Листок 0. Кольца и поля

Пусть R – ассоциативное коммутативное кольцо с единицей и F – поле.

1. Найти все идеалы в кольце а) $\mathbb{Z}$; б) F; в) $F[x]$; г) $M_n(F)$ (кольцо матриц размера $n \times n$, здесь имеются в виду двухсторонние идеалы).

2. Привести пример идеала в кольце а) $F[x, y]$; б) $\mathbb{Z}[x]$, не являющегося главным.

3. Доказать, что $a \in R$ не лежит ни в каком собственном идеале $\Leftrightarrow$ a – обратим.

4. Найти все обратимые элементы в кольце степенных рядов $\mathbb{R}[[x]]$.

5. Доказать, что $f = a_0 + a_1 x + \dots a_n x^n \in R[x]$ – обратим $\Leftrightarrow$ a_0 – обратим и $a_1 \dots a_n$ – нильпотентны.

6. Доказать, что $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$ $\Leftrightarrow$ числа a и b взаимно просты.

7. Вывести формулу для функции Эйлера: если $n = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, то $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_n})$.

8. Верно ли, что группа $\mathbb{Z}_n^*$ циклична для всех натуральных значений n ?

9. Доказать, что множество всех нильпотентных элементов кольца R образует идеал U и в R/U нет нильпотентных элементов.

10. Найти все делители нуля в кольце а) $\mathbb{Z}_n$; б) $\mathbb{C} \oplus \mathbb{C}$; в) $M_n(F)$; г) функций на отрезке $[0, 1]$; д) непрерывных функций $C[0, 1]$.

11. Доказать, что конечномерная алгебра без делителей нуля является алгеброй с делением (телом). Это же утверждение для конечного кольца.

12. Доказать, что $f = a_0 + a_1 x + \dots a_n x^n \in R[x]$ – делитель нуля $\Leftrightarrow \exists a \in R : af = 0$.

13. Доказать, что идеал $I \lhd R$ является максимальным $\Leftrightarrow$ R/I – поле.

14. Доказать, что идеал $I \lhd R$ является простым $\Leftrightarrow$ R/I – область целостности $\Leftrightarrow$ существует гомоморфизм $\phi : R \to F$ в некоторое поле и $I = Ker\phi$.

15. Найти все максимальные идеалы и все простые идеалы в кольцах а) $\mathbb{Z}$; б) $\mathbb{C}[x]$; в) $\mathbb{R}[x]$.

16. Найти все максимальные идеалы в кольце $C[0, 1]$.

17. Доказать, что в кольце $\mathbb{Z}$ нет минимальных идеалов. Привести несколько примеров колец, обладающих минимальными идеалами.

18. Привести пример кольца, где есть только один максимальный идеал.

19. Доказать, что всякий гомоморфизм поля в кольцо либо нулевой, либо есть изоморфизм на подполе.

20. Установить изоморфизм $\mathbb{R}[x]/(x^2 - 1) \cong \mathbb{R} \oplus \mathbb{R}$.

21. Для каких значений $a, b \in \mathbb{R}$ кольца $\mathbb{R}[x]/(x - a)$ и $\mathbb{R}[x]/(x - b)$ изоморфны ?

22. Описать факторкольцо $\mathbb{R}[x]/(x^2 + ax + b)$.

23. Является ли а) образ идеала; б) прообраз идеала при гомоморфизме идеалом ?

24. Доказать, что всякая конечная подгруппа мультипликативной группы поля является циклической.

25. Привести пример несовершенного поля.

Листок 1. Поля разложения.

1. Доказать, что над полем характеристики 0 неприводимый многочлен не имеет кратных корней. Верно ли это в характеристике p?

Пусть A - факториальное кольцо, K - его поле частных.

2. Назовем элемент $f \in A[X]$ примитивным, если его коэффициенты просты в совокупности. Доказать, что произведение примитивных многочленов - примитивный многочлен.

3. (Лемма Гаусса). Если $f \in A[X]$ приводим над K, то f разлагается в $A[X]$ в произведение многочленов меньшей степени.

4. (Признак Эйзенштейна). Пусть $f = a_0 X^n + a_1 X^{n-1} + \dots + a_n \in A[X]$. Предположим, что для некоторого неприводимого $p \in A$ выполнено: $p \not| a_0, p | a_i, i > 0, p^2 \not| a_n$. Тогда f неприводим над K.

5. Найти минимальный многочлен над $\mathbb{Q}$ для $\sqrt[n]{a}, a \in \mathbb{Q}$, такого что $|a| \notin \mathbb{Q}^p$ для любого простого $p \mid n$.

6. Найти минимальные многочлены следующих чисел над $\mathbb{Q}$:

а) $\sqrt{2}+\sqrt{3}$ б) $\sqrt{6+3\sqrt{2}}$ в) $\sqrt{\sqrt{2}+\sqrt{-2}}$

г) $\cos\frac{\pi}{12}$ д) $\cos\frac{\pi}{5}$ е) $\cos\frac{\pi}{10}$

7. (Квадратичные расширения). Доказать, что расширение полей $K \subseteq L$ имеет степень 2 тогда и только тогда, когда L есть поле разложения над K многочлена степени 2. Описать автоморфизмы L над K.

8. Описать поля разложения кубических многочленов.

9. Найти степень полей разложения следующих многочленов над $\mathbb{Q}$:

а) X^4-2 б) X^4+4 в) X^p-1, p - простое г) $X^{p^k}-1$

д)$(X^2-2)(X^2-3)(X^2-5)(X^2-7)$ е) $(X^3-2)(X^3-3)(X^3-5)$

10. Найти все подполя конечного поля $\mathbb{F}_{p^n}$.

11. Найти поля разложения многочленов над полем характеристики p:

а) $X^{p^k}-1$ б) X^p-X-a.

12. Найти степень поля разложения многочлена X^p-T над

а) $\mathbb{C}(T)$ б) $\mathbb{Q}(T)$ в) $\mathbb{Z}_p(T)$.

