1. Многочлены и расширения полей

1.1. **Совершенные поля.** Поле называется *совершенным*, если его любое алгебраическое расширение сепарабельно.

(1) Докажите, что алгебраическое расширение совершенного поля совершенно; сепарабельное замыкание совершенного поля является алгебраическим замыканием.
(2) Докажите, что поле совершенно тогда и только тогда, когда оно нулевой характеристики (т.е. содержит поле $\mathbb{Q}$) или оно характеристики $p > 0$ (т.е. содержит поле $\mathbb{F}_p$) и каждый его элемент – p-ая степень. Например, конечные поля совершенны.
(3) Пусть $K|L$ – нетривиальное расширение полей конечного типа[1] и L совершенно. Докажите, что если K совершенно, то оно конечно.
(4) Пусть $B \to A$ –гомоморфизм ассоциативных колец и M – A-бимодуль (т.е. $A \otimes A^{\mathrm{op}}$-модуль). *Дифференцированием* A над B со значениями в M называется морфизм B-бимодулей $\partial : A \to M$, удовлетворяющий правилу Лейбница: $\partial(fg) = f\partial g + \partial f \cdot g$ для всех $f, g \in A$. Рассмотрим A-бимодуль $A \otimes_B A$. Гомоморфизм умножения $m : A \otimes_B A \xrightarrow{\times} A$ является морфизмом A-бимодулей. Пусть $\mathfrak{m} \subset A \otimes_B A$ – ядро m. Это – A-бимодуль в $A \otimes_B A$. Предположим, что A коммутативно. Тогда $\mathfrak{m}$ – идеал в $A \otimes_B A$. (i) Докажите, что $d : A \to \mathfrak{m}/\mathfrak{m}^2 =: \Omega_{A|B}$, $da := 1 \otimes a - a \otimes 1$, является дифференцированием кольца A над B, причём универсальным, т.е. любое дифференцирование кольца A над B однозначно пропускается через d. (ii) Докажите, что $A \otimes_B A \to \Omega_{A|B}$, $x \otimes y \mapsto xdy$, сюръективно, а ядро порождено элементами $(f + g) \otimes h - f \otimes h - g \otimes h$, $h \otimes (f + g) = h \otimes f + h \otimes g$, $h \otimes (fg) - hf \otimes g - hg \otimes f$ (правило Лейбница) и $f \otimes g = 0$, если g лежит в образе B. Другими словами, $\Omega_{A|B}$ канонически изоморфен A-модулю конечных формальных сумм $\sum_j f_j dg_j$, где $f_j, g_j \in A$, с такими соотношениями.
(5) Пусть $K|k$ – расширение полей. Тогда $\Omega_{K|k}$ – K-векторное пространство. Докажите, что а) множество подмножеств T в K таких, что K алгебраично над $k(T)$, имеет минимальные элементы (относительно включения);[2] б) все минимальные элементы из пункта а) имеют одинаковую мощность (которая называется *степенью трансцендентности* расширения полей $K|k$); в) $\dim_K \Omega_{K|k}$ совпадает со степенью трансцендентности (см. пункт б)) расширения $K|k$ в случае нулевой характеристики; г) в случае положительной характеристики p поля K имеется равенство $\Omega_{K|k} = \Omega_{K|K^pk}$; кроме того, поле K совершенно тогда и только тогда, когда $\Omega_{K|\mathbb{Z}} = 0$.

1.2. **Алгебраические расширения.**

(1) Докажите, что (а) конечное расширение[3] полей алгебраично,[4] (б) композит двух конечных подрасширений любого расширения полей конечен, (в) алгебраическое расширение является объединением конечных расширений, (г) композит любого семейства алгебраических расширений алгебраичен.
(2) Пусть $K|k$ – алгебраическое расширение полей и $S \subseteq K$ – некоторое множество, порождающее $K|k$. Докажите, что следующие условия на расширение $K|k$ эквивалентны: (i) любой неприводимый над k многочлен не имеет кратных корней в K; (ii) в кольце $K \otimes_k K$ нет ненулевых нильпотентов; (iii)$_S$ минимальный многочлен над k каждого элемента S не имеет кратных корней ни в одном из расширений поля k; (iv)$_S$ для каждого элемента $x \in S$ любое дифференцирование поля $k(x)$ над k – нулевое.

