«Можно, конечно, ничего не объяснять. Но я не сторонник подобного поведения, ведь рано или поздно все мы сталкиваемся с проблемами, выросшими из недоговоренностей»

Зловещие тени групп

группа «Поврче»

Определения:

1. ***Группа*** G – это пара объектов $(M, *)$ (где M – некоторое *множество*, а $*$ – некоторая бинарная *операция*), которые связаны следующими 4мя свойствами:
   а) $\forall a, b \in M : a * b \in M$ (т.е. операция $*$ не выводит нас за пределы M)
   б) $\exists \epsilon \in M : \forall a \in M : \epsilon * a = a * \epsilon = a$ (т.е. в M есть такой элемент ϵ (его называют ***нейтральным*** по операции $*$), что для любого a из M выполняется $\epsilon * a = a * \epsilon = a$; можно сказать, что ϵ *действует* на M *тождественно*)
   в) $\forall a, b, c \in M : a * b * c = (a * b) * c = a * (b * c)$ (т.е. скобки можно раскрывать в любом порядке; это свойство называется ***ассоциативностью***)
   г) $\forall a \in M \ \exists b \in M : a * b = b * a = \epsilon$ (т.е. для любого элемента a из M существует ***обратный*** к нему элемент b; такой элемент b обычно обозначается a^{-1})
2. Операция $*$ ***коммутативна***, если $\forall a, b \in M : a * b = b * a$ (т.е. «от перемены мест слагаемых ничего не меняется»).

   Группа G называется *абелевой*, если её групповая операция $(*)$ коммутативна.

   Примечание: Для удобства операцию $*$ обычно называют *умножением* (а если она коммутативна, то *сложением*), несмотря на то, что $*$ может не иметь ничего общего с известными нам арифметическими операциями.

   Если какой-то элемент a мы «умножаем» на себя n раз, то мы будем говорить, что мы *возводим* a *в* n*-тую степень* ($\underbrace{a * a * \ldots * a}_{n} = a^n$).
3. Группа G называется ***циклической***, если она *порождена* лишь одним элементом a (т.е. все элементы мн-ва M — это целые степени элемента a, т.е. $\exists a \in M : \ \forall b \in M \ \exists n \in \mathbb{Z} : b = a^n$).
4. ***Первообразный корень*** циклической группы G — это такой элемент $a \in M$, что он *порождает* все остальные элементы M (т.е. $\forall b \in M \ \exists n \in \mathbb{Z} : b = a^n$).
5. ***Подгруппа*** H группы $G = (M, *)$ — это пара $(N, *)$, где N — подмножество M. При этом, естественно, H должна быть *группой* (см.свойства выше)

Примечание: Через $\mathbb{R}^*$ обозначается $\mathbb{R}\backslash\{0\}$.

Для разминки и лучшего усвоения новых понятий поймем, какими новоизученными свойствами обладают известные нам объекты.

1. Какие из указанных числовых множеств с операциями являются группами? Какие из них абелевы, какие цикличны?:
   а) $(A, +)$, где A — одно из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
   б) $(A, \cdot)$, где A — одно из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
   в) $(A^*, \cdot)$, где A — одно из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
   г) $(n\mathbb{Z}, +)$, где n — натуральное число, а $n\mathbb{Z}$ — мн-во целых чисел, которые делятся на n;
   д) $(\mathbb{Z}_m, +)$, где $\mathbb{Z}_m$ — мн-во остатков по модулю m;
   е) $(\mathbb{Z}_p^*, \cdot)$, где p простое;
   ж) $(\mathbb{Z}_m^*, \cdot)$, где m не простое;
   з) $(\{1, 1\}, \cdot)$;
   и) множество степеней данного вещественного числа $a \neq 0$ с целыми показателями относительно умножения;
   к) $\mathbf{U}_n$, множество всех комплексных корней фиксированной степени $n \in \mathbb{N}$ из 1 относительно умножения;
   л) $\mathbf{U}_\infty$, множество комплексных корней всех степеней из 1 относительно умножения;
   м) множество комплексных чисел с фиксированным модулем r относительно умножения;
   н) множество ненулевых комплексных чисел с модулем, не превосходящим фиксированное число r, относительно умножения;
   о) множество ненулевых комплексных чисел, расположенных на лучах, выходящих из начала координат и образующих с лучом Ox углы $\alpha_1, \alpha_2, \ldots, \alpha_n$, относительно умножения;
   п) множество всех непрерывных монотонных (т.е. $x < y \Rightarrow f(x) < f(y)$) отображений $f : [0, 1] \to [0, 1]$, для которых $f(0) = 0, f(1) = 1$, относительно суперпозиции
   р) множество движений плоскости относительно операции суперпозиции

Я ***~~иллюзорен~~*** изоморфен со всех сторон

группа «Поврче»

Определения:

Порядок группы $G = (M, *)$ — это количество элементов в множестве M (обозначается $|G|$; если M — бесконечно, говорят, что группа тоже бесконечная и $|G| = \infty$).