13. Доказать, что для любого простого p и любого $n \in \mathbb{N}$ существует неприводимый многочлен $f \in \mathbb{Z}_p[X]$ степени n.

Листок 2. Расширения Галуа.

1. Доказать, что если $K \subseteq L$ – расширение Галуа, $\alpha, \beta \in L$ сопряжены над K, то существует $\varphi \in \mathrm{Gal(L/K)}$ такой, что $\varphi(\alpha)=\beta$. Верно ли, что если $K \subseteq L$ – конечное сепарабельное расширение полей и α и β – элементы поля L, сопряженные над K, то существует автоморфизм L над K такой, что $\phi(\alpha)=\beta$?

2. Являются ли следующие расширения расширениями Галуа поля $\mathbb{Q}$? Если да, то описать группу Галуа.

а) $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ б) $\mathbb{Q}(\sqrt{6+3\sqrt{2}})$ в) $\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{-2}})$

г) $\mathbb{Q}(\sqrt[3]{2}+\sqrt{2})$ д) $\mathbb{Q}(\cos\frac{\pi}{12})$ е) $\mathbb{Q}(\cos\frac{\pi}{5})$

3. Доказать, что группа Галуа многочлена $f \in K[T]$ степени n естественно изоморфна подгруппе в S_n. Эта подгруппа лежит в A_n тогда и только тогда, когда дискриминант f принадлежит K^2.

4. Найти группу Галуа многочлена $T^n+X_1T^{n-1}+\cdots+X_n$ над полем $K(X_1,\cdots,X_n)$.

5. Доказать, что каждая конечная группа изоморфна группе Галуа некоторого конечного расширения Галуа.

6. Привести пример башни полей $K \subseteq L \subseteq M$, такой что расширения $K \subseteq L$, $L \subseteq M$ нормальны, а $K \subseteq M$ - ненормально. С помощью соответствия Галуа "перевести" эту ситуацию на язык групп.

7. Привести пример несепарабельного многочлена.

8. Описать группы Галуа многочленов степени 2 и 3.

9. При каких условиях поле разложения биквадратного трехчлена имеет степень 4 ? Описать в этом случае группу Галуа.

10. Описать все расширения Галуа поля $\mathbb{Q}$ с группами Галуа $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_4$.

11. Доказать, что каждое конечное расширение конечного поля является расширением Галуа и найти группу Галуа.

12. Описать группы Галуа многочлена T^4-5 над полями:

а) $\mathbb{Q}$ б) $\mathbb{Q}(\sqrt{5})$ в) $\mathbb{Q}(\sqrt{-5})$ г) $\mathbb{Q}(\sqrt{-1})$.

13. Доказать, что расширение $K \subseteq L$ нормально тогда и только тогда, когда для любого расширения $L \subseteq M$ и любого K-изоморфизма $\varphi: L \to M$ выполнено: $\varphi(L)=L$.

14. Доказать, что если степень поля L разложения многочлена fg над K равна произведению степеней полей L_1 раложения f и L_2 разложения g, то для групп Галуа имеем: $\mathrm{Gal(L/K)}=\mathrm{Gal(L_1/K)}\times\mathrm{Gal(L_2/K)}$.

15. Описать группы Галуа многочленов над $\mathbb{Q}$:

а) $(T^2-2)(T^2-3)(T^2-5)(T^2-7)$ б) $(T^3-2)(T^3-3)(T^3-5)$

16. Описать группу Галуа многочлена X^n-T над полем $\mathbb{C}(T)$.

17. Описать автоморфизмы поля $\mathbb{Q}(\sqrt[n]{a})$, $a \in \mathbb{Q}, a>0$.

18. Пусть G - конечная группа автоморфизмов поля L, $H \subseteq G$ - подгруппа. Доказать, что группа автоморфизмов поля L^H над L^G изоморфна $N_G(H)/H$.

Листок 3. Круговые расширения и конечные поля.

Круговым расширением поля K называется поле разложения многочлена $x^n - 1$ над полем K. Пусть ξ обозначает первообразный корень из 1 степени n и пусть $C_n(x)$ есть минимальный многочлен для ξ.

1. Пусть $\overline{C}_n(x) = \prod_\xi (x - \xi)$, где ξ пробегает все первообразные корни степени n из 1. Доказать, что над $\mathbb{Q}$

1) $x^n - 1 = \prod_{d|n} \overline{C}_d(x)$;

2) $\overline{C}_n(x)$ есть многочлен с целыми коэффициентами;

3) если p есть простое число, взаимно простое с n, то ξ^p является корнем многочлена $C_n(x)$ (рассмотреть редукцию по модулю p);

4) $\overline{C}_n(x) = C_n(x)$.

2. Показать, что над $\mathbb{Q}$ $C_2 = x+1$, $C_3 = x^2+x+1$, $C_4 = x^2+1$, $C_5 = x^4+x^3+x^2+x+1$, $C_6 = x^2-x+1$, $C_8 = x^4+1$, $C_9 = x^6+x^3+1$, $C_{10} = x^4-x^3+x^2-x+1$, $C_{12} = x^4-x^2+1$ и $C_p = x^{p-1} + x^{p-2} + \ldots + 1$, где p – простое.

3. Проверить, что расширение $\mathbb{Q}(\xi) : \mathbb{Q}$ есть расширение Галуа и найти его группу Галуа.

4. Над полем конечной характеристики многочлен $\overline{C}_n(x)$ может быть приводим. Разложить на неприводимые множители $\overline{C}_8(x)$ над полем $\mathbb{F}_3$.

5. Доказать, что отрезок длины x можно построить с помощью циркуля и линейки из данных отрезков длин $a, b, \ldots$ тогда и только тогда, когда x принадлежит нормальному расширению степени 2^m поля рациональных функция от величин $a, b, \ldots$.

6. Для каких значений n круговое расширение $\mathbb{Q}(\xi) : \mathbb{Q}$ имеет степень 2^m ?

