ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
Московский технический университет связи и информатики

Кафедра Теории вероятностей и прикладной математики

Демин Д.Б.

Учебно-методическое пособие
по курсу

Дополнительные главы алгебры

Часть 2

для студентов 2 курса дневного обучения
направления 01.03.04 «Прикладная математика»

Москва 2018

План УМД на 2017/2018 уч. год

Учебно-методическое пособие
по курсу

Дополнительные главы алгебры

Часть 2

для направления 01.03.04 «Прикладная математика»

Составитель: Д.Б. Демин, к.ф.-м.н., доцент

Предлагаемое учебное пособие по курсу «Дополнительные главы алгебры» включает в себя специальные разделы алгебры, касающиеся теории групп, колец и полей. Этот курс изучается студентами направления 01.03.04 «Прикладная математика» на 2-м курсе в четвертом семестре и является логическим продолжением курса «Линейная алгебра и аналитическая геометрия», изучаемого на 1-м курсе в первом и втором семестрах. В пособии приведены: тематика лекционных и практических занятий, список рекомендуемой литературы, краткое изложение основ курса, список вопросов и задания для самостоятельного решения.

Издание утверждено на заседании кафедры ТВиПМ. Протокол № 8 от «17» апреля 2018 г.

Рецензент: А.Г. Кюркчан, д.ф.-м.н., профессор

ВВЕДЕНИЕ

Предлагаемое учебно-методическое пособие по курсу «Дополнительные главы алгебры», часть 2 является продолжением учебно-методического пособия «Дополнительные главы алгебры», часть 1, вышедшего в 2017 г. Оно включает в себя специальные разделы алгебры такие как прямое произведение групп, кольца и поля, факторкольца и расширения полей. Это пособие необходимо для изучения дисциплины «Дополнительные главы алгебры» студентами направления 01.03.04 «Прикладная математика» на 2-м курсе в четвертом семестре. Эта дисциплина является логическим продолжением дисциплины «Линейная алгебра и аналитическая геометрия», изучаемой на 1-м курсе в первом и втором семестрах. Целью пособия является познакомить студентов с основными понятиями и методами высшей алгебры и привить им соответствующий математический язык. В пособии приведены: тематика лекционных и практических занятий, список рекомендуемой литературы, краткое изложение основ курса, список вопросов и задания для самостоятельного решения.

Содержание курса

1. Введение в абстрактную алгебру. Алгебраические операции, их свойства. Таблица Кэли. Алгебраические структуры. Отношения. Отношение эквивалентности. Виды отображений. Группоид, полугруппа, моноид.
2. Группы. Примеры групп. Подгруппы. Порядок элемента группы. Циклические группы. Симметрическая группа подстановок. Теорема Кэли. Характеристика группы.
3. Изоморфизмы групп. Гомоморфизмы групп. Теоремы о изоморфизме и гомоморфизме. Примеры. Ядро гомоморфизма.
4. Смежные классы. Примеры. Индекс подгруппы в группе. Теорема Лагранжа. Отношение сопряженности.
5. Нормальные делители. Факторгруппа. Прямое произведение (прямая сумма групп).
6. Кольца и алгебры. Примеры колец. Кольцо целых чисел. Кольцо многочленов. Кольца классов вычетов. Подкольцо. Обратимые элементы кольца, делители нуля.
7. Идеалы. Главные идеалы. Максимальные и простые идеалы. Идеалы в кольцах многочленов. Факторкольцо.
8. Деление с остатком в кольцах целых чисел и многочленов над кольцом целых чисел. Евклидовы кольца. Идеалы в евклидовых кольцах.

9. Поля. Примеры полей. Поле рациональных дробей. Конечные поля. Поле классов вычетов. Характеристика поля. Подполе. Конечные и алгебраические расширения полей.

Список литературы

Основная литература:

1. Курош А.Г. Курс высшей алгебры. СПб.: Лань, 2008.
2. Кострикин А.И. Введение в алгебру. Т.1, Т.3. М.: МЦНМО, 2012.
3. Сборник задач по алгебре. Под ред. А.И.Кострикина. М.: МЦНМО, 2012.
4. Сборник задач по математике для втузов. Ч. 1. Под ред. А.В. Ефимова и А.С. Поспелова. М.: Физматлит, 2014.

Дополнительная литература:

5. Ван дер Варден Б.Л. Алгебра. СПб.: Лань, 2004.
6. Куликов Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993.
7. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. СПб.: Лань, 2015.
8. Винберг Э.Б. Курс алгебры. М.: Изд-во «Факториал Пресс», 2001.
9. Демин Д.Б. Учебно-методическое пособие по курсу «Дополнительные главы алгебры», часть 1. Для студентов 2 курса направления 010304 «Прикладная математика». М.: МТУСИ, 2017.

ПРЯМОЕ ПРОИЗВЕДЕНИЕ ГРУПП

Группа G раскладывается в *прямое произведение* своих подгрупп G_1, G_2, … , G_k, если:

1) каждый элемент $g \in G$ единственным образом представляется в виде $g = g_1 g_2 \dots g_k$, где $g_i \in G_i$;
2) $g_i g_j = g_j g_i$ для $\forall$ $g_i \in G_i$, $g_j \in G_j$, $i \neq j$ (т.е. элементы g_i и g_j коммутируют).

Для прямого произведения групп используется обозначение:
$G = G_1 \times G_2 \times \dots \times G_k$.

В случае аддитивной группы G вместо прямого произведения говорят о *прямой сумме* и обозначают ее так: $G = G_1 \oplus G_2 \oplus \dots \oplus G_k$. Если группа G конечна, то очевидно, что $|G| = |G_1| \cdot |G_2| \cdot \dots |G_k|$.

Из условия 1) следует, что $G_i \bigcap G_j = \{e\}$ при $i \neq j$, а из условия 2) получаем правило умножения элементов группы $G = G_1 \times G_2 \times \ldots \times G_k$:

$$(g_1 g_2 \ldots g_k)(g'_1 g'_2 \ldots g'_k) = (g_1 g'_1)(g_2 g'_2)\ldots(g_k g'_k), \;\; g_i, g'_i \in G_i .$$

Из определения прямого произведения видно, что каждая из подгрупп G_i нормальна в G, поэтому условие 2) можно заменить требованием, чтобы группы G_i, $i = 1,\ldots,k$ были нормальны в G.

Теорема. Группа G раскладывается в прямое произведение своих подгрупп G_1 и G_2, если:

1) подгруппы G_1 и G_2 нормальны в G;
2) $G_1 \bigcap G_2 = \{e\}$;
3) $G = G_1 G_2$, т.е. каждый элемент $g \in G$ представляется в виде $g = g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$.

Примеры прямых произведений.

1) Пусть $G = \{e, a, b, c\}$ – нециклическая группа 4-го порядка, тогда в ней $a^2 = b^2 = c^2 = e$, а произведение любых двух элементов из a, b, c равно третьему. Таким образом, группа G содержит три циклические подгруппы 2-го порядка и раскладывается в прямое произведение любых двух из этих подгрупп, например: $G = \{e, a\} \times \{e, b\}$.
2) Возможность и единственность представления комплексного числа z, отличного от нуля, в тригонометрической форме означает, что:
   $\boldsymbol{C}^* = \boldsymbol{R}_+^* \times T$, где $T = \{z \in \boldsymbol{C}^* : |z| = 1\}$.
   Именно: $z = |z| \cdot (\cos\varphi + i \sin\varphi) = |z| e^{i\varphi}$, $\varphi = \arg z$.

Если G раскладывается в прямое произведение своих подгрупп G_1, G_2, т.е. $G = G_1 \times G_2$, то такое произведение принято называть внутренним прямым произведением. Дадим определение внешнего прямого произведения групп.

Прямым произведением групп $G_1, G_2, \ldots, G_k$ называется совокупность последовательностей $(g_1, g_2, \ldots, g_k)$, где $g_i \in G_i$ ($i = 1,\ldots,k$) с покомпонентной операцией умножения элементов:

$$(g_1, g_2, \ldots, g_k) \cdot (g'_1, g'_2, \ldots, g'_k) = (g_1 g'_1, g_2 g'_2, \ldots, g_k g'_k).$$

Очевидно, таким образом, получается группа $G = G_1 \times G_2 \times \ldots \times G_k$.

В частном случае, при $k = 2$, прямым произведением групп G_1 и G_2 называется множество $G_1 \times G_2$ всех упорядоченных пар (g_1, g_2), где

$g_1 \in G_1$, $g_2 \in G_2$, с бинарной операцией $(g_1, g_2) * (g_1', g_2') = (g_1 \cdot g_1',\ g_2 \circ g_2')$, где $*, \cdot, \circ$ – бинарные операции на $G_1 \times G_2$, G_1 и G_2.

При аддитивной записи групп, естественно говорить о прямой сумме групп $G_1 \oplus G_2$.

В $G_1 \times G_2$ содержатся подгруппы $G_1 \times e_2$, $e_1 \times G_2$, изоморфные соответственно G_1 и G_2 (e_1 и e_2 – нейтральные элементы в группах G_1 и G_2). Отображение $\varphi: G_1 \times G_2 \to G_2 \times G_1$, заданное равенством $\varphi(g_1, g_2) = (g_2, g_1)$, устанавливает изоморфизм групп $G_1 \times G_2$ и $G_2 \times G_1$.

Отождествляя каждый элемент $g \in G_i$ с последовательностью $(e, \ldots, g, \ldots, e) \in G_1 \times \ldots \times G_i \times \ldots \times G_k$, получим вложение группы G_i в группу $G_1 \times \ldots \times G_i \times \ldots \times G_k$ в виде подгруппы. Т.е. группа $G_1 \times \ldots \times G_i \times \ldots \times G_k$ есть прямое произведение таких подгрупп (см. первое определение). Внешнее прямое произведение групп отождествляется с декартовым произведением.

Если некоторая группа G раскладывается в прямое произведение своих подгрупп G_1, …, G_k, то отображение $\varphi: G_1 \times \ldots \times G_k \to G$ (когда $(g_1, \ldots, g_k) \ \to g_1 \ldots g_k$) является изоморфизмом групп. Доказательство этого утверждения из определения о разложении группы G в прямое (внутренне) произведение своих нормальных подгрупп G_1, …, G_k.

Так, отображение $\varphi: G_1 \times G_2 \to G$, где $G_1, G_2 \lhd G$, $G_1 \bigcap G_2 = \{e\}$, определяется следующим образом: $\varphi((g_1, g_2)) = g$, $\forall g = g_1 g_2$. Тогда

$\varphi((g_1, g_2)(g_1', g_2')) = \varphi((g_1 g_1', g_2 g_2')) = g_1 g_1' g_2 g_2' =$ (в силу нормальности G_1 и G_2) $=$ $g_1 g_2 g_1' g_2' = \varphi((g_1 g_2, g_1' g_2')) = \varphi((g_1, g_2))\varphi((g_1', g_2')) = gg'$.

Далее, если $\varphi((g_1, g_2)(g_1', g_2')) = e_1 e_2$, то $g_1 g_1' = e_1,\ g_2 g_2' = e_2$, т.е. $\operatorname{Ker}\varphi = e$. Отсюда эпиморфность φ очевидна. Значит φ удовлетворяет всем условиям изоморфизма.

Теорема. Пусть $G = G_1 \times G_2$ и $G_1' \lhd G_1, G_2' \lhd G_2$. Тогда $G_1' \times G_2' \lhd G$ и $G/(G_1' \times G_2') \cong (G_1/G_1') \times (G_2/G_2')$. В частности $G/G_1 \cong G_2$.

Пример 1. Рассмотрим группу автоморфизмов группы G, которую обозначают как $AutG$. Для $\forall g \in G$ отображение $\varphi(g)$: $x \to gxg^{-1}$, $x \in G$ является автоморфизмом:

$$\varphi(g)(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = (\varphi(g)x)(\varphi(g)y).$$

Такой автоморфизм называется внутренним автоморфизмом, определяемым элементом g.

Отображение $f: g \to \varphi(g)$ является гомоморфизмом группы G в группу $AutG$: $\varphi(gh)x = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = \varphi(g)\varphi(h)x$. Его ядро $\operatorname{Ker} f$ есть центр $Z(G)$: $Z(G) = \{z \in G : zg = gz, \forall g \in G\}$. Его образ $\operatorname{Im} f$ есть подгруппа группы $AutG$, называемая группой внутренних автоморфизмов группы G и обозначаемая через $IntG$. По теореме о гомоморфизме $IntG \cong G/Z(G)$.

Пример 2. Покажем, что при $n \geq 3$ центр группы подстановок S_n тривиален, т.е. $Z(S_n) = \{e\}$ и следовательно $Int\,S_n \cong S_n$. Найдем сначала группу $Aut\,S_3$. Так как при любом изоморфизме групп порядки элементов сохраняются, то всякий автоморфизм φ группы S_n переводит транспозиции в транспозиции. Но любая группа S_n порождается транспозициями, поэтому автоморфизм φ определяется тем, как он переставляет транспозиции. Следовательно $|Aut\,S_3| \leq |S_3| = 3! = 6$. Но группа $Int\,S_3 \cong S_3$, поэтому $|Int\,S_3| = |S_3| = 6$ и $Int\,S_3 \subseteq Aut\,S_3$. Тогда $Aut\,S_3 = Int\,S_3$.

Прямая сумма абелевых групп

Определение 1. Аддитивная абелева группа A разлагается в прямую сумму своих подгрупп A_1, $\ldots, A_k$, если каждый элемент $a \in A$ единственным образом представляется в виде $a = a_1 + \ldots + a_k$. $a_i \in A_i$ $(i = \overline{1,k})$. Такую прямую сумму обозначают так: $A = A_1 \oplus \ldots \oplus A_k$.

В случае двух подгрупп A_1, A_2 единственность представления $a \in A$ в виде $a = a_1 + a_2$ $(a_1 \in A_1, a_2 \in A_2)$ равносильна тому, что $A_1 \cap A_2 = 0$.

Определение 2. Прямой суммой (аддитивных) абелевых групп A_1, $\ldots, A_k$ называется абелева группа $A_1 \oplus \ldots \oplus A_k$, составленная из всех последовательностей вида $(a_1, \ldots, a_k)$, $a_i \in A_i$ с покомпонентной операцией сложения.

Прямая сумма в смысле определения 1 называется внутренней, а прямая сумма в смысле определения 2 – внешней.

Например, $\underbrace{Z \oplus \ldots \oplus Z}_{n} = Z^n$.

Отметим, что если группы A_1, $\ldots, A_k$ конечны, то $|A_1 \oplus \ldots \oplus A_k| = |A_1| \cdot \ldots |A_k|$.

Пример. Бесконечная циклическая абелева группа Z не может быть разложена в прямую сумму своих двух ненулевых подгрупп, так как ее собственными подгруппами являются группы nZ, $n \in N$, а их прямая сумма также будет подгруппой вида nZ (также: $mn \in mZ \bigcap nZ$, где $mn \neq 0$).

Теорема. Если число $n = k \cdot l$, где числа k и l взаимно простые, т.е. $(k,l) = 1$, то $Z_n \cong Z_k \oplus Z_l$.

Для доказательства теоремы достаточно указать в группе $Z_k \oplus Z_l$ элемент порядка kl. Таким элементом, например, будет являться $(\overline{1}_k, \overline{1}_l)$. Действительно, пусть $Z_n = < a >$. Из теории чисел известно, что если $(k,l) = 1$, то найдутся такие числа u и v из Z_n, что $ku + lv = 1$. Тогда $a = uka + vla = ub + vc$. Число ka имеет порядок l, так как $lka = na = 0$. Аналогично, la имеет порядок k. Таким образом, любой элемент из $< a >$ можно представить как сумму элементов из циклических подгрупп $< b >$ и $< c >$ порядков l и k.

