Кондрашев Валодя

Г Р У П П Ы

СЛ 1
01.09
1988г

ГРУППОЙ называется множество G, в котором задана операция ✻, ставящая в соответствие элементам g и h из G элемент g✻h (произведение), и кроме того выделен элемент e и каждому g∈G сопоставлен обр(g)∈G, так что

(Г1) $\forall f,g,h\in G$ $(f✻g)✻h = f✻(g✻h)$ (ассоциативность);

(Г2) $\forall g\in G$ $e✻g=g✻e=g$ (существование единичного элемента);

(Г3) $\forall g\in G$ $g✻обр(g)=обр(g)✻g=e$ (сущ. обратного элемента).

Группа, в которой $\forall g,h$ $g✻h=h✻g$ называется КОММУТАТИВНОЙ или АБЕЛЕВОЙ (в честь Н.Х.Абеля, но вовсе не потому что он это придумал).

Если G состоит из конечного числа элементов n, то группа G называется КОНЕЧНОЙ, а число n – ее ПОРЯДКОМ.

Очень часто, имея дело с группами, пишут g·h (или gh) вместо g✻h, g^{-1} вместо обр(g) и 1 вместо e (для абелевой группы также: g+h, -g и 0). Вместо ((..((g✻g)✻g)..)✻g)✻g <n раз g> мы будем писать g^n.

1. Примеры групп.

а) (АДДИТИВНАЯ группа кольца) G= $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}[\sqrt{2}],\mathbb{Z}_m,\mathbb{R}[x],...$ (g✻h=g+h).

б) (МУЛЬТИПЛИКАТИВНАЯ группа поля) $П^*=П\setminus\{0\}$, где П= $\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_p,..$ (g✻h=gh).

в) (ГРУППА ЕДИНИЦ кольца) K^*= множество обратимых элементов кольца K (так, $R[[x]]^*$= ряды с ненулевым свободным членом, $\mathbb{Z}_m^*$=взаимно простые с m остатки). Операция ✻ – умножение.

г) (Группа ПЕРЕСТАНОВОК) Множество всех взаимно-однозначных отображений множества M на себя. Операция – композиция отображений. Группа перестановок множества {1,2,3,..,n} обозначается S_n.

д) Группа движений плоскости. <три осевые симметрии>

е) Группа симметрий множества M на плоскости – все движения плоскости, отображающие M на себя.

ж) (МОДУЛЯРНАЯ группа) $PSL_2(\mathbb{Z})$ = дробно-линейные преобразования верхней полуплоскости $\{Im(z)>0\}$ $z\mapsto(az+b)/(cz+d)$, $a,b,c,d\in\mathbb{Z}$, $ad-bc=1$.

и) (Одномерный тор) $\mathbb{T}=\{z\in\mathbb{C}:|z|=1\}$, операция – умножение.

к) (Ур-ние Пелля) $\{(x,y):x^2-57y^2=1;x,y\in\mathbb{Z}\}$, $(x,y)✻(u,v)=(xu+57yv,xv+yu)$.

л) (Мультипликативная формальная группа) G = $x\cdot\mathbb{R}[[x]]$ = формальные ряды без свободного члена, f✻g = f+g+fg (чему равно обр(f)?).

м) $\mathbb{R}/\mathbb{Z}$ = $\{x\in\mathbb{R}: 0\le x<1\}$, x✻y = {x+y} ({a}– дробная часть числа a).

н)* (Групповой закон на кубике) Пусть $G=\{(x,y)\in\mathbb{R}^2: y^2=x^3+ax+b\}\cup\{\infty\}$–кубическая кривая на плоскости с добавленной к ней точкой ∞. Будем считать также, что все вертикальные прямые на плоскости (и только они) проходят через ∞. Для M,N∈G определим M✻N: проведем прямую MN (если M=N, то проводим касательную к G в M), найдем ее третью точку пересечения с G – точку L и положим M✻N=L' – точка симметричная L относительно оси Ox ($\infty'=\infty$). Каков геометрический смысл ассоциативности умножения в этой группе? Задайте умножение формулами.

2. (Следствия из аксиом) Пусть G – группа, a,b,c,d∈G. Докажите, что

а) если $\forall g\in G$ ga=g, то a=e; б) ab=e ⇒ b=обр(a); в) обр(обр(a))=a;

г) обр(ab)=обр(b)обр(a); д) (a(b(cd)))=(((ab)c)d); е) если $\forall g\in G$ g·g=e, то группа G абелева.

а) обр(g)✻ б) обр(a)✻ в) обр(a) обр(обр(a))=e г) обр(gh)gh=e ✻ обр h ✻ обр g

д) раскрыть скобки е) ghhg=e ⇒ gh=обр(hg) ⇒ gh=hg.

3. ПОРЯДКОМ элемента g группы G называется минимальное положительное целое число n, тч g^n=e. Если такого n не существует, то говорят, что g имеет бесконечный порядок. Обозначим порядок g через пор(g).

а) g^n=e титтк n⋮пор(g) б) пор(fg)=пор(gf) в) Чему равен пор(g^n), если пор(g)=k ? г) Если fg=gf, то пор(fg) ⋮ НОК(пор(f),пор(g)); а если fg≠gf, то не обязательно (в частности пор(fg) может быть ∞).

д) Любой элемент конечной группы имеет конечный порядок.

е) Найдите все порядки элементов в $\mathbb{Z}_{60}$; $\mathbb{Z}_{19}^*$; S_7.

ж) Найдите все элементы конечного порядка в $\mathbb{C}^*$; группе движений пл-ти.

и) Пусть F– некоторая комбинация поворотов граней кубика Рубика, тогда, делая F достаточно много раз, мы вернемся в исходное состояние.

к) Порядок конечной группы делится на порядок любого ее элемента. <Указание: рассмотрите диаграммы "умножения на g" по аналогии с АР7>

л) (Теорема ЭЙЛЕРА) a,m∈N, НОД(a,m)=1 ⇒ $a^{\varphi(m)}\equiv 1 \pmod m$ (φ–функция Эйлера из АР6)

м) (Теорема ФЕРМА для Гауссовых чисел) $\forall\alpha,\beta\in\mathbb{Z}[i]$, β–простое $\alpha^{N(\beta)-1}\equiv 1 \pmod\beta$.

1	а	б	в	г	д	е	ж	з	и	к	л	м	н*	2а	б	в	г	д	е	3а	б	в	г	д	е	ж	з	и	к	л	м	н
+	+	+	+	+	+	4.12		+	30.11	26.11				+	+	+		+	+														

19.11 26.11 23.12