Группы подстановок и разрешимость

1.1. Подстановка $\sigma \in S_n$ называется циклом длины k и обозначается $(i_1 i_2 \dots i_k)$, если $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \dots,\ \sigma(i_k) = i_1$ и на остальных элементах $\sigma(j) = j$. Два цикла σ_1 и σ_2 называются независимыми, если множества переставляемых σ_1 и σ_2 элементов не пересекаются. Количество k переставляемых циклом σ элементов называется длиной цикла σ. Покажите, что всякая подстановка из S_n однозначно разлагается в произведение независимых циклов. С помощью этого утверждения докажите, что порядок произвольной подстановки есть наименьшее общее кратное длин независимых циклов из ее разложения.

[Напомним, что порядком $\mathrm{ord}(g)$ элемента g группы G называется наименьшее натуральное k, такое что $g^k = e_G$. Если такого натурального нет, то по определению $\mathrm{ord}(g) = \infty$. Порядок элемента g - это число элементов в циклической подгруппе $\langle g \rangle \equiv \{e,\ g,\ g^2, \dots\}$, порожденной элементом g.]

1.2. Для любого цикла $(i_1 i_2 \dots i_k)$ и любой подстановки $\tau \in S_n$ имеет место:

$$\tau \circ (i_1 i_2 \dots i_k) \circ \tau^{-1} = (\tau(i_1)\tau(i_2) \dots \tau(i_k)).$$

1.3. Рассмотрим действие S_n на себе сопряжениями:

$$\mathrm{Ad} : S_n \to \mathrm{Aut}\, S_n,\ \ \tau \mapsto \mathrm{Ad}_\tau : S_n \to S_n,\ \ \mathrm{Ad}_\tau(\sigma) = \tau \circ \sigma \circ \tau^{-1}.$$

Используя результат предыдущей задачи, покажите, что число орбит (или, что то же, число классов эквивалентности $\sigma_1 \sim_{\mathrm{Ad}} \sigma_2 \Leftrightarrow \exists \tau : \sigma_2 = \mathrm{Ad}_\tau(\sigma_1)$) этого действия равно числу неупорядоченных разбиений n в сумму натуральных чисел.

1.4. Проверьте следующие сформулированные на первой лекции предложения:
1). Группа S_n порождается транспозициями (то есть, по определению, всеми циклами длины 2).
2). Группа A_n порождается произведениями пар транспозиций.
3). Группа A_n порождается всеми циклами длины 3.
4). Если $n \geq 5$, то A_n порождается произведениями пар независимых транспозиций.

1.5. Для любой группы G коммутант $[G, G] \equiv G'$ есть наименьшая нормальная подгруппа, факторгруппа по которой абелева.

1.6.
1).Для любого натурального n, $S_n' = A_n$.
[Легко убедиться - например, перебором делителей числа 6 - что $[S_3, S_3] = A_3$. Значит, S_n' содержит все тройные циклы. Также, в силу **1.5.**, $S_n' \subseteq A_n$.]
2).$A_4' = V_4$ - четверная группа Клейна ($V_4 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}$).
3). Если $n \geq 5$, то $A_n' = A_n$ (и, значит, S_n неразрешима при $n \geq 5$).

1.7. Если подгруппа $G \subseteq S_n$ содержит все транспозиции и действует транзитивно на $\{1, \dots n\}$ (то есть любые две точки связаны подстановкой из G), то $G = S_n$.

1.8.
1). Всякая подгруппа разрешимой группы разрешима.
2). Прямое произведение двух разрешимых групп разрешимо.
3). Если группа H разрешима и если существует сюръективный гомоморфизм $\varphi : G \to H$ с абелевым ядром, то G разрешима.
4). Если G разрешима и $\varphi : G \to H$ сюръективен, то H разрешима.

1.9. Для произвольной группы G обозначим

$$G^{\mathrm{ab}} = G/[G, G].$$

Факторгруппа G^{ab} абелева и называется естественной абелианизацией группы G. Пусть $\pi : G \to G^{\mathrm{ab}}$ - каноническая проекция. Покажите, что для любой абелевой группы H и любого гомоморфизма $\varphi : G \to H$ существует единственный гомоморфизм $\Phi : G^{\mathrm{ab}} \to H$ такой, что $\varphi = \Phi \circ \pi$.

1.10. Для любого гомоморфизма $\psi : G_1 \to G_2$ существует естественный гомоморфизм $\psi^{\mathrm{ab}} : G_1^{\mathrm{ab}} \to G_2^{\mathrm{ab}}$, а соответствие $\psi \mapsto \psi^{\mathrm{ab}}$ сохраняет композицию и переводит тождественные гомоморфизмы в тождественные (иначе говоря, ab - функтор из категории групп в категорию абелевых групп).

Кольца, идеалы, гомоморфизмы

2.1. Для ненулевого кольца A следующие утверждения эквивалентны:
1). A - поле.
2). В A есть только два идеала - нулевой идеал и идеал (1) (то есть совпадающий с A).
3). Любой гомоморфизм из A в ненулевое кольцо инъективен.