Следствие. Если $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ (где p_i – простые числа, k_i - положительные целые числа), то $Z_n \cong Z_{p_1^{k_1}} \oplus \ldots \oplus Z_{p_s^{k_s}}$.

Группа G называется неразложимой группой, если ее нельзя разложить в прямую сумму двух или нескольких групп.

Конечная группа, порядок которой есть степень простого числа p, называется *примарной* или p-группой.

Таким образом, всякая конечная циклическая группа раскладывается в прямую сумму примарных циклических групп.

Теорема. Всякая примарная циклическая группа неразложима.

Итак, всякая прямая сумма $A_1 \oplus \ldots \oplus A_k$ циклических групп $A_1, \ldots, A_k$ взаимно простых порядков $n_1, \ldots, n_k$ является циклической группой порядка $n = n_1 \cdot \ldots \cdot n_k$. В общем случае, если $НОК(n_1, \ldots, n_k) \neq n_1 \cdot \ldots \cdot n_k$, то абелева группа $A = A_1 \oplus \ldots \oplus A_k$ не является циклической (так как в A нет элемента порядка $n = n_1 \cdot \ldots \cdot n_k$).

Теорема. Всякая конечно порожденная абелева группа A разлагается в прямую сумму примарных и бесконечных циклических подгрупп, причем набор порядков этих подгрупп определен однозначно.

Если любой элемент $a \in A$ представить в виде линейной комбинации $a = a_1 u_1 + \ldots + a_k u_k$. $a_i \in Z$, $u_i \in A$, то говорят, что группа A порождается совокупностью элементов $\{u_1, \ldots, u_k\}$. Эта система называется порождающей системой. Тогда: $A \cong Z_{u_1} \oplus \ldots \oplus Z_{u_m} \oplus \underbrace{Z \oplus \ldots \oplus Z}_{k-m}$, где $u_1,\ldots,u_m$ – натуральные числа ($m \le k$) и $u_i \,|\, u_{i+1}$, $i = 1,\ldots,m-1$.

Замечание. если группа A конечна, то в ее разложении не может быть бесконечных слагаемых, т.е. она раскладывается в прямую сумму своих примарных циклических подгрупп (см. теорему выше).

Примеры. **1.** Так аддитивные группы Z и Q неразложимы, так как для любых двух ненулевых элементов в них существует ненулевое общее кратное, т.е. любые две ненулевые циклические подгруппы в этих группах обладают ненулевым пересечением.

2. Мультипликативная группа R^* раскладывается в прямое произведение мультипликативной группы R_+^* и мультипликативной группы $C_2 = \{1,-1\}$. Действительно, в пересечении групп R_+^* и C_2 содержится только 1, так как это есть единичный элемент и в R_+^*. С другой стороны, всякое положительное действительное число есть произведения его самого на 1, а всякое отрицательное – есть произведение его модуля на –1.

3. Найти прообразы элементов $\overline{1}_3 \in Z_3$ и $\overline{1}_5 \in Z_5$ при изоморфизме $Z_{15} \cong Z_3 \oplus Z_5$, переводящем $\overline{1}_{15}$ в $(\overline{1}_3, \overline{1}_5)$. $Z_3 = \{0,1,2\}$, $Z_5 = \{0,1,2,3,4\}$. Найдем $a,b \in Z_{15}$ такие, что $a \equiv 1(\mathrm{mod}3)$, $b \equiv 1(\mathrm{mod}5)$ и $a+b \equiv 1(\mathrm{mod}15)$. Такими числами будут $a = 10$ и $b = 6$. Рассмотрим подгруппы $5Z_3 = \{0,5,10\} = \langle 5 \rangle_3$, $3Z_5 = \{0,3,6,9,12\} = \langle 3 \rangle_5$. Так как $\overline{1}_{15} = \overline{10}_{15} + \overline{6}_{15} = 16 = 1$, где $\overline{10}_{15} \in 5Z_3$, $\overline{6}_{15} \in 3Z_5$, т.е. $1 = 5u + 3v$, где $u = -1$, $v = 2$. Тогда $5u = -5 \equiv 10(\mathrm{mod}15)$ есть прообраз $\overline{1}_3 \in Z_3$, а $3v = 6$ – прообраз $\overline{1}_5 \in Z_5$. Из этого решения следует, что $Z_{15} = 5Z_{15} + 3Z_{15}$.

4. Пусть $G = Z_{15} \oplus Z_{18}$. Так как $Z_{15} = 5Z_{15} + 3Z_{15}$, а $Z_{18} = 9Z_{12} + 2Z_{18}$, и $Z_{15} \cong Z_3 \oplus Z_5$, а $Z_{18} \cong Z_2 \oplus Z_9$, тогда $G \cong Z_2 \oplus Z_3 \oplus Z_5 \oplus Z_9$.

Перечисление конечных абелевых групп

Совокупность всех абелевых групп разбивается отношением изоморфизма на непересекающиеся классы изоморфных групп. Для каждого $n \in N$ существует конечное число $T(n)$ различных классов абелевых групп порядка n.

Теорема. Если $n = q_1^{m_1} \cdot \ldots \cdot q_r^{m_r}$ (где q_i – простые числа), то число $T(n)$

различных классов абелевых групп порядка n равно числу различных наборов $(q_1^{k_{11}},\dots,q_1^{k_{1t_1}},\dots,q_r^{k_{r1}},\dots,q_r^{k_{rt_r}})$ таких, что $m_i = k_{i1}+\dots+k_{it_i}$, $k_{i1}\ge\dots\ge k_{it_i}>0$, $i=\overline{1,r}$. Представление натурального числа m в виде суммы набора невозрастающих натуральных чисел назовем разбиением числа m и обозначим через $R(m)$ число таких разбиений числа m. Тогда

$$T(n)=T(q_1^{m_1})\cdot\ldots\cdot T(q_r^{m_r})=R(m_1)\cdot\ldots\cdot R(m_r).$$

Пример. Пусть $n=36=3^2\cdot 2^2$. Тогда $T(n)=T(3^2)\cdot T(2^2)=R(2)\cdot R(2)$. Так как $2=2$ и $2=1+1$, то $R(2)=2$. Отсюда $T(36)=2\cdot 2=4$. т.е. число классов изоморфных абелевых групп порядка 36 равно 4. Вот эти группы:

$$G_1 = Z_9\oplus Z_4\cong Z_{36},\ G_2=Z_3\oplus Z_3\oplus Z_4,\ G_3=Z_9\oplus Z_2\oplus Z_2,$$
$$G_4=Z_3\oplus Z_3\oplus Z_2\oplus Z_2.$$

Среди абелевых групп порядка p^n, $n\in N$ (p – простое число) всегда содержится циклическая группа порядка p^n и группа экспоненты, т.е. группа типа $(\underbrace{p,\dots,p}_{n})$, называемая элементарной p-группой.

Задания для самостоятельного решения

1. Разлагаются ли в прямое произведение нееденичных подгрупп группы:
   а) S_3; б) A_4; в) S_4.
2. Разложить в прямую сумму группы:
   а) Z_8; б) Z_{24}; в) Z_{60}.
3. Покажите, что порядок элемента $a=(a_1,\dots,a_n)$ группы $A_1\times\ldots\times A_n$ равен НОК чисел $ord(a_i)$ ($i=\overline{1,n}$), т.е. $ord(a)=НОК(ord(a_1),\dots,ord(a_n))$.
4. Найти порядки каждого из элементов группы $Z_2\oplus Z_2$.
5. Найти количество элементов порядка 10 в группе $Z_4\oplus Z_4\oplus Z_{25}$.
6. Найти число классов изоморфных абелевых групп порядка 54.
7. Изоморфны ли группы $Z_6\oplus Z_{36}$ и $Z_{12}\oplus Z_{18}$?
8. Доказать, что
   а) группа S_n порождается транспозицией (1 2) и циклом (1 2 3 … n);
   б) группа A_n порождается тройными циклами.

