Семинар №4. Кольца, поля, полукольца

Теоретический материал: гл. 2, 2.3, 2.6; гл.3, 3.1-3.3. Статья: *Белоусов А.И.* О некоторых свойствах полуколец (выложена на персональной странице автора).

Задача №1 (2.9, стр. 172). Является ли полем множество чисел вида $x+y\sqrt{2}$, где $x,y\in\mathbb{Q}$ (рациональные числа) с обычными операциями сложения и умножения.

Решение

Свойства числовых операций проверять не нужно: они известны. Здесь нужно убедиться в том, что определенное в условии задачи множество $M=\{x+y\sqrt{2}:x,y\in\mathbb{Q}\}$ замкнуто относительно операций сложения и умножения, то есть сумма и произведение двух чисел из M принадлежит M.

Это легко проверить:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in M;$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in M$$

Кроме этого, нейтральные элементы 0 и 1 представляются как числа из этого же множества M:

$0=0+0\sqrt{2},1=1+0\sqrt{2}$.

Множество M можно уподобить множеству комплексных чисел, у которых есть действительная и мнимая части. Здесь же мы можем говорить о рациональной и иррациональной части.

Итак, мы имеем числовую алгебру $\mathbf{M}=(M,+,\cdot,0,1)$, которая, очевидно, является кольцом и подалгеброй поля действительных чисел.

Чтобы ответить на вопрос, является ли это кольцо полем, нужно проверить обратимость по умножению произвольного ненулевого числа из множества M.

Имеем:

$$(a+b\sqrt{2})^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2},a^2+b^2\neq 0.$$

Знаменатель этой дроби не может оказаться равным нулю, так как тогда мы получили бы, что $\frac{a}{b}=\sqrt{2}$, но отношение рациональных чисел не может быть иррациональным числом.

Итак, любой ненулевой элемент множества M обратим по умножению, и

$$(a+b\sqrt{2})^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in M, a^2+b^2\neq 0,$$

так как обе дроби в написанной выше формуле являются рациональными числами (что совершенно очевидно).

Итак, алгебра $\mathbf{M}=(M,+,\cdot,0,1)$ есть поле. Оно является расширением поля рациональных чисел (то есть содержит последнее в качестве подполя).

Задача №2 (2.12, стр. 173). Кольцо $\mathbf{R}=(R,+,\cdot,0,1)$ называется булевым, если его умножение идемпотентно, то есть для любого $x\ x\cdot x=x^2=x$ Доказать, что:

1) $(\forall x)(x+x=0)$, то есть любой элемент противоположен сам себе: $-x=x$;

2) любое булево кольцо коммутативно;

3) в любом булевом кольце, имеющем более двух элементов, есть делители нуля.

Решение

1) Рассмотрим выражение $(x+x)^2=(x+x)(x+x)=x^2+x^2+x^2+x^2=x+x+x+x.$

Но одновременно $(x+x)^2=x+x.$ То есть $x+x+x+x=x+x$, откуда и получаем $x+x=0$.

2) Преобразуем выражение $(x+y)^2=(x+y)(x+y)=x^2+xy+yx+y^2=x+xy+yx+y.$

Но так как $(x+y)^2=x+y$, то есть $x+xy+yx+y=x+y$, откуда $xy+yx=0$, и, в силу свойства (1), $xy=-yx=yx$.

3) Рассмотрим произведение $x(x+1)$, полагая, что $x\neq 0, x\neq 1$ (что возможно, так как по условию в носителе кольца не менее трех элементов, то есть кроме 0 и 1 есть еще какие-то элементы). Тогда в записанном выше произведении оба сомножителя отличны от нуля, а их произведение равно нулю:
$x(x+1)=x^2+x=x+x=0$, что и доказывает утверждение п. 3.

Задача решена.

Замечание. Булевым кольцом является кольцо подмножеств произвольного множества M -

$R_M=(2^M,\Delta,\cap,\varnothing,M)$.

Делителями нуля в нем будут два любых непересекающихся множества (которые всегда найдутся, если в исходном множестве не менее двух элементов).

Булевым кольцом будет также поле вычетов по модулю 2 (поле $\mathbb{Z}_2$), причем это единственное поле вычетов, являющееся одновременно булевым кольцом.

