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.

Suppose there exist d distinct homomorphisms ϕ_i for $i = 1, \cdots, d$. For any j, $\prod_{i=1}^{d}(\phi_j(x) - a_i) = \phi_j(\prod_{i=1}^{d}(x - a_i)) = \phi_j(f(x)) = 0$, so $\phi_j(x) \in K$ is a root of $f(x)$. Thus $x - \phi_i(x)$ divides $f(x)$ for each i. Since ϕ_i is uniquely determined by the value $\phi_i(x)$, $\phi_i(x) \neq \phi_j(x)$ whenever $i \neq j$. Thus $f(x) = \prod_{i=1}^{d}(x - \phi_i(x))$, and $f(x)$ is separable. □

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?

$\square$

2. Galois Theory II (P.8)

Exercise. (Problem 1) Recall that p is prime and q is a power of p. Define $F_q : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ by $F_q(a) = a^q$. Show that $F_q \in \operatorname{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q)$.

Proof. $F_q(a+b) = (a+b)^q = a^q + b^q$ since $p \mid \binom{q}{i}$ for $1 \leq i \leq q-1$. Thus F_q preserves addition, and it is clear that F_q preserves multiplication, so F_q is a homomorphism. Moreover, any element in $\mathbb{F}_q$ satisfies $x^q - x = 0$, so $F_q(a) = a^q = a$ for any $a \in \mathbb{F}_q$. $\square$

Exercise. (Problem 2) Show that $F_p : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$, $F_p(a) = a^p$ is not an element of $\operatorname{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ unless $q = p$.

Proof. If $q = p$, we are done. Suppose $q > p$. Let $\langle \alpha \rangle = (\mathbb{F}_q)^*$. Then the order of α is $q - 1$, so $F_p(\alpha) = \alpha^p \neq \alpha$. $\square$

Exercise. (Problem 3) Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree r. Explain why $f(x)$ has a root $\alpha \in \mathbb{F}_{q^r}$.

Proof. Let $f(x) = \sum_{i=0}^{r} a_i x^i$. Since $\langle f(x) \rangle$ is a maximal ideal, $\mathbb{F}_q[x]/\langle f(x) \rangle$ is a field with an $\mathbb{F}_q$-basis $\{1, x, \cdots, x^{d-1}\}$. Thus the field contains q^r elements. By the uniqueness of a finite field, there exists an isomorphism $\phi : \mathbb{F}_{q^r} \to \mathbb{F}_q[x]/\langle f(x) \rangle$. Let $\alpha = \phi^{-1}(x)$. Then $\phi(\sum_{i=0}^{r} a_i \alpha^i) = \sum_{i=0}^{r} a_i x^i = 0$. Thus $\mathbb{F}_{q^r}$ contains a root of $f(x)$. $\square$

3. 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 $f(x)$. $\square$