КОЛЬЦА

Кольцо в отличие от группы – это алгебраическая структура с двумя бинарными операциями, называемыми обычно сложением и умножением.

Аксиомы кольца подсказаны свойствами операций над вещественными числами.

Кольцом называется непустое множество K, на котором заданы две (бинарные алгебраические) операции "+" (сложение) "·" (умножение), удовлетворяющие следующим свойствам (аксиомы кольца):

1) относительно сложения K – это абелева группа, называемая аддитивной группой кольца K: $(K, +)$;
2) $(K, \cdot)$ – полугруппа;
3) операции сложения и умножения связаны дистрибутивными законами $a(b+c) = ab + ac$, $(a+b)c = ac + bc$, для $\forall a,b,c \in K$.

Замечание: в некоторых случаях рассматривают кольца, в которых операция ассоциативности относительно умножения не выполняется, т.е. $(K, \cdot)$ не полугруппа, а только группоид. Такие кольца называют не ассоциативными. Мы будем в дальнейшем рассматривать только ассоциативные кольца.

Итак, алгебраическая структура $(K, +, \cdot)$ – кольцо. Если $(K, \cdot)$ – моноид, то $(K, +, \cdot)$ называется *кольцом с единицей*.

Следствия из аксиом кольца:

1. $a \cdot 0 = 0 \cdot a = 0$, $\forall a \in K$ (0 – это нейтральный (нулевой) элемент в абелевой группе $(K, +)$;
2. $a \cdot (-b) = (-a)b = -ab$, $\forall a,b \in K$;
3. $a \cdot (b-c) = ab - ac$, $(a-b)c = ac - bc$, $\forall a,b,c \in K$.

Кольцо K называется *коммутативным*, если операция умножения в нем коммутативна, т.е. $a \cdot b = b \cdot a$, $\forall a,b \in K$.

Единицей кольца K называется элемент, обозначаемый 1 или e, для которого $a \cdot 1 = 1 \cdot a = a$, $\forall a \in K$. Как и в группах, в кольце не может быть двух различных единиц, но может не быть ни одной.

Замечание. Если $1 = 0$, то $\forall a \in K$: $a = a \cdot 1 = a \cdot 0 = 0$, т.е. кольцо K состоит из одного нуля. Поэтому, если кольцо содержит больше одного элемента, то $1 \neq 0$.

Примеры колец.

1. Числовые множества $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ – это коммутативные кольца с единицей относительно обычных операций сложения и умножения. Множество $m\boldsymbol{Z}$ целых чисел, кратных m, будет в $\boldsymbol{Z}$ подкольцом (без единицы при (m>1). Очевидны включения: $\boldsymbol{Z} \subset \boldsymbol{Q} \subset \boldsymbol{R}$.
2. Множество квадратных матриц $M_n(\boldsymbol{R})$ порядка n с операциями сложения и умножения матриц – это кольцо с единицей, где $1 = E$.

Оно называется полным матричным кольцом над $\boldsymbol{R}$. Это кольцо некоммутативно. Можно рассматривать и кольцо квадратных матриц $M_n(K)$ порядка n над произвольным коммутативным кольцом K.

3. Множество функций $f(x)$ $(x \in X, f(x) \in K)$, определенных на заданном подмножестве числовой прямой, является коммутативным кольцом с единицей относительно обычных операций сложения и умножения функций
4. Множество $\boldsymbol{R}^2$ упорядоченных пар действительных чисел (a,b), $a,b \in \boldsymbol{R}$ является коммутативным кольцом с единицей: $(a,b)+(c,d)=$ $=(a+c,b+d)$, $(a,b)(c,d)=(ac,bd)$, нулевой элемент $(0,0)$, единичный элемент $(1,1)$, а противоположным элементом для (a,b) будет $(-a,-b)$.
5. Множество многочленов $f(x)$ произвольной степени с элементами из некоторого кольца K образует кольцо многочленов, которое принято обозначать как $K[x]$: $f(x)=\sum_{i=0}^{n} a_i x^i$, $a_i \in K$, $n = \deg f \geq 0$.
6. Множество векторов в трехмерном геометрическом пространстве с обычной операцией сложения векторов и векторным умножением $a \times b$ является некоммутативным не ассоциативным кольцом. Однако в нем выполняются следующие тождества: $a \times a = \theta$, $a \times b +$ $+ b \times a = \theta$, $(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = \theta$ (тождество Якоби), где θ – нулевой вектор.
7. Пусть M – произвольное множество, а 2^M – множество всех его подмножеств. Можно показать, что 2^M – ассоциативное коммутативное кольцо относительно операций симметрической разности $M \Delta N = (M \setminus N) \bigcup (N \setminus M)$ и пересечения $M \bigcap N$, взятых в качестве сложения и умножения соответственно.
8. Группа $Z_m = \{0,1,2,\ldots,m-1\}$, $m \in N, m > 1$ образует коммутативное кольцо с единицей, которое принято называть кольцом (классов) вычетов. Операции сложения и умножения выполняются по модулю m: $\bar{k}_m \oplus \bar{l}_m = \overline{k+l}_m$, т.е. $k + l \equiv \overline{k+l} (\mathrm{mod}\, m)$, аналогично $\bar{k}_m \otimes \bar{l}_m = \overline{k \cdot l}_m$ $(k,l \in Z_m)$. Здесь элементы $\bar{k}$ являются классами вычетов и их можно представить так: $\bar{k}_m = \bar{k} = \{k\}_m = \{k + mZ\}$, причем $\bar{k}$ пробегает целые значения от 0 до $m-1$.

Элемент a кольца K называется обратимым, если для него существует такой элемент $b \in K$, что $a \cdot b = b \cdot a = e$ (e – единица (1) кольца K). Элемент b, обратный к a принято обозначать как a^{-1}: $aa^{-1} = a^{-1}a = 1$.

Множество K^* всех обратимых элементов кольца K образует группу по умножению. Например, в кольце целых чисел Z группой по умножению будет множество $Z^* = \{1, -1\}$, которое изоморфно группе корней из единицы C_2. Другой пример: в кольце многочленов $K[x]$ группа $(K[x])^* = K^*$, так как $f(x)g(x) = 1 \Leftrightarrow \deg f + \deg g = 0$, т.е. $\deg f = \deg g =$ $= 0$, а это означает, что обратимыми будут только элементы из K.

Подкольца

Подмножество L кольца K называется *подкольцом*, если L является кольцом относительно операций сложения и умножения, заданных в K.

Теорема (*признак подкольца*). Подмножество L кольца K является подкольцом тогда и только тогда, когда: 1. $\forall a, b \in L$: $a + b \in L, ab \in L$; 2. $\forall a \in L$: $-a \in L$.

Нулем подкольца L является нуль кольца K. Отметим, что не всегда единица подкольца совпадает с единицей кольца. Например, в кольце матриц второго порядка с рациональными элементами рассмотрим подкольцо $B = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix}, a \in Q \right\}$. Нетрудно заметить, что единицей в этом подкольце является матрица $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$, тогда как единицей всего кольца является единичная матрица E.

Подкольцо коммутативного кольца является коммутативным кольцом. Само кольцо и нулевое подкольцо называются *тривиальными* (*несобственными*) подкольцами, остальные подкольца – *нетривиальными* (*собственными*) подкольцами. Если порядок кольца не превышает 2, то у него нет собственных подколец. Если кольцо L является подкольцом кольца K, то очевидно, что множество $(L, +)$ является подгруппой группы $(K, +)$. Отсюда следует, что порядок любого подкольца конечного кольца есть делитель порядка кольца. Если $(K, +)$ является циклической группой простого порядка, то такое кольцо не имеет собственных подколец.

