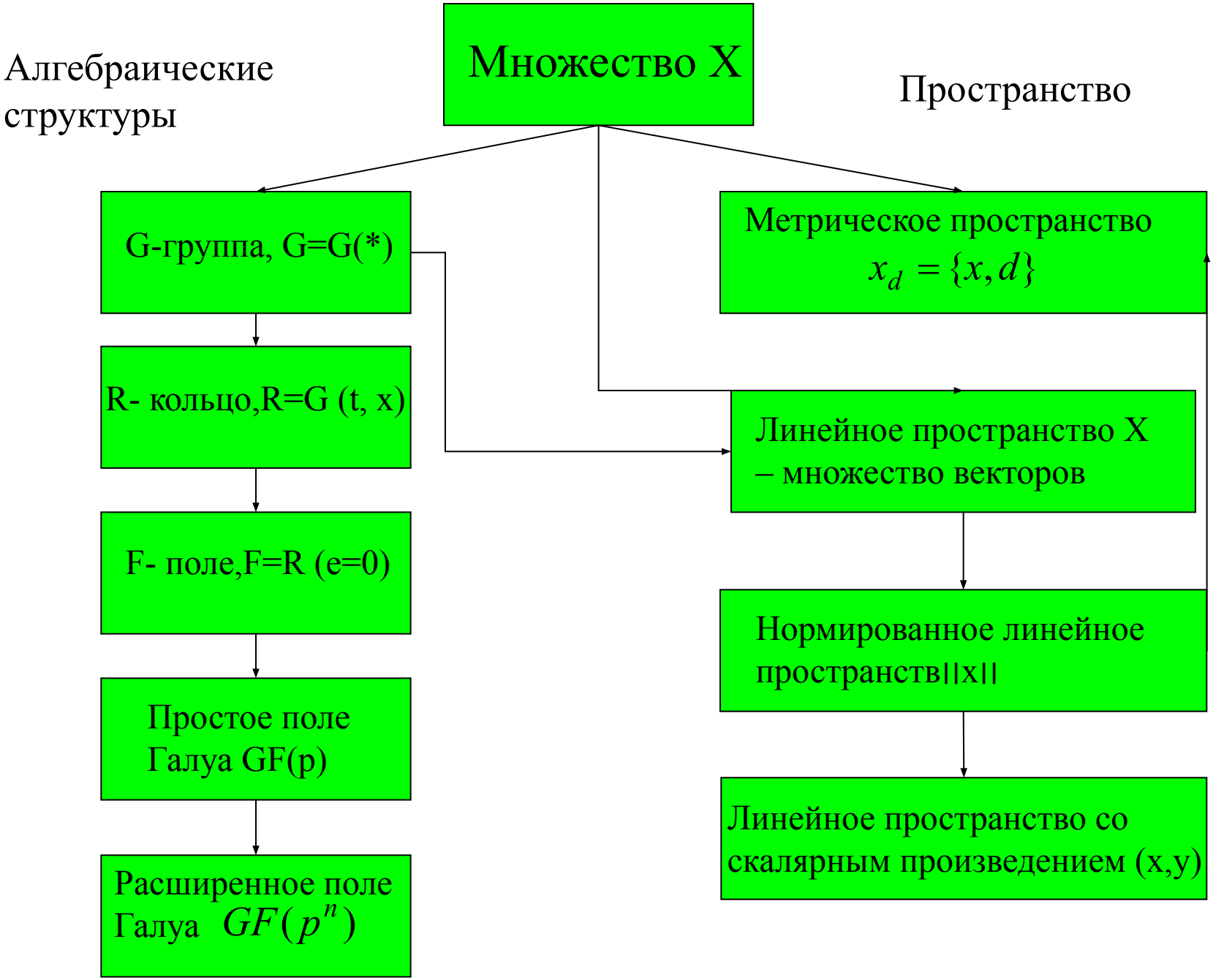
Математические основы дисциплины


Алгебраические структуры
Множество X
Пространство
G-группа, G=G(*)
R- кольцо,R=G (t, x)
F- поле,F=R (e=0)
Простое поле Галуа GF(p)
Расширенное поле Галуа $GF(p^n)$
Метрическое пространство $x_d = \{x, d\}$
Линейное пространство X – множество векторов
Нормированное линейное пространств||x||
Линейное пространство со скалярным произведением (x,y)

Группа

Определение 1: Множество G называется группой относительно бинарной операции (*), если выполняются следующие свойства:

1) Замкнутость: $\forall \alpha,\beta \in G;\ \gamma = \alpha*\beta : \gamma \in G$
2) Ассоциативность: $\forall \alpha,\beta,\gamma \in G; \alpha*(\beta*\gamma)=(\alpha*\beta)*\gamma$
3) Наличие нейтрального элемента:

   $\exists e \in G: \quad \forall \alpha \in G; \quad \alpha*e = e*\alpha = \alpha$
4) Наличие обратного элемента:

   $\forall \alpha \in G \quad \exists \alpha^{-1} \in G: \alpha * \alpha^{-1} = \alpha^{-1} * \alpha = e$

- *Примечание:* Если элементы группы обладают коммутативным свойством:

  $\forall \alpha,\beta \in G$; $\alpha*\beta = \beta*\alpha$, то такая группа называется группой Абеля или коммутативной.

