Кольца и поля

Чтобы подступиться к группам начнём сначала с полей и колец — они наиболее похожи на обычные числа по своей структуре. Дадим сначала определения:

Группой G называется множество G с заданной на нём операцией «умножения» $\cdot : G\times G \to G$, удовлетворяющей следующим аксиомам:

I. Существует нейтральный элемент 1, такой, что

$$1 \cdot g = g \cdot 1 = g, \ \forall g \in G,$$

II. Для любого элемента группы существует обратный, т. е.

$$\forall g \in G \ \exists g^{-1} \in G \ : \ g \cdot g^{-1} = g^{-1} \cdot g = 1,$$

III. Справедлива ассоциатоивность:

$$a(bc) = (ab)c.$$

Множество, удовлетворяющее только пункту **III.** определения группы называется *полугруппой.*

Полугруппа с нейтральным элементом называется *моноидом.*

Кольцом R (коммутативным ассоциативным с единицей) называется множество с двумя операциями «+» и «-», такими, что относительно сложения R — абелева группа, а относительно умножения R — моноид, причём справедлива дистрибутивность: $a\cdot(b+c) = a\cdot b + a\cdot c$, $(b+c)\cdot a = b\cdot a + c\cdot a$.

Телом T называется кольцо, каждый ненулевой элемент которого обратим по умножению.

Поле F — коммутативное тело. Примеры колец: целые числа $\mathbb{Z}$, остатки $\mathbb{Z}_n$, многочлены $\mathbb{R}[x]$.

Примеры полей: рациональные ($\mathbb{Q}$), действительные ($\mathbb{R}$) и комплексные ($\mathbb{C}$) числа, остатки по простому модулю (см. задачу 3), рациональные функции $\mathbb{Q}(x) = \left\{\frac{P(x)}{Q(x)} \middle| \ P, Q \in \mathbb{Q}[x], \ Q \neq 0\right\}$.

1. Докажите, что в любом кольце $0\cdot x = x\cdot 0 = 0$ для любого x.

2. Докажите, что кольцо остатков $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое.

3. Какие элементы обратимы в кольцах $\mathbb{Z}_4, \ \mathbb{Z}_6, \ \mathbb{Z}_n$? Найдите делители нуля.

Будем через $R[\sqrt{d}]$, где R кольцо и $d \in R$, обозначать множество формальных выражений $\{a+b\sqrt{d} | \ a, b \in R\}$ с «обычными» сложением и умножением. Можно проверить, что $R[\sqrt{d}]$ — это кольцо. Например, $\mathbb{R}[\sqrt{-1}] = \mathbb{C}$ — поле комплексных чисел.

4. Найдите все обратимые элементы кольца гауссовых чисел $\mathbb{Z}[\sqrt{-1}]$.

5. Докажите, что в поле $\mathbb{Z}_p$ верно «правило двоечника»: $(a+b)^p = a^p + b^p$.

6. Найдите все такие d, что $\mathbb{Q}[\sqrt{d}]$ — поле.

7. Решите в $\mathbb{Z}_p$ уравнение $x^2 = 1$, вычислите произведение всех ненулевых элементов поля $\mathbb{Z}_p$ и докажите теорему Вильсона: если p — простое, то $(p-1)!+1$ делится на p.

8. Решите в натуральных числах уравнение: $a! + b! = c!$

Кольцо многочленов

Рассмотрим ещё один важный пример кольца — это кольцо многочленов

$$R[x] = \{a_n x^n + ... + a_0 |\ a_i \in R, n \in \mathbb{Z}_{\geqslant 0}\},$$

где R — некоторое кольцо.

Примеры: кольцо многочленов с действительными коэффициентами $\mathbb{R}[x]$, кольцо многочленов с целыми коэффициентами $\mathbb{Z}[x]$, кольцо многочленов над кольцом вычетов $\mathbb{Z}_n[x]$.

Непостоянный многочлен называется неприводимым, если он не может быть разложен в произведение непостоянных многочленов меньших степеней.

Пример: любой квадратный трёхчлен с отрицательным дискриминантом неприводим в $\mathbb{R}[x]$.

1. Докажите, что многочлен $x^3 - 5$ неприводим в $\mathbb{Q}[x]$.

