Конечные поля и алгебраические числа

Определение 1. *Характеристикой* поля F называется наименьшее число n такое, что $1+1+...+1=0$ (всего n слагаемых). Если такого числа нет, то говорят, что характеристика поля равно 0.

Упражнение 1. Докажите, что характеристика поля либо 0 либо простое число p.

Упражнение 2. Докажите, что если характеристика поля F равна p, то F содержит $\mathbb{Z}_p$ как подполе.

1. Докажите, что количество элементов конечного поля делится на характеристику поля.

2. Докажите, что если количество элементов конечного поля равно p^k, где p — характеристика поля.

Упражнение 3. Напомним малую теорему Ферма: для любого $a \in \mathbb{Z}_p$, $a \neq 0$, $a^{p-1}=1$. Сформулируйте и докажите ее аналог для любого конечного поля.

Упражнение 4. Является ли полем множество остатков многочленов $\mathbb{R}[x]$ с действительными коэффициентами по модулю многочлена
а) x^2-1; б) x^2+1?

Определение 2. Число называется *алгебраическим*, если оно является корнем некоторого многочлена с рациональными коэффициентами. Говорят, что алгебраическое число имеет *степень* d, если оно является корнем *неприводимого* многочлена с рациональными коэффициентами степени d.

Упражнение 5. Является ли число $\sqrt[3]{2}+\sqrt{3}$ алгебраическим?

Упражнение 6. Число α является алгебраическим тогда и только тогда, когда числа $1, \alpha, \alpha^2, \ldots$ являются линейно зависимыми над $\mathbb{Q}$.

Определение 3. Если α — алгебраическое число, то существует многочлен P с рациональными коэффициентами такой, что $\alpha^{-1}=P(\alpha)$.

Упражнение 7. Докажите, что числа вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, $a,b,c \in \mathbb{Q}$ образуют поле.

Определение 4. Пусть $\alpha \in \mathbb{C}$. Через $\mathbb{Q}(\alpha)$ обозначается минимальное подполе комплексных чисел, содержащее α.

Определение 5. Если α — алгебраическое число степени d. Докажите, что выражения вида $a_0+a_1\alpha+\ldots+a_{d-1}\alpha^{d-1}$

3. Если α — алгебраическое число степени d. Докажите, что выражения вида $a_0+a_1\alpha+\ldots+a_{d-1}\alpha^{d-1}$ образуют поле (т.е. степень расширения $\mathbb{Q}(\alpha)$ над $\mathbb{Q}$ равна d).

4. а) Докажите, что сумма алгебраических чисел — алгебраическое число. б) Докажите, что алгебраические числа образуют поле.