Порядок элемента g группы $G = (G, *)$ — это такое *наименьшее* натуральное число n, что $g^n = \epsilon$, где ϵ — нейтральный элемент (обозначается $ord(g)$ или $|g|$; если g ни в какой натуральной степени не обращается в ϵ, говорят, что $ord(g) = \infty$).

Изоморфизм групп $G = (G, *)$ и $H = (H, \circ)$ — это такое ***биективное*** *отображение* $f : G \to H$, что $\forall g_1, g_2 \in G$ выполняется $f(g_1 * g_2) = f(g_1) \circ f(g_2)$ (То есть мы можем сначала перемножить g_1, g_2, а потом результат отобразить в H, а можем сначала отобразить g_1, g_2 в H, а затем их образы перемножить; в обоих случаях результат одинаков).

Гомоморфизм групп $G = (G, *)$ и $H = (H, \circ)$ — это такое *отображение* $f : G \to H$ (уже *не обязательно* биективное!!!), что $\forall g_1, g_2 \in G$ выполняется $f(g_1 * g_2) = f(g_1) \circ f(g_2)$.

Автоморфизм группы G — это *изоморфизм* $f : G \to G$ (отображение G в *себя*).

1. Докажите: (a) единственность нейтрального элемента ϵ в любой группе;
   (b) для любого $g \in G$ докажите единственность обратного к нему элемента g^{-1}.
2. Докажите, что в конечной группе каждый элемент имеет конечный порядок.
3. Докажите, что порядок любого элемента группы делит порядок этой группы.
4. Доказать, что во всякой группе:
   (а) элементы x и yxy^{-1} имеют одинаковый порядок;
   (б) элементы ab и ba имеют одинаковый порядок;
5. Найдите все неизоморфные между собой группы (a) порядка 3; (b) порядка 4.
6. Докажите, что все циклические группы одинакового порядка изоморфны между собой.
7. Какие из указанных ниже совокупностей отображений множества $M = 1, 2, ..., n$ в себя образуют группу относительно умножения:
   а) множество всех отображений; б) множество всех инъективных отображений;
   в) множество всех сюръективных отображений;

г) множество всех биективных отображений;

е) множество всех нечетных перестановок;

д) множество всех четных перестановок; ж) множество всех транспозиций;

з) множество всех перестановок, оставляющих неподвижными элементы некоторого подмножества $S \subseteq M$;

и) множество всех перестановок, при которых образы всех элементов некоторого подмножества $S \subseteq M$ принадлежат этому же подмножеству S;

к) множество $\{\epsilon, (12)(34), (13)(24), (14)(23)\}$;

л) множество $\{\epsilon, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$.

8. Какие из отображений групп $f : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ являются гомоморфизмами?:
(a) $f(z) = |z|$; (b) $f(z) = 2|z|$; (c) $f(z) = \frac{1}{|z|}$; (d) $f(z) = 1+|z|$; (e) $f(z) = |z|^2$;
(f) $f(z) = 1$; (g) $f(z) = 2$; (h) $f : (\mathbb{C}^*, \cdot) \to (\mathbb{R}, +)$; $f(z) = arg(z)$.

9. Доказать, что полуинтервал $[0, 1)$ с операцией $\oplus$, где $\alpha \oplus \beta$ дробная часть числа $\alpha + \beta$, является группой. Какой из групп из задачи 1 из прошлого листа изоморфна эта группа? Доказать, что всякая ее конечная подгруппа является циклической.

10. Пусть G — множество всех вещественных чисел, отличных от -1. Доказать, что G является группой относительно операции $* : x * y = x + y + xy$.

11. Для каких групп G отображение $f : G \to G$, определенное правилом:
(а) $f(x) = x^2$; (б) $f(x) = x^{-1}$, является гомоморфизмом? При каком условии эти отображения являются изоморфизмами?

12. Постройте какой-нибудь изоморфизм между группами:
(a) $(\mathbb{Z}_4, +)$ и $(\mathbb{Z}_5^*, \cdot)$; (b) $(\mathbb{R}, +)$ и $(\mathbb{R}_+, \cdot)$; (c) S_4 и группа движений тетраэдра;

13. Найти все автоморфизмы группы $(\mathbb{Z}, +)$.

14. Доказать, что для любого рационального числа $a \neq 0$, отображение $f : x \to ax$ является автоморфизмом группы $(\mathbb{Q}, +)$. Найти все автоморфизмы группы $\mathbb{Q}$.

15. Доказать, что:
   а) множество всех автоморфизмов произвольной группы является группой относительно композиции;
   б) отображение $\sigma : x \to axa^{-1}$, где a — фиксированный элемент группы G, является автоморфизмом группы G (это называется ***внутренним автоморфизмом***);
   в) множество всех внутренних автоморфизмов произвольной группы является группой относительно композиции.