Примеры:

1. Множество целых чисел X=Y

- * - умножение
- 1),2),3) e=1-выполняются,4)-нет

Значит X=Y не является группой.

2. Множество мнимых чисел X=J

- * - сложение
- 1),2),3) e=0,4) -выполняются,

Значит X=J является группой.

3. Множество кодовых комбинаций на все сочетания x={000,001,010,011,101,110,111}

- $\oplus$ - суммирование кодовых комбинаций по модулю 2 (mod 2), без переноса в старший разряд.
- 1),2),3) e=000,4) – выполняются

$$\begin{array}{r} 101 \\ \oplus\ 101 \\ \hline 000 \end{array}$$

Значит X является группой.

Подгруппа

Определение 2: Подмножество G_0 группы G обладающее свойствами группы называется подгруппой

Пример:

$G_0 = \{000,001,010,011\}$

1),2),3) e=000,4) – выполняются, значит G_0 - подгруппа

Кольцо

Определение 3: Множество R являющееся группой относительно бинарной операции сложения называется кольцом, если относительно операции умножения оно обладает свойствами:

1) Замкнутость: $\forall \alpha,\beta \in R;\ \gamma = \alpha \cdot \beta : \gamma \in R$
2) Ассоциативность: $\forall \alpha,\beta,\gamma \in R; \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
3) Дистрибутивность: $\forall \alpha,\beta,\gamma \in R:$

$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma \ ; (\alpha + \beta) \cdot \gamma = \alpha \gamma + \beta \gamma$

Примеры:

1. Множество вещественных чисел R.
2. Множество многочленов A(x) с коэффициентами из R.

Поле F

Определение 4: Кольцо F называется полем, если относительно бинарной операции умножения этого кольца, выполняются свойства:

1) Наличие нейтрального элемента e.

$\exists e \in F: \forall \alpha \in F;\ e \cdot \alpha = \alpha \cdot e = \alpha.$

2) Наличие обратного элемента:

$\forall \alpha \in F \quad \exists \alpha^{-1} \in F: \alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = e$

3) $\alpha, \beta \in F \qquad \alpha \cdot \beta = 0 \Leftrightarrow \alpha = 0 \quad \beta = 0$

Пример: F=R множество вещественных чисел

Простое поле Галуа

Определение 5: Множество целых чисел GF(p):{0,1,2,…,p-1} образует простое поле Галуа относительно бинарной операции сложения по модулю p и умножения по модулю p, если эти операции выполняются следующим образом:

$a \oplus b = c \Leftrightarrow a + b = c + k \cdot p$, где k-целое число, $c<p$.

$a \odot b = d \Leftrightarrow a \cdot b = d + l \cdot p$, где l-целое число, $c<d$.

- $a \oplus b = c = rest\frac{a+b}{p}$
- $a \cdot b = d = rest\frac{a \cdot b}{p}$

Пример: p=7- модуль GF(p)={0,1,2,3,4,5,6}

p=7

$5 \oplus 6 = rest\frac{5+6}{7} = rest\frac{11}{7} = 4$

$5+6 = 11 = 4 + 1 \cdot 7$

$5 \cdot 6 = rest\frac{5 \cdot 6}{7} = 2 \quad rest\frac{30}{7}$

$5 \cdot 6 = 30 = 2 + 4 \cdot 7$

Модулярный многочлен(ММ)

Определение 6:

Многочлен $A(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ называется модулярным, если коэф-ты этого многочлена принадлежат простому полю Галуа, причем при сложении ММ и произведении ММ приведение подобных осуществляется по правилу сложения и перемножения по mod p.

Неприводимый ММ

- *Определение 7:* Многочлен M(x) степени n, с коэф-ми из простого поля Галуа называется неприводимым ММ, если он делится без остатка и на себя или на единицу,т.е. не имеет корней в простом поле Галуа.

Расширенное поле Галуа

Определение 8: Множество ММ степени не выше n-1 с коэф-ми из простого поля Галуа GF(p) образуют $GF(p^n)$ относительно бинарных операций сложения и умножения по модулю p(mod p) и по модулю M(x)(mod M(x)).