

MATH 601 (DUE 11/6)

HIDENORI SHINOHARA

CONTENTS

1. Galois Theory II (P.2)	1
2. Galois Theory II (P.8)	2
3. Factoring Polynomials with Coefficients in Finite Fields	3

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, $F[x]/(f(x)) \rightarrow K$.

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 $\phi_i : F[x]/(f(x)) \rightarrow K$ 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 $i = 1, \dots, d$. 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. \square

Lemma 1.1. Let $\phi : F \rightarrow F'$ be an isomorphism. Let $K = F[v_1, \dots, v_n]$. Suppose that for each v_i , there exists a separable $f_i \in F[x]$ such that $f_i(v_i) = 0$. (f_i 's need not be irreducible.) Let L be the splitting field of $f = \prod f_i$. Then there exist $[K : F]$ homomorphisms $\Phi : K \rightarrow L$ such that $\Phi = \phi$ on F .

Proof. We will use induction on n . Suppose $n = 1$. The minimal polynomial for v_1 divides f_1 , and f_1 is a separable function, so the minimal polynomial has $[K : F]$ distinct roots. Therefore, there exist $[K : F]$ homomorphisms from K to L .

Suppose that we have shown this proposition for $n \leq k$ for some $k \in \mathbb{N}$. Let $n = k + 1$. By the inductive hypothesis ($n = 1$), we have $[F[v_1] : F]$ homomorphisms ψ from $F[v_1]$ to L . In other words, we have $[F[v_1] : F]$ isomorphisms ψ from $F[v_1]$ to $F[\psi(v_1)]$.

$$\begin{array}{ccc}
K & \xrightarrow{\Phi} & L \\
| & & | \\
F[v_1] & \xrightarrow{\psi} & F[\psi(v_1)] \\
| & & | \\
F & \xrightarrow{\phi} & F'
\end{array}$$

Now, by applying the inductive hypothesis on the “upper” half of the diagram, we get $[K : F[v_1]]$ lifts of each ψ . Therefore, in total, we get $[K : F] = [K : F[v_1]][F[v_1] : F]$ homomorphisms Φ that agree with ϕ on F . \square

Exercise. (Problem 2) Let $F \subset F[v_1, \dots, v_r] = K$ be an algebraic field extension such that the irreducible monic 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 monic polynomial of w . Set $d = \deg(g(x))$. Show that there are exactly d distinct F -algebra homomorphisms, $F[w] \rightarrow L$.

Proof. By applying Lemma 1.1 to the whole diagram, we know that there exist $[K : F]$ F -algebra homomorphisms Φ . Moreover, by applying Lemma 1.1 to the “upper” half of the diagram, each $\psi : F[w] \rightarrow F[\psi(w)]$ can be lifted to exactly $[K : F[w]]$ distinct homomorphisms.

$$\begin{array}{ccc}
K & \xrightarrow{\Phi} & L \\
| & & | \\
F[w] & \xrightarrow{\psi} & F[\psi(w)] \\
| & & | \\
F & \xrightarrow{\text{Id}} & F'
\end{array}$$

This implies that there has to be exactly $[K : F]/[K : F[w]] = [F[w] : F]$ homomorphisms. In other words, there are exactly d homomorphisms. \square

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

Proof. By Problem 1 and 2, this is trivial because $F[w]$ is isomorphic to $F[x]/(f(x))$ by Lemma 2.1 (Field Extension handout). \square

2. GALOIS THEORY II (P.8)

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

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 $a \in \mathbb{F}_q$.