2.2. Пусть $T \subset A$ - некоторое подмножество. Идеал $(T) = \{\sum a_i t_i \mid a_i \in A,\ t_i \in T\}$, состоящий из всех конечных линейных комбинаций элементов множества T, называется идеалом, порожденным T. Докажите, что (T) - наименьший по включению идеал, содержащий T.

2.3. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $n \geq 2$ - семейство попарно взаимно простых идеалов A (т.е. $i \neq j \Rightarrow \mathfrak{a}_i + \mathfrak{a}_j = (1)$). Тогда:
1). $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \ldots \mathfrak{a}_n$;
2). $A/(\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n) \simeq \prod_{i=1}^{n} (A/\mathfrak{a}_i)$.

2.4. Пусть A, B - коммутативные кольца. Тогда всякий идеал в прямом произведении $A \times B$ имеет вид $\mathfrak{a} \times \mathfrak{b}$, где $\mathfrak{a}, \mathfrak{b}$ - идеалы в сомножителях.

2.5. Всякий простой идеал в прямом произведении $A \times B$ имеет вид $\mathfrak{p} \times (1)$ или $(1) \times \mathfrak{q}$, где $\mathfrak{p}, \mathfrak{q}$ - простые.

2.6. Элемент $e \in A$ называется идемпотентом, если $e = e^2$. Идеал $\mathfrak{a} \subset A$ называется идемпотентным идеалом, если $\mathfrak{a}^2 = \mathfrak{a}$. Покажите, что идеал (e) имеет структуру коммутативного кольца (с e в качестве единицы; заметим, что это не подкольцо A). Далее покажите, что кольцо A изоморфно прямому произведению колец $(e) \times (1 - e)$.

2.7. Пусть A - кольцо, e, e' - идемпотенты. Тогда следующее верно:
1). Идеал (e) идемпотентен.
2). Если $\mathfrak{a}$ - главный идемпотентный идеал, то существует идемпотент f, такой что $\mathfrak{a} = (f)$.
3). $(e) = (e') \Rightarrow e = e'$.
4). Положим $e'' = e + e' - ee'$. Тогда e'' - идемпотент, и $(e, e') = (e'')$.
5). Пусть $e_1, \ldots, e_s$ - идемпотенты. Тогда существует идемпотент f, такой что $(e_1, \ldots, e_s) = (f)$.

2.8. Найдите все делители нуля в $\mathbb{Z}/m\mathbb{Z}$.

2.9. Сколько идемпотентов имеет кольцо $\mathbb{Z}/m\mathbb{Z}$?

2.10. Опишите все автоморфизмы (изоморфизмы на себя) кольца $\mathbb{Z}/m\mathbb{Z}$.

2.11. На лекции мы определили эпиморфизмы и мономорфизмы коммутативных колец как такие, на которые можно сокращать справа и слева соответственно. Именно, гомоморфизм $f : A \to B$ называется эпиморфизмом, если для любых $g_1, g_2 : B \to C$ $(\forall C)$ из равенства $g_1 \circ f = g_2 \circ f$ следует $g_1 = g_2$ (мономорфизмы определяются аналогично). Точно так же эпи- и мономорфизмами в произвольной категории $\mathcal{C}$ называются стрелки, допускающие соответствующее сокращение. Если объекты в $\mathcal{C}$ - множества с некоторой структурой (в нашем случае это коммутативные кольца), то имеют смысл понятия «сюръективный морфизм» и «инъективный морфизм». Легко видеть, что всякая сюръекция (инъекция) является эпиморфизмом (мономорфизмом), но обратное, вообще говоря, неверно (пример - вложение $\mathbb{Z} \to \mathbb{Q}$). Более того, среди привычных нам конкретных категорий мономорфизмы чаще совпадают с инъекциями, чем эпиморфизмы - с сюръекциями. Покажите, что такое различие между «правым» и «левым» имеет место и в интересующем нас случае категории коммутативных колец:

1). Проверьте, что вложение $\mathbb{Z} \to \mathbb{Q}$ - эпиморфизм (и очевидно не сюръективный морфизм).
2). Докажите, что всякий мономорфизм коммутативных колец инъективен.

Простые идеалы, радикалы, локальные кольца, булевы кольца

3.1. Пусть A - кольцо, $\mathcal{J}_A \equiv \cap_{\mathfrak{m}\in \mathrm{Max}\, A}\mathfrak{m}$ - его радикал Джекобсона. Тогда $x \in \mathcal{J}_A \Leftrightarrow \forall y \in A \Rightarrow 1 - xy$ обратим в A.

3.2. Пусть $\mathfrak{p}_1,\ \mathfrak{p}_2$ - простые идеалы. Верно ли, что $\mathfrak{p}_1 + \mathfrak{p}_2$ и $\mathfrak{p}_1 \cap \mathfrak{p}_2$ - простые идеалы?