Например, в кольце целых чисел Z подмножества mZ ($m = 0, 1, 2, 3, \ldots$) образуют полный список подколец кольца Z.

Элементы кольца называются *перестановочными*, если $ab = ba$. Очевидно, что кольцо K коммутативно, когда любые его два элемента перестановочны. Обозначим через $Z(K)$ подмножество элементов кольца K, перестановочных с любым его элементом, т.е. $Z(K) = \{a \in K : xa = ax$, $\forall x \in K\}$. Ясно, что $\{0\} \subseteq Z(K) \subseteq K$. Множество $Z(K)$ называется *центром* кольца K и является его подкольцом. Кольцо, у которого $Z(K) = \{0\}$ называется кольцом без центра.

Целостные, факториальные и евклидовы кольца

Если $a \neq 0$, $b \neq 0$, а $ab = 0$, то элементы a и b кольца K называют *делителями нуля*.

Коммутативное кольцо с единицей $1 \neq 0$ и без делителей нуля называется *целостным кольцом* или *областью целостности*.

Например, множество целых чисел Z является областью целостности, также и множество $Z[i] = \{x + iy, x, y \in Z\}$ всех целых гауссовых чисел является целостным, а вот множество матриц порядка n с вещественными элементами является некоммутативным кольцом с единицей и с делителями нуля при $n \geq 2$. Также кольцо Z_4 является кольцом с делителями нуля, так как в нем $\overline{2} \cdot \overline{2} = \overline{0}$.

В целостных кольцах для $\forall a, b \in K : ab = 0$, если $a = 0$ или $b = 0$. Это аналогично свойству сокращения: $ac = bc$ и $c \neq 0$, тогда $a = b$.

Отметим, что обратимые элементы кольца не могут быть делителями нуля. Именно, пусть $a \neq 0$: если $ab = 0$, тогда $a^{-1}(ab) = 0$, а отсюда $(a^{-1}a)b = b = 0$. Аналогично, если $ba = 0$, то $b = 0$.

Элементы a, b области целостности K называются *ассоциированными*, если существует $\varepsilon \in K^*$ такой, что $a = \varepsilon \cdot b$ (пишут $a \sim b$). Например, в кольце Z множество $Z^* = \{1, -1\}$, поэтому числа a и $-a$ ассоциированны.

Пусть K – целостное кольцо. Если для $\forall a, b \in K, b \neq 0$ существует элемент $q \in K$ такой, что $a = qb$, то говорят, что a делится на b и пишут $a \vdots b$ (b делит a обозначают как $b \mid a$). Если $a \vdots b$, то существует единственный элемент $q \in K$ такой, что $a = qb$, который принято называть частным.

Отношение делимости обладает многими свойствами, важными из которых являются следующие: **1.** если $a \neq 0$, то $a \vdots a$; **2.** если $a \vdots b$ и $b \vdots c$, то $a \vdots c$; **3.** если $a \vdots b$, то $a \vdots \varepsilon b$, $\varepsilon \in K^*$; **4.** любой элемент из K делится на любой элемент из K^*; **5.** если $a \vdots b$ и $b \vdots a$, то $a = \varepsilon \cdot b$, где $\varepsilon \in K^*$.

Ненулевой необратимый элемент a кольца называется *простым*, если он имеет лишь тривиальные делители, в противном случае элемент a называется составным. *Тривиальными* делителями a являются элементы ε и $\varepsilon \cdot a$. где $\varepsilon \in K^*$. В кольце многочленов $K[x]$ простой элемент называется неприводимым многочленом.

Таким образом, область целостности разбивается на 4 класса: нулевой элемент, обратимые элементы, простые элементы, составные элементы. Простые и составные элементы кольца принято называть *регулярными*.

Если p – простой элемент из области целостности K, то элемент $\varepsilon \cdot p$ также является простым, где $\varepsilon \in K^*$.

Представление элемента $a \in K$ в виде произведения простых элементов: $a = p_1 p_2 ... p_n$ $(n \geq 1)$, называется *факторизацией* элемента a.

Целостное кольцо K называется *кольцом с факторизацией*, если любой ее регулярный элемент допускает факторизацию.

Критерий кольца с факторизацией. Целостное кольцо K является кольцом с факторизацией, если на множестве его регулярных элементов a можно определить функцию $\theta(a)$ со значениями из N, обладающую свойством: $\theta(ab) > \theta(a)$.

Например, в кольце целых чисел Z функцию θ определяют следующим образом: $\theta(a) = |a|$, Тогда для $\forall a,b \in Z$, не равных 0 и ± 1, $\theta(ab) = |ab| = |a| \cdot |b| > |a| = \theta(a)$.

В кольце многочленов $K[x]$ положим $\theta(f(x)) = \deg f$, тогда, если $\deg f \geq 1$ и $\deg g \geq 1$, то $\theta(f(x)g(x)) = \deg f + \deg g > \deg f = \theta(f(x))$.

Если в кольце с факторизацией любой регулярный элемент обладает однозначной факторизацией, то оно называется *факториальным кольцом*.

Например, кольца Z, Q, R, $Z[x]$, $Q[x]$, $R[x]$ являются факториальными кольцами. Гауссово кольцо $Z[i]$ также факториально, хотя в нем число 5 имеет два разложения, именно: $5 = (1-2i)(1+2i) = (-2-i)(-2+i)$. Но, так как $Z[i]^* = \{\pm 1, \pm i\}$, а $1-2i = i(-2-i)$, $1+2i = -i(-2+i)$, поэтому обе факторизации числа 5 эквивалентны.

Теорема. Если в кольце с факторизацией K любой простой элемент, делящий произведение двух регулярных элементов, делит один из сомножителей, то это кольцо является факториальным.

Область целостности K называется *евклидовым кольцом*, если на множестве $K \setminus \{0\}$ определена функция e со значениями из множества $N \setminus \{0\}$ такая, что: **1.** если $a \vdots b$, то $e(a) \geq e(b)$; **2.** для $\forall a,b \neq 0$ существуют

q, r такие, что $a = bq + r$, где либо $r = 0$, либо $e(r) < e(b)$. Функцию e принято называть евклидовой нормой.

Например, кольцо целых чисел Z является евклидовым. Достаточно положить $e(a) = |a|$, $\forall a \in Z$. Докажите, что и кольцо $Z[i]$ является евклидовым, если в качестве $e(a+bi)$ взять число $a^2 + b^2$.

Кольцо многочленов $K[x]$, где K – поле, также является евклидовым. В нем евклидова норма $e(f(x)) = \deg f$.

Теорема. Евклидово кольцо факториально.

Гомоморфизм и изоморфизм колец

Пусть $(K, +, \cdot)$ и $(K', \oplus, \otimes)$ – кольца. Отображение $f : K \to K'$ называется *гомоморфизмом*, если оно сохраняет все операции, т.е. если

$$f(a+b) = f(a) \oplus f(b),\ f(a \cdot b) = f(a) \otimes f(b).$$

Образ $\operatorname{Im} f$ гомоморфизма f является подкольцом кольца K', а ядро $\operatorname{Ker} f$ – подкольцом кольца K. При этом $Ker\ f = \{a \in K : f(a) = 0'\}$ ($0'$ – нуль в кольце K').

Гомоморфизм $f : K \to K'$ называется: *мономорфизмом*, если $\operatorname{Ker} f = 0$; *эпиморфизмом*, если $\operatorname{Im} f = K'$; *изоморфизмом*, если отображение $f : K \to K'$ мономорфно и эпиморфно (т.е. биективно). Изоморфизм колец K и K' обозначается так: $K \cong K'$.