Finally, in order to show that F_q is bijective, it suffices to check if it is injective since \mathbb{F}_{q^r} is finite. $F_q(a) = 0 \implies a^q = 0 \implies a = 0$, so F_q is indeed injective. \square

Exercise. (Problem 2) Show that $F_p : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_{q^r}$, $F_p(a) = a^p$ is not an element of $\text{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ 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 $\{1, x, \dots, x^{r-1}\}$. Thus the field contains q^r elements. By the uniqueness of a finite field, there exists an isomorphism $\phi : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q[x]/\langle f(x) \rangle$. 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

Exercise. (Problem 4) With $f(x)$ as in the previous problem, show that $f(x) = \prod_{i=0}^{r-1} (x - \alpha^{q^i}) \in \mathbb{F}_{q^r}[x]$. Conclude that \mathbb{F}_{q^r} is a splitting field for $f(x)$ over \mathbb{F}_q .

Proof. Let $G = \langle F_q \rangle \leq \text{Aut}(\mathbb{F}_{q^r})$. Then G is a finite subgroup because $(F_q)^r = F_{q^r} = \text{Id}$. Moreover, $\mathbb{F}_{q^r}^G = \mathbb{F}_q$ because \mathbb{F}_q is exactly the set of all the roots of $x^q - x$. By Theorem 11 (iv) from Galois Theory II, f must factor as a product of linear polynomials in $\mathbb{F}_{q^r}[x]$. \square

Exercise. (Problem 5) Prove $\text{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q) \simeq \mathbb{Z}/(r)$. Prove $|\text{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q)| = [\mathbb{F}_{q^r} : \mathbb{F}_q]$.

Proof. Let $G = \langle F_q \rangle \leq \text{Aut}(\mathbb{F}_{q^r})$ as in the previous problem. We claim that $\text{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q) = G$. By Problem 1, $G \leq \text{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. By Proposition 12 from Galois Theory II, $[\mathbb{F}_{q^r} : \mathbb{F}_q] \leq |G|$, so $r \leq |G|$. On the other hand, by Theorem 8 from Galois Theory II, $|\text{Aut}(\mathbb{F}_{q^r}/\mathbb{F}_q)| \leq [\mathbb{F}_{q^r} : \mathbb{F}_q] = r$. \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 $\mathbb{F}_q = \{a_1, \dots, a_q\}$. 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

Exercise. (Problem 10) Let $f(x) \in \mathbb{F}_q[x]$ be square free. Describe, $h(x) = \gcd(x^{q^2} - x, f(x))$, in terms of the irreducible quadratic polynomials which divide $f(x)$ and whatever other information is necessary.

Proof. Since every element in \mathbb{F}_q is a root of $x^{q^2} - x$, $h(x)$ is divisible by all the linear polynomials that divide $f(x)$.

Let $g(x) \in \mathbb{F}_q[x]$ be an irreducible monic quadratic polynomial. Then $\mathbb{F}_q[x]/(g(x)) \cong \mathbb{F}_{q^2}$ with an isomorphism ϕ . Then $\phi(x)$ is a root of $g(x)$. Thus $g = (x - \alpha)(x - \beta)$ in $\mathbb{F}_{q^2}[x]$.

Moreover, every element in \mathbb{F}_{q^2} is a root of $x^{q^2} - x$. Thus $g = (x - \alpha)(x - \beta) \mid x^{q^2} - x$. Therefore, $h(x)$ is divisible by all the irreducible monic quadratic polynomials that divide $f(x)$.

Finally, the set of roots of $x^{q^2} - x$ is exactly \mathbb{F}_{q^2} . Since $[\mathbb{F}_{q^2} : \mathbb{F}_q] = 2$, the degree of the minimal polynomial of each element must be either 1 or 2. In other words, $x^{q^2} - x$ is a product of some linear and quadratic polynomials in $\mathbb{F}_q[x]$.

Therefore, $h(x)$ is exactly the product of all the irreducible monic polynomials of degree 1 or 2 that divide $f(x)$. ($x^{q^2} - x$ may or may not be square free, but $f(x)$ is square free, so $h(x)$ must be square free.) \square

Lemma 3.1. Suppose $f \in \mathbb{F}_q[x]$ is irreducible. Let $d \in \mathbb{N}$. Then $f \mid (x^{q^d} - x)$ if and only if $\deg(f) \mid d$.