Системы линейных уравнений в поле вычетов

Задача №3. Решить систему линейных уравнений в поле $\mathbb{Z}_{23}$:

$$\begin{cases} x-5y+z=1 \\ 21x-19y+22z=-21 \\ 5x+17z=5 \end{cases}$$

Решение

Решаем стандартно методом Гаусса, но с учетом того, что все вычисления проводятся по модулю 23, то есть везде в качестве результата пишем остаток от деления на 23 (или противоположный к нему в данном поле).

Запишем основную и расширенную матрицу, упростив 2-ю строку использованием противоположных элементов:

$$\begin{pmatrix} 1 & -5 & 1 & 1 \\ -2 & 4 & -1 & 2 \\ 5 & 0 & -6 & 5 \end{pmatrix}.$$

Первое элементарное преобразование состоит в том, что ко 2-й строке прибавляется 1-я, умноженная на 2, а из 3-й строки вычитается 1-я, умноженная на 5.

В результате получим матрицу:

$$\begin{pmatrix} 1 & -5 & 1 & 1 \\ 0 & -6 & 1 & 4 \\ 0 & 2 & -11 & 0 \end{pmatrix}.$$

Теперь к 3-й строке, умноженной на 3, прибавляем 2-ю:

$$\begin{pmatrix} 1 & -5 & 1 & 1 \\ 0 & -6 & 1 & 4 \\ 0 & 0 & -9 & 4 \end{pmatrix}.$$

Привели основную матрицу к верхнетреугольной форме, получив тем самым уравнение для z:

$-9z=4$, или, что то же самое:

$14z=4$.

Сокращая на 2, получим:

$7z=2$.

Тогда

$$z = 7^{-1} \cdot 2 = 10 \cdot 2 = 20 = -3.$$

(Не пишем никаких дробей! Никаких 2/7!).

Мультипликативная операция нашего поля обозначена просто точкой, которую зачастую опускают. Ниже будет приведен один из алгоритмов вычисления мультипликативных обратных в полях вычетов, но в данном случае его легко угадать: 7x10=70=1 (mod 23).

Замечание. Еще проще, если догадаться, что 2 = -21. Тогда сразу сокращаем на 7 и получаем -3.

Уравнение для y:

$$-6y - 3 = 4,$$
$$-6y = 7,$$
$$y = (-6)^{-1}7 = -4 \cdot 7 = -5 = 18.$$

Находим x:

$$x - 5(-5) - 3 = 1,$$
$$x + 2 - 3 = 1,$$
$$x = 2.$$

Сделаем проверку:

2-5(-5)-3=1,

(-2)2+4(-5)+3=-1+3=2,

5(2)-6(-3)=10+18=5.

Верно.

Ответ: $x = 2, y = 18, z = 20.$

Вычисление мультипликативных обратных в полях вычетов

Согласно малой теореме Ферма (см. п. 2.7, стр. 155-157) для любого ненулевого элемента a поля $\mathbb{Z}_p$ выполняется $a^{p-1} = 1$. Умножая это равенство на обратный к a, получим $a^{-1} = a^{p-2}$. Это и есть формула для вычисления обратного по умножению. Показатель степени можно взять по модулю порядка данного элемента, если он окажется меньше порядка мультипликативной группы поля, то есть числа p-1.

Например, при решении системы в предыдущей задаче мы могли бы вычислить обратный к 7 следующим образом (разложив показатель степени на сумму степеней двойки):

$7^{-1} = 7^{21} = 7^{16} \cdot 7^4 \cdot 7;$

$7^4 = (7^2)^2 = 3^2 = 9; 7^8 = (7^4)^2 = 9^2 = 12; 7^{16} = 12^2 = (-11)^2 = 6;$

$7^{-1} = 6 \cdot 9 \cdot 7 = 8 \cdot 7 = 10.$

Все вычисления выполняются по модулю 23! В данном конкретном случае проще было обратный угадать, ответив на нехитрый вопрос: на какое число надо умножить 7, чтобы в результате получилось число, при делении на 23 дающее остаток 1? Ясно, что этот неизвестный множитель есть 10.

Можно было предварительно вычислить порядок 7 в данном поле. Здесь рассуждаем так. Порядок любого элемента конечной группы, в силу теоремы Лагранжа (п. 2.7), должен быть делителем порядка всей мультипликативной группы поля вычетов. В данном случае это 22. Нетривиальных делителей у числа 22 два: 2 и 11. Но $7^2 = 3 \neq 1$. Вычисляем $7^{11} = 7^8 \cdot 7^2 \cdot 7 = 12 \cdot 3 \cdot 7 = 13 \cdot 7 = -1$. Поскольку число 11 простое, то 11-я степень 7 – наименьшая положительная степень 7, дающая -1. Значит, порядок 7 равен 22, то есть порядку всей группы $\mathbb{Z}_{23}^*$. В качестве побочного результата получаем, что группа $\mathbb{Z}_{23}^*$ циклическая, и 7 – один из ее образующих элементов.