3.3. (Prime Avoidance Lemma):
1). Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ - простые идеалы, $\mathfrak{a}$ - идеал, содержащийся в $\cup_{i=1}^n \mathfrak{p}_i$. Тогда $\mathfrak{a} \subseteq \mathfrak{p}_i$ для некоторого i.
2). Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ - некоторые идеалы, $\mathfrak{p}$ - простой идеал, содержащийся в $\cap_{i=1}^n \mathfrak{a}_i$. Тогда существует i такой что $\mathfrak{a}_i \subseteq \mathfrak{p}$. Если $\mathfrak{p} = \cap_{i=1}^n \mathfrak{a}_i$, то $\exists i :\ \mathfrak{p} = \mathfrak{a}_i$.

3.4. Утверждения, аналогичные описанным в предыдущей задаче, имеют место для векторных пространств. Пусть K - бесконечное поле, V - конечномерное векторное пространство над K; пусть $W_1, \ldots, W_n$ - его собственные подпространства. Тогда:
1). $\cup_{i=1}^n W_i \neq V$.
2). Если $W \subseteq \cup_{i=1}^n W_i$ - подпространство, то $\exists i : W \subseteq W_i$.

3.5. (Свойства радикала). Пусть $\mathfrak{a},\ \mathfrak{b}$ - идеалы в A, $r(\mathfrak{a})$ - радикал идеала. Докажите следующие элементарные свойства:
1). $\mathfrak{a} \subseteq r(\mathfrak{a})$.
2). $r(r(\mathfrak{a})) = r(\mathfrak{a})$.
3). $r(\mathfrak{ab}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.
4). $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$.
5). $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.
6). Если $\mathfrak{p}$ - простой идеал, то $r(\mathfrak{p}^n) = r(\mathfrak{p}) = \mathfrak{p}$.
7). Если $r(\mathfrak{a})$ и $r(\mathfrak{b})$ взаимно просты, то $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты.

Локальные кольца

3.6. Кольцо A называется локальным, если оно имеет единственный максимальный идеал.
1). Пусть A - кольцо, $\mathfrak{m}$ - подмножество всех необратимых элементов. Тогда A - локальное $\Leftrightarrow \mathfrak{m}$ - идеал (и в этом случае $\mathfrak{m}$ будет максимальным идеалом локального кольца).
2). Пусть K - поле. Тогда для $n \geq 1$ кольцо $K[x]/(x^n)$ - локальное. Как выглядит его максимальный идеал?
3). Полем вычетов локального кольца A с максимальным идеалом $\mathfrak{m}$ называется факторкольцо $K = A/\mathfrak{m}$. Проверьте, что факторгруппа $\mathfrak{m}/\mathfrak{m}^2$ имеет структуру векторного пространства[1] над K.

3.7. Пусть A - кольцо, $\mathcal{R}$ - его нильрадикал. Следующие утверждения равносильны:
1). A имеет ровно один простой идеал.
2). Любой элемент A является либо единицей, либо нильпотентом.
3). $A/\mathcal{R}$ - поле.

3.8. Пусть кольцо A таково, что любой его элемент x удовлетворяет уравнению $x^n = x$ для некоторого $n > 1$, зависящего от x. Покажите, что любой простой идеал в A максимален.

Булевы кольца

3.9. Пусть $\mathbb{Z}_2 \equiv \mathbb{Z}/2\mathbb{Z}$ - поле из двух элементов, X - некоторое множество. Обозначим через $\mathbb{Z}_2^X$ множество всех функций $f : X \to \mathbb{Z}_2$. Очевидно, это множество - кольцо относительно поточечных операций сложения и умножения. Покажите, что всякий элемент $f \in \mathbb{Z}_2^X$ есть характеристическая функция χ_S некоторого подмножества $S \subseteq X$ (то есть отображение $\chi_S : X \to \mathbb{Z}_2,\ \chi_S(x) = 1 \Leftrightarrow x \in S$). Далее, если $\mathcal{P}(X)$ - множество всех подмножеств X, то оно имеет структуру кольца с операциями симметрической разности Δ и пересечения $\cap$ в качестве сложения и умножения. Это кольцо канонически изоморфно $\mathbb{Z}_2^X$.

3.10. Кольцо A называется булевым, если для любого $x \in A$ выполнено $x^2 = x$ (то есть всякий элемент булева кольца является идемпотентом). Очевидно, $\mathbb{Z}_2^X$ (предыдущая задача) булево. Докажите следующие свойства булевых колец:
1). $x + x = 0$ для всякого $x \in A$.
2). Любой простой идеал $\mathfrak{p}$ максимален, и $A/\mathfrak{p} = \mathbb{Z}_2$.
3). Любой идеал, порожденный конечной системой элементов, является главным.[2]
4). Если A - булево, то его нильрадикал $\mathcal{R}$ и радикал Джекобсона $\mathcal{J}$ совпадают и равны нулевому идеалу.