2. При каких n многочлен $x^d + ... + x^2 + x + 1$ неприводим в $\mathbb{Q}[x]$?[Комплексные числа]

3. Найдите НОД$(x^m - 1, x^n - 1)$ в $\mathbb{Q}[x]$.

4. Докажите, что наибольший общий делитель двух многочленов существует и единственен.

5. Могут ли два взаимно простых многочлена из $\mathbb{Q}[x]$ иметь общий иррациональный корень? [Минимальный многочлен]

6. Может ли неприводимый многочлен в $\mathbb{Q}[x]$ иметь кратный иррациональный корень? [Производная и предыдущая задача]

   По аналогии с кольцом остатков целых чисел $\mathbb{Z}_n$ можно построить кольцо многочленов $K[x]/(P(x))$ для заданного кольца K и многочлена с коэффициентами из этого поля. Элементами множества $K[x]/(P)$ служат классы эквивалентности многочленов по модулю P: $Q + (P)$ — грубо говоря, остатки от деления на P.

7. Докажите, что кольцо $K[\sqrt{d}]$ изоморфно кольцу $K[x]/(x^2 - d)$. Как следствие, комплексные числа это $\mathbb{R}[x]/(x^2 + 1)$. Изоморфизм колец R_1 и R_2 — это биекция $\varphi : R_1 \to R_2$, уважающая сложение и умножение, т. е. $\varphi(ab) = \varphi(a)\varphi(b)$ и $\varphi(a + b) = \varphi(a) + \varphi(b)$. Изоморфность означает одинаковость в алгебре.

8. Пусть НОД$(m, n) = d$, где m и n — целые числа. Докажите, что найдутся такие целые a и b, что $am+bn = d$ (*линейное представление НОДа*). Докажите аналогичное утверждение для многочленов.

9. Подумайте, когда кольцо $K[x]/(P)$ является полем. Рассмотрите частные случаи: $\mathbb{R}[x]/(x^2 - 1)$, $\mathbb{R}[x]/(x^2 + 4)$, $\mathbb{R}[x]/(x^2 + 1)$. [Используйте предыдущую задачу]

Гауссовы числа

[Винберг]

Гауссовы целые числа — это комплексные числа с целыми действительной и мнимой частями. Гауссово число называется *простым*, если оно не может быть представлено в виде произведения двух необратимых в этом кольце элементов.

Чтобы делить с остатком в гауссовых числах, необходимо ввести некоторый вес каждого числа, иначе мы не сможем понять, когда деление с остатком закончено. Например, у целых чисел весом служил модуль, а у многочленов — степень. Введём норму гауссова числа $a+bi$:

$$N(a+bi) = a^2 + b^2.$$

1. Докажите, что для любых гауссовых чисел a и b

$$N(ab) = N(a)N(b).$$

2. Какие из данных гауссовых чисел простые: $1+i, 3, 5, 3+i$? Докажите, что гауссовы числа — это кольцо $\mathbb{Z}[i]$.

3. Докажите, что $N(ab) \geqslant N(a)$, и равенство выполняется только в случае, если b обратим.

4. Докажите, что для любых $a, b \in \mathbb{Z}[i]$, где $b \neq 0$, существуют такие q и r из $\mathbb{Z}[i]$, что $a = qb + r$, и либо $r = 0$, либо $N(r) < N(b)$.

   И вообще, абстрактное кольцо R без делителей нуля (*целостное*) с функцией $N : R\backslash\{0\} \to \mathbb{Z}_+$ — весом (или нормой), называется *евклидовым.*

   Теорема. *В евклидовом целостном кольце всякий необратимый ненулевой элемент может быть разложен на простые множители, причём это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы.*

   Кольца, удовлетворяющие теореме, называются *факториальными.*

   Следствие. *Кольца* $\mathbb{Z}$, $K[x]$ *— факториальные.*

   Но есть кольца, в которых это не так:

5. Докажите, что евклидово кольцо $\mathbb{Z}[\sqrt{-5}]$ с нормой $N(a+b\sqrt{-5}) = a^2 + 5b^2$ не факториально. [Рассмотрите число 6]

6. Когда уравнение $x^2 + 1 = 0$ имеет решение в поле $\mathbb{Z}_p$? [Обсудить общую ситуацию]