Пример. отображение $f : Z \to Z_m$, $f(a) = \overline{a}$, $\overline{a} \in Z_m$ является эпиморфизмом с ядром $\operatorname{Ker} f = mZ$.

Нулю и противоположному элементу $(-a)$ элемента a кольца K при гомоморфизме $f : K \to K'$ соответствуют нуль и противоположный элемент из кольца K'. Если K – кольцо с единицей, то при гомоморфизме $f : K \to K'$ единице из K соответствует единица из K'.

Изоморфные кольца тождественны по своим алгебраическим свойствам и математический интерес представляют собой только те свойства колец, которые сохраняются при изоморфизме.

Если кольцо K коммутативно, то при гомоморфизме $f : K \to K'$ кольцо K' также будет коммутативным. Если K – целостное кольцо, то кольцо K' не обязано быть целостным. При этом K' может быть целостным кольцом, даже когда K – не целостное кольцо.

Изоморфный образ целостного кольца есть целостное кольцо.

ПОЛЕ

Если в определении кольца аксиому 2 заменить на более сильное условие: множество $K\setminus\{0\}$ является мультипликативной группой, то получим класс колец с делением, которые принято называть *телом*.

Таким образом, *тело* – это кольцо без делителей нуля и каждый ненулевой элемент в нем обратим.

Поле P – это коммутативное кольцо с единицей $1\neq 0$, в котором каждый ненулевой элемент обратим. Группа P^* называется мультипликативной группой поля, причем $P^* = P\setminus\{0\}$.

Кольцо, состоящее из одного нуля, не считается полем, поэтому поле минимально может состоять из двух элементов: нулевого и единичного.

Примерами полей являются множества Z, Q, R, а также Z_p (p – простое число). В дальнейшем будут показаны другие примеры полей.

В любом поле P: $ab=0$, если $a=0$ или $b=0$ (как и в целостном кольце). Поле представляет собой гибрид двух абелевых групп – аддитивной и мультипликативной, связанных законом дистрибутивности.

Произведение ab^{-1} в поле P принято записывать в виде дроби: a/b. Дробь a/b, имеющая смысл при $b\neq 0$, есть решение уравнения $bx=a$.

Действия с дробями, подчиняются следующим правилам:

1. $a/b = c/d \;\Leftrightarrow\; ad = bc$, $b,d\neq 0$;
2. $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd}$, $\dfrac{a}{b}\dfrac{c}{d}=\dfrac{ac}{bd}$, $b,d\neq 0$;
3. $-\dfrac{a}{b}=\dfrac{-a}{b}=\dfrac{a}{-b}$, $b\neq 0$; $\left(\dfrac{a}{b}\right)^{-1}=\dfrac{b}{a}$, $a,b\neq 0$.

Итак, частные a/b составляют некоторое поле, которое принято называть полем частных. Например, поле рациональных чисел Q есть поле частных кольца целых чисел Z.

Подмножество F поля P называется подполем, если 1) F является подкольцом кольца P; 2. $\forall a\in F, a\neq 0\ \ \exists a^{-1}\in F$; 3. $1\in F$. Всякое подполе F является полем относительно тех же операций, что и в самом поле P.

Поле P называется простым, если в нем нет других подполей, кроме самого поля P. Простыми полями являются множества Q и Z_p.

Теорема. В каждом поле P содержится одно и только одно простое поле P_0. Это простое поле либо изоморфно Q, либо Z_p (p – простое).

В случае $F\subset P$ говорят также, что поле P является расширением своего подполя F.

Если взять в поле P пересечение F_1 всех его подполей, содержащих подполе F и некоторый элемент $a \in P$ и $a \notin F$, то F_1 будет минимальным подполем, содержащим множество $\{F, a\}$. В этом случае говорят, что расширение F_1 поля F получено присоединением к F элемента a и обозначают это так: $F_1 = F(a)$. Аналогично, можно говорить о подполе $F_1 = F(a_1,...,a_n)$ поля P, полученном присоединением к подполю F n элементов $a_1,...,a_n \in P$. Например, $R(i) = C$.

Пример. Множество $Q(\sqrt{2})$ чисел вида $a + b\sqrt{2}$, $a,b \in Q$ является полем. Здесь $(\sqrt{2})^2 = 2 \in Q$ и $(a+b\sqrt{2})^{-1} = (a-b\sqrt{2})/(a+b\sqrt{2})(a-b\sqrt{2}) =$

$$= (a-b\sqrt{2})/(a^2-2b^2) = a/(a^2-2b^2) - b\sqrt{2}/(a^2-2b^2) \in Q(\sqrt{2}).$$

Вообще, если целое число k отлично от 1 и не делится на квадрат простого числа, то $Q(\sqrt{k})$ является полем (при $k < 0$, считать $\sqrt{k} = i\sqrt{|k|}$. При $k = -1$ получим $Q(\sqrt{-1}) = Q(i) = \{a+bi, a,b \in Q\}$. Тогда $Z[i] \subset Q(i)$.

Рассмотрим кольца Z и Z_p (p – простое число). Очевидно, что $Z_p^* = \{1,2,...,p-1\}$ и $ord(Z_p^*) = p-1$. Тогда $\forall a \in Z$: $a^{p-1} \equiv 1(\mathrm{mod}\, p)$. Это утверждение называют *малой теоремой Ферма*. Справедливо и более общее утверждение.

Теорема Эйлера. $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, где $(a,m) = 1$, а $\varphi(m)$ –функция Эйлера, которая равна числу всех взаимно простых чисел из множества 1, 2, …, $m-1$ с числом m. Фактически, $\varphi(m)$ есть порядок группы Z_m^*. Если $m = p$, то $\varphi(p) = p-1$, а если $m = p_1^{k_1}...p_s^{k_s}$ (где p_i – простые числа), то $\varphi(m) = \left(p_1^{k_1} - p_1^{k_1-1}\right)...\left(p_s^{k_s} - p_s^{k_s-1}\right)$.

Определим понятие характеристики поля. Характеристика поля P – это минимальное число p в равенстве $\underbrace{1+1+...+1}_{p} = 0$ (1 – единица поля). Если это равенство невозможно, то поле называют полем характеристики нуль, т.е. его простое подполе изоморфно Q. Поле P является полем простой (конечной) характеристики p, если его простое подполе P_0 изоморфно Z_p. Соответственно пишут: $\mathrm{char}\, P = p > 0$.

Обычно поле Z_p обозначают как F_p или $GF(p)$ (поле Галуа). Отметим, что $GF(q)$ – это конечное поле, состоящее из q элементов, где $q = p^n$ (p – простое число). Способы получения таких полей будут показаны в следующем разделе.

ИДЕАЛЫ КОЛЕЦ И ФАКТОРКОЛЬЦА

Обобщая конструкцию кольца вычетов Z_n, можно рассматривать отношения эквивалентности, согласованные с операциями, в произвольных кольцах. Так как кольцо состоит в основном из аддитивной группы, то такое отношение должно быть отношением сравнимости по модулю некоторой подгруппы. Выясним, какой должна быть эта подгруппа для того, чтобы отношение эквивалентности было согласовано с умножением.

Отношение сравнимости по модулю I (K – кольцо, $I \subset K$ – аддитивная подгруппа) согласовано с умножением тогда и только тогда, когда для $\forall x \in I$, $\forall a \in K$ имеют место включения $ax \in I$ и $xa \in I$. Аддитивная подгруппа I, удовлетворяющая этим условиям, называется (двусторонним) *идеалом* кольца K. То, что I – идеал K, обозначается так: $I \lhd K$. Соответственно, если подгруппа I удовлетворяет первому (второму) из этих условий, то она называется *левым (правым) идеалом*. В коммутативных кольцах нет разницы между левыми, правыми и двусторонними идеалами.

Понятие идеала кольца является аналогом понятия нормальной подгруппы в теории групп.