7. Задача о построении правильного n-угольника приводит к числу

$$2cos\frac{2\pi}{n} = \xi + \xi^{-1}.$$

Вычислить степень $[\mathbb{Q}(\xi + \xi^{-1}) : \mathbb{Q}]$. При каких значениях n правильный n-угольник может быть построен с помощью циркуля и линейки ?

Всюду далее p обозначает простое число и $q = p^n$. Поле из q элементов обозначено $\mathbb{F}_q$.

8. Составить схему включения для подполей поля $\mathbb{F}_{2^{30}}$.

9. Доказать, что всякое отображение конечного поля в себя является полиномиальным отображением.

Укажем три способа явной реализации поля $\mathbb{F}_q$.

Первый способ. Пусть $f(x)$ есть неприводимый многочлен степени n над $\mathbb{F}_p$ и через α обозначим некоторый его корень. Тогда значения многочленов степени меньшей n от α образуют набор из p^n элементов, которые и составляют поле $\mathbb{F}_q$ относительно операций сложения и умножения в фактор-кольце $\mathbb{F}_p[x]/(f(x))$.

10. Составить таблицы сложения и умножения для конечных полей, заданных указанным способом для а) $p = 2$, $f(x) = x^2 + x + 1$, б) $p = 3$, $f(x) = x^2 + 1$.

11. Пусть $x \in \mathbb{F}_{16}$ – корень многочлена $x^4 + x + 1 \in \mathbb{F}_2[x]$. Найти все элементы в $\mathbb{F}_{16}$, сопряженные с x, над полем а) $\mathbb{F}_2$, б) $\mathbb{F}_4$.

Второй способ.

12. Доказать, что $\mathbb{F}_q$ есть круговое расширение с показателем $q - 1$ над всяким своим подполем.

Пусть ξ есть первообразный корень степени $q - 1$ из единицы над полем $\mathbb{F}_p$. Тогда $\mathbb{F}_q = \{0, \xi, \xi^2, \ldots, \xi^{q-1}\}$. Для вычислений в указанной реализации следует разложить многочлен $\overline{C}_{q-1} \in \mathbb{F}_p[x]$ на неприводимые множители и зафиксировать тот множитель, корнем которого является ξ.

13. Опишите полученную реализацию для поля $\mathbb{F}_9$. Установите изоморфизм между построенным полем и реализацией из задачи 10, б).

Третий способ.

Всякому многочлену $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ можно сопоставить матрицу A размера $n \times n$:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

Из линейной алгебры известно, что $f(A) = 0$, поскольку f есть характеристический многочлен матрицы A. Предположим, что f – неприводимый многочлен из $\mathbb{F}_p[x]$. Тогда все элементы поля $\mathbb{F}_q$ можно представить многочленами от матрицы A степени $< n$ с естественными операциями сложения и умножения.

14. Построить матричную реализацию для поля $\mathbb{F}_9$ и многочлена $x^2 + 1$.

15. При помощи матричной реализации доказать, что в реализации из задачи 13 имеем $\xi^6 + \xi = \xi^3$, где ξ – корень многочлена $x^2 + x + 2$ над полем $\mathbb{F}_3$.

Дополнительный листок.

Приложения функции Мебиуса.

Функция Мебиуса $\mu(n) = 1$, если $n = 1$; $= (-1)^k$, если $n = p_1p_1 \ldots p_k$ – различные простые; =0, если n делится на квадрат простого числа.

1. Доказать, что $\sum_{d|n} \mu(d) = 1$ при $n = 1$ и 0 при $n > 1$.

2. (аддитивная формула обращения Мебиуса.) Пусть f и g – две произвольные функции из $\mathbb{N}$ в M ($M = \mathbb{Z}, \mathbb{R}, F[x]$ и т.д.), связанные соотношением

$$f(n) = \sum_{d|n} g(d).$$

Тогда

$$g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d).$$

3. (мультипликативная формула обращения Мебиуса.) В условиях предыдущей задачи если функции связаны соотношением

$$f(n) = \prod_{d|n} g(d),$$

то

$$g(n) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}.$$

4. Используя аддитивную формулу обращения Мебиуса, доказать, что число $A_{m,q}$ неприводимых многочленов со старшим коэффициентом 1 степени m над полем из q элементов может быть вычислено по формуле

$$A_{m,q} = \frac{1}{m} \sum_{d|m} \mu(\frac{m}{d}) q^d.$$

5. Оцените вероятность того, что при достаточно больших значениях q случайно выбранный многочлен со старшим коэффициентом 1 степени m над полем из q элементов неприводим.

6. Используя мультипликативную формулу обращения Мебиуса, доказать, что для многочлена $C_n(x)$ деления круга над $\mathbb{Q}$ имеет место формула

$$C_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

7. Найти

1) Сумму корней степени n из 1;

2) Произведение первообразных корней степени n из 1;

3) Сумму первообразных корней степени n из 1.

Листок 4. Целые расширения колец.

1. Пусть A – целозамкнутая область, K – ее поле частных, L – расширение Галуа поля K, G – группа Галуа L над K и B – целое замыкание A в L. Показать, что $\sigma(B) = B \;\; \forall \sigma \in G$ и $A = B^G$.

2. Пусть $A \subset B$ – конечное расширение целозамкнутых колец, K – поле частных кольца A, L – поле частных кольца B и известно, что расширение $K \subset L$ сепарабельно. Доказать, что существует целозамкнутое кольцо C, конечная группа его автоморфизмов G и подгруппа H группы G такие, что $C^G = A$ и $C^H = B$.

3. Пусть A – область целостности, а K – ее поле частных и известно, что $\forall\; x \in K \;\; x \in A$ или $x^{-1} \in A$ (допускаются оба включения).

1) Привести пример такой ситуации;

2) Доказать, что A целозамкнута.

4. Пусть A – подкольцо области целостности B, а C – целое замыкание A в B. Пусть $f, g \in B[x]$ и известно, что $fg \in C[x]$, причем старший коэффициент fg равен 1. Доказать, что $f, g \in C[x]$.