7. Найдите все простые в $\mathbb{Z}$ числа p, которые просты также в $\mathbb{Z}[i]$. [$\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[x]/(x^2+1)$, следствие и задачи 9 и 11]

8. Докажите, что простые элементы $\mathbb{Z}[i]$ суть (с точностью до ассоциированности) простые натуральные числа вида $4k+3$; числа вида $a+bi$, где a^2+b^2 — простое (в $\mathbb{Z}$) и число $1+i$. [Во втором случае срабатывает простое рассуждение с нормами]

9. Докажите, что натуральное число n представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда в его разложение на простые множители в $\mathbb{Z}$ все множители вида $4k+3$ входят в чётной степени. [Следствие]

10. Найдите число таких представлений в предыдущей задаче.

Немного о группах

[Алексеев]

1. Докажите, что в группе единичный элемент единственен. Докажите, что в любой группе обратный к данному элемент единственен.

2. Докажите, что $(ab)^{-1} = b^{-1}a^{-1}$, а также обобщение данного равенства.

Группа называется *абелевой* (или *коммутативной*), если в ней для любых двух элементов $ab = ba$, т. е. a и b *коммутируют.*

3. Какие группы абелевы: группа вращений треугольника, группа перестановок из n элементов S_n, группа вращений квадрата, группа симметрий квадрата, группа симметрий ромба, группа симметрий прямоугольника?

4. Пусть в группе G для любого элемента g выполнено: $g^2 = e$. Докажите, что G — абелева.

5. Докажите, что $a^m = a^{-m}$ для любого целого m и любого $g \in G$. Проверьте остальные свойства целой степени.

Циклическая группа — это группа, порождённая одним элементом, т. е. $G = \{g^0 = e, g, g^2, g^3, \ldots\}$.

Примеры: группа вычетов по модулю n: $\mathbb{Z}_n$, группа целых чисел $\mathbb{Z}$. Первая группа конечная, а вторая — бесконечная.

6. Пусть G — конечная циклическая группа. Наименьшее неотрицательное n, для которого $a^n = e$ называется порядком элемента a. Докажите, что среди элементов $e, a, a^2, \ldots$ нет двух одинаковых. Докажите, что для любого целого m элемент $a^m = a^k$ для $0 \leqslant k < n$.

Очевидно, любая конечная циклическая группа — это $\mathbb{Z}_n$ для некоторого n. (Слово «это» заменяют в алгебре на «изоморфно»).

7. Докажите, что группа вращений правильного n–угольника — это $\mathbb{Z}_n$.

8. Пусть порядок элемента g равен n. Чему равен порядок элемента g^m, $m \in \mathbb{Z}$?

Биекция групп $\varphi : G_1 \to G_2$ называется *изоморфизмом*, если она «уважает операции в группах», т. е. $\varphi(ab) = \varphi(a)\varphi(b)$.

9. Какие из следующих групп изоморфны: группа вращений квадрата, группа симметрий ромба, группа симметрий прямоугольника, группа остатков $\mathbb{Z}_4$?

10. Докажите, что любая циклическая группа n-го порядка изоморфна $\mathbb{Z}_n$.

11. Как может быть устроена группа из двух элементов? а из трёх? четырёх? Найдите все возможные варианты (с точностью до изоморфизма).

12. Приведите пример двух групп одинаковых порядков, но не изоморфных друг другу.

13. Докажите, что группа действительных чисел по сложению изоморфна группе положительных действительных чисел по умножению.

Подмножество группы, являющееся группой, называется *подгруппой.*

14. Пусть H — подгруппа в группе G. Докажите, что единичные элементы в G и H совпадают. Докажите, что обратный элемент к $h \in H$ в подгруппе H совпадает с обратным к нему же в объемлющей группе G.

15. Для того, чтобы H было подгруппой G необходимо и достаточно, чтобы выполнялись следующие условия: 1) если a и b содержатся в H, то элемент ab (произведение в группе G) содержится в H; 2) если a содержится в H, то и a^{-1} (в группе G) содержится в H. Докажите.

16. Опишите все подгруппы в группе остатков $\mathbb{Z}_n$.

17. Опишите все подгруппы в группе целых чисел $\mathbb{Z}$.