[1] В силу естественной аналогии $\mathfrak{m}/\mathfrak{m}^2$ называется кокасательным пространством локального кольца A; при этом касательное пространство - это множество линейных функционалов $\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, K)$.
[2] Это утверждение следует из задачи 2.7.

Спектр кольца

4.1. Пусть $X_f \subseteq \operatorname{Spec} A$ - главное открытое подмножество, $\varphi : A \to B$ - гомоморфизм колец, которому соответствует отображение $\varphi^* : \operatorname{Spec} B \to \operatorname{Spec} A$. Найдите прообраз X_f при φ^*.

4.2. Пусть A - коммутативное кольцо. Следующие утверждения эквивалентны:
1). Пространство $\operatorname{Spec} A$ несвязно.
2). $A \simeq A_1 \times A_2$, где $A_1,\ A_2 \neq 0$.
3). A содержит идемпотентный элемент $e \neq 0;\ 1$.

4.3. Опишите $\operatorname{Spec}(\mathbb{Z}/n\mathbb{Z})$.

4.4. (Неприводимые пространства) Топологическое пространство X называется неприводимым (или гиперсвязным), если X непусто и всякая пара непустых открытых подмножеств X имеет непустое пересечение. Очевидно, среди неприводимых пространств хаусдорфовым является только пространство, состоящее из одной точки.
1). X неприводимо $\Leftrightarrow$ любое непустое открытое подмножество всюду плотно в X.
2). X неприводимо $\Leftrightarrow$ множество внутренних точек любого собственного замкнутого подмножества X пусто.
3). Пример: пусть X - произвольное бесконечное множество. Тогда пустое множество и коконечные множества (то есть такие, дополнения к которым конечны) образуют открытую топологию (а именно, минимальную топологию, в которой X является T_1-пространством). Коконечная топология на бесконечном множестве X обладает свойством неприводимости.
4). Всякое неприводимое пространство связно.
5). Пусть $Y \subseteq X$ - подпространство X. Тогда Y называется неприводимым подпространством, если Y неприводимо в индуцированной из X топологии. Покажите, что замыкание $\overline{Y}$ неприводимого подпространства Y есть неприводимое подпространство. Далее, любое неприводимое подпространство содержится в некотором максимальном неприводимом подпространстве. Максимальные неприводимые подпространства пространства X замкнуты и покрывают X (они называются неприводимыми компонентами X).

4.5. $\operatorname{Spec} A$ - неприводимое пространство $\Leftrightarrow$ нильрадикал $\mathcal{R}_A$ - простой идеал.

4.6. Докажите, что множество простых идеалов кольца содержит минимальные по включению элементы.

4.7. Неприводимые компоненты $\operatorname{Spec} A$ имеют вид $V(\mathfrak{p}_{\min})$, где $\mathfrak{p}_{\min}$ - минимальный по включению простой идеал.

4.8. Пусть X - топологическое пространство. Тогда X бикомпактно тогда и только тогда, когда для него выполнено следующее свойство:

– Всякая система $\{V_\alpha \mid \alpha \in \mathfrak{A}\}$ замкнутых подмножеств, любая конечная подсистема которой имеет непустое пересечение ($\forall \alpha_1, \ldots, \alpha_s \in \mathfrak{A} \Rightarrow V_{\alpha_1} \cap \ldots \cap V_{\alpha_s} \neq \emptyset$), вся имеет непустое пересечение.

Кольца непрерывных функций

В этом листочке везде кроме задачи 5.6 топологическое пространство X предполагается вполне регулярным.[3]

5.1. Пусть $C(X,\mathbb{R})$ - кольцо вещественнозначных непрерывных функций на X. Для функции $f \in C(X,\mathbb{R})$ обозначим через $Z(f) \subseteq X$ множество нулей f. Докажите, что всякое открытое подмножество X содержит множество вида $Z(f)$.

5.2. Всякое множество $Z(f)$ является пересечением счетного числа открытых множеств.

5.3. Пусть $S \subseteq C(X,\mathbb{R})$ - произвольное подмножество. Обозначим через $\mathcal{Z}(S) = \{Z(f) \mid f \in S\}$ семейство множеств нулей функций из S. Пусть $I \lhd C(X,\mathbb{R})$ - собственный идеал. Тогда:

1). $\mathcal{Z}(I)$ замкнуто относительно конечных пересечений и не содержит пустое множество.

2). $\mathcal{Z}(I)$ замкнуто относительно расширения: если $Z(f) \subseteq Z'$, где $f \in I$, то $Z' \in \mathcal{Z}(I)$.

Обратно, если для системы $\mathcal{Z}(S)$ множеств вида $Z(f)$ имеют место свойства 1) и 2), то $S = I$ - некоторый (собственный) идеал в $C(X,\mathbb{R})$.[4]

Идеал I будет максимальным тогда и только тогда, когда помимо свойств 1) и 2) для $\mathcal{Z}(I)$ выполнено следующее:

3). Если $Z' \notin \mathcal{Z}(I)$, то существует $Z \in \mathcal{Z}(I)$, такое что $Z \cap Z' = \emptyset$.