В любом ненулевом кольце K есть, по крайней мере, два идеала – нулевой и само кольцо K. Такие идеалы называют несобственными. Остальные идеалы называют собственными (нетривиальными) идеалами.

Отметим, что в любом поле нет собственных идеалов.

Примеры. 1) Пусть K – коммутативное кольцо и $a \in K$. Тогда подмножество aK есть идеал в K: $aK \lhd K$. Действительно, $\forall x, y \in K$ имеем: $ax + ay = a(x + y) \in aK$, $(ax)y = a(xy) \in aK$. Из этого примера следует, что все подмножества mZ в кольце целых чисел Z являются идеалами.

2) В кольце многочленов $P[x]$ над полем P подкольца вида $f(x)P[x]$ являются идеалами, а все ненулевые подкольца, содержащиеся в P, и, в частности само поле P, не являются идеалами. Идеал $f(x)P[x]$ фактически состоит из многочленов, кратных многочлену $f(x)$.

3) Рассмотрим гомоморфизм $f : K \to K'$ колец (K, +, $\cdot$) и (K', $\oplus$, $\otimes$). Покажем, что ядро этого гомоморфизма является идеалом. Действительно, $Ker\ f = \{a \in K : f(a) = 0'\} \subset K$ – подкольцо. Если $J = Ker\ f \subset K$, то $J \cdot x \subseteq J$, т.к. $f(zx) = f(z) \otimes f(x) = 0' \otimes f(x) = 0'$ для $\forall z \in J, \forall x \in K$. Значит $zx \in J$, тогда $JK \subset J$ и $KJ \subset J$,т.е. $J = \mathrm{Ker}\ f$ – идеал в K.

4) В кольце $Z_4[x]$ подкольцо $2Z_4[x]$ многочленов, имеющих коэффициенты 0 и 2, является идеалом. Подкольцо $2Z_4$ является идеалом в $2Z_4[x]$. Но при этом подкольцо $2Z_4$ не является идеалом в $Z_4[x]$ (докажите это). Таким образом, отношение «быть идеалом» не транзитивно на множестве подколец какого-либо кольца.

Отметим некоторые свойства операций над идеалами.

1. Если I – идеал, а L – подкольцо кольца K, то $I+L$ является подкольцом кольца K, а $I \bigcap L$ – идеал кольца L.
2. Если I и J – идеалы в кольце K, то $I+J$ – идеал кольца K.
3. Если $\{I_\alpha, \alpha \in A\}$ – произвольное семейство идеалов кольца K, то $T = \bigcap\limits_{\alpha \in A} I_\alpha$ – идеал кольца K.

Пусть I – идеал кольца K и пусть для $\forall a,b \in K$: $a \equiv a'(\mathrm{mod} I)$, $b \equiv b'(\mathrm{mod} I)$, .т.е. $a' = a + x$, $b' = b + y$ ($a', b', x, y \in I$). Тогда

$a'b' = ab + ay + bx + xy \equiv ab(\mathrm{mod} I)$.

Это означает согласованность отношения сравнимости по модулю I с умножением. Отсюда следует, что в факторгруппе K/I (K является аддитивной абелевой группой, а тогда I - нормальная подгруппа в K) можно определить операцию умножения по правилу: $(a+I) \otimes (b+I) = ab + I$.

Элементами факторгруппы K/I являются смежные классы $a+I$, которые принято называть классами вычетов по модулю идеала I, сложение которых определяется так: $(a+I) \oplus (b+I) = (a+b) + I$, -$(a+I) = -a + I$.

Для краткости записи положим: $a + I = \overline{a}$. Тогда $\overline{a} \oplus \overline{b} = \overline{a+b}$, $\overline{a} \otimes \overline{b} = \overline{ab}$. В частности, $\overline{0} = I = 0 + I$ (нулевой элемент в аддитивной группе K/I), $\overline{1} = 1 + I$ (1 – единица кольца K, если оно есть кольцо с единицей). Итак, факторгруппа $K/I = \overline{K} = \{\overline{a}, a \in K\}$ наделена операциями $\oplus$ и $\otimes$, для которых выполнены все аксиомы кольца, так как операции над классами вычетов в $\overline{K}$ сводятся к операциям над элементами из K. Проверим выполнение дистрибутивности: $(\overline{a} \oplus \overline{b}) \otimes \overline{c} = \overline{(a+b)c} = \overline{ac+bc} =$

$= \overline{ac} \oplus \overline{bc} = \overline{a} \otimes \overline{c} \oplus \overline{b} \otimes \overline{c}$. Это означает, что отображение $f: K \to \overline{K}$, $f(a) = \overline{a}$ является эпиморфизмом колец K и $\overline{K}$ с ядром $Ker\ f = I$. Таким образом, построенное множество $\overline{K} = K/I$ является кольцом, которое принято называть *факторкольцом* кольца K по идеалу I.

Из этого общего случая следует, что факторгруппа Z/mZ является факторкольцом, которое изоморфно кольцу Z_m ($m \in N, m > 1$).

Указанный выше эпиморфизм $f: K \to K/I$, $f(a) = \bar{a}$ принято называть каноническим гомоморфизмом кольца K на факторкольцо K/I.

Здесь имеет место теорема о гомоморфизме колец, аналогичная теореме о гомоморфизме групп.

Теорема. Пусть $f: K \to K'$ – гомоморфизм колец. Тогда образ гомоморфизма $\operatorname{Im} f \cong K/\operatorname{Ker} f$, причем $\operatorname{Ker} f = I$ является идеалом кольца K, т.е. $K/I \cong \operatorname{Im} f$.

Примеры. 1) Пусть K – поле и $c \in K$ – его произвольный элемент. Отображение $f: K[x] \to K, f(x) \to f(c)$ является гомоморфизмом. При этом $f(x) = (x-c)q(x) + f(c)$ (теорема Безу). Тогда ядро этого гомоморфизма состоит из многочленов. делящихся на $(x-c)$. Следовательно, $K[x]/(x-c)K[x] \cong K$.

2) Пусть $x^2 + px + q \in R[x]$ есть квадратный трехчлен с отрицательным дискриминантом и $c \in C$ – один из его комплексных корней. Отображение $f: R[x] \to C, f(x) \to f(c)$ является гомоморфизмом. Его образ совпадает со множеством C, а ядро состоит из многочленов, делящихся на $x^2 + px + q = (x-c)(x-\bar{c})$. Следовательно, $R[x]/(x^2 + px + q)R[x] \cong C$.

Пусть K – коммутативное кольцо с единицей. Для любого подмножества S кольца K совокупность линейных комбинаций $a_1x_1 + .. + a_mx_m$ ($x_i \in S, a_i \in K$) является наименьшим идеалом, содержащим S. Оно называется идеалом, порожденным подмножеством S, и обозначается как (S).

В частности, идеал $I = aK = (a)$, порожденный одним элементом a, называется *главным идеалом*.

Целостное кольцо, в котором всякий идеал является главным, называется *кольцом главных идеалов*.

Докажите самостоятельно, что кольцо Z, любое поле P и кольцо многочленов $P[x]$ являются кольцами главных идеалов.

Пусть выбраны многочлены $f(x), g(x) \in P[x]$, где P – поле. Тогда включение $f(x)P[x] \subset g(x)P[x]$ справедливо тогда и только тогда, когда $g(x)$ делит $f(x)$. Поэтому равенство $(f(x)) = (g(x))$ выполняется тогда и только тогда, когда многочлены $f(x)$ и $g(x)$ ассоциированы.

Не всякое коммутативное кольцо с единицей является кольцом главных идеалов. Так например, в кольце $Z_4[x]$ идеал, порожденный множеством $S = \{2, x\}$, не является главным.

Укажем несколько теорем, касающихся колец главных идеалов.

Теорема 1. Всякое евклидово кольцо является кольцом главных идеалов.