Замечания. 1) Замечание по поводу простого показателя степени (11) выше имеет такой смысл. Порядок элемента a конечной группы можно найти, вычислив наименьший положительный показатель степени k такой, что $a^k = -1$. Тогда понятно, что порядок элемента a будет равен $2k$. Но надо быть уверенным в том, что k - наименьший показатель степени с таким свойством. Если это простое число, то так и есть. В случае составного k это может быть неверно. Например, пусть в группе $\mathbb{Z}_{31}^*$ для некоторого a получилось $a^{15} = -1$. Но $15 = 3 \cdot 5$, и может оказаться, что $a^3 = -1$ или $a^5 = -1$.

2) **Важно не перепутать**: *при вычислении целых степеней элементов мультипликативных групп вычетов (то есть мультипликативных групп полей вычетов $\mathbb{Z}_p$, где p - простое число) показатель степени следует брать по модулю порядка группы, то есть числа $p-1$, но все вычисления проводить по модулю p.*

Можно проверить, что порядок 8 в группе $\mathbb{Z}_{23}^*$ равен 11 (проверить!). Тогда, например,

$8^{2020} = 8^{2020 \bmod 11} = 8^7 = 8^4 \cdot 8^2 \cdot 8 = (-5)^2 (-5) \cdot 8 = -10 \cdot 8 = 12.$

Вычисления проводим по модулю 23! И используем переход к противоположному элементу.

Например, $8^2 = 64 = 18(\mathrm{mod}\,23) = -5$ в аддитивной группе поля. Также используем в вычислениях то свойство, что в любом кольце произвольная четная степень взаимно противоположных элементов дает один и тот же результат – как в обычной арифметике. В частности, для любого a $(-a)^2 = a^2$. Рекомендуется это доказать самостоятельно.

Системы линейных уравнений в полукольцах с тривиальной итерацией

Полукольцо $\mathbf{S} = (S, +, \cdot, 0, 1)$ называется полукольцом с тривиальной итерацией, если итерация любого элемента в нем равна единице полукольца.

В таких полукольцах легко решать системы линейных уравнений, так как для линейного уравнения вида

$$x = ax + b$$

наименьшее решение, даваемое формулой $x = a^* b$, совпадает со свободным членом:

$x = b$.

Задача №4

В полукольце $S_{[1,2]} = ([1,2], \max, \min, 1, 2)$ решить систему

$$\begin{cases} x_1 = 1,2x_1 + 1,6x_2 + 1,3x_3 + 1,1 \\ x_2 = 1,6x_1 + 1,3x_2 + 1,1x_3 + 1,7 \\ x_3 = 1,01x_1 + 1,4x_3 + 1,8 \end{cases}$$

Для удобства записи мы переобозначили операции: + означает max, а точка (как правило, опускаемая) – min. То есть $a + b = \max(a, b), a \cdot b = \min(a, b)$.

Решение

Действуя по схеме последовательного исключения неизвестных (стр. 199-201), получим, исключая x_1:

$$x_1 = (1,2)^* (1,6x_2 + 1,3x_3 + 1,1) = 1,6x_2 + 1,3x_3 + 1,1,$$

Так как итерация любого элемента в этом полукольце с тривиальной итерацией есть единица полукольца – нейтральный элемент по умножению.

Подставляя полученное выражение во 2-е и 3-е уравнения, получим:

$$\begin{cases} x_2 = 1,6(1,6x_2 + 1,3x_3 + 1,1) + 1,3x_2 + 1,1x_3 + 1,7 \\ x_3 = 1,01(1,6x_2 + 1,3x_3 + 1,1) + 1,4x_3 + 1,8 \end{cases}$$

После приведения подобных членов в правых частях будем иметь:

$$\begin{cases} x_2 = 1,6x_2 + 1,3x_3 + 1,7 \\ x_3 = 1,01x_2 + 1,4x_3 + 1,8 \end{cases}$$

Исключаем второе неизвестное:

$x_2 = 1,3x_3 + 1,7$.