5.4. Пусть X нормально и $Y \subseteq X$ замкнуто в X. Докажите теорему Титце о расширении:

– Для любой непрерывной функции $f : Y \to \mathbb{R}$ существует непрерывная функция $F : X \to \mathbb{R}$, такая что $F_{|Y} = f$.

5.5. Идеал I кольца $C(X,\mathbb{R})$ называется *свободным*, если $\cap_{f\in I} Z(f) = \emptyset$. Покажите, что кольцо $C(X,\mathbb{R})$ содержит свободный идеал тогда и только тогда, когда X не бикомпактно.

5.6. Пусть X - топологическое пространство, x_0 - какая-то его точка. Пусть f, g - непрерывные функции, определенные в окрестностях U_f, U_g точки x_0. Объявим их эквивалентными, если существует окрестность $U \subseteq U_f \cap U_g$, на которой f и g совпадают. Множество $C(X,\mathbb{R})_{x_0}$ классов эквивалентности непрерывных функций по этому отношению образуют кольцо (с поточечными сложением и умножением - проверьте корректность этого определения), которое называется *кольцом ростков*[5] непрерывных функций в x_0. Покажите, что это кольцо локальное, и найдите его поле вычетов.

[3] T_1-пространство X называется вполне регулярным, если для любой точки $x \in X$ и любого не содержащего ее замкнутого подмножества A существует непрерывная функция $f : X \to [0;1]$, равная единице в точке x и нулю во всех точках A. Такие пространства еще называют пространствами Тихонова или $T_{3\frac{1}{2}}$-пространствами.

[4] Свойства (1) и (2) означают, что $\mathcal{Z}(I)$ - фильтр на множестве X (даже собственный фильтр - то есть не совпадающий со всем множеством $\mathcal{P}(X)$).

[5] Английское название - ring of germs.

Расширения полей

6.1. Пусть K - поле, L - некоторое расширение K. Если элемент $u \in L$ алгебраичен над K, то множество всех многочленов $f \in K[x]$, для которых $f(u) = 0$, есть идеал I в $K[x]$. Так как $K[x]$ - кольцо главных идеалов, то $I = (m_u)$ для некоторого многочлена $m_u(x)$. Многочлен m_u называется *минимальным многочленом* элемента u. *Степенью элемента u над K* называется степень его минимального многочлена.

1). Проверьте, что m_u неприводим.

2). Покажите, что следующие числа алгебраичны над $\mathbb{Q}$: $\sqrt{2}+\sqrt{3}$, $\sqrt[3]{2}+\sqrt{3}$, $\sqrt{2}+\sqrt[4]{-2}$, $e^{\frac{2\pi i}{p}}$ (p - простое). Найдите их степени и минимальные многочлены.

6.2. Пусть $K \subset L$ - расширение полей, $\alpha,\ \beta \in L$ - алгебраические элементы. Тогда элементы $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, α/β тоже алгебраические.

6.3. В условиях предыдущей задачи расширение $K \subset K[\alpha,\beta]$ конечно и размерность $[K[\alpha,\beta] : K] \leq \deg\alpha \deg\beta$.

6.4. Если K алгебраически замкнуто, L - конечное расширение, то $L = K$.

6.5. Пусть $K \subset L$ - конечное расширение. Рассматривая L как векторное пространство над K, определим для любого $u \in L$ линейный оператор $T(u)$:

$$T(u)x = ux,\ \ x \in L.$$

Обозначим через $\operatorname{tr} u$ след оператора $T(u)$. Определим скалярное умножение в L:

$$\langle u, v\rangle = \operatorname{tr} uv.$$

Проверьте, что оно симметрично и билинейно. Если $\operatorname{char} K = 0$, то $\langle\ ,\ \rangle$ невырождено.

6.6. Пусть $K = \mathbb{Q}$, $L = \mathbb{Q}[e^{\frac{2\pi i}{p}}]$ - поле деления круга (p - простое число). Опишите скалярное произведение в L.

Конечные поля

7.1. Пусть F - конечное поле характеристики p.
1). Докажите, что $|F| = p^n$ для некоторого $n \in \mathbb{N}$.
2). Докажите, что всякий элемент поля F является корнем уравнения $x^{p^n} - x = 0$.

7.2. Докажите, что конечное поле не является алгебраически замкнутым.

7.3. Пусть K - алгебраически замкнутое поле характеристики p. Обозначим через $\mathbb{F}_{p^n}$ множество корней уравнения $x^{p^n} - x = 0$ в K. Покажите, что $\mathbb{F}_{p^n}$ - подполе K, состоящее из p^n элементов. Докажите, что любое поле из p_n элементов изоморфно $\mathbb{F}_{p^n}$.

7.4. Пусть F - конечное поле. Тогда мультипликативная группа F^* - циклическая.

