MATH 601 (DUE 10/23)

HIDENORI SHINOHARA

Contents

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 endormophism, $F : K \to K$ 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 $i : R \to S$ be the inclusion map. Let $\phi : \mathbb{Z} \to R$ be the unique ring homomorphism.

Then $i \circ \phi : \mathbb{Z} \to S$ 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 $\psi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ 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 $f(x) \in \mathrm{GCD}(f(x), f'(x))$ 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 that $L[x]$ contains 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, $x^p - t = (x - y)^p$, so the only root is y and the multiplicity is p.

□

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 $\mathrm{GCD}(f(x), f'(x)) = F^*$ 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 $h(x) \in F[x]$.

- $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}, n \geq 1$ 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 $n - 1 = \deg(f'(x)) = \deg(uh(x)) + \deg(f(x)) \geq n$. This is a contradiction, so $g(x)$ must be a unit. Therefore, $\mathrm{GCD}(f(x), f'(x)) = F^*$. □

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. Therefore, $GCD(f(x), f'(x)) \neq F^{\times}$, 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. Let ϕ be the only ring homomorphism from $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Then $\phi(a) = (a, a + (2), a + (10))$ for any $a \in \mathbb{Z}$. If $\phi(a) = (0, 0, 0)$, then $a = 0$. Since $\ker(\phi) = (0)$, the characteristic is 0. $\square$

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. Let n be the order of a and b. Then $\langle a \rangle, \langle b \rangle$ are both subgroups of K^* with n elements. By Proposition 4.1 in the Field Extension handout, they are the n-th roots of 1 contained in F. In other words, $\langle a \rangle = \langle b \rangle$. $\mathbb{Z}/p[a] = \{\sum_{i=0}^{n} a_i a^i \mid n \geq 0, a_i \in \mathbb{Z}/p\}$, so it is the collection of all linear combinations of $\langle a \rangle$ over $\mathbb{Z}/p$. Similarly, $\mathbb{Z}/p[b]$ is the collection of all linear combinations of $\langle b \rangle$ over $\mathbb{Z}/p$. Since $\langