полями являются:

1. Любое поле $\mathbf{k}$ является линейным пространством над самим собой.
2. $\mathbb{Q}(i)$ есть поле над $\mathbb{Q}$.
3. $\mathbb{C}((z))$ — над $\mathbb{C}$.
4. $\mathbf{k}^n = \{\,(\lambda_1, \dots, \lambda_n)\,\}$, где все операции определяются почленно.

Теорема. Если $\dim V = n$, то $V \cong \mathbf{k}^n$.

Подпространство — это подмножество линейного пространства, замкнутое относительно операций сложения и умножения на число.

Линейной оболочкой системы векторов $\langle v_1, \dots, v_n\rangle$ называется множество их линейных комбинаций, т.е. выражений вида $\lambda_1 v_1 + \dots +$

$\lambda_n v_n$. Линейная оболочка — это минимальное подпространство, содержащее данные векторы. Примеры линейных оболочек:

$$\begin{aligned}\langle(1;0;0),(0;1;0)\rangle &= \{\,(\lambda_1,\lambda_2,0)\,\}\\ \langle(1;2;-3),(2;-5;3),(1,0,-1)\rangle &= \{\,(\lambda_1,\lambda_2,\lambda_3)\mid \lambda_1+\lambda_2+\lambda_3=0\,\}\end{aligned}$$

Линейным оператором $A\colon V\to W$ называется отображение, сохраняющее операции сложения и умножения на число. Примеры:

1. $\mathbf{k}=\mathbb{Q},\quad V=\mathbb{Q}(i),\quad A(x)=ix,$
2. $\mathbf{k}=\mathbb{Q},\quad V=\mathbb{Q}(i),\quad A(x)=\overline{x},$
3. $\mathbf{k}=\mathbb{Q}(i),\quad V=\mathbb{Q}(i),\quad A(x)=\overline{x}$ — не линейный оператор, т.к. $A(i\cdot i)\neq iA(i)$.

Матрицей оператора $A\colon V\to W$ в базисах $\{\,e_1,\dots,e_n\,\}\subset V$, $\{\,v_1,\dots,v_m\,\}\subset W$ называется таблица $n\times m$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{m1} & a_{m2} & \dots & a_{mn}\end{pmatrix},$$

где a_{ij} определяется с помощью равенства $A(e_k)=a_{1k}v_1+a_{2k}v_2+\ldots+a_{mk}v_m$. Примеры:

1. $V=W=\mathbf{k}^2,\ A(x)=\lambda x$; в любом базисе $A=\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$.
2. $V=W=\mathbb{Q}(i),\ A(x)=ix$; в базисе $\{\,1,i\,\}$ имеем $A=\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$.
3. $V=W=\mathbb{Q}(i),\ A(x)=\overline{x}$; в базисе $\{\,1,i\,\}$ имеем $A=\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$.

Найдем действие матрицы на вектор:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{m1} & a_{m2} & \dots & a_{mn}\end{pmatrix}\cdot\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_n\end{pmatrix}=\begin{pmatrix} a_{11}\lambda_1+a_{12}\lambda_2+\ldots+a_{1n}\lambda_n\\ \dots\dots\dots\dots\dots\dots\dots\dots\\ \dots\dots\dots\dots\dots\dots\dots\dots\\ a_{m1}\lambda_1+a_{m2}\lambda_2+\ldots+a_{mn}\lambda_n\end{pmatrix}$$

Пусть есть два оператора $A\colon V\to W$, $B\colon W\to U$, размерности V, W и U равны n, m и l соответственно, тогда матрица их композиции

ВА есть $n \times l$ матрица $\|c_{ij}\|$,

$$c_{ij} = \sum_{1 \leqslant k \leqslant m} b_{ik} a_{kj}$$

Линейное преобразование $A\colon V \to V$ называется *обратимым*, если у него есть обратное. Обратное преобразование всегда линейно. Критерии обратимости (для конечномерного V):

1. A — отображение на, т.е. $A(V) = V \quad \Longleftrightarrow \quad A$ — вложение, т.е. $A^{-1}(0) = 0$.
2. Любой базис переходит в базис $\Longleftrightarrow$ какой-то базис переходит в базис.
3. $\det A \neq 0$

Следом матрицы $\|a_{ij}\|$ называется сумма ее диагональных элементов.

