Опр. Группы

Группой наз-ся мн-во G с определенной на нем бинарной алгебраической операцией „$*$" (т.е. $\forall\ a,b \in G \quad a*b \in G$).

Причем „$*$" удовл след. аксиомам:

① Ассоциативность

$(a*b)*c = a*(b*c)\ \forall a,b,c \in G$

② $\exists$ нейтр эл-та

$\exists\ \varepsilon \in G : \forall\ a \in G \hookrightarrow (a*\varepsilon) = (\varepsilon * a) = a$

③ $\exists$ обр-го эл-та

$\forall a \in G \quad \exists a^{-1} : a*a^{-1} = a^{-1}*a = \varepsilon$

Утв. В $\forall\ G$ нейтр. эл-т единственен

Д-во.

Пусть $\varepsilon_1, \varepsilon_2$ – нейтр

$\varepsilon_1 = \varepsilon_1 * \varepsilon_2 = \varepsilon_2$. ■

Утв. В $\forall\ G$ $\forall a \in G \hookrightarrow$ левый к a = правый к a = a^{-1}
(обр.) (обр.)

Д-во

$c \cdot a = \varepsilon$ – левый обр

$a \cdot b = \varepsilon$ – правый

$b = \varepsilon * b = (c*a)*b = c*(a*b) = c*\varepsilon = c$. ■

Опр. Если $\forall\ a,b \in G \hookrightarrow a*b = b*a \Rightarrow G$ – абелева.

Опр. кольцо – мн-во R с опред. на нём „$+$" сложением и „$*$" умножением.

Причем эти оп-ии удовл след ак.

① $(R,+)$ – абелева группа

② $(x \cdot y) \cdot z = x(y,z)$ ассоц.

③ $(x+y)\,z = xz + yz$

$x(y+z) = xy + xz$

Опр. Кольцо наз-ся коммутативным, если $\forall xy \hookrightarrow xy = yx$

Опр. Кольцо с 1, если $\exists$ „1": $x \cdot 1 = 1 \cdot x = x\ \forall x \in R$

Пусть R - кольцо $a, b \in R$. - делители 0 в кольце R, если

а) $a \neq 0, b \neq 0$

б) $a \cdot b = 0$

Кольцо вычетов по mod n

$n \in \mathbb{N} > 1$

$a, b \in \mathbb{Z}$ сравнимы по mod n, если они имеют одинаковые остатки по mod n

$a \equiv b \ (n)$

Утв. $a_1 \equiv a_2 \ (n)$ $b_1 \equiv b_2 \ (n)$

$a_1 \pm b_1 \equiv a_2 \pm b_2 \ (n)$

$a_1 b_1 \equiv a_2 b_2 \ (n)$

Отношение сравнимости - отношение эквивалентности.

$a \equiv b \Leftrightarrow a, b$ в одному классу.

Число классов $= n$

$\bar{0}, \bar{1} \ldots \overline{n-1}$

Если опр-ть $\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$, то

$(\mathbb{Z}_n, +, \cdot)$

$(\mathbb{Z}_n, +)$ абелева группа

$\bar{0}$ - нейтральный

$\bar{a} + -\bar{a} = \bar{0}$

$\mathbb{Z}_n$ - коммутативное кольцо с 1=1

Утв. Пусть R^* - мн-во всех обр-х эл-в кольца с 1.

Тогда $(R^*, \cdot)$ - группа

Опр. Пара мн-во F, с опр-ми на нем оп-ми сложения и умножения, если эти оп-ии удовл. след. усл-м.

1. $(F, +)$ - абелева группа с нейтр эл-м 0
2. $(F \setminus \{0\}, \cdot)$ - абелева группа с нейтр эл-м 1.
3. $(x+y)z = xz + yz$ - дистрибутивность

Note $P^* = F \setminus \{0\}$ - группа обр-х эл-в

№2
Р.2

Опр. Поле - коммутативное кольцо с единицей, в котором группа обр-х эл-в $-F\setminus\{0\}$.

$(F,+)$ - аддитивная группа

$(F^*,*)$ - мультипликативная группа.