5. В обозначениях предыдущей задачи показать, что целое замыкание $A[x]$ в $B[x]$ есть $C[x]$. В частности, если A есть целозамкнутая область, то область $A[x]$ также целозамкнута.

6. Пусть A – область целостности и G – конечная группа ее автоморфизмов.

1) Доказать, что если A целозамкнута, то и подкольцо инвариантных элементов A^G целозамкнуто;

2) Привести пример, где A^G целозамкнуто, а A – нет;

3) Доказать, что A цело над A^G.

7. Какие из следующих колец являются целозамкнутыми :

1) $\mathbb{C}[x, y]/(x - y^2)$; 2) $\mathbb{C}[x, y]/(x^3 - y^2)$; 3) $\mathbb{C}[x, y, z]/(x^2 - yz)$?

8. Описать кольцо целых алгебраических чисел в поле $\mathbb{Q}(\sqrt{d})$, где d – целое число, свободное от квадратов.

9. Пусть $d \in \mathbb{C}[x]$ есть многочлен без кратных корней. Описать целое замыкание кольца $\mathbb{C}[x]$ в поле $\mathbb{C}(x)(\sqrt{d})$.

10. Рассмотрим в поле $\mathbb{Q}(\xi)$, где $\xi^p = 1$ и p – простое число, элемент $v = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}$, целый над $\mathbb{Z}$.

1) Показать, что модуль дискриминанта многочлена $x^{p-1} + x^{p-2} + \ldots + 1$ есть степень числа p (рассмотреть редукции по всевозможным простым модулям) и вывести отсюда, что знаменателями рациональных чисел $a_0, a_1 \ldots a_{p-2}$ могут быть только степени числа p;

2) Напомним, что два элемента кольца называются ассоциированными ($a \sim b$), если одно из них равно второму, умноженному на обратимый элемент кольца. Проверить, что в кольце целых поля $\mathbb{Q}(\xi)$ имеют место ассоциированности :

$$1 - \xi \sim 1 - \xi^k \quad (k = 1, 2 \ldots p - 1), \qquad p \sim (1 - \xi)^{p-1};$$

3) Доказать, что если какое-либо целое рациональное число делится на $(1 - \xi)$, то оно делится и на p;

4) Вместо разложения числа v по степеням ξ рассмотреть его разложение по степеням $(1 - \xi)$ и доказать, что коэффициенты $a_0, a_1 \ldots a_{p-2}$ на самом деле являются целыми рациональными числами.

11. Пусть Γ – подполугруппа с нулем в $\mathbb{Z}_+$. Найти критерий целозамкнутости полугруппового кольца $\mathbb{C}(\Gamma)$.

12. Тот же вопрос для конечно порожденной подполугруппы в $\mathbb{Z}_+ \times \mathbb{Z}_+$.

Листок 5. Нетеровы кольца и модули.

1. Являются ли нетеровыми следующие кольца?

а) кольцо функций, непрерывных на отрезке;

б) кольцо степенных рядов $\mathbf{k}[[X_1]]$;

в) кольцо степенных рядов от z с бесконечным радиусом сходимости;

г) кольцо ростков функций, голоморфных в точке $z = 0$;

д) кольцо таких $f \in \mathbf{k}[z]$, что $f^{'}(0) = f^{''}(0) = \cdots = f^{(k)}(0) = 0$;

е) кольцо таких многочленов $f \in \mathbf{k}[z, w]$, что $\frac{\partial f}{\partial w}|_{z=0} = 0$;

ж) кольцо $\mathbf{k}[X_1, \cdots, X_k, \cdots]$.

2. Верно ли, что подкольцо нетерова кольца - нетерово?

Идеал $\mathfrak{q}$ кольца A называется *неприводимым*, если для любых идеалов $\mathfrak{q}_1, \mathfrak{q}_2$ из $\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ следует $\mathfrak{q} = \mathfrak{q}_1$ или $\mathfrak{q} = \mathfrak{q}_2$. Идеал называется *примарным*, если все делители 0 в фактор-кольце $A/\mathfrak{q}$ являются нильпотентами. *Радикалом* идеала $\mathfrak{q}$ называется множество $\sqrt{\mathfrak{q}}$ элементов $a \in A$ таких, что для некоторого $k \in \mathbb{N}$ $a^k \in \mathfrak{q}$.

3. Доказать, что радикал идеала является идеалом.

4. Доказать, что радикал примарного идеала $\mathfrak{q}$ прост. В этом случае говорят, что $\mathfrak{q}$ является $\sqrt{\mathfrak{q}}$-*примарным* идеалом.

5. Если $\mathfrak{p}$ - простой идеал, $\mathfrak{q}_1, \mathfrak{q}_2$ - $\mathfrak{p}$-примарные, то $\mathfrak{q}_1 \cap \mathfrak{q}_2$ - тоже $\mathfrak{p}$-примарный идеал.

6. (Теорема Ласкера-Нетер и примарное разложение).

а) В нетеровом кольце любой идеал есть пересечение конечного числа неприводимых.

б) В нетеровом кольце каждый неприводимый идеал примарен.

в) В нетеровом кольце каждый идеал есть пересечение конечного числа примарных идеалов с попарно различными радикалами.

7. В нетеровом кольце для любого идеала $\mathfrak{a}$ существует такое $k \in \mathbb{N}$, что $(\sqrt{\mathfrak{a}})^k \subseteq \mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$.

A-модуль M называется нетеровым, если любая возрастающая цепочка подмодулей в M стабилизируется.

8. Доказать, что модуль M нетеров тогда и только тогда, когда любой подмодуль $N \subseteq M$ конечно-порожден. Следовательно, конечно-порожденный модуль над нетеровым кольцом нетеров.

Композиционным рядом длины n модуля M называется максимальная цепочка вида $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$, где все включения строгие.

9. Если модуль M обладает композиционным рядом, то он нетеров а также любая убывающая цепочка подмодулей стабилизируется (такие модули называются *артиновыми*).