[1] Расширение полей $K|k$ *конечно порождено* или *конечного типа*, если найдётся конечное подмножество $S \subset K$ такое, что любое подполе в K, содержащее k и S совпадает с K.

[2] т.е. такие подмножества T в K, что из $T \supseteq T'$ для некоторого $T \neq T' \subseteq K$ следует неалгебраичность поля K над $k(T)$.

[3] Расширение полей $K|k$ *конечно*, если K конечномерно как k-векторное пространство.

[4] Расширение полей $K|k$ *алгебраично*, если каждый элемент K является корнем некоторого ненулевого многочлена над k.

Алгебраическое расширение $K|k$ называется *сепарабельным*, если выполняются эквивалентные условия (i)–(iv); элемент x некоторого алгебраического расширения поля k называется *сепарабельным*, если сепарабельно расширение $k(x)|k$.

(3) Докажите, что конечное сепарабельное расширение полей порождается любым «достаточно общим» элементом этого расширения. Приведите пример конечного расширения полей, которое не порождается никаким из своих элементов.

(4) Докажите, что следующие условия на алгебраическое расширение полей $K|k$ эквивалентны: (i) в $K \setminus k$ нет элементов сепарабельных над k, (ii) для каждого $\alpha \in K$ найдётся такое целое $n \geqslant 0$, что $\alpha^{p^n} \in k$, (iii) минимальный многочлен любого элемента поля K над k имеет вид $X^{p^n} - a$ для некоторого целого $n \geqslant 0$ и некоторого $a \in k$.

Если условия выполняются, то расширение $K|k$ называют *чисто несепарабельным*.

(5) Верно ли, что а) сепарабельное расширение сепарабельного расширения сепарабельно; б) чисто несепарабельное расширение чисто несепарабельного расширения чисто несепарабельно?

(6) Докажите, существование и единственность с точностью до изоморфизма сепарабельного, совершенного и алгебраического замыканий любого поля. Докажите, что мощности всех трёх таких замыканий любого бесконечного поля совпадают с мощностью самого поля. Докажите, что алгебраическое (=сепарабельное) замыкание любого конечного поля счётно.

(7) Докажите, что правая размерность любого тела над любым подполем совпадает с левой размерностью над тем же подполем.

(8) Пусть A – тело, конечномерное (слева) над сепарабельно замкнутым подполем k. Докажите, что A коммутативно и чисто несепарабельно над k. (В частности, $A = k$ если k алгебраически замкнуто.)

(9) Алгебраическое расширение полей $K|k$ называется *расширением Галуа*, если k совпадает с неподвижным полем группы всех автоморфизмов поля K, тождественных на k. Докажите, что расширение $K|k$ является расширением Галуа тогда и только тогда, когда оно нормально[5] и сепарабельно.

(10) Пусть $K|k$ – расширение полей. Докажите, что алгебра $K \otimes_k K$ изоморфна прямой сумме полей тогда и только тогда, когда расширение $K|k$ конечно и сепарабельно. Что это за поля (например, если $K|k$ – расширение Галуа)?

(11) Расширение Галуа называется *абелевым*, если его группа абелева. Докажите, что расширение, полученное присоединением корней из единицы, абелево.

(12) Предположим, что поле k содержит ровно n корней из единицы степени n. (а) Постройте естественную биекцию между абелевыми расширениями поля k периода n и подгруппами мультипликативной группы $k^\times/k^{\times n}$ (по модулю n-ных степеней). (б) Если k – поле характеристики p, то постройте естественную биекцию между (i) абелевыми расширениями поля k периода p и подгруппами аддитивной группы $k/\wp(k)$ (по модулю элементов вида $a^p - a$ для всех $a \in k$), (ii) абелевыми расширениями поля k периода p^n и подгруппами аддитивной группы $\mathbb{W}_{p,n}(k)/\wp(\mathbb{W}_{p,n}(k))$ (по модулю элементов вида $F(a) - a$ для всех $a \in \mathbb{W}_{p,n}(k)$, где эндоморфизм F кольца векторов Витта $\mathbb{W}_{p,n}(k)$ индуцирован возведением в степень p на поле k).

[5]Алгебраическое расширение $K|k$ *нормально*, если любой неприводимый многочлен над k становится произведением неприводимых многочленов над K равных степеней.