MATH 601 (DUE 11/6)

HIDENORI SHINOHARA

Contents

1. Galois Theory II (P.2)

Exercise. (Problem 1) Let $f(x) \in F[x]$ be an irreducible polynomial of degree d. Let $F \subset K$ be a field extension such that $f(x)$ factors as a product of linear polynomials in $K[x]$. Show that $f(x)$ is separable if and only if there exist d distinct F-algebra homomorphisms, $F[x]/(f(x)) \to K$.

Proof. Without loss of generality, assume $f(x)$ is monic and $f(x) = \prod_{i=1}^{d}(x - a_i)$ for some $a_i \in K$.

Suppose $f(x)$ is separable. Then $a_i \neq a_j$ for all $i \neq j$. For each i, let $\phi_i : F[x]/(f(x)) \to K$ be an F-algebra homomorphism such that $x \mapsto a_i$ and $a \mapsto a$ for all $a \in F$. Then each ϕ_i is distinct because $\phi_i(x) \neq \phi_j(x)$ whenever $i \neq j$. Thus we showed the existence of d distinct F-algebra homomorphisms.

Show the other direction.

□

Exercise. (Problem 2) Let $F \subset F[v_1, \cdots, v_r] = K$ be an algebraic field extension such that the irreducible manic polynomial, $f_i(x) \in F[x]$, for v_i is separable for each i. Let $F \subset L$ be a splitting field of $f(x) := \prod_{i=1}^{r} f_i(x) \in F[x]$. Let $w \in K$ and let $g(x) \in F[x]$ be the minimal manic polynomial of w. Set $d = \deg(g(x))$. Show that there are exactly d distinct F-algebra homomorphisms, $F[w] \to L$.

Proof.

Because of Problem 3, I don't think I'm supposed to show that g is separable.

□

Exercise. (Problem 3) Let $F \subset F[v_1, \cdots, v_r] = K$ be as in the previous problem. Let $w \in K$. Show that the monic irreducible polynomial of w is separable.

Proof.

Can I just use the results of Problem 1 and 2?

□

2. Factoring Polynomials with Coefficients in Finite Fields

Exercise. (Problem 9) Let $\mathbb{F}_q$ be a field with $q = p^m$ elements. Let $f(x) \in \mathbb{F}_q[x]$ be square free. Describe $\gcd(x^q - x, f(x))$ in terms of the linear factors of $f(x)$.

Proof. Since $(x^q - x)' = -1$, $\gcd(x^q - x, (x^q - x)') = 1$. Thus $x^q - x$ is square free by Problem 7 from last week. Thus $x^q - x = \prod_{i=1}^{q}(x - a_i)$ where $\mathbb{F}_q = \{a_1, \cdots, a_q\}$. Each linear factor (if any) of $f(x)$ is associate to $x - a_i$ for some i. Since $f(x)$ is square free, $\gcd(x^q - x, f(x))$ is the product of all the linear factors of $f(x)$. $\square$