10. Все композиционные ряды имеют одинаковую длину, которая обозначается $l(M)$ и называется *длиной модуля.*

11. Если A - нетерово кольцо, $\mathfrak{m}$ - такой идеал, что элементы $A \setminus \mathfrak{m}$ обратимы в A, $\mathfrak{a}$ - идеал, содержащий $\mathfrak{m}^k$, то A-модуль $A/\mathfrak{a}$ обладает композиционным рядом.

Листок 6. Аффинные алгебраические многообразия и схемы – первое знакомство.

Пусть $\mathbb{A}^n$ есть n-мерное аффинное пространство. Во всех задачах кроме задач 2, 3, 13, 14 и 18 основное поле будет предполагаться полем комплексных чисел.

1. Привести пример аффинного подмногообразия в $\mathbb{A}^2$, на котором имеется непостоянная обратимая регулярная функция.

2. Пусть A – нетерово кольцо с единицей. Доказать, что $f \in A$ – обратим тогда и только тогда, когда f не обращается в ноль ни в одной точке $\mathrm{Spec}\, A$.

3. Пусть R – нетерово кольцо и I – идеал в R. Доказать, что среди простых идеалов, содержащих I, имеется только конечное число минимальных.

4. Доказать, что аффинное алгебраическое многообразие, определяемое конечномерной алгеброй, состоит из конечного числа точек.

5. Доказать, что неприводимое аффинное многообразие связно (в топологии Зарисского). Верно ли обратное ?

6. Рассмотрим аффинное многообразие, заданное в $\mathbb{A}^n$ одним уравнением $f(X_1, \ldots, X_n) = 0$. Такие многообразия называют *гиперповерхностями*. Для каких многочленов f соответствующая гиперповерхность а) неприводима б) приведена ?

7. Показать, что при естественном отождествлении $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ топология Зарисского на $\mathbb{A}^2$ не совпадает с произведением топологий множителей $\mathbb{A}^1$.

8. Верно ли, что отображение аффинных алгебраических многообразий, непрерывное в топологии Зарисского, является морфизмом ?

9. Показать, что проекция на одну из координатных осей $\mathbb{A}^n \to \mathbb{A}^1$ не всегда переводит замкнутые множества в замкнутые.

10. *Скрученной кубической кривой* называется кривая $Y = \{(t, t^2, t^3) \mid t \in \mathbb{C}\} \subset \mathbb{A}^3$. Найти образующие идеала $I(Y)$.

11. Какие из следующих аффинных многообразий изоморфны друг другу : (1) $\mathbb{A}^1$; (2) $\{y = x^2\} \subset \mathbb{A}^2$; (3) $\{y^2 = x^2 - 2x + 1\} \subset \mathbb{A}^2$; (4) $\{y^2 = x^3\} \subset \mathbb{A}^2$; (5) $Ox \cup Oy \subset \mathbb{A}^2$; (6) $Ox \cup \{y = x^2\} \subset \mathbb{A}^2$; (7) $Ox \cup \{x = y^2\} \subset \mathbb{A}^2$; (8) $\{x = y^2\} \cup \{y = x^2\} \subset \mathbb{A}^2$; (9) $Ox \cup Oy \cup \{x = y\} \subset \mathbb{A}^2$; (10) $Ox \cup Oy \subset \mathbb{A}^3$; (11) $Ox \cup Oy \cup Oz \subset \mathbb{A}^3$.

12. Пусть $Y = \{x^2 - yz = 0, xz - x = 0\} \subset \mathbb{A}^3$. Найти неприводимые компоненты Y и описать их простые идеалы.

13. Привести пример неприводимого многочлена $f \in \mathbb{R}[x, y]$, множество нулей которого приводимо в $\mathbb{R}^2$.

14. Доказать, что над алгебраически незамкнутым полем всякое аффинное многообразие является гиперповерхностью.

15. Пусть $I \subset \mathbb{C}[x, y, z, w]$ – идеал, порожденный минорами размера 2×2 матрицы

$$\begin{pmatrix} x & y & z \\ y & z & w \end{pmatrix}$$

и пусть $S = \mathbb{C}[x, w]$, $R = \mathbb{C}[x, y, z, w]/I$.

1) Доказать, что R – свободный конечно порожденный S-модуль;

2) Построить вложение $R \to \mathbb{C}[X, Y]$;

3) Показать, что многообразие $\mathrm{Spec}\, R$ приведено и неприводимо.

16. Рассмотрим пересечение многобразий $y = a$ и $y = x^n$ в $\mathbb{A}^2$. Для каких значений n и a это пересечение а) приведено б) неприводимо ?

17. Рассмотрим гиперповерхность C, заданную уравнением $x^2 = y^2 z$ в $\mathbb{A}^3$. Пусть C_a обозначает прообраз в C точки $z = a$ при проекции на ось Oz. Структуру схемы на C_a определяет фактор-кольцо $\mathbb{C}[C]/(z - a)\mathbb{C}[C]$. Для каких значений a схема C_a а) приведена б) неприводима ?

18. Описать замыкания точек и регулярные функции на схеме $\mathrm{Spec}\, \mathbb{Z}$.

Листок 7. Отображения аффинных многообразий.

1. Существует ли доминантный морфизм

а) из $\mathbb{A}^2$ в $\mathbb{A}^3$;

б) из $\mathbb{A}^1$ в $\mathbb{A}^1 \setminus \{0\}$?

2. Существует ли сюрьективный морфизм из $\mathbb{A}^1 \setminus \{0\}$ в $\mathbb{A}^1$?

3. Морфизм $\varphi : X \to Y$ называется *вложением*, если образ $\varphi(X)$ замкнут и $\varphi : X \to \varphi(X)$ - изоморфизм. Доказать, что любой морфизм является композицией вложения в $\mathbb{A}^n$ и проекции $\mathbb{A}^n$ на $\mathbb{A}^m$ (указание: рассмотреть график).

