Приложение 1. ГРУППЫ, КОЛЬЦА, ПОЛЯ

Для криптографии алгебра является одним из основных инструментов в теоретических исследованиях и практических построениях криптографических преобразований. Поэтому в этом прил.1 даны некоторые основные стандартные понятия и определения, которые используются в алгебре.

Группы

Группой называется множество G, на котором определена ассоциативная бинарная операция $\circ$, содержащее элемент e такой, что для любого элемента $a \in G$ выполняется

$$e \circ a = a \circ e = a,$$

и существует элемент a^{-1} такой, что

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Указанный элемент e называется **единицей** группы. Элемент a^{-1} называется **обратным** к элементу a. Легко показать, что единица группы единственна и что элемент, обратный к данному элементу, также определяется однозначно. Если операция $\circ$ коммутативна, то группа называется **коммутативной**, или **абелевой.**

Заметим, что не все коммутативные операции ассоциативны. Например, если в качестве операции $\circ$ использовать среднее арифметическое двух вещественных чисел, то эта коммутативная операция не ассоциативна. Действительно:

$$(a \circ a) \circ b = a \circ b = (a+b)/2,$$
$$a \circ (a \circ b) = a \circ ((a+b)/2) = (3a+b)/4.$$

Примерами абелевых групп являются:

- множества Z целых, Q рациональных, R действительных и C комплексных чисел с соответствующими операциями сложения;
- множества $Q\backslash\{0\}$, $R\backslash\{0\}$ и $C\backslash\{0\}$ отличных от нуля рациональных, действительных и комплексных чисел с соответствующими операциями умножения.

В теории групп используется две равноправных и эквивалентных друг другу терминологических системы: аддитивная и мультипликативная. В аддитивной системе групповую операцию называют операцией сложения, а группы в аддитивной записи для краткости иногда будем назвать **аддитивными**. Группы, операцию в которых называют умножением, иногда именуются **мультипликативными** группами.

Операцию аддитивной группы принято обозначать знаком +, операцию мультипликативной группы обозначают знаком умножения x, или • **(**или ее обозначение, по умолчанию, опускают).

Единичный элемент аддитивной группы обозначается 0 и называется **нулем**. Элемент аддитивной группы, обратный к элементу a, обозначается

$-a$ и называется **противоположным** к этому элементу. Единичный элемент мультипликативной группы обозначается 1 и называется **единицей**. А элемент о**братный** к a обозначается через a^{-1}.

Ассоциативность операции $\circ$ позволяет записывать кратное произведение

$$(\cdots((a \circ a) \circ a) \circ \cdots a) \circ a,$$

опуская скобки

$$a \circ a \circ a \circ \ldots \circ a.$$

Такая формула называется ***k*-ой степенью** элемента a. В аддитивных группах k-я степень элемента

a обозначается $k \cdot a$, в мультипликативных группах используется обозначение a^k. По определению,

$$0 \cdot a = 0 \text{ и } a^{(0)} = 1.$$

В аддитивной группе определяется операция **вычитания** $a - b$ по следующей формуле

$$a - b = a + (-b)$$

Результат $a - b$ называется **разностью** элементов a и b**.**

В мультипликативной группе определяется операция **деления** a/b по следующей формуле

$$a/b = a \cdot b^{-1}.$$

Результат a/b, или называется **частным** от деления элемента a на элемент b.

Рассмотренные выше примеры аддитивных и мультипликативных групп представляют бесконечные группы. Группа, определенная на конечном множестве G, называется **конечной**. **Тривиальная (единичная)** группа определена на одноэлементном множестве $\{e\}$ и содержит только единицу. Число элементов конечныой группы называется **порядком** группы. Порядок тривиальной группы равен 1**,** простейшая нетривиальная группа имеет порядок 2.