Подставляя это в уравнение для 3-го неизвестного, получим:

$x_3 = 1,01(1,3x_3 + 1,7) + 1,4x_3 + 1,8,$

$x_3 = 1,4x_3 + 1,8,$

$x_3 = 1,8$

Тогда $x_2 = 1,3 \cdot 1,8 + 1,7 = 1,7$

$x_1 = 1,6 \cdot 1,7 + 1,3 \cdot 1,8 + 1,1 = 1,6$.

Ответ: $x_1 = 1,6; x_2 = 1,7; x_3 = 1,8$.

Заметим, что рассматриваемое полукольцо является симметричным (п. 3.4), и алгебра

$S^*_{[1,2]} = ([1,2], \min, \max, 2,1)$ также полукольцо (с тривиальной итерацией), называемое двойственным к исходному.

Рекомендуется самостоятельно решить ту же систему в этом двойственном полукольце, понимая теперь уже + как min, а точку как max.

Задача №5

Решить в полукольце $\mathbf{D}_{200} = (D_{200}, НОК, НОД, 1, 200)$ делителей числа 200 по операциям НОК и НОД систему

$$\begin{cases} x_1 = 40x_1 + 25x_2 + 10x_3 + 100 \\ x_2 = 20x_1 + 5x_2 + 100x_3 + 10 \\ x_3 = 50x_1 + 25x_2 + 40x_3 + 25 \end{cases}$$

Решение

Поскольку это полукольцо также является полукольцом с тривиальной итерацией, то действуем так же, как и предыдущей задаче. Обозначения операций изменены, как и в предыдущей задаче: + означает НОК (наименьшее общее кратное), точка (обычно опускаемая) – НОД (наибольший общий делитель).

Из первого уравнения выражаем первое неизвестное через остальные:

$$x_1 = 25x_2 + 10x_3 + 100 \cdot$$

Подставим это выражение во 2-е и 3-е уравнения:

$$\begin{cases} x_2 = 20(25x_2 + 10x_3 + 100) + 5x_2 + 100x_3 + 10 \\ x_3 = 50(25x_2 + 10x_3 + 100) + 25x_2 + 40x_3 + 25 \end{cases}$$

Приводя подобные члены в правых частях, получим:

$$\begin{cases} x_2 = 5x_2 + 100x_3 + 20 \\ x_3 = 25x_2 + 40x_3 + 50 \end{cases}$$

Далее:

$$\begin{cases} x_2 = 100x_3 + 20 \\ x_3 = 25(100x_3 + 20) + 40x_3 + 50 \end{cases}$$

$$x_3 = 200x_3 + 50,$$

$$x_3 = 50, x_2 = 100 \cdot 50 + 20 = 100,$$

$$x_1 = 25 \cdot 100 + 10 \cdot 50 + 100 = 100$$

Ответ: $x_1 = 100, x_2 = 100, x_3 = 50$.

Предлагается самостоятельно решить ту же систему в двойственном полукольце

$$\mathbf{D}^*_{200} = (D_{200}, НОД, НОК, 200, 1),$$

то есть + есть НОД, точка – НОК.

Замечание. Такие системы в полукольцах с тривиальной итерацией можно решать несколько быстрее, отклоняясь от строгого следования схеме последовательного исключения неизвестных.

Можно сразу зачеркнуть все «рекурсивные» слагаемые в правых частях, то есть те, которые содержат неизвестное, стоящее слева. И можно не заботиться о них при приведении подобных членов.

Тогда решение задачи №4 будет выглядеть так:

$$\begin{cases} x_1 = 1,6x_2 + 1,3x_3 + 1,1 \\ x_2 = 1,6x_1 + 1,1x_3 + 1,7 \\ x_3 = 1,01x_1 + 1,8 \end{cases}$$

(переписали исходную систему без рекурсивных слагаемых).

Делаем подстановку выражения для первого неизвестного во второе и третье уравнения:

$$\begin{cases} x_2 = 1,6(1,6x_2 + 1,3x_3 + 1,1) + 1,3x_2 + 1,1x_3 + 1,7 \\ x_3 = 1,01(1,6x_2 + 1,3x_3 + 1,1) + 1,4x_3 + 1,8 \end{cases}$$

Но при приведении подобных не выписываем слагаемое с x_2 в первом уравнении и слагаемое с x_3 во втором:

$$\begin{cases} x_2 = 1,3x_3 + 1,7 \\ x_3 = 1,01x_2 + 1,8 \end{cases}$$

Уравнение для x_3:

$$x_3 = 1,01(1,3x_3 + 1,7) + 1,4x_3 + 1,8,$$

откуда сразу получаем

$$x_3 = 1,8$$

Остальные неизвестные определяются, как выше.

