

HOMEWORK 5-6. DUE FRIDAY MAY 9

Always $K \subseteq L$ denotes a field extension.

HAND IN: 7.4.9, 7.5.2, 7.5.4, 7.5.5, 7.5.8* (**bonus problem**)

AND

1. Let $f, g \in K[x]$ Prove: $\gcd(f, g)$ computed in $K[x]$ is the same as $\gcd(f, g)$ computed in $L[x]$.
2. (i) Let L be a field, $\sigma: L \rightarrow L'$ an isomorphism, K a subfield of L and $K' = \sigma(K) \subseteq L'$. Prove: $\lambda \rightarrow \sigma\lambda\sigma^{-1}$ is an isomorphism $\text{Aut}_K(L) \rightarrow \text{Aut}_{K'}(L')$.
 (ii) Prove: If $K \subseteq M \subseteq L$ are ANY fields and $\sigma \in \text{Aut}_K(L)$, then $\text{Aut}_{\sigma(M)}(L) = \sigma \text{Aut}_M(L) \sigma^{-1}$.
3. Use the proof of the Primitive Element Theorem to express each of the following fields L as a simple extension of \mathbb{Q} (i.e., $L = \mathbb{Q}(\alpha)$):
 - (i) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$,
 - (ii) $\mathbb{Q}(i, \sqrt{3})$,
 - (iii) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$,
 - (iv) a (minimal) splitting field of $x^5 - 2$.
 Prove that you really have found a single element α such that $L = \mathbb{Q}(\alpha)$.
4. (i) Prove that the group $G = \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ has order 4.
 (ii) Write down all subgroups of G , and for each subgroup identify the fixed field as a simple extension of \mathbb{Q} .
5. (Definition: If L is a (minimal) splitting field of an irreducible polynomial $f \in K[x]$, then the roots of f in L are said to be *conjugates* in L). Find **all** of the conjugates (over \mathbb{Q}) of the following numbers:
 - (i) $\sqrt{5}$, (ii) $\sqrt[4]{5}$, (iii) $\sqrt{2} + \sqrt{5}$, (iv) $\sqrt{1 + \sqrt{5}}$, (v) $\sqrt[3]{1 + \sqrt{5}}$, and (vi) $\sqrt{1 + \sqrt{1 + \sqrt{5}}}$.
 (Hint: Find the minimal polynomial)

DO NOT HAND IN: 7.4.4, 7.5.1, 7.5.3

AND

6. Let $L \subseteq \mathbb{C}$ be a splitting field of $x^p - 2 \in \mathbb{Q}[x]$, where p is a prime.
 - (i) Prove: $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$.
 - (ii) Deduce: $\dim_{\mathbb{Q}} L \leq p(p-1)$.
 - (iii) Prove: $\dim_{\mathbb{Q}} L = p(p-1)$. (Why do p and $p-1$ divide this?)
 - (iv) Prove: $x^p - 2 \in \mathbb{Q}(\zeta_p)[x]$ is irreducible.
7. Prove: If f_1, \dots, f_r are nonconstant polynomials in $K[x]$ then there exists an extension field $L \supseteq K$ such that each polynomial f_i splits into linear factors.
8. Let $a, b \in \mathbb{Z}$. Prove: $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ if and only if $a = t^2b$ for some $t \in \mathbb{Q}$.
9. (i) Find the minimal polynomial of $2^{1/2^m}$ over $\mathbb{Q}(2^{1/m})$ for any positive integer m ; prove your claim.
 More generally, if m and n are positive integers and $m|n$, find the minimal polynomial of $2^{1/n}$ over $\mathbb{Q}(2^{1/m})$, and prove you're correct.

Definition: The *field of algebraic numbers* is the set $\bar{\mathbb{Q}}$ of all complex numbers that are algebraic over \mathbb{Q} .

(ii) Prove: $\bar{\mathbb{Q}}$ is infinite-dimensional over \mathbb{Q} . (Hint: $x^n - 2$.)

(iii) Prove: If $f \in \bar{\mathbb{Q}}[x]$ is nonconstant then f has a root in $\bar{\mathbb{Q}}$. (Hint: f has coefficients.)

Deduce that f splits into a product of linear factors in $\bar{\mathbb{Q}}[x]$.

(Thus, $\bar{\mathbb{Q}}$ has a property in common with \mathbb{C} , but it's countable hence not \mathbb{C} . This property of a field is called "algebraically closed".)