discriminant is always a perfect square,

ASSIGNMENT VI, ALGEBRA II, HKU, SPRING 2025
DUE AT 11:59PM ON FRIDAY MAY 2, 2025

Note the new due date of this assignment.

The first 6 problems are practice problems for Test 2 on Thursday April 17, 2025. Some of them will be discussed in the tutorial on Wednesday April 16, 2025.

Most of Problems 7-16 are on facts we proved in class and proofs can be found in the lecture notes and slides of lectures, but you should try to work them out on your own before consulting the lecture notes.

$x^5+x+1 = (x^3+x^2+1)(x^2+x+1)$ so split $(x^3+x^2+1) = \mathbb{F}_2[x]/\langle x^3+x^2+1\rangle$

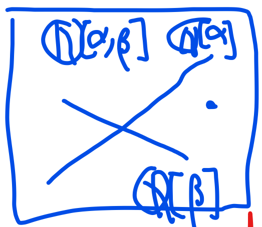
(1) Construct the splitting field L of $f(x) = x^5 + x + 1 \in \mathbb{F}_2[x]$. What is $|L : \mathbb{F}_2|$? 6 How many elements does L have? 2^6

(2) Let $f(x) = x^5+2x^4+4x^3-6x+2 \in \mathbb{Q}[x]$ and let α be a root of f in $\mathbb{C}$. Determine whether or not $\sqrt[3]{2} \in \mathbb{Q}(\alpha)$.

(3) Let β be any root of

$$g(x) = -x^{19} + i\sqrt[5]{11}x^4 + \frac{\sqrt[3]{5}+191}{\sqrt{37}+1}x^3 + 1 \in \mathbb{C}[x]$$ finite ext of $\mathbb{Q}$

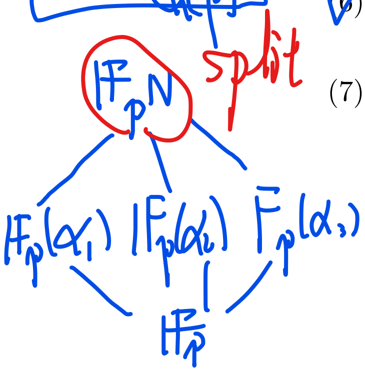
in $\mathbb{C}$. Show that β is a root of a polynomial with coefficients in $\mathbb{Q}$.



(4) Let $p > 2$ be a prime number. Show that if the angle $\frac{2\pi}{p}$ is constructable by a ruler and a compass, then $p-1$ must be a power of 2.

(5) Let p be a prime number and let $g(x)$ be any irreducible polynomial in $\mathbb{F}_p[x]$. Show that $\mathbb{F}_p[x]/\langle g(x)\rangle$ is a splitting field of $g(x)$ over $\mathbb{F}_p$.

(6) Show that is K is a field of characteristic 0, then every finite extension of K is simple (this is the Primitive Element Theorem for characteristic 0).



(7) Let $K \subset L$ be a finite field extension. Starting from the definitions, prove (resp. state) the following statements (resp. definitions). You should try them on your own first and only consult the lectures notes and slides of lectures if necessary.

(a) $\mathrm{Aut}_K(L)$ is a finite group;

(b) If $L = K(\alpha)$ is a simple extension of K, and if $p(x) \in K[x]$ is the minimal polynomial of α over K and R_p is the set of roots of f on L, then

$$\phi_\alpha : \ \mathrm{Aut}_K(L) \longrightarrow R_p, \ \ \sigma \longmapsto \sigma(\alpha),$$

is a bijection, and thus $|\mathrm{Aut}_K(L)| \leq |L : K|$;

(c) State the definition (as given in class) for $K \subset L$ to be a Galois extension.

(d) State Artin's theorem on construction of Galois extensions;

(e) Use Artin's theorem to prove that $K \subset L$ is Galois if and only if $L^G = K$;

(8) Prove that splitting fields over any field K of characteristic 0 is Galois.

(9) Compute the Galois group of the nth cyclotomic extension of $\mathbb{Q}$;

(10) Compute the Galois group of the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ for any prime number p and any integer ≥ 1;

(11) Let K be any field and let M be a splitting field of some $f(x) \in K[x]$ over K. Show that for any field extension $M \subset L$, every $\sigma \in \mathrm{Aut}_K(L)$ maps M to M.

(12) State the Theorem on Galois Correspondence for finite Galois extensions;

(13) Understand the Galois correspondence in the case of the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, where p is a prime number and positive integer n.

(14) Let $L \subset \mathbb{C}$ be the splitting field of $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. Describe all intermediate fields $\mathbb{Q} \subset M \subset L$; Determine all sub-groups of $\mathrm{Gal}(L/\mathbb{Q})$, and describe the Galois correspondence for L as an extension of $\mathbb{Q}$.

(15) Let $K \subset L$ be a finite Galois field extension with Galois group $G = \mathrm{Gal}(L/K)$, and let $\alpha \in L$. Let $G\alpha = \{\sigma(\alpha) : \sigma \in G\} = \{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r\}$, where $\alpha_i \neq \alpha_j$ for $i, j \in [1, r]$ and $i \neq j$. Show that

$$q(x) = (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_r)$$

is the minimal polynomial of α in $K[x]$.

(16) Determine whether or not the following extensions of $\mathbb{Q}$ are Galois:

$$L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{5}); \quad L_2 = \mathbb{Q}(e^{2\pi i/9}); \quad L_3 = \mathbb{Q}(\sqrt[9]{2}); \quad L_4 = \mathbb{Q}\left(\sqrt{3 + \sqrt{7}}\right).$$