Порядком элемента g группы G называется наименьшее число n такое, что $g^n = e$. Порядок элемента g иногда далее обозначается $\mathrm{ord}\ g$. Элемент, порядок которого равен порядку группы, если он существует, называется **образующим** (**примитивным**) элементом группы. Все ненулевые элементы группы могут быть представлены в виде степени образующего (примитивного) элемента. Группа, имеющая образующий элемент, называется **циклической**,

Отношением эквивалентности называется бинарное отношение, которое обладает свойствами транзитивности, рефлексивности и симметричности.

Множество, на котором задано это отношение, разбивается на классы эквивалентности $[a]$, где a – представитель класса. Совокупность классов эквивалентности есть **фактор-множество** множества, на котором определено это бинарное отношение эквивалентности.

Так, на множестве Z целых чисел относительно натурального числа τ можно определить отношение

$$\{(x,y) \setminus x \equiv y \bmod m\},$$

где $x \equiv y \bmod m$ означает, что число τ делит разность $x - y$. Это отношение называется **отношением сравнения по модулю *m***, а классы эквивалентности по этому отношению — **классами, или классами вычетов по модулю *m***.

Фактор-множество по этому отношению сокращенно обозначают Z_m, аналогично, классы конгруэнтности обозначаются просто $[a]_m$.

Легко видеть, что

$$x \equiv y \bmod m$$

тогда и только тогда, когда

$$x \bmod \tau \equiv y \bmod m,$$

где $x \bmod \tau$ и $y \bmod \tau$ – остаток от деления числа x или числа y на m.

На фактор-множестве Z_m можно определить арифметические операции. Сумму классов эквивалентности определяют следующим образом:

$$[x]_m + [y]_m = [x+y]_m.$$

Удобно в качестве представителей классов $[x]_\tau$ использовать наименьшие неотрицательные элементы $x \bmod m$ классов. Тогда операцию сложения можно описать в обозначениях этих представителей:

$$[x]_m+[y]_m = [(x+y) \bmod m]_m.$$

Легко показать, что фактор множество Zm с только что описанной операцией сложения есть аддитивная группа с нулевым элементом $[0]_m$ и что противоположный к элементу $[a]_\tau$ группы есть элемент $-[a]_m = [\tau-a]_\tau$. Аналогично, на фактор множестве Z_m вводится операция умножения по модулю m, т. е.

$$[x]_m \cdot [y]_m=[x \cdot y]_m = [(x \cdot y) \bmod m]_m.$$

При этом множество ненулевых классов конгруэнтности $[a]_m$, $a \neq 0$, имеющих обратный класс $[a^{-1}]_m$, где

$$a \cdot a^{-1} \bmod m \equiv 1,$$

образует мультипликативную группу, которая обозначается Z_m^*.

Мультипликативной единицей является класс $[1]_m$. Множество классов, взаимно простых с модулем m, как раз и и представляют группу Z_m^*. Порядок группы Z_m^* обозначается $\varphi(m)$, так определенная функция называется функцией Эйлера.

Группы Z_m^* и Z_m совпадают тогда и только тогда, когда m – простое число. Рассмотренные аддитивная и мультипликативная группы Z_m и Z_m^* изоморфны аддитивной и мультипликативной группам, заданным на множестве наименьших неотрицательных представителей этих классов, в соответствии с операциями сложения и умножения по модулю τ на множестве этих представителей. Поэтому часто вместо группы на фактор-множестве рассматривают группы на множестве представителей классов, при этом представителей этих множества $Z_m = \{0,1,\ldots,m-1\}$ и $Z_m^*=\{[a], a$ и τ взаимно просты$\}$ обозначают так же, как множества классов.

Подмножество H группы G, замкнутое относительно операций группы и являющееся группой с этими же операциями, называется **подгруппой** данной группы. Например, тривиальная группа есть подгруппа любой

группы.

Теорема (Лагранжа). Если m – порядок группы G, а n – порядок элемента $g \in G$, то

$$g^m = e$$

и $m \equiv 0 \bmod n$ (порядок элемента делит порядок группы).

Теорема. Для любой группы G при любом натуральном k порядок t элемента a^k определяется равенством

$$t = \delta/(k, \delta)$$

где $\delta = \operatorname{ord} a$. В частности, $\operatorname{ord} a^k = \delta$ тогда и только тогда, когда $(k,\delta) = 1$ (k и δ – взаимно просты).

Кольца. Поля. Многочлены над полем

Кольцом называется множество R с операциями сложения и умножения такими, что R является абелевой группой относительно сложения и умножения ассоциативна и дистрибутивна относительно операции сложения:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$
$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Следствием определения кольца является свойство – для любого a

$$a \cdot 0 = 0 \cdot a = 0.$$

Примерами колец служат множества Z целых, Q рациональных и R действительных чисел с операциями сложения и умножения. Кольцо, в котором из уравнения $a \; Ч \; b = 0$ следует, что $a = 0$ или $b = 0$, называется областью **целостности**. Если в кольце имеется

мультипликативная единица, то кольцо называется **кольцом с единицей**. Ниже рассматриваются только кольца с единицей.

Элемент a' кольца с единицей такой, что $a \cdot a' = 1$, называется **обратным к элементу** a. Элемент, обратный к элементу a кольца обозначается a^{-1}. Каждый элемент кольца имеет не более одного обратного к нему элемента. Элемента, обратного к нулевому элементу кольца, не существует. Множество элементов кольца, имеющих обратный элемент, составляет мультипликативную группу кольца R, которая обозначается R^*.

Полем называется кольцо F с единицей, множество ненулевых элементов которого с операцией умножения является абелевой группой. Эта группа называется мультипликативной группой поля. Примерами бесконечных полей являются поля Q рациональных, R действительных и C комплексных чисел.

Подмножество F поля Q, замкнутое относительно обеих операций и являющееся полем, называется **подполем**, что обозначается F Q. Поле, которое не имеет подполя, не совпадающего с самим полем, называется **простым** полем. Существует единственное простое бесконечное поле.– это поле Q рациональных чисел.

Конечные поля называются **полями Галуа** – по имени французского математика Эвариста Галуа. Далее рассматриваются и используются, как правило, конечные поля.

Порядком поля называется число элементов. Конечное поле порядка q обозначается $GF(q)$, или F_q.

Пример. Простейшим полем является поле из двух элементов – поле $GF(2)$. Операции этого поля определяются таблицами, из которых следует, что сложение соответствует булевой функции сложения по модулю 2, а умножение – конъюнкции.

+	A		·	A	
B	0	1	b	0	1
0	0	1	0	0	0
1	1	0	1	0	1

Пример. Если p – простое число, то целые числа {0, 1, 2, …, p – 1} образуют поле $G(p)$. При этом все операции (сложения, вычитания, умножения, деления) выполняются по модулю p.

Пример. Если p – простое число, а n – натуральное, то поле, которое содержит $N = p^n$ элементов, не может быть образовано из совокупности целых чисел по модулю N. Действительно, для $p = 2$ и $n = 2$ число элементов $N = p^n = = 2^2 = 4$. В множестве классов вычетов по модулю 4 элемент 2 не имеет обратного, так как $2 \cdot 2 = 0 \mod 4$. Т. е. множество, состоящее из четырех элементов, совсем не похоже на поле $G(N)$, которое состоит из $p^n = N$ элементов. Элементами поля, которое состоит из p^n элементов, являются все многочлены степени не более (n – 1) с коэффициентами из поля $G(p)$. Чтобы подчеркнуть эту разницу между представленными полями, поля из p^n элементов обозначают через $G(p^n)$ (вместо $G(N)$). Поля $G(p^n)$ будут рассматриваться ниже. Мультипликативная группа конечного поля порядка q обозначается $GF(q)^*$ и имеет порядок на единицу меньше порядка поля.