Утв. В ∀ поле ≠ делителей нуля.

Д-во (от пр-го)

Пусть $a\neq 0$, $b\neq 0$, $a\cdot b=0$

$a\cdot b=0$

$a^{-1}a\cdot b=0$

$1\cdot b=0$

$b=0$?! ▨

Т2 Кольцо Z_n классов вычетов по модулю n - поле $\Leftrightarrow$ n - простое

Д-во

$a)\Rightarrow$

Пусть Z_n - поле. Покажем, что n - пр-е

Пусть n - составное $\Rightarrow n=p\cdot q$

$1<p$ $\quad \bar{p},\bar{q}\neq\bar{0}$

$q\leq n-1$

$\bar{p}\bar{q}=\overline{p\cdot q}=\bar{n}=\bar{0}\Rightarrow \bar{p}$ и $\bar{q}$ - делители нуля ?!

$b)\Leftarrow$

Пусть n - простое. Покажем Z_n - поле.

Единственное, что надо показать,

что ∀ $\bar{a}\neq 0$ в Z_n есть обр-й и $\acute{a}$

$\bar{0}\cdot\bar{a}$, $\bar{1}\cdot\bar{a}$, ... $\overline{n-1}\cdot\bar{a}$

Покажем, что все эти пр-я попарно разл-ны в Z_n

Пусть $\bar{k}\bar{a}=\bar{l}\bar{a}$ $\quad 0\leq k<l\leq n-1$

$\bar{k}\bar{a}-\bar{l}\bar{a}=0$

$(\bar{k}-\bar{l})\bar{a}=0$

$(l-k)a\equiv 0 \pmod n$

$(l-k)\cdot a \vdots n$

Если пр-е целых чисел делится на пр-е число, то хотя бы один из мн-й делится на него.

$0<l-k\leq n-1$

Т.к. полученные эл-ты попарно различные и их n штук $\Rightarrow$ все эл-ты Z_n

$\exists b : \bar{b} \cdot \bar{a} = 1 \quad b \neq \bar{0}$ ▨

12) Поле из n эл-в $\Leftrightarrow n = p^k$, p - простое

Def Кратные единицы

F - поле, $0, 1 \in F$

$\underbrace{1+1\ldots+1}_{n} = n_F$ - n-я кратная единица $\in F$

$0_F = 0$ - нулевая кр-я ед.

$(-n)_F \overset{def}{=} -n_F$

Т.е. $\forall n \in \mathbb{Z}$ в поле $\exists\, n_F$

Def хар-ка поля F - наименьшее $n \in \mathbb{N} : n_F = 0$.

Если $\forall n \in \mathbb{N} \hookrightarrow n_F \neq 0 \Rightarrow \operatorname{char} F = 0$.

Пример

$\mathbb{Q}, \mathbb{R}, \mathbb{C} \Rightarrow \operatorname{char} = 0$

p - пр-е $\mathbb{Z}_p$ $\operatorname{char} \mathbb{Z}_p = p$

Утв хар-ка поля - либо 0 либо пр-е число

Д-во Пусть $\operatorname{char} F = n$, $n = p \cdot q$ $1 < p$ $q \leq n-1$

$p_F, q_F \neq 0$

$p_F \cdot q_F = (\overbrace{1+\ldots 1}^{p})(\overbrace{1+\ldots 1}^{q}) = \overbrace{1+\ldots+1}^{p \cdot q} = (pq)_F = n_F = 0$

Но в поле нет делителей 0 ?! ▨

Note $n_F + m_F = (n+m)_F$

$n_F m_F = (nm)_F$

G - группа с операцией „$*$"

Def Непустое $H \subset G$ - подгруппа G, если

H - группа относительно „$*$".