Докажем эту теорему. Пусть I – идеал кольца K, и $a \in I$ – наименьший по норме элемент I. Тогда для $\forall b \in I$: $b = aq + r$. Отсюда $r = b - aq \in I$. Но, так как $a, b \in I$ и $r < a$, то $r = 0$. Значит $b = aq$ и $I = (a)$ есть главный идеал.

Из этой теоремы следует, что кольца Z и $P[x]$ (P – поле) являются кольцами главных идеалов. Отметим, что кольцо $Z[x]$ не является кольцом главных идеалов и соответственно не евклидово, так как в нем при делении двух многочленов с целыми коэффициентами можно получить остаточный многочлен с рациональными коэффициентами.

В евклидовом кольце естественным образом вводится понятие наибольшего общего делителя (НОД) двух и более элементов кольца.

Определение. Элемент d евклидова кольца K называется *наибольшим общим делителем* элементов $a_1, \ldots, a_n$ и обозначается $НОД(a_1, \ldots, a_n)$, или коротко $(a_1, \ldots, a_n)$, если $a_i \vdots d$ $(\forall i = \overline{1, n})$ и d делится на любой общий делитель элементов $a_1, \ldots, a_n$.

Если существует $НОД(a_1, \ldots, a_n)$, то он определяется с точностью до ассоциированности элементов $a_1, \ldots, a_n$.

Теорема 2. В любом евклидовом кольце K (и соответственно кольце главных идеалов) для любой пары элементов $a, b \in K$ существует их НОД d, при этом $d = ax + by$, где $x, y \in K$.

Для доказательства этой теоремы достаточно рассмотреть в K идеал $I = (x, y) = \{ax + by,\ a, b \in K\}$, порожденный элементами x, y. Так как I является главным идеалом, то найдется такой элемент $d \in I$, что $(x, y) = (d)$.

Теорема 3. Пусть a – ненулевой необратимый элемент кольца главных идеалов K. Факторкольцо $K/(a)$ (по идеалу $I = (a)$) является полем тогда и только тогда, когда элемент a прост в K.

Действительно, пусть $\bar{x}$ – смежный класс $x + (a) \in K/(a)$. Если $a = bc$, где b и c – необратимые элементы, то $\bar{b} \cdot \bar{c} = \overline{bc} = \bar{a} = 0$. Но $b, c \neq 0$, значит в кольце $K/(a)$ есть делители нуля, поэтому оно полем не является.
Обратно, если a – простой элемент в K, то для $\forall x \in (a)$, элементы x и a взаимно просты, т.е. $НОД(x, a) = xu + av = 1$. Отсюда, переходя к смежным классам, получим $\bar{x}\bar{u} + \bar{a}\bar{v} = \bar{1}$. Значит $\bar{x}\bar{u} \equiv \bar{1} (\mathrm{mod}(a))$, т.е. в кольце $K/(a)$ существует смежный класс $\bar{u}$, обратный к $\bar{x}$. Поэтому $K/(a)$ – поле.

Из теоремы 3 следует, что факторкольцо $P[x]/(f(x))$ (где P – поле) является полем тогда и только тогда, когда многочлен $f(x)$ является неприводимым в $P[x]$. Неприводимые многочлены не могут быть разложены в произведение многочленов положительной степени.

Пусть $\deg f(x)=n$, тогда факторкольцо $P[x]/(f(x))=P[x]/f(x)P[x]$ состоит из смежных классов вида $\{a_{n-1}\bar{x}^{n-1}+\ldots+a_1\bar{x}+a_0,\ a_i\in P\}$, которые являются бесконечными множествами, если P – бесконечное поле. Так как идеал $I=(f(x))$ является нулевым элементом в кольце $P[x]/(f(x))$, то число $\bar{x}$ есть корень полинома $f(x)$: $f(\bar{x})=\bar{0}=I$. Если при этом многочлен $f(x)$ будет неприводимым в $P[x]$, то по теореме 3 факторкольцо $P[x]/(f(x))$ будет полем $P'=P[x]/(f(x))\cong P(\bar{x})$, которое является расширением поля P, в котором $f(x)$ имеет хотя бы один корень.

Теорема 4. Факторкольцо K/I коммутативного кольца с единицей K по идеалу I является полем тогда и только тогда, когда идеал I является максимальным в K.

Идеал I является *максимальным* в кольце K, если не существует идеала I' такого, что $I\subset I'\subset K$ ($I\neq I'$), т.е. идеал I не содержится ни в каком другом идеале, кроме самого кольца K.

Теорема 5. Факторкольцо $F_p[x]/(f(x))$ является полем конечного порядка p^n, изоморфным полю Галуа $GF(p^n)$, тогда и только тогда, когда многочлен $f(x)$ является неприводимым многочленом степени n в кольце $F_p[x]$. Здесь $F_p=GF(p)\cong Z_p$ – поле порядка p (p простое число из N).

Например, возьмем факторкольцо $Z_2[x]/(f(x))$ по неприводимому многочлену второго порядка. Коэффициентами всех многочленов в $Z_2[x]$ являются только числа 0 и 1, поэтому многочленами второго порядка в нем являются: $x^2, x^2+1, x^2+x, x^2+x+1$. Из них неприводимым является только многочлен x^2+x+1 (проверьте!). Тогда, в соответствии с теоремой 5, факторкольцо $Z_2[x]/(x^2+x+1)$ есть поле, изоморфное полю $GF(4)$. Поле $GF(4)$ состоит из элементов 0, 1, α и β, где $\alpha^2=\beta$, $\beta^2=\alpha$, $\alpha\beta=\beta\alpha=1$, $\alpha+\alpha=\beta+\beta=0$, $\alpha+\beta=\beta+\alpha=1$. Поле $Z_2[x]/(x^2+x+1)$ состоит из смежных классов $\bar{0}=I=f(\bar{x})$, $\bar{1}$, $\bar{x}$, $\bar{x}+\bar{1}$. Здесь $\bar{x}^2=\bar{x}+\bar{1}$ (так как $f(\bar{x})=\bar{x}^2+\bar{x}+\bar{1}=\bar{0}$), $(\bar{x}+\bar{1})(\bar{x}+\bar{1})=\bar{x}^2+\bar{1}\equiv\bar{x}$, $\bar{x}(\bar{x}+\bar{1})=\bar{1}$, $\bar{x}+\bar{x}=\bar{0}$, $(\bar{x}+\bar{1})+(\bar{x}+\bar{1})=\bar{0}$, $\bar{x}+(\bar{x}+\bar{1})=\bar{1}$. Таким образом, изоморфизм полей

$Z_2[x]/(x^2+x+1)$ и $GF(4)$ очевиден.

Можно легко показать, что факторкольцо $R[x]/(x^2+1)$ есть поле (так как x^2+1 неприводим в $R[x]$), изоморфное полю $R(i)$. Здесь мнимая единица i есть один из корней многочлена x^2+1, и она не принадлежит R, т.е. получили простое расширение поля R до поля $R(i)$, которое в свою очередь изоморфно полю комплексных чисел C.

Задания для самостоятельного решения

1. Является ли факторкольцо $Q[x]\big/(x^2)$ областью целостности?
2. Докажите, что кольцо $Z[\sqrt{2}]$ евклидово.
3. Найти все идеалы кольца Z_{36}.
4. Опишите факторкольцо $Z[i]/(2)$. Есть ли в нем делители нуля?
5. Найти все максимальные идеалы в кольцах Z и Z_{36}.
6. Опишите факторкольцо $R[x]\big/(x^3-1)$. Является ли оно полем?
7. Постройте таблицы Кэли для операций сложения и умножения в кольцах $Z_2[x]/(x^2)$, $Z_2[x]/(x^2+1)$, $Z_2[x]/(x^2+x)$. Каким конечным кольцам они изоморфны?
8. Докажите изоморфность колец $Q[x]/(x^2-2)$ и $Q[\sqrt{2}]$.