Два поля $F^{(1)}$ и $F^{(2)}$ называются **изоморфными**, если существует биекция φ: $F^{(1)} \leftarrow F^{(2)}$, сохраняющая операции. Эта биекция и обратная к ней функция φ^{-1} называются **изоморфизмами**.

Заметим, что фактор-множество Z_p кольца Z целых чисел по модулю простого числа p является полем порядка p и что все конечные поля простого порядка p являются простыми и изоморфны друг другу, т. е. такие

поля составляют класс всех простых конечных полей.

Определение. Пусть F – подполе поля H и α – некоторый элемент поля H ($\alpha \sqcup H$). Минимальное поле, которое содержит поле F и элемент α, называют **простым расширением поля** F, которое получено присоединением к полю F элемента α. Это расширение будем обозначать через $F(\alpha)$.

Понятие поля позволяет вводить и использовать большое разнообразие колец, элементы которых определяются как многочлены

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

с коэффициентами a_i из данного поля F. Такие многочлены называются **многочленами над полем** F. Наибольшее число d такое, что коэффициент $a_d \neq 0$ называется **степенью** многочлена $f(x)$. Если при этом $a_d = 1$, то многочлен степени d называется **нормированным**. Степень многочлена $f(x)$ обозначается $\deg f(x)$. Число ненулевых коэффициентов многочлена будем называть его **весом**. Степень нулевого многочлена естественно определить как -1. Многочлен степени не более $n-1$ над полем F представим упорядоченным набором $(a_0, a_{1\ldots,}, a_{n-1})$ коэффициентов. Иногда удобно использовать наборы длины, полученные добавлением старших нулевых элементов a_i, $i > \deg(x)$.

Кольцо многочленов над полем F образуется всеми многочленами над F. Оно обозначается $F[x]$. Операции сложения и умножения кольца $F[x]$ определяются теми же правилами, по которым складываются или перемножаются многочлены над действительным полем. Операция **сложения** сопоставляет двум многочленам $p_1(x)$ и $p_2(x)$ вида

$$p_1(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$$

и

$$p_2(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} + b_nx^n$$

их сумму

$$p_1(x) + p_2(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_{n-1} + b_{n-1})x^{n-1} + (a_n + b_n)x^n.$$

Здесь и ниже в слагаемых формул, подобных формуле в правой части, имеются в виду операции сложения и умножения в поле F. Результатом операции **умножения** двух многочленов $p_1(x)$ и $p_2(x)$ является многочлен

$$p(x) = p_1(x) \cdot p_2(x) = c_0 + c_1x + \ldots + c_{2\tau-3}x^{2\tau-3} + c_{2\tau-2}x^{2\tau-2}$$

где $c_i = a_t b_l$, г $t + l = i$.

Нулем кольца многочленов является многочлен 0, все коэффициенты которого нулевые, т. е. равны аддитивной единице поля. Единицей кольца многочленов является многочлен 1 нулевой степени, Кольцо многочленов не является полем, так как не всякий многочлен имеет обратный к нему элемент кольца. Кольцо многочленов над полем F будем обозначать через $F[x]$.

Говорят, что многочлен g делит многочлен f , если существует многочлен h такой, что $f = g \cdot h$, где $f, g, h \sqcup F[x]$.

Наибольшим общим делителем (НОД) двух многочленов f и g кольца $F[x]$ называется нормированный многочлен наибольшей степени, который делит каждый из этих многочленов.