Proof. Let $d \in \mathbb{N}$ be given. Let $n = \deg(f)$. Then $\mathbb{F}_q[x]/(f(x)) = \mathbb{F}_{q^n}$ contains a root α of $f(x)$.

Suppose $n \mid d$. $\alpha^{q^n} - \alpha = 0$ implies $0 = (\alpha^{q^n} - \alpha)^{q^n} = \alpha^{q^{2n}} - \alpha^{q^n} = \alpha^{q^{2n}} - \alpha$. By repeating this process, we get $\alpha^{q^d} - \alpha = 0$ since $n \mid d$. Thus α satisfies $f(x)$ and $x^{q^d} - x$, and $f(x)$ is irreducible. Thus $f \mid x^{q^d} - x$.

Suppose $f(x) \nmid (x^{q^d} - x)$. Since $f(x)$ is an irreducible polynomial with a root α , it must be the minimal polynomial of α . Thus $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$. $f(x) \nmid (x^{q^d} - x)$ implies that α satisfies $x^{q^d} - x$. Thus $\alpha \in \mathbb{F}_{q^d}$. Then $d = [\mathbb{F}_{q^d} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q]$, so $n \mid d$. \square

Exercise. (Problem 11) Given a square free polynomial $f(x) \in \mathbb{F}_q[x]$, describe how to use repeated gcd calculations to factor $f(x)$ as $f = f_1 f_2 \cdots f_r$, where each f_i is a product of distinct irreducible factors of degree i .

Proof. We will use Lemma 3.1 above. We will start with $n = 1$.

- If $f(x)$ is a unit, terminate.
- Calculate $h(x) = \gcd(x^{q^n} - x, f(x))$. This is the product of all irreducible polynomials of $f(x)$ of degree n by Lemma 3.1.
- Record $h(x)$. Set $f(x) = f(x)/h(x)$ and $n = n + 1$. Repeat.

Then the h 's that we record are the products of distinct irreducible of factors of degree i for each i . \square

Exercise. (Problem 12) Prove the following criterion for a degree n polynomial $f(x) \in \mathbb{F}_q[x]$ to be irreducible: $f(x)$ is irreducible if and only if

- $\gcd(f(x), x^{q^n} - x) = f(x)$, and
- For each proper divisor d of n , $\gcd(f(x), x^{q^d} - x) = 1$.

Proof. Suppose $f(x)$ is irreducible. By Lemma 3.1, $\gcd(f(x), x^{q^n} - x) = f(x)$. Since the same lemma implies that $x^{q^d} - x$ cannot be divided by any irreducible polynomial of degree $> d$, $\gcd(f(x), x^{q^d} - x) = 1$.

Suppose the two conditions are met. We will show that $f(x)$ is irreducible. Let $g(x)$ be an irreducible polynomial that divides $f(x)$. Since $\gcd(f(x), x^{q^d} - x) = 1$ for each proper divisor d of n , $\gcd(g(x), x^{q^d} - x) = 1$ as well. By the lemma, $\deg(g(x)) \nmid d$. Since $\gcd(f, x^{q^n} - x) = f$, $\gcd(g, x^{q^n} - x) = g$. By the lemma, $\deg(g) \mid n$. Therefore, $\deg(g)$ is a divisor of n that is not a proper divisor of n . In other words, $\deg(g) = n$, so f is irreducible. \square

Exercise. (Problem 13) Suppose $f(x) \in \mathbb{F}_q[x]$ is a product of m distinct monic irreducible polynomials of degree r . To what ring is $\mathbb{F}_q[x]/(f(x))$ isomorphic?

Proof. By the Chinese remainder theorem, $\mathbb{F}_q[x]/(f(x)) = \mathbb{F}_q[x]/(f_1) \times \cdots \times \mathbb{F}_q[x]/(f_m)$. Thus $\mathbb{F}_q[x]/(f(x)) = \mathbb{F}_{q^r} \times \cdots \times \mathbb{F}_{q^r}$ (m times) \square