7.5. Пусть F - поле характеристики p. Обозначим через $\varphi : F \to F$ отображение Фробениуса:

$$x \mapsto x^p.$$

1). Покажите, что φ - гомоморфизм (колец).
2). Если F конечно или алгебраически замкнуто, то φ - автоморфизм.
3). Приведите пример поля, для которого гомоморфизм Фробениуса необратим.
4). Докажите, что $\binom{p^n}{k}$ делится на p при $0 < k < p^n$.
5). Пусть $F = \mathbb{F}_{p^n}$. Найдите порядок φ в группе автоморфизмов поля $\mathbb{F}_{p^n}$.
6). Группа $\operatorname{Aut}\mathbb{F}_{p^n}$ циклическая и порождается φ.

7.6. При каких n и m поле $\mathbb{F}_{p^n}$ содержит поле $\mathbb{F}_{p^m}$? Найдите $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$.

7.7. Пусть f - неприводимый многочлен степени n над $\mathbb{F}_p$.
1). Докажите, что все корни f лежат в $\mathbb{F}_{p^n}$.
2). Докажите, что f не имеет кратных корней.
3). Если $x \in \mathbb{F}_{p^n}$, то x является корнем неприводимого многочлена f над $\mathbb{F}_p$ степени d, $d|n$.

7.8. 1). Докажите тождество

$$x^{p^n} - x = \prod_{d|n} \prod_{\deg f = d} f(x),$$

где $f(x)$ - неприводимые над $\mathbb{F}_p$ многочлены со старшим коэффициентом 1. Обозначим число таких многочленов степени d через $\psi(d)$.
2). Покажите, что $p^n = \sum_{d|n} d\psi(d)$. Получите выражение для ψ, используя обращение Мебиуса.

Модули

8.1. Для любого A-модуля M имеется изоморфизм $\mathrm{Hom}(A, M) \simeq M$.

8.2. 1). Пусть $M_1,\ M_2$ - подмодули M. Тогда $(M_1+M_2)/M_1 \simeq M_2/(M_1 \cap M_2)$ и следующая диаграмма коммутативна:

$$\begin{array}{ccc} M_2 & \longrightarrow & M_2/(M_1 \cap M_2) \\ \downarrow & & \downarrow \simeq \\ M_1 + M_2 & \longrightarrow & (M_1 + M_2)/M_1 \end{array}$$

стрелки которой даются естественными гомоморфизмами вложения и проекции.

2). Пусть $N \subseteq M \subseteq L$ - A-модули. Тогда $(L/N)/(M/N) \simeq L/M$. Имеет место коммутативная диаграмма

$$\begin{array}{ccc} L & \longrightarrow & L/M \\ \downarrow & & \downarrow \simeq \\ L/N & \longrightarrow & (L/N)/(M/N) \end{array}$$

в которой все стрелки - корректно определенные естественные проекции.

3). Пусть K - поле, $A = K[x, y, z]/(xy - z^2)$; обозначим через $\overline{x},\ \overline{y},\ \overline{z}$ образы $x,\ y,\ z$ в A. Покажите, что идеал $\mathfrak{p} = (\overline{x},\ \overline{z}) \lhd A$ - простой.

8.3. Пусть $\mathfrak{p}$ - простой идеал в A. Тогда $\mathfrak{p}[x]$ - простой идеал в $A[x]$. Верно ли, что $\mathfrak{m}[x]$ всегда максимален, когда $\mathfrak{m}$ максимальный?

8.4. Пусть $\mathfrak{a} \lhd A$ - идеал, содержащийся в радикале Джекобсона кольца A, M - некоторый A-модуль, N - конечно порожденный A-модуль. Пусть $\phi : M \to N$ - гомоморфизм. Тогда если индуцированный гомоморфизм $M/\mathfrak{a}M \to N/\mathfrak{a}N$ сюръективен, то и ϕ сюръективен.

8.5. Пусть $0 \to M' \to M \to M'' \to 0$ - точная последовательность A-модулей. Если M' и M'' конечно порождены, то и M конечно порожден. Верно ли обратное?

8.7. Покажите, что в категории $\mathbf{Mod}_A$ всякий эпиморфизм[6] сюръективен, а всякий мономорфизм инъективен.

8.8. Пусть M, N, P - A-модули. Обозначим через $\mathrm{Bilin}\,(M, N; P)$ множество всех A-билинейных функций $f : M \times N \to P$. Покажите, что элементы множества $\mathrm{Bilin}\,(M, N; P)$ находится в естественном взаимно однозначном соответствии с элементами множества $\mathrm{Hom}(M, \mathrm{Hom}(N, P))$. Отсюда покажите, что существует естественный изоморфизм

$$\mathrm{Hom}(M \otimes N, P) \simeq \mathrm{Hom}(M, \mathrm{Hom}(N, P)).$$

[6] т.е. стрелка, на которую можно сокращать справа - см. задачу 2.11.