4. Описать образ морфизма $\varphi : \mathbb{A}^2 \to \mathbb{A}^3$, $\varphi(x, y) = (x, xy, xyz)$.

5. Доказать, что каждый регулярный автоморфизм $\mathbb{A}^1$ имеет вид $x \to ax + b$ для некоторых $a, b \in \mathbf{k}, a \neq 0$.

6. Доказать, что если полиномы $f_1, \cdots, f_n \in \mathbf{k}[T_1, \cdots, T_n]$ задают автоморфизм $\mathbf{A}^n \to \mathbf{A}^n$, то их якобиан $J = \frac{\partial(f_1, \cdots, f_n)}{\partial(T_1, \cdots, T_n)}$ принадлежит k.

7. Доказать, что для любых $a, b \in k^*, P \in k[T]$ пара полиномов $ax, by + P(x)$ определяет автоморфизм $\mathbb{A}^2$ и такие автоморфизмы образуют группу.

8. Найти область определения функции $\frac{1-y}{x}$ на кривой $x^2 + y^2 = 1$.

9. Доказать, что открытое подмножесто $\mathbb{A}^3 \setminus Ox$ не аффинно.

10. Для каждой из следующих кривых $X \subset \mathbb{A}^2$ построить явно бирациональный изоморфизм $\mathbb{A}^1 \to X$, найти области определения изоморфизма и обратного к нему. Описать множество рациональных точек кривой X.

а) $X : y^2 = x^2 + x^3$; б) $X : x^3 = y^3 - y^4$; в) $X : x^2 + y^2 = 5$.

11. Пусть $f \in k[T_1, \cdots, T_n]$ - полином степени 2 без свободного члена, $X = \mathcal{V}(f)$ - квадрика. Пусть L - любая гиперплоскость не проходящая через начало координат O. Для точки $x \in X$ определим $\pi(x)$ как точку пересечения прямой Ox с L. Доказать, что отображение $\pi : X \to L$ рационально и найти его область определения. При каком условии π будет бирациональным изоморфизмом?

Многообразие называется *рациональным*, если оно бирационально изоморфно $\mathbb{A}^k$ для некоторого k.

12. Пусть гиперповерхность $X \subseteq \mathbb{A}^n$ задана уравнением $F_{m-1}(x_1, \cdots, x_n) + F_m(x_1, \cdots, x_n) = 0$, где F_{m-1}, F_m - ненулевые однородные формы степеней $m-1$ и m соответственно. Доказать, что если X неприводима, то она и рациональна (указание: построить отображение как в задаче 11).

13. Доказать, что $\operatorname{Spec} R$ из задачи 15 листка 6 рационально.

14. Доказать, что в характеристике 0 любое аффинное многообразие бирационально изоморфно гиперповерхности в $\mathbb{A}^n$ (указание: воспользоваться теоремой о примитивном элементе).

Пусть X, Y, Z - аффинные многообразия, $\varphi : X \to Y, \psi : Z \to Y$ - морфизмы. *Расслоенным произведением* X и Z над Y называется прообраз диагонали $\Delta = \{(y, y)\} \subseteq Y \times Y$ относительно морфизма $\varphi \times \psi : X \times Z \to Y \times Y$. Оно обозначается $X \times_Y Z$ и задается как $\{(x, z) | \varphi(x) = \psi(z)\} \subseteq X \times Z$.

15. а) Верно ли, что $X \times_Y Z$ всегда приведено?

б) Если X, Y, Z неприводимы, верно ли, что $X \times_Y Z$ неприводимо?

Листок 8. Размерность и касательное пространство.

Гладкие и особые точки.

Пусть $\mathbb{A}^n$ есть n-мерное аффинное пространство. Во всех задачах основное поле будет предполагаться полем комплексных чисел.

1. Доказать, что всякое подмногообразие коразмерности один в $\mathbb{A}^n$ является гиперповерхностью.

2. Описать простой идеал, отвечающий кривой $\{x = t^3, y = t^4, z = t^5 \mid t \in \mathbb{C}\}$ в $\mathbb{A}^3$. Доказать, что этот идеал не может быть порожден двумя элементами (в этой ситуации говорят, что кривая не является *полным пересечением*).

3. Показать, что не всякое подмногообразие коразмерности один на неприводимом аффинном многообразии X может быть выделено в X одним уравнением.

4. Пусть $f_1, \ldots, f_k, g$ – рациональные функции на $\mathbb{A}^n$. Доказать, что если g постоянна на поверхностях уровня семейства $\{f_1, \ldots, f_k\}$, то она представима в виде рациональной дроби от $f_1, \ldots, f_k$.

5. Пусть $\{f = 0\}$ – гиперповерхность в $\mathbb{A}^n$, проходящая через ноль. Сформулировать условие гладкости этой гиперповерхности в точке ноль в терминах коэффициентов многочлена f.

6. Доказать, что гиперповерхность 2-го порядка, имеющая особую точку, является конусом.

7. Доказать, что если гиперповерхность 3-го порядка имеет две особые точки, то прямая, их соединяющая, лежит на гиперповерхности.

8. Описать плоские кривые 3-го порядка, имеющие три различных особых точки.

9. Привести пример двух неизоморфных плоских кривых C_1 и C_2 таких, что на них есть по одной особой точке P_1 и P_2 и $C_1 \setminus P_1 \cong C_2 \setminus P_2 \cong \mathbb{A}^1 \setminus \{0\}$.

10. Найти множество особых точек гиперповерхностей а) $xy + z^3 + w^2 = 0$; б) $x^3 + y^2z + w^5 = 0$ в $\mathbb{A}^4$.

11. *Аффинной алгебраической группой* называется аффинное многообразие G с заданной на нем структурой группы такой, что отображение умножения $G \times G \to G$ и вычисление обратного элемента $G \to G$ являются морфизмами. Доказать, что аффинная алгебраическая группа есть гладкое многообразие.

12. Доказать, что множество всех а) невырожденных; б) унимодулярных; в) ортогональных; г) симплектических матриц фиксированного размера есть аффинная алгебраическая группа и вычислить ее размерность (Указание: описать касательное пространство в единице).

