115. Группы

Пусть G — множество с операцией $*$ (каждой паре f, g элементов G поставлен в соответствие элемент $f * g$; порядок важен!). Множество G называется *группой*, если

1) $(f * g) * h = f * (g * h)$ для любых $f, g, h \in G$;

2) существует *единичный элемент* $e \in G$, для которого $e * g = g * e = g$ при любом $g \in G$;

3) для любого элемента $g \in G$ существует *обратный элемент* $g^{-1} \in G$, для которого $g^{-1} * g = g * g^{-1} = e$.

Операцию $*$ иногда называют «умножением», и вместо $g * h$ пишут просто gh.

Группы, в которых $g * h = h * g$ для любых $g, h \in G$, называются *коммутативными* или *абелевыми*. (Иногда при этом групповую операцию называют «сложением».)

115.1. Выяснить, являются ли группами следующие множества (с указанными операциями) и какие из этих групп коммутативны: (**а**) натуральные числа с операцией сложения; (**б**) целые числа с операцией сложения; (**в**) ...с операцией умножения; (**г**) рациональные числа с операцией умножения; (**д**) остатки по модулю 5 с операцией сложения; (**е**) ...с операцией умножения; (**ж**) ненулевые остатки по модулю 5 с операцией умножения; (**з**) то же для модуля 10; (**и**) векторы на плоскости с операцией сложения; (**к**) ...только векторы с положительными координатами; (**л**) ...с целыми координатами; (**м**) комплексные числа с операцией умножения; (**н**) ... только ненулевые комплексные числа; (**о**) по модулю равные 1; (**п**) по модулю равные 2; (**р**) движения плоскости (с операцией композиции); (**с**) ...сохраняющие ориентацию; (**т**) ...не сохраняющие ориентации; (**у**) повороты; (**ф**) переносы; (**х**) перестановки чисел $1 \dots n$ с операцией умножения; (**ц**) ...только чётные перестановки; (**ч**) циклы длины 3; (**ш**) скорости в теории относительности (числа в интервале от -1 до 1, складываемые по формуле $u * v = (u+v)/(1+uv)$; за единицу скорости выбрана скорость света); (**щ**) фигуры (множества точек) на плоскости с операцией симметрической разности ($A * B = A \bigtriangleup B$ состоит из точек, принадлежащих ровно одной из фигур A и B).

115.2. Доказать, что произведение n сомножителей не зависит от расстановки скобок. (Аккуратное рассуждение требует индукции по n.)

115.3. Доказать (**а**) правило сокращения: если $x * y = x * z$, то $y = z$; (**б**) что в группе не может быть двух единичных элементов. (**в**) что у каждого элемента есть единственный обратный.

Если групповая операция записывается как умножение, то обратный элемент обозначается a^{-1}.

115.4. Как найти $(ab)^{-1}$, зная a^{-1} и b^{-1}?

115.5. Определить a^n (где a — элемент группы, n — целое число) и проверить равенство $a^{m+n} = a^m a^n$.

115.6. Доказать, что для любого элемента a конечной группы найдётся целое положительное n, для которого a^n равно e (единичному элементу).

Наименьшее n с таким свойством называется *порядком* элемента a; оно является периодом последовательности $\dots a^{-2}, a^{-1}, a^0 = e, a^1 = a, a^2, a^3 \dots$ и обозначается $\operatorname{ord}(a)$.

115.7.* Доказать, что $\operatorname{ord}(fg) = \operatorname{ord}(gf)$.

115.8.* В группе выбраны три элемента a, b, c. Сколько различных может быть среди чисел $\operatorname{ord}(abc)$, $\operatorname{ord}(acb)$, $\operatorname{ord}(bac)$, $\operatorname{ord}(bca)$, $\operatorname{ord}(cab)$, $\operatorname{ord}(cba)$?

115.9. Пусть $\operatorname{ord}(g) = 57$. Чему равно $\operatorname{ord}(g^6)$? Сформулировать и доказать общее утверждение.

115.10.* Доказать, что если порядок любого элемента группы (кроме единицы) равен 2, то группа коммутативна.

115.11. Найдите все элементы конечного порядка (а) в группе ненулевых комплексных чисел (по умножению); (б) в группе движений плоскости.

115.12. Пусть a — фиксированный элемент конечной группы G. Доказать, что операция «левого умножения» на a (переводящая x в ax) является перестановкой элементов группы и состоит из циклов одинаковой длины. Будет ли операция «правого умножения» на a состоять из циклов той же длины?

115.13. (Продолжение) Доказать, что порядок любого элемента конечной группы делит порядок (число элементов) группы.

115.14. Доказать малую теорему Ферма: если целое число a взаимно просто с целым положительным числом n, то то $a^{\varphi(n)}$ mod 1 по модулю n. (Здесь $\phi(n)$ — количество чисел от 1 до n, взаимно простых с n.)

115.15.* Существует ли бесконечная группа, любой элемент которой имеет конечный порядок?

Если любой элемент группы является (положительной или отрицательной) степенью элемента a, элемент a называется *образующей* группы, а группа называется *циклической*.

115.16. Бывают ли нециклические группы из 1, 2, 3, 4, 5 и 6 элементов?

115.17. Будет ли группа ненулевых остатков при делении на 11 (с операцией умножения) циклической?

Подмножество H группы G называют *подгруппой*, если оно само является группой относительно той же операции, то есть содержит единицу, произведение любых двух своих элементов и обратный к любому своему элементу.

115.18. Какие имеются подгруппы в группе остатков по модулю 10 (с операцией сложения)?

115.19. . . . в группе перестановок трёх элементов?

115.20. Верно ли, что пересечение подгрупп — подгруппа? А объединение?

115.21. Доказать, что любая подгруппа группы $\mathbb{Z}$ целых чисел (по сложению) имеет вид $n\mathbb{Z}$, то есть состоит из всех кратных некоторого числа n.

115.22.* Пусть $X \subset \mathbb{R}$ — подгруппа аддитивной группы вещественных чисел. Доказать, что либо X состоит из всех кратных некоторого числа x, либо X всюду плотна в $\mathbb{R}$ (пересекается с любым интервалом). Какой случай из двух имеет место для множества чисел вида $m + n\sqrt{2}$ (где $m, n \in \mathbb{Z}$)?

115.23. Множество элементов gh, где g — фиксированный элемент G, а h пробегает все элементы H, называется *левым смежным классом* G по H и обозначается gH. Доказать, что (а) все смежные классы содержат одно и то же количество элементов; (б) любые два смежных класса либо не пересекаются, либо совпадают.

115.24. (Теорема Лагранжа) Пусть G — конечная группа, H — ее подгруппа. Докажите, что порядок H делит порядок G. (Указание: G разбивается на смежные классы.) Как вывести отсюда, что порядок группы делится на порядок любого её элемента?

115.25.* Описать все конечные подгруппы группы движений плоскости.

115.26.* Сколько элементов циклической группы порядка n имеют порядок k?

115.27.* Пусть n — целое положительное число. Доказать, что сумма чисел $\varphi(d)$ для всех делителей d числа n равна n. (Например, при $n = 6$ имеем $\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1 + 1 + 2 + 2 = 6$.)

115.28.* Доказать, что любая группа простого порядка является циклической.

115.29.* Подмножество H конечной группы G замкнуто относительно умножения (произведение любых двух элементов из H лежит в H). Доказать, что H — подгруппа.

115.30.* В конечной группе квадрат любого элемента равен единице. Каков может быть порядок этой группы?