Многочлен $f \sqcup F[x]$ называется **неприводимым**, если $f = g \cdot h$ только в том случае, когда либо g либо h является константой. Неприводимые многочлены среди многочленов играют ту же роль, что и простые числа среди целых чисел. Каждый многочлен из кольца может быть представлен в виде произведения неприводимых многочленов

единственным образом. Знание неприводимых многочленов над конечными полями нужно, по крайней мере, для того, чтобы строить эти поля. Если p – простое число, $G(p)$ – конечное поле с операциями по модулю p, n – натуральное число, $g(x)$ – неприводимый многочлен степени n, то конечное поле $G(p^n)$, которое состоит из $N = p^n$ элементов, состоит из многочленов степени n – 1. В этом случае результат **произведения элементов** $f_1(x)$ и $f_2(x)$ поля $G(p^n)$ – это **остаток от деления** многочлена $f(x) = f_1(x) \cdot f_2(x)$ на неприводимый многочлен $g(x)$. Т. е.

$$f_1(x) \cdot f_2(x) \equiv r(x) \bmod g(x),$$

где $r(x)$ – остаток от деления $f_1(x) \cdot f_2(x)$ на $g(x)$.

Определение 2. Пусть F – подполе поля H и $f(x)$ – многочлен над полем F. Обозначим через α корень многочлена $f(x)$ в поле H (заметим, что не в F). Тогда простое расширение $F(\alpha)$ (см. определение 1) называют **простым алгебраическим расширением**, которое получается путём присоединения к полю F корня α многочлена f. Если многочлен f – неприводимый над полем F многочлен степени n, то расширение $F(\alpha)$ называют **простым алгебраическим расширением поля *F* степени *n*.**

В последнем случае любой элемент u $F(\alpha)$ можно представить как линейную комбинацию степеней α^i, $i = 0, 1, \ldots, n - 1$, т. е. u представимо в виде

$$w = c_0 + c_0 a + \ldots + c_{n-1} a^{n-1},$$

где c_i, $i = 0, 1, \ldots, n - 1$ – элементы поля F.

Полем разложения многочлена f над полем F называют минимальное расширение H поля F, в котором многочлен f разлагается в произведение линейных над полем H многочленов. Справедливо следующее утверждение.

Теорема. Пусть f – многочлен над полем F. Тогда

- существует поле разложения многочлена f над полем

F;

- любые поля разложения многочлена f над полем F изоморфны.

Пример. Если Q – поле, состоящее из всех рациональных чисел, тогда $Q(\sqrt{2})$ есть поле разложения многочлена $f(x) = x^2 - 2$. Чтобы получить поле разложения многочлена $f(x) = x^3 - 2 = (x -)(x^2 + x\sqrt{2} + 1)$, надо к полю Q присоединить корни уравнения $x^3 - 2 = (x -)(x^2 + x\sqrt{2} + 1) = 0$.

Справедливо следующее утверждение для полей $G(p^n)$ (p – простое число, p^n – число элементов в поле).

Теорема. Если $G(p^n)$ есть поле с $N = pn$ элементами, то каждый элемент его удовлетворяет уравнению $x^N - x = 0$ и $G(p^n)$ – это в точности множество корней этого уравнения. Обратно, для любой степени простого числа p ($N= p^n$) поле разложения над $F(p)$ многочлена $x^N - x = 0$ есть поле из N элементов.

Среди неприводимых многочленов особую роль играют **примитивные многочлены**, корни которых являются примитивными (порождающими) элементами поля разложения этого многочлена. Примитивные многочлены широко используются в криптографии для построения линейных рекуррентных последовательностей (ЛРП) максимально возможной длины. ЛРП применяются, например, при построении датчиков случайных чисел.

Во многих книгах даны таблицы неприводимых многочленов невысоких степеней. Более того, ввиду важности для приложений неприводимые и примитивные многочлены уже давно табулированы и сведены в таблицы, имеющиеся в некоторых учебниках.

Напомним, что элемент $\alpha \sqcup F$ называется корнем многочлена $f \sqcup F(x)$, если $f(\alpha) = 0$. Имеется связь между делимостью многочленов и корнями. Эта связь формулируется теоремой Безу.

Теорема (теорема Безу). Элемент α поля F тогда и только тогда будет корнем многочлена $f \sqcup F(x)$, когда $x - \alpha$ делит $f(x)$.