13. Пусть $X \subset \mathbb{A}^n$ – неприводимое аффинное подмногообразие, $x = (0, \ldots, 0) \in X$, $\mathbb{A}^{n+1} = \mathbb{A}^n \times \mathbb{A}^1$, $\tilde{X} = \{(a,t) \mid a \in \mathbb{A}^n, t \in \mathbb{A}^1, ta \in X\}$ и $\phi : \tilde{X} \to \mathbb{A}^1$, $\psi : \tilde{X} \to \mathbb{A}^n$ – проекции.

а) Доказать, что $\tilde{X}$ состоит из двух неприводимых компонент $\tilde{X} = \tilde{X}_1 \cup \tilde{X}_2$, $\tilde{X}_1 = \overline{\phi^{-1}(\mathbb{A}^1 \setminus \{0\})}$, $\tilde{X}_2 = \{(a,0) \mid a \in \mathbb{A}^n\}$.

б) Пусть ϕ_1 и ψ_1 – ограничения проекций на $\tilde{X}_1$. Показать, что $\psi_1(\tilde{X}_1)$ есть замыкание множества точек на всех секущих многообразия X, проходящих через x.

Множество $C_x = \psi_1\phi_1^{-1}(0)$ называется *касательным конусом* к X в точке x.

в) Пусть $X = \{F_1 = 0, \ldots, F_m = 0\} \subset \mathbb{A}^n$. Задать уравнениями касательных конус в нуле к X.

г) Пусть T_x есть касательное пространство к X в точке x. Доказать, что $C_x \subset T_x$ и для гладких точек $C_x = T_x$.

д) Найти касательное пространство и касательный конус в нуле к кривой $\{x^2 = y^3\} \subset \mathbb{A}^2$.

г) Описать касательные конуса к точкам плоской кривой.

14. Пусть $Y = \{f = 0\}$ – кривая в $\mathbb{A}^2$, проходящая через начало координат и $f = f_1 + f_2 + \ldots + f_d$, где f_i – однородный многочлен степени i. *Кратностью* $\mu_0(Y)$ точки 0 называется наименьшее число r такое что $f_r \neq 0$. Это же определение подходит для любой точки после параллельного переноса ее в начало координат.

Пусть Y и Z – две различные кривые в $\mathbb{A}^2$, заданные уравнениями $f = 0$ и $g = 0$ и пусть $P \in Y \cap Z$. Определим *кратность пересечения* $(Y * Z)_P$ кривых Y и Z в точке P как длину $\mathbb{C}[x,y]_{(P)}$-модуля $\mathbb{C}[x,y]_{(P)}/(f,g)$.

а) Показать, что кратность пересечения конечна и что $(Y * Z)_P \geq \mu_P(Y)\mu_P(Z)$. (воспользоваться задачей 11 листка 5). б) Показать, что для всех кроме конечного числа прямых L, проходящих через P, имеет место равенство $(L * Y)_P = \mu_P(Y)$.

Листок 9. Конечные морфизмы, нормальные многообразия.

1. Доказать, что над полем $\mathbb{C}$ в смысле "обычной" топологии прообраз компакта при конечном морфизме является компактом (морфизмы с этим свойством называют *собственными*).

2. (Лемма Нетер о нормализации) Доказать, что для любого неприводимого многообразия X размерности n существует конечный морфизм X на $\mathbb{A}^n$.

3. Нормальны ли следующие кривые ? Если нет, построить нормализацию.

а) $y^2 = x^2 + x^3$; б) $x^3 = y^3 - y^4$; в) $y^2 = x^5 - x^2$.

4. Доказать, что конус $x_1^2 + \ldots + x_n^2 = 0$ в $\mathbb{A}^n$ нормален при $n \geq 3$.

5. Доказать, что кривая $F_n(x,y) + F_{n-1}(x,y) = 0$ ненормальна, если F_n, F_{n-1} – однородные формы степеней $n, n-1$ соответственно, $n \geq 3$.

6. С помощью критерия нормальности гиперповерхности проверить нормальность следующих многообразий:

а) $x_1^d + \ldots + x_n^d = 0$;

б) $x^3 + y^2z + w^5 = 0$;

в) $x^2y^2 + y^2z^2 + z^2w^2 - xyzw = 0$;

г) $x^3 + y^3 + z^3 + a(x+y+z)^3 = 0$, $a \in k$ – параметр.

Назовем *степенью* конечного отображения $\phi : X \to Y$ неприводимых многообразий X, Y $deg_\phi = dim_{k(Y)} k(X)$. Назовем морфизм ϕ *сепарабельным*, если расширение полей $k(Y) \subset k(X)$ сепарабельно.

7. Доказать, что если Y нормально, то для любого $y \in Y$ $\mid \phi^{-1}(y) \mid \leq deg\phi$. Верно ли это без предположения о нормальности Y ?

Назовем точку $Y \in Y$ *точкой ветвления*, если $\mid \phi^{-1}(y) \mid < deg\phi$.

8. В условиях предыдущей задачи доказать, что множество точек ветвления замкнуто в Y, а если ϕ – сепарабелен, то собственно.

Пусть конечная группа действует автоморфизмами аффинного многообразия X и H – подгруппа в G. Обозначим через X/G аффинное многообразие $Speck[X]^G$, а через $\pi_{X,G}$ морфизм факторизации $X \to X/G$, определенный вложением $k[X/G] = k[X]^G \subset k[X]$. Аналогично определим $\pi_{X,H} : X \to X/H$. Наконец через $\pi_{X,G,H}$ обозначим морфизм $X/H \to X/G$, определенный вложением $k[X]^G \subset k[X]^H$.