Теорема. Определитель и след матрицы оператора не зависят от базиса, в котором он записан.

Часть 2. Расширения полей.

Кольцо многочленов с коэффициентами из поля $\mathbf{k}$ (многочленов над $\mathbf{k}$) обозначается $\mathbf{k}[t]$.

Теорема. Для всех $A, B \in \mathbf{k}[t]$, $B \neq 0$, существуют такие Q и R, что

$$A = QB + R \qquad \deg R < \deg Q$$

У этой теоремы есть два формальных следствия:

1. Любой идеал в кольце многочленов главный.
2. Верна основная теорема арифметики, т.е. кольцо $\mathbf{k}[t]$ факториально.

Пусть P — неприводимый многочлен. Тогда для любого A существуют такие B и C, что $AB = CP + 1$ и $AB \equiv 1 \pmod P$. Таким образом, остатки от деления на P образуют поле, оно обозначается

$\mathbf{k}[t]/(P)$. Вообще говоря, для произвольного $A \in \mathbf{k}[t]$ фактор $\mathbf{k}[t]/(A)$ является кольцом. Очевидно, $\mathbf{k}[t]/(A)$ — векторное пространство над $\mathbf{k}$ и $\dim \mathbf{k}[t]/(A) = \deg A$.

Например, пусть $P = t+1$, $Q = t^2+1$. Тогда $\mathbb{R}[t]/(P) = \mathbb{R}$, $\mathbb{R}[t]/(Q) = \mathbb{C}$.

Многочлен $P(t)$, не имевший корней в поле $\mathbf{k}$, приобретает корень в поле $\mathbf{k}[t]/(P)$, а именно, его корнем будет (класс элемента) $t \in \mathbf{k}[t]/(P)$. Поэтому говорят, что поле $\mathbf{k}[t]/(P)$ получается из $\mathbf{k}$ присоединением корня многочлена P.

Если $\mathbf{k} \subset \mathbf{K}$ — поля, причем $\dim_{\mathbf{k}} \mathbf{K} = n < \infty$, то говорят, что $\mathbf{K}$ — *конечное (алгебраическое) расширение* поля $\mathbf{k}$, и пишут, что $[\mathbf{K} : \mathrm{k}] = n$.

Если $\mathbf{k} \subset \mathbf{K}$, $P \in \mathbf{k}[t]$ разлагается над $\mathbf{K}$ на линейные множители, то $\mathbf{K}$ — *поле разложения*.

Часть 3. Классификация конечных полей.

Теорема Галуа. Если p простое, то существует единственное поле из p^n элементов. Если в поле q элементов, то $q = p^n$ для некоторых p и n.

Доказательство.

1. Пусть $\#\mathbf{F} = q$. Рассмотрим такие элементы этого поля: 1, $1+1$, $1+1+1$, ... Для некоторого p случится

$$\underbrace{1 + \ldots + 1}_{p \text{ раз}} = 0.$$

При этом p должно быть простым, иначе в поле были бы делители нуля.

Единица порождает в $\mathbf{F}$ подполе, изоморфное $\mathbb{F}_p$. Поле $\mathbf{F}$ является линейным пространством над $\mathbb{F}_p$, откуда

$$\#\mathbf{F} = p^{\dim \mathbf{F}}.$$

2. Существование поля из q элементов.

Пусть $\mathbf{K} \supset \mathbb{F}_p$ — какое-нибудь поле разложения $t^q - t$. Внутри $\mathbf{K}$ возьмем подмножество

$$\mathbf{L} = \{\, x \mid x^q = x \,\}.$$

Лемма. $\mathbf{L}$ — поле.

