MAT 314: HOMEWORK 6

DUE TH, MARCH 23, 2023

Problems marked by asterisk (*) are optional for MAT 314 students but required for MAT535 students.

Throughout this problem set, $\mathbb{F}$ is a field.

1. In this problem, you can use without proof the fact that for a positive integer k which is not a square of another integer, $\sqrt{k}$ is irrational – e.g. $\sqrt{2}$, $\sqrt{5}$ are irrational.

(a) Show that equation $x^2 - 5 = 0$ has no roots in $\mathbb{Q}(\sqrt{2})$. Deduce from this that in the chain of extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{5})$, each extension has degree 2.

(b) Let $\alpha = \sqrt{2} + \sqrt{5}$. Find the minimal polynomial of α over $\mathbb{Q}$ and show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

(c) Repeat the previous part for $\alpha' = \sqrt{2} - \sqrt{5}$.

(d) Show there exists a field isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha')$ which sends α to α'.

2. Let $F \subset L$ be an extension and K_1, K_2 - two intermediate field extensions: $F \subset K_1 \subset L$, $F \subset K_2 \subset L$. A *composite* K_1K_2 is defined to be the smallest subfield in L containing K_1 and K_2.

Prove that if K_1, K_2 are finite extensions of F, then so is K_1K_2, and $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$

3. Let us call a number $\alpha \in \mathbb{C}$ *constructible* if it can be obtained from rational numbers by repeatedly using arithmetic operations and operation of taking a square root of a number. E.g. $\alpha = \sqrt{3 + \sqrt{-1}} - \sqrt{5 - 7\sqrt{3}}$.

(a) Prove that α is constructible if and only if one can find a chain of field extensions $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$, where $[K_{i+1} : K_i] = 2$ and $\alpha \in K_n$.

(b) Prove that if α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ for some k. [In fact, it is "if and only if" — we will prove it later.]

(c) Prove that $\sqrt[3]{2}$ is not constructible.

4. Let $\mathbb{F}$ be a field of characteristic zero.

For a polynomial $f = \sum a_k x^k \in \mathbb{F}[x]$, define its derivative by

$$Df = \sum_{k \geq 1} k a_k x^{k-1} \in \mathbb{F}[x].$$

(a) Show that the derivative satisfies familiar rules: $D(f + g) = Df + Dg$, $D(fg) = (Df)g + f(Dg)$.

(b) Show that if $\mathbb{E} \supset \mathbb{F}$ is an extension of $\mathbb{F}$, and $a \in \mathbb{E}$ is a root of f of order $m \geq 1$ (i.e., $f(x) = (x - a)^m g(x)$, and $g(a) \neq 0$), then a is a root of Df of order $m - 1$. Is this true if $\mathbb{F}$ has positive characteristic?

(c) Show that f has no multiple roots (in any extensions of $\mathbb{F}$) iff $\gcd(f, Df) = 1$. In particular, it holds if f is irreducible, so if an irreducible polynomial $f \in \mathbb{F}[x]$ of degree d factors in a some extension $\mathbb{E}$, then it has has exactly d distinct roots in $\mathbb{E}$.

Continued on next page

***5.** Let $\mathbb{F}$ be a field of characteristic $p > 0$.

(a) Show that the map $Fr\colon \mathbb{F} \to \mathbb{F}$ given by $Fr(x) = x^p$ is a homomorphism of fields. Deduce from this that if $\mathbb{F}$ is finite, then Fr is a bijection. [It is called the *Frobenius automorphism*].

(b) Show that the the set $\{x \in \mathbb{F} \mid x^p = x\}$ is a subfield in $\mathbb{F}$, which is isomorphic to $\mathbb{Z}_p$. [Hint: how many different roots does the polynomial $x^p - x$ have?]