18. Опишите все симметрии правильного тетраэдра, включающие вращения относительно прямых и отражения относительно плоскостей. Все симметрии тетраэдра образуют группу. Сколько в ней элементов? На какую группу она похожа? Есть ли в ней циклические подгруппы, если да, то сколько их?

19. Исследуйте группу вращений правильного тетраэдра (т. е. симметрии относительно плоскостей отсутствуют).

20. Верно ли, что $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Тот же вопрос для $\mathbb{Z}_2$ и $\mathbb{Z}_6$. При каком условии группы $\mathbb{Z}_m \times \mathbb{Z}_n$ и $\mathbb{Z}_{mn}$ изоморфны?

Отображение групп $\varphi : G_1 \to G_2$, «уважающее умножение», называется *гомоморфизмом.*

Пример: изоморфизм является частным случаем гомоморфизма.

21. Докажите, что $\varphi(a^{-1}) = (\varphi(a))^{-1}$ и $\varphi(e) = e$.

22. Докажите, что образ $\mathrm{Im}\varphi$ — подгруппа в группе G_2.

Ядром гомоморфизма φ называется множество тех элементов $g \in G_1$, которые отправляются в нейтральный элемент: $\operatorname{Ker}\varphi := \{g|\ \varphi(g) = e\}$.

23. Докажите, что ядро $\operatorname{Ker}\varphi$ гомоморфизма — подгруппа в G_1.

Теорема. (О гомоморфизме) $\operatorname{Im}\varphi \cong G_1/\operatorname{Ker}\varphi$.

Цепные дроби и уравнения Пелля

[Бугаенко уравнения Пелля]

Конечное цпеной дробью называется выражение

$$[a_0, a_1, ..., a_n] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + ... \frac{1}{a_{n-1} + \frac{1}{a_n}}}}},$$

где числа a_i — целые.

Любое действительное число α можно разложить в «почти цепную дробь», т. е. $\alpha = [a_0, ..., \alpha_n]$, где $a_i \in \mathbb{N}$, а $\alpha_n \in \mathbb{R}$. Для этого нужно на каждом шаге выделять целую часть, а дробную — переворачивать $\left(x = \frac{1}{\frac{1}{x}}\right)$.

Если проделывать этот процесс долго, то мы будем приближаться к числу α всё ближе, т. е. $\lim\limits_{n\to\infty} [a_0, ..., a_n] = \alpha$ — но это не очевидно!

1. Докажите, что цепная дробь является конечной только в том случае, если исходное число было рациональным.

2. Представьте числа $\frac{7}{11}$ и $\sqrt{3}$ в виде цепных дробей.

3. Как представление обыкновенной дроби в непрерывном виде связано с алгоритмом Евклида?

4. Докажите, что если цепная дробь бесконечна и циклична, то она имеет вид $a + b\sqrt{d}$ для целых a, b и натурального d, т. е. является квадратичной иррациональностью.

Обозначим $r_n = [a_, ..., a_n] = \frac{p_n}{q_n}$ — *подходящая дробь*.

5. Докажите, что последовательности p_n и q_n удовлетворяют следующим рекуррентным соотношениям:

$$\begin{cases} p_{n+1} = p_n a_{n+1} + p_{n-1}, \\ q_{n+1} = q_n a_{n+1} + q_{n-1}. \end{cases}$$

Как следствие, последовательности p_n и q_n монотонно возрастают по абслоютной величине, т. е. $p_n,\ q_n \to \infty$.

6. Докажите, что при всех $n \geqslant 1$

$$p_{n-1} q_n - p_n q_{n-1} = (-1)^n.$$

7. Пусть натуральное число n чётно, и $m > n$. Тогда $r_n < \alpha$ и $r_n < r_m$. Если же n нечётно, и $m > n$, то $r_n > \alpha$ и $r_n < r_m$.

8. Докажите, что $|r_n - r_{n+1}|$ можно сделать сколь угодно маленькой, начиная с некоторого номера N (т. е. $\lim\limits_{n\to\infty} |r_n - r_{n+1}| = 0$).

Из задач выше и некоторых утверждений анализа следует

Теорема. *Последовательность подходящих дробей r_n сходится к числу α.*

9. Почему

$$\left|\frac{p_n}{q_n} - \alpha\right| \leqslant \frac{1}{q_n^2}?$$

Оказывается, справедлива следующая неожиданная

Теорема. *Если несократимая дробь $\frac{p}{q}$ очень хорошо приближает число α, а именно*

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2},$$

то она является подходящей для числа α.

10. Из предыдущей теоремы выведите, что среди подходящих дробей числа $\sqrt{d}$ есть решения уравнения Пелля $x^2 - dy^2 = 1$.

[Подходящие дроби вокруг нас: размер листа бумаги, в музыке, астрономии, ...]

Тетраэдры

[Прасолов]

[Вывести формулу для объёма тетраэдра]

1. Докажите, что объём тетраэдра равен шестой части произведения двух скрещивающихся рёбер на синус угла между ними.

2. (Теорема Менелая для тетраэдра) В произвольном тетраэдре $KLMN$ точки A, B, C и D принадлежат рёбрам KN, NL, LM и MK соотвтетственно. Для того, чтобы точки A, B, C и D лежали в одной плоскости, необходимо и достаточно, чтобы выполнялось равенство:
$$\frac{KA}{AN} \cdot \frac{NB}{BL} \cdot \frac{LC}{CM} \cdot \frac{MD}{DK} = 1.$$

3. Сфера касается сторон пространственного четырёхугольника. Докажите, что точки касания лежат в одной плоскости.

4. Докажите, что любая плоскость, проходящая через середины двух скрещивающихся рёбер тетраэдра, делит его объём пополам.

5. Докажите, что сумма квадратов длин рёбер тетраэдра равна учетверённой сумме квадратов расстояний между серединами его противоположных рёбер. [Достройте тертаэдр до параллелепипеда]

6. У пирамиды $SABCD$ в основании лежит выпуклый четырёхугольник $ABCD$ с перпендикулярными диагоналями, причём высота из точки S падает в их точку пересечения O. Докажите, что основания перпендикуляров, опущенных из точки O на боковые грани пирамиды, лежат на одной окружности.

7. (Теорема синусов для трёхгранного угла) Пусть α, β и γ — плоские углы трёхгранного угла, а A, B и C — противолежащие им двугранные углы. Докажите, что
$$\frac{\sin\alpha}{\sin A} = \frac{\sin\beta}{\sin B} = \frac{\sin\gamma}{\sin C}.$$

8. (Две теоремы косинусов для трёхгранного угла) В обозначениях предыдущей задачи докажите:

a. $\cos\alpha = \cos\beta\cos\gamma + \sin\beta\sin\gamma\cos A$,

b. $\cos A = -\cos B\cos C + \sin B\sin C\cos\alpha$.

[Полярные углы]

9. Докажите, что сумма двух плоских углов двугранного угла больше третьего плоского угла.

10. Докажите, что сумма плоских углов двугранного угла меньше 2π, а сумма его двугранных углов — больше π.

11. Существует ли тетраэдр, все двугранные углы которого тупые? Верно ли, что если все плоские углы трёхгранного угла тупые, то и все его двугранные углы тоже? А если наоборот?

12. Докажите, что в произвольном трёхгранном угле биссектрисы двух плоских углов и угла, смежного с третьим плоским углом, лежат в одной плоскости. [Постройте вспомогательный тетраэдр так, чтобы данная плоскость была серединной для него]

13. **a.** В трёхгранный угол $SABC$ вписана сфера, касающаяся граней SBC, SCA и SAB в точках A_1, B_1 и C_1. Выразите величину угла ASB_1 через плоские углы данного трёхгранного угла.

b. Вписанная и вневписанная сферы тетраэдра $ABCD$ касаются грани ABC в точках P и P' соответственно. Докажите, что прямые AP и AP' симметричны относительно биссектрисы угла BAC.

Линейные диофантовы уравнения. Алгоритм Евклида.

Пифагоровы тройки и рациональная параметризация окружности.

Уравнения Пелля.

Темы, близкие к формуле Крофтона (метод усреднения и геометрические неравенства).

Точки пересечения диагоналей правильных многоугольников.

Стереометрия: тетраэдры. Теоремы косинусов и синусов.

Сферическая геометрия.

Рациональная параметризация кривых.

Pentagramma mirificum