9. Пусть $\phi : Y \to Z$ – конечный морфизм нормальных аффинных многообразий. Доказать, что существует нормальное аффинное многообразие X, конечная группа его автоморфизмов G и подгруппа $H \subset G$ такие, что имеются морфизмы ψ и ξ, определяющие коммутативную диаграмму:

$$\begin{array}{ccccc} X & \xrightarrow{\pi_{X,H}} & X/H & \xrightarrow{\xi} & Y \\ & & \downarrow \pi_{X,G,H} & & \downarrow \phi \\ X & \xrightarrow{\pi_{X,G}} & X/G & \xrightarrow{\psi} & Z \end{array}$$

10. Каково условие неразветвленности конечного морфизма $\pi_{X,G,H} : X/H \to X/G$ в точке $\pi_{X,G}(x)$?

Теорема Гильберта об инвариантах. Пусть X – аффинное многообразие, $G \subset Aut(X)$ – конечная группа, порядок G не делится на $char\ k$.

11. Определим оператор Рейнольдса $\natural$ на $k[X]$: $f^\natural = \frac{1}{|G|}(\sum_{g \in G} g(f))$. Доказать, что если $f \in k[X]^G$, то для любого $h \in k[X]$ $(fh)^\natural = fh^\natural$.

12. Доказать, что если V – линейное пространство, действие $G : V$ линейно, $f_1, \ldots, f_n$ – однородные многочлены, порождающие идеал в $k[V]$, порожденный такими $f \in k[V]^G$, что $f(0) = 0$, то $k[V]^G = k[f_1^\natural, \ldots, f_n^\natural]$.

13. Доказать, что алгебра $k[X]$ имеет систему образующих, линейная оболочка которых G-инвариантна.

14. Вывести из задач 11, 12, 13, что алгебра $k[X]^G$ конечно порождена.

15. Построить пространство орбит для группы, состоящей из всех диагональных матриц порядка n, элементы которых – корни степени m из 1.

16. Описать образующие инварианты для группы $\{\pm E\} \subset GL(V)$.

17. Построить пространство орбит V/G для $G = \{diag(\mu, \mu^{-1}) \mid \mu^m = 1\}$, $V = \mathbb{A}^2$.

18. В условиях предыдущей задачи построить пространство орбит V/H, где H – группа, порожденная G и оператором, переставляющим базисные вектора.

Экзамен по коммутативной алгебре.

17 мая 1998 года.

1. Найти минимальный многочлен элемента $\lambda = \alpha^2+\alpha+1$ в поле $\mathbb{Q}(\alpha)$, $\alpha^3-\alpha-1=0$.

2. Описать все расширения Галуа поля $\mathbb{Q}$ с группой Галуа $\mathbb{Z}_6$. Привести явный пример такого расширения.

3. Найти образ морфизма:

а) $\mathbb{C}^3 \to \mathbb{C}^3$, $(x, y, z) \to (xyz, y^3z, x^3z^2)$;

б) $\mathbb{C}^3 \to \mathbb{C}^6$, $(x, y, z) \to (x^2, y^2, z^2, xy, yz, zx)$.

4. Привести пример целозамкнутой подалгебры в $\mathbb{C}[x, y]$, содержащей мономы y^5, xy^6, x^3y^5, но не содержащей моном x^4y^5.

5. а) Описать подмногообразие особых точек в многообразии вырожденных матриц размера 3×3.

б) Аналогичное задание для матриц размера $n \times n$.

6. Пусть $M_{p\times q}$ – аффинное пространство матриц размера $p \times q$. Рассмотрим морфизм

$$\phi : M_{1\times 2} \times M_{2\times 2} \to M_{1\times 2}, \qquad \phi(A, B) = AB.$$

а) Описать неприводимые компоненты замкнутого подмногообразия $\phi^{-1}(0, 0)$. Найти задающие их уравнения и размерности.

б) Приведена ли схема $\phi^{-1}(0, 0)$?

7. Для всякого идеала $I \lhd k[x_1, \dots, x_n]$ определим его *проективизацию* $\tilde{I} \lhd k[x_0, x_1, \dots, x_n]$ как идеал, порожденный однородными многочленами $F(x_0, x_1, \dots, x_n)$, такими что $F(1, x_1, \dots, x_n) \in I$. Пусть $I = (x_1^2 + x_2, x_1^2 + x_3) \lhd k[x_1, x_2, x_3]$.

а) Доказать, что $\tilde{I}$ не порождается $x_1^2 + x_2x_0, x_1^2 + x_3x_0$.

б) Найти какую-нибудь систему порождающих идеала $\tilde{I}$.

8. а) При каком условии на многочлен $F \in \mathbb{C}[x_1, \dots, x_n]$ гиперповерхность X, заданная уравнением $y^2 = F(x_1, \dots, x_n)$, неприводима и нормальна ?

б) Описать нормализацию многообразия X.

9. а) Доказать, что группа $SL_2(\mathbb{C})$ рациональна как аффинное алгебраическое многообразие. Построить явно бирациональный изоморфизм этого многообразия и $\mathbb{C}^3$.

б) Доказать, что $SL_2(\mathbb{C})$ и $\mathbb{C}^3$ не изоморфны.

Литература

[1] Атья М., Макдональд И., Введение в коммутативную алгебру. М.: Мир, 1972.

[2] ван дер Варден Б. Л., Алгебра. М.: Наука, 1979 (главы 6, 8, 15, 16,17).

[3] Винберг Э. Б. Лекции по алгебре. Второй курс, первый и второй семестр. Издательство МК НМУ, Москва, 1995.

[4] Винберг Э. Б. Онищик А. Л. Семинар по группам Ли и алгебраическим группам. М.: Наука, 1988 (глава 2).

[5] Крафт Х. Геометрические методы в теории инвариантов. М.: Мир, 1987 (приложение 1).

[6] Шафаревич И. Р. Основы алгебраической геометрии. М.: Наука, 1988 (том 1 глава 1 п. 1, 2, 3).

[7] Хамфри Дж. Линейные алгебраические группы. М.: Наука, 1980 (глава 1).

[8] Хартсхорн Р. Алгебраическая геометрия. М.: Мир, 1981. (глава 1).

[9] Eisenbud D. Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics 150, Springer 1996.