В самом деле, если $x^q = x$ и $y^q = y$, то

$$(xy)^q = xy, \left(\frac{x}{y}\right)^q = \frac{x}{y}, \quad (x+y)^p = x^p + y^p \Rightarrow (x+y)^q = x^q + y^q = x + y$$

По построению $\mathbf{K}$

$$t^q - t = \prod_{i=1}^{q}(t - \alpha_i)$$

Если мы докажем, что все α_i различны, то поле $\mathbf{L}$ будет содержать ровно q элементов. Для этого нужно доказать, что у многочлена $t^q - t$ нет кратных корней, то есть нет общих корней у него и у его производной. Но у его производной вообще нет корней:

$$(t^q - t)' = qt^{q-1} - 1 = -1$$

3. Единственность поля из q элементов.

Наше поле $\mathbf{F}$ содержит в себе мультипликативную группу $\mathbf{F}^* = \mathbf{F} \setminus \{0\}$. Порядок этой группы равен $q-1$, поэтому $\forall x \in \mathbf{F}^*$ имеем $x^{q-1} = 1$ и $\forall x \in \mathbf{F}$ имеем $x^q - x = 0$. Значит, этот многочлен имеет q корней в поле $\mathbf{F}$ и раскладывается на линейные множители, откуда $\mathbf{F}$ — поле разложения $t^q - t$ над $\mathbb{F}_p$.

С другой стороны, если есть некоторое поле разложения $t^q - t$, то в нем можно выделить подполе $\mathbf{L}$ корней этого многочлена, которое будет минимальным полем разложения $t^q - t$, то есть наше поле содержит подполе из q элементов, а, значит, с ним совпадает. Значит, любое поле из q элементов есть минимальное поле разложения $t^q - t$. $\square$

Часть 4. Автоморфизм Фробениуса.

Автоморфизмом поля K над L называется отображение $\alpha\colon K \to K$, удовлетворяющее условиям:

1. $\alpha(x+y) = \alpha(x) + \alpha(y)$
2. $\alpha(xy) = \alpha(x)\alpha(y)$
3. $\alpha(\lambda x) = \lambda\alpha(x)$ для всех $\lambda \in L$

Примером является отображение $\gamma \mapsto \overline{\gamma}$ — автоморфизм $\mathbb{Q}(i)$ над $\mathbb{Q}$, а также $\mathbb{C}$ над $\mathbb{R}$.

Автоморфизмом Фробениуса называется отображение $\mathbb{F}_{p^n}$ в себя, $\mathrm{Fr}(x) = x^p$, $\mathrm{Fr}^k(x) = x^{p^k}$.

Теорема. Если $q = p^n$, то $\{\,\mathrm{Id}, \mathrm{Fr}, \mathrm{Fr}^2, \ldots, \mathrm{Fr}^{n-1}\,\}$ — все автоморфизмы $\mathbb{F}_q$ над $\mathbb{F}_p$.

Доказательство цикличности группы $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$ без изменений переносится на случай мультипликативной группы $\mathbb{F}_q^*$. Пусть ζ — первообразный корень. Тогда $\zeta^q - \zeta = 0$. Пусть P — неприводимый над $\mathbb{F}_p$ многочлен, такой, что $P(\zeta) = 0$.

Существует естественный гомоморфизм $\mathbb{F}_p[t]/(P) \to \mathbb{F}_q$, при котором $t \mapsto \zeta$. Но так как ζ порождает группу $\mathbb{F}_q^*$, то это гомоморфизм на, то есть изоморфизм. Поэтому

$$\mathbb{F}_q = \mathbb{F}_p[t]/(P) \quad \Rightarrow \quad \deg P = \dim \mathbb{F}_q = n$$

Значит, у многочлена P в поле $\mathbb{F}_q$ есть ровно n корней. Так как ζ — первообразный корень, то любой автоморфизм α задается своим значением $\alpha(\zeta)$, а, т.к. $\alpha(\zeta)$ — корень P, то автоморфизмов не больше, чем корней P, то есть их не больше n.

Но n разных автоморфизмов уже указаны, значит, других нет.

Группа автоморфизмов $\mathbb{F}_q$ над $\mathbb{F}_p$ называется *группой Галуа* $\mathbb{F}_q$ над $\mathbb{F}_p$ и обозначается $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p)$. Из последней теоремы следует, что

$$\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$$