Но использовать такую упрощенную схему рекомендуется всё же при достаточном опыте записи подробных решений, с использованием полной «схемы Гаусса».

Задачи для самостоятельного решения

1) Решить системы линейных уравнений:

$$\begin{cases} 11x - 5y + 7z = 5 \\ x + y - z = 7 \\ 17x - 3y + 6z = 12 \end{cases}$$ в Z_{19};

$$\begin{cases} x+2y+z=10 \\ 2x-y+3z=1 \\ 5x+y+6z=2 \end{cases}$$ в Z_{11}.

2) Найти элемент, обратный к a по умножению, в поле Z_p. Является ли циклическая подгруппа, порожденная элементом a, всей группой Z_p*?

а) $a=17, p=31$;

б) $a=19, p=37$;

в) $a=21, p=43$.

3) Задача 3.3 (к главе 3, стр. 223)

4) Более трудные задачи: 2.14, 2.15, 2.16 и 2.19.

Указания

2.15(б)

Пусть ненулевой элемент a кольца без делителей нуля обратим слева, то есть существует такой элемент a^L (левый обратный) такой, что $a^L a=1$. Тогда $a^L(aa^L-1)=a^L(aa^L)-a^L=(a^La)a^L-a^L=1\cdot a^L-a^L=a^L-a^L=0$,

но так как $a^L\neq 0$, то $aa^L-1=0$ (нет делителей нуля!), и $aa^L=1$, то есть левый обратный является и правым обратным для a.

Аналогично доказывается, что из существования правого обратного следует, что он совпадет в таком кольце с левым обратным.

Чтобы доказать аналогичное утверждение для конечного кольца, используйте отображение сдвига, как это сделано в доказательстве теоремы 2.9 (п. 2.4, стр. 141).

Именно, предполагая, что ненулевой элемент a конечного кольца обратим слева, то есть, что существует такой элемент a^L (левый обратный) такой, что $a^La=1$, определим отображение f_a (левого сдвига на a) множества ненулевых элементов кольца в себя так, что $f_a(x)=ax$. Докажем, что это инъекция.

Пусть $ax=ay$. Тогда $a(x-y)=0$. Умножая это равенство на a^L слева, получим $x-y=0$ и $x=y$. Но инъекция конечного множества в себя есть биекция, откуда каждый ненулевой элемент кольца имеет единственный прообраз при отображении левого сдвига. В том числе, для единицы получим, что существует

такой ненулевой x, что $ax=1$, и этот x и есть правый обратный к a. Остается показать, что он совпадает с левым обратным (самостоятельно!).

Подобным же рассуждением доказывается, что правый обратный, существующий по предположению, совпадает с левым обратным.

2.16(а)

Пусть оба произведения xy и yx обратимы. Обозначим соответствующие обратные как $(xy)^{-1}$ и $(yx)^{-1}$ соответственно.

Тогда $(xy)(xy)^{-1}=x(y(xy)^{-1})=1$, что означает, что элемент $y(xy)^{-1}$ есть правый обратный к x. Левый обратный для x и оба обратных для y найдите самостоятельно.

Дополнения

Доказательство ассоциативности операции min (для чисел)

Надо доказать, что для любых вещественных чисел *a*, *b* и *c*

$$\min(\min(a,b),c)=\min(a,\min(b,c)).$$

Случай 1: $a\le b$

Тогда

$$\min(\min(a,b),c)=\min(a,c),$$

$$\min(a,\min(b,c))=\begin{cases}\min(a,c),\text{если } b>c\\ \min(a,b)=\min(a,c)=a,\ \text{если } b\le c(a\le b\le c)\end{cases}.$$

Случай 2: $a>b$

$$\min(\min(a,b),c)=\min(b,c),$$

$$\min(a,\min(b,c))=\begin{cases}\min(a,b)=\min(b,c)=b,\ \text{если } b\le c\\ \min(a,c)=\min(b,c)=c,\text{если } b>c(a>b>c).\end{cases}$$

Доказательство дистрибутивности min относительно max

Надо доказать, что для любых вещественных чисел *a*, *b* и *c*

$$\min(a,\max(b,c))=\max(\min(a,b),\min(a,c)).$$

Случай 1. $b\le c$

1.1. $a\le b\le c$

$\min(a,\max(b,c)) = \min(a,c) = a$,
$\max(\min(a,b),\min(a,c)) = \max(a,a) = a$.

1.2 $b \le a \le c$

$\min(a,\max(b,c)) = \min(a,c) = a$,
$\max(\min(a,b),\min(a,c)) = \max(b,a) = a$.

1.3 $b \le c \le a$

$\min(a,\max(b,c)) = \min(a,c) = c$,

$\max(\min(a,b),\min(a,c)) = \max(b,c) = c$

Случай 2. $b > c$

2.1 $a \ge b > c$

$\min(a,\max(b,c)) = \min(a,b) = b$,
$\max(\min(a,b),\min(a,c)) = \max(b,c) = b$.

2.2 $b \ge a > c$

$\min(a,\max(b,c)) = \min(a,b) = a$,
$\max(\min(a,b),\min(a,c)) = \max(a,c) = a$.

2.3 $b > c \ge a$

$\min(a,\max(b,c)) = \min(a,b) = a$,

$\max(\min(a,b),\min(a,c)) = \max(a,a) = a$.

Доказано.

Доказательство дистрибутивности числового сложения относительно операции min приведено в Учебнике, стр. 168 (по 7 изд, п. 3.1).

Доказательство теоремы Эйлера

Теорема Эйлера: *для любого натурального k и целого a, взаимно простого с k, число* $a^{\varphi(k)} = 1$ *(mod k), где* $\varphi(k)$ *– количество всех натуральных чисел, взаимно простых с k и меньших k*.

(Заметим, что для простого *k* значение $\varphi(k) = k - 1$, и мы получаем частный случай теоремы Эйлера, известный как ***малая теорема Ферма***).

♦Разложим число *a* по модулю *k*, представив его в виде $a=mk+r$, где $0 < r < k$. Воспользовавшись формулой бинома Ньютона, получим

$(mk+r)^{\varphi(k)}=(mk)^{\varphi(k)}+\ldots+\varphi(k)\,(mk)r^{\varphi(k)-1}+r^{\varphi(k)}=r^{\varphi(k)} \pmod k$.

Более того, число *r* взаимно просто с *k*. Действительно, если бы это было не так, то указанные числа имели бы общий делитель *s*>1, но тогда и сумма *mk+r* делилась бы на *s*, и числа *a* и *k* не были бы взаимно простыми. Следовательно, *r* есть элемент группы всех обратимых элементов кольца $\mathbf{Z}_k$. Рассмотрим тогда в этой группе циклическую подгруппу, порожденную элементом *r*. Ее порядок *l*, равный порядку ее образующего элемента, т.е. *r*, по теореме Лагранжа есть делитель порядка всей группы обратимых элементов кольца $\mathbf{Z}_k$, который равен $\varphi(k)$. Т.е. для некоторого целого *q* выполняется $\varphi(k)=ql$. Следовательно, мы имеем: $r^{\varphi(k)}=r^{ql}=(r^l)^q=1 \pmod k$, что и требовалось доказать. ♦

Образующие элементы конечной циклической группы

> *Если a - образующий элемент конечной циклической группы порядка n, то его степень a^r будет образующим тогда и только тогда, когда число r взаимно просто с n.*

(См. лекцию №11.)

◄Пусть нашлось число $m<n$, что для некоторого $k>1, НОД(k,n)=1$, выполняется $(a^k)^m=a^{km}=1$. Ясно, что $km\geq n$, но, ввиду взаимной простоты чисел k и n, $km\neq n$. Следовательно, $km>n$. Пусть km кратно n, но тогда, поскольку k не делится на n, а $m<n$, то оба этих числа, k и m, должны иметь отличные от 1 и от n делители n, что, очевидно, невозможно по условию. Итак, km не делится на n, и, раскладывая km по модулю n, получим: $km=sn+r, r=\mathrm{mod}(km,n)>0$. Тогда $a^{km}=a^{sn+r}=a^r=1$, что невозможно, так как $r<n$.

Утверждение доказано►.

Замечание. Можно доказать, что *только* степени элемента a, взаимно простые с n, будут порождать группу.

Действительно, пусть $НОД(k,n)=s>1$. Тогда для некоторых l и q имеем $k=ls, n=qs$ и $a^{kq}=a^{lsq}=a^{l\cdot n}=1$, то есть существует меньшая n степень элемента a^k, а именно $q<n$, равная единице, то есть порядок a^k меньше n и он не порождает всю группу.