Аддитивные функторы

9.1. (Splitting Lemma) Пусть $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ - точная последовательность A-модулей. Тогда следующие утверждения равносильны:
1). $M \simeq M' \oplus M''$.
2). $\exists \alpha : M \to M' \ : \ \alpha \circ f = \mathrm{Id}_{M'}$.
3). $\exists \beta : M'' \to M \ : \ g \circ \beta = \mathrm{Id}_{M''}$.
(Говорят, что точная последовательность $0 \to M' \to M \to M'' \to 0$ расщепляется, если она обладает одним из этих свойств.)

9.2. (Проективные модули) Модуль P называется проективным, если для любого гомоморфизма $f : P \to M''$ и любого сюръективного гомоморфизма $g : M \to M''$ существует такой гомоморфизм $h : P \to M$, что $f = g \circ h$. Иначе говоря, любая диаграмма вида

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

с точной строкой включается в коммутативную диаграмму

$$\begin{array}{ccccc} & & & & P \\ & & & \swarrow & \downarrow \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

1). Прямая сумма модулей является проективным модулем $\Leftrightarrow$ проективно каждое прямое слагаемое.
2). Всякий свободный модуль проективен.
3). Модуль P проективен $\Leftrightarrow$ P - прямое слагаемое некоторого свободного модуля.
4). Модуль P проективен $\Leftrightarrow$ любая точная последовательность $0 \to M' \to M \to P \to 0$ расщепляется.
5). Абелева группа (то есть $\mathbb{Z}$-модуль) проективна $\Leftrightarrow$ она свободна. То же верно для модулей над любым кольцом главных идеалов.[7]
6). Если A - коммутативное кольцо с идемпотентом e, то (e) - проективный A-модуль.
7). Если A - локальное кольцо, то всякий конечно порожденный проективный A-модуль является свободным.[8]

9.3. Пусть $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ - кольцо вычетов по модулю $n > 1$. Каждому делителю d числа n соответствует точная последовательность

$$0 \to d\mathbb{Z}_n \to \mathbb{Z}_n \to d'\mathbb{Z}_n \to 0,$$

где $d' = n/d$. Покажите, что эта последовательность расщепляется (или, что то же, $d'\mathbb{Z}_n$ - проективный $\mathbb{Z}_n$-модуль) тогда и только тогда, когда числа d и d' взаимно просты. Приведите пример проективного модуля, не являющегося свободным.

9.4. Пусть $T : \mathbf{Mod}_A \to \mathbf{Mod}_A$ - аддитивный функтор. Тогда если точная последовательность

$$0 \to M' \to M \to M'' \to 0$$

расщепляется, то последовательность образов

$$0 \to T(M') \to T(M) \to T(M'') \to 0$$

точна и расщепляется.

Аддитивный функтор (одного аргумента) $T : \mathbf{Mod}_A \to \mathbf{Mod}_A$ называется точным, если всякий раз, когда точна последовательность $M' \to M \to M''$, последовательность

$$T(M') \to T(M) \to T(M'')$$

[7] Достаточно доказать, что над КГИ всякий подмодуль свободного модуля свободен, и воспользоваться пунктом 3.

[8] Капланский показал, что это верно и для произвольных - необязательно конечно порожденных - модулей над локальным кольцом.

также точна. Аналогично вводится понятие точного функтора нескольких аргументов.

9.5. Функтор T точен $\Leftrightarrow$ любая точная последовательность $0 \to M' \to M \to M'' \to 0$ переходит в точную последовательность $0 \to T(M') \to T(M) \to T(M'') \to 0$.

Свойства точности справа и слева определяются аналогично точности (в том виде, в каком это сделано в предыдущей задаче): например, T точен справа, если всякая точная последовательность

$$0 \to M' \to M \to M'' \to 0$$

переводится в точную последовательность

$$T(M') \to T(M) \to T(M'') \to 0.$$

9.6. Пусть $T(M, N)$ - аддитивный функтор двух аргументов, ковариантный по первому и контравариантный по второму.[9] Тогда следующие утверждения равносильны:

1). T точен справа.

2). Для любых точных последовательностей $M' \to M \to M'' \to 0$ и $0 \to N' \to N \to N''$ имеют место точные последовательности

$$T(M', N) \to T(M, N) \to T(M'', N) \to 0$$
$$T(M, N'') \to T(M, N) \to T(M, N') \to 0.$$

3). Для любых точных последовательностей $M' \to M \to M'' \to 0$ и $0 \to N' \to N \to N''$ имеет место точная последовательность

$$T(M', N) \oplus T(M, N'') \xrightarrow{\phi} T(M, N) \to T(M'', N') \to 0,$$

в которой ϕ - прямая сумма гомоморфизмов $T(M', N) \to T(M, N)$ и $T(M, N'') \to T(M, N)$.

(Аналогичную эквивалентность можно сформулировать для случая точного слева T.)

9.7. Функтор Hom_A точен слева. Функтор $\otimes_A$ точен справа.

9.8. Модуль P - проективный $\Leftrightarrow$ $\mathrm{Hom}_A(P, -)$ - точный функтор.