Note У G и H одинаковые нейтр эл-ты

Д-во

e_G и e_H

$e_H e_H = e_H$

$e_H^{-1} e_H e_H = e_H^{-1} e_H$

$\underline{e_H = e_G e_H = e_G}$ ▨

§2 р3 Def изоморфизм групп

$(G_1, *)$ $(G_2, *)$

Отображение φ из G_1 в G_2 - изоморфизм, если

① φ - взаимнооднозначно

② φ сохраняет операцию

$\forall a, b \in G_1 \quad \varphi(a * b) = \varphi(a) * \varphi(b)$

Note Если убрать взаимнооднозначность - гомоморфизм

Простое подполе

F - поле с опер. „*"

Def $\emptyset \neq S \subset F$ S - подполе, если

а) S - подкольцо кольца F

б) S замкнуто отн слож.

$a, b \in S \Rightarrow a - b \in S$

в) S замкнуто отн умн.

$a, b \in S \Rightarrow a \cdot b \in S$

г) $\forall a \neq 0$ в S должен быть a^{-1}

Утв Пересечение ∀ мн-ва подполей - подполе

Def Поле F - пр-е, если $\nexists$ подполей $\subsetneq F$.

Th ① У всякого поля F есть простое подполе и при том только одно

Д-во

а) Д-м ∃-е

D - пересечение всех подполей F

P - подполе F

P сод-ся в ∀ подполе F.

Пусть $M \subset P \hookrightarrow M \subset F \Rightarrow P \subset M \Rightarrow P = M$

$\Rightarrow$ P - пр-е

б) Пусть P и P_1 - два пр-х подполя F

$P \cap P_1 \subset P \overset{\text{пр-е}}{\Rightarrow} P \cap P' = P \Rightarrow P = P_1$

$P \cap P_1 \subset P_1 \overset{\text{пр-е}}{\Rightarrow} P \cap P' = P_1$

12 (об описании пр-х подполей)

Простое подполе поля $\mathbb{F}$ изоморфно $\mathbb{Q}$, если $\mathrm{char}\,F=0$,
и пр-е подполе поля F изоморфно $\mathbb{Z}_p$, если $\mathrm{char}\,F=p$, p-пр-е

Д-во,

а) Пусть $\mathrm{char}\,F=0$

$$\begin{array}{ccc} \mathbb{Z} & \to & F \\ \downarrow & & \downarrow \\ n & \to & n_F \end{array} \qquad \begin{array}{l} n_F + m_F = (n+m)_F \\ n_F m_F = (nm)_F \end{array}$$

Покажем, что данное отн-е не склеивает точки (инъективно)

Пусть $n \neq m$, $n, m \in \mathbb{Z}$

Предположим $n_F = m_F$

$n_F - m_F = 0 \Rightarrow (n-m)_F = 0 \Rightarrow n = m$ - прот.

Образом раз. числа $\frac{m}{n}$ будем считать решение ур. я $n_F x = m_F$ $n_F \neq 0$

$$n_F^{-1} \cdot \begin{array}{l} n_F x_1 = m_F \\ n_F x_2 = m_F \end{array} \Rightarrow x_1 = x_2 = n_F^{-1} \cdot m_F \Rightarrow \frac{m}{n} \to \frac{m_F}{n_F} \text{ - реш. ур-я}$$

(легко пр-ть, что это гомоморфизм, т.к. сложение и умножение полей пронск-т по обычным пр-м)

Проверим инъективность $\frac{m}{n} \neq \frac{m'}{n'}$ (не сокр. дроби)

$$\overset{\mathrm{char}\,F=0}{\Rightarrow} (mn' - nm')_F = 0 \Rightarrow n'm - m'n = 0 \Rightarrow \frac{m}{n} = \frac{n'}{n'}$$

Такой гомоморфизм можно построить в $\forall$ подполе F.

Пусть D-пр-е подполе. $\mathbb{Q} \subset D$. D-пр-е $\Rightarrow \mathbb{Q} = D$

б) $\mathrm{char}\,F = p$ $0_F, 1_F \dots (p-1)_F$.

Полученные пр-е единицы обр-ют подполе, изоморфное $\mathbb{Z}_p$.

Изоморфизм -,, отображивание символа F

Т.е. $\mathbb{Z}_p \subset D$-пр-е подполе $\Rightarrow \mathbb{Z}_p = D$.
(т.к. D зад-т крайние единицы)