

MATH 601 (DUE 10/23)

HIDENORI SHINOHARA

CONTENTS

1. Field Extension

1

1. FIELD EXTENSION

Exercise. (Problem 1) Let p be a prime number. Let $K = \mathbb{Z}/p\mathbb{Z}(t)$ be the fraction field of $\mathbb{Z}/p\mathbb{Z}[t]$.

- (i) What is the characteristic of K ?
- (ii) What is the characteristic of any extension field of K ?
- (iii) Show that the Frobenius endomorphism, $F : K \rightarrow K$ is not a ring isomorphism.
- (iv) Let $f(x) = x^p - t \in K[x]$. Prove that $f(x)$ is irreducible.
- (v) Prove that $f(x)$ is not a separable polynomial.
- (vi) Construct an explicit field extension $K \subset L$ such that $f(x) \in L[x]$ has a factor of positive degree $< p$.
- (vii) With f and L above find all the roots of $f(x)$ in L and determine their multiplicities.

Proof.

- (i) We will prove in general that if $R \subset S$ are both commutative rings with 1, they have the same characteristic. Let $i : R \rightarrow S$ be the inclusion map. Let $\phi : \mathbb{Z} \rightarrow R$ be the unique ring homomorphism.

Then $i \circ \phi : \mathbb{Z} \rightarrow S$ is a ring homomorphism, and this is the only homomorphism from \mathbb{Z} to S by the uniqueness.

$$\begin{aligned} a \in \ker(\phi) &\iff \phi(a) = 0 \\ &\iff i(\phi(a)) = 0 && (i \text{ is injective}) \\ &\iff a \in \ker(i \circ \phi). \end{aligned}$$

Thus $\ker(\phi) = \ker(i \circ \phi)$, so R and S have the same characteristic.

Therefore, $\mathbb{Z}/p\mathbb{Z}$ has the same characteristic as K . The kernel of $\psi : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ is (p) , so the characteristic of K is p .

- (ii) Using the result that we proved in (i), we conclude that the characteristic of any extension field of K is p .

(iii) Suppose that it is a ring isomorphism. Let $a/b \in K$ be chosen such that $F(a/b) = t$.

$$\begin{aligned} \left(\frac{a}{b}\right)^p = t &\implies a^p = tb^p \\ &\implies p \deg(a) = \deg(t) + p \deg(b) \\ &\implies p(\deg(a) - \deg(b)) = 1. \end{aligned}$$

However, $p \geq 2$, so this is impossible. Therefore, F is not a ring isomorphism.

- (iv) t is an irreducible element in $\mathbb{Z}/p\mathbb{Z}[t]$ because $t = ab$ implies that the degree of a or b must be 0, which implies that one of them is a unit. By Corollary 4 on P.300 (Dummit and Foote), $\mathbb{Z}/p\mathbb{Z}[t]$ is a principal ideal domain and unique factorization domain. By Proposition 2 on P.284 (Dummit and Foote), t is a prime element in $\mathbb{Z}/p\mathbb{Z}[t]$. By the Eisenstein irreducibility criterion from the Factorization in Integral Domain handout, $x^p - t$ is irreducible in $K[x]$ because $-t \in (t)$ but $-t \notin (t^2)$.
- (v) $f'(x) = px^{p-1} = 0$. Thus $f(x) \in \text{GCD}(f(x), f'(x))$ and $f(x) = x^p - t$ is not a unit. By Lemma 3.2 of the Field Extension handout, $f(x)$ is not separable.
- (vi) Let $L = K[y]/(y^p - t)$. Since $y^p - t$ is irreducible in $K[y]$, $(y^p - t)$ is a maximal ideal in $K[y]$. Thus L is a field. Then $x^p - t$ has a root in L because $y^p - t = 0$. This implies the existence of a linear factor of $x^p - t$.
- (vii) In $L[x]$, $(x - y)^p = \sum_{i=0}^p \binom{p}{i} x^i (-y)^{p-i} = x^p - y^p$ because $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$. Since $y^p = t$, $x^p - y^p = x^p - t$. Therefore, the only root is y and the multiplicity is p . \square

Exercise. (Problem 2) Let F be a field of characteristic 0. Let $f(x) \in F[x]$ be an irreducible polynomial. Then $f(x)$ is separable.