9.9. Всякий проективный модуль P - плоский.

[9] Как было отмечено на лекции, изменение числа аргументов и замена ковариантности по какому-либо аргументу на контравариантность несущественны.

Локализация

10.1. Пусть $S \subset A$ - мультипликативно замкнутое подмножество. Определим операцию S^{-1}, действующую на A-модули и их гомоморфизмы, следующим образом: модулю M поставим в соответствие модуль частных $S^{-1}M$, а стрелке $\varphi : M_1 \to M_2$ - стрелку $S^{-1}\varphi : \frac{m_1}{s} \mapsto \frac{\varphi(m_1)}{s}$. Проверьте, что эта операция дает (аддитивный) ковариантный функтор $S^{-1} : \mathbf{Mod}_A \to \mathbf{Mod}_A$, и покажите, что этот функтор точен.

10.2. (Свойства локализации) Пусть $N,\ P$ - подмодули A-модуля M, $S \subset A$ - мультипликативная система. Тогда:
1). $S^{-1}(N+P) = S^{-1}N + S^{-1}P$.
2). $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
3). $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ (изоморфизм $S^{-1}A$-модулей).
4). S^{-1}-модули $S^{-1}M$ и $S^{-1}A \otimes_A M$ изоморфны.
5). $S^{-1}A$ - плоский A-модуль.

10.3. (Насыщенные системы) Мультипликативная система $S \subset A$ называется насыщенной, если $x,\ y \in S \Leftrightarrow xy \in S$.
1). Пусть S насыщенна и не содержит нулевой элемент (то есть не совпадает со всем кольцом A). Докажите, что $A \setminus S$ - объединение простых идеалов.
2). Всякая мультипликативная система S содержится в некоторой насыщенной системе S'. Для любой S существует наименьшая содержащая ее насыщенная система $\overline{S}$ (она называется насыщением S).
3). Если $0 \notin S$, то дополнение к $\overline{S}$ совпадает с объединением простых идеалов, не пересекающихся с S.
4). $S^{-1}A \simeq \bar{S}^{-1}A$.

10.4. Мультипликативная система $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ насыщенна $\Leftrightarrow$ $\mathfrak{p}$ - минимальный простой идеал.

10.5. Опишите насыщенные мультипликативные системы в $\mathbb{Z}$.

10.6. Пусть $f,\ g \in A$ - элементы кольца, X_f и X_g - главные открытые множества в $\operatorname{Spec} A$. Тогда, если $X_f = X_g$, то кольца частных A_f и A_g изоморфны.

10.7. В обозначениях предыдущей задачи пусть $X_g \subseteq X_f$. Тогда существует целое $n > 0$ и $u \in A$, такие что $g^n = uf$. Из этого следует, что корректно определен гомоморфизм ограничения

$$\operatorname{res}_{X_f,X_g} : A_f \to A_g,\ \ a/f^m \mapsto au^m/g^{mn}$$

1). Гомоморфизм $\operatorname{res}_{X_f,X_g}$ зависит только от X_f и X_g (не от $f,\ g$).
2). Если $X_f = X_g$, то $\operatorname{res}_{X_f,X_g}$ - тождественное отображение.
3). Если $X_h \subseteq X_g \subseteq X_f$, то $\operatorname{res}_{X_f,X_h} = \operatorname{res}_{X_g,X_h} \circ \operatorname{res}_{X_f,X_g}$

10.8. Пусть $\varphi : A \to S^{-1}A$ - канонический гомоморфизм ($\varphi(a) = a/1$). Докажите, что индуцированное отображение $\varphi^* : \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ - гомеоморфизм $\operatorname{Spec} S^{-1}A$ на его образ в $\operatorname{Spec} A$. Также докажите, что X_f гомеоморфно $\operatorname{Spec} A_f$.

Локальные свойства

11.1. Пусть $\varphi : M \to N$ - гомоморфизм A-модулей. Следующие утверждения равносильны:
1). φ инъективен.
2). $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ инъективен для любого простого идеала $\mathfrak{p}$.
3). $\varphi_{\mathfrak{m}}$ инъективен для любого максимального идеала $\mathfrak{m}$.
Такая же эквивалентность имеет место для сюръективных гомоморфизмов. Иначе говоря, свойство гомоморфизма быть сюръективным или инъективным - локальное свойство.

11.2. Свойство A-модуля M быть плоским модулем - локальное.

11.3. Верно ли, что свойство модуля быть проективным - локальное свойство?

11.4. Покажите, что свойство кольца A иметь тривиальный нильрадикал - локальное:

$$\mathcal{R}_A = 0 \Leftrightarrow \forall \mathfrak{p} \Rightarrow \mathcal{R}_{A_{\mathfrak{p}}} = 0.$$

11.5. Верно ли, что свойство кольца быть областью целостности локально?

11.6. Пусть топология Зарисского $\operatorname{Spec} A$ удовлетворяет первой аксиоме отделимости. Покажите, что тогда она уже хаусдорфова.