Proof. Let $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$ be an irreducible polynomial with $a_n \neq 0$. Since $f(x)$ is irreducible, $f(x)$ is neither a unit nor 0. Since F is a field, all polynomials of degree 0 are units. Thus $\deg(f(x)) = n \geq 1$. It suffices to show that $\text{GCD}(f(x), f'(x)) = F^*$ by Lemma 3.2. Let $g(x) \in F[x]$ be given such that $g(x) \mid f(x), g(x) \mid f'(x)$. Since $f(x)$ is irreducible, either $g(x)$ is a unit or there exists a unit $u \in F^*$ such that $g(x) = uf(x)$. Suppose $g(x)$ is not a unit. Since $g(x) \mid f'(x)$, $f'(x) = h(x)g(x) = uh(x)f(x)$ for some $h(x) \in F[x]$. Thus $\deg(f'(x)) = \deg(uh(x)) + \deg(f(x))$.

- $f'(x) = \sum_{i=1}^n i a_i x^{i-1}, n \geq 1$ and $a_n \neq 0$. Since F is a field of characteristic 0, $na_n \neq 0$. Therefore, $\deg(f'(x)) = n - 1$.
- $\deg(uh(x)) \geq 0$.
- $\deg(f(x)) = n$.

However, this implies that $n - 1 \geq 0 + n = n$. This is a contradiction, so $g(x)$ must be a unit. Therefore, $\text{GCD}(f(x), f'(x)) = F^*$. \square

Exercise. (Problem 3) Let F be a field. Let $f(x) \in F[x]$ be an irreducible polynomial which is not separable. Show that $f'(x) = 0 \in F[x]$.

Proof. Suppose $f(x)$ is irreducible. Then $f(x) \neq 0$ and $f(x)$ is not a unit by definition. Thus $\deg(f(x)) \geq 1$.

Since $f(x)$ is not separable, there exists a non-unit $g(x) \in F[x]$ such that $g(x) \mid f(x)$ and $g(x) \mid f'(x)$ by Lemma 3.2 from the Field Extension handout. Since $f(x)$ is irreducible and $g(x)$ is not a unit, $f(x)$ is the product of $g(x)$ and a unit. This implies that $\deg(f(x)) = \deg(g(x))$.

Since $g(x) \mid f'(x)$, $f'(x) = h(x)g(x)$. If $f'(x) = 0$, we are done. Suppose otherwise. Then $\deg(f'(x)) = \deg(h(x)) + \deg(g(x)) = \deg(h(x)) + \deg(f(x)) \geq \deg(f(x))$. However, by the definition of the $'$ operator, $\deg(f'(x)) < \deg(f(x))$. This is a contradiction, so $f'(x) = 0$. \square

Exercise. (Problem 4) Let F be a field of prime characteristic p . Let $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$ be an irreducible polynomial. Give a necessary and sufficient criterion for $f(x)$ to be inseparable in terms of the coefficients a_i .

Proof. We claim that $\forall i, (i \notin p\mathbb{Z} \implies a_i = 0)$ is a necessary and sufficient criterion.

- Suppose $f(x)$ is inseparable. By Lemma 5.5 from the Field Extension handout, $f'(x) = 0$. If $f'(x) = 0$, then $ia_i = 0$ for each i . Since p is a prime, a_i must be 0 if $i \notin p\mathbb{Z}$.
- Suppose $\forall i, (i \notin p\mathbb{Z} \implies a_i = 0)$. Then $f'(x) = 0$, so $f(x) \mid f(x), f(x) \mid f'(x)$ and $f(x)$ is not a unit since $f(x)$ is irreducible. Therefore, $\text{GCD}(f(x), f'(x)) \neq F^\times$, so f is inseparable by Lemma 3.2.

Hence, $\forall i, (i \notin p\mathbb{Z} \implies a_i = 0)$ is a necessary and sufficient criterion. \square

Exercise. (Problem 5) What is the characteristic of the ring $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$?

Proof. Then ϕ is injective, so the characteristic is 0.

$1 \mapsto (1, 1, 1)$

\square

Exercise. (Problem 6) Let K be a finite field of characteristic p . Let $a, b \in K^*$ be two elements which have the same order in this finite group. Show that $\mathbb{Z}/p[a] = \mathbb{Z}/p[b]$ as subfields of K .

Proof.

Can I just say they both have the same number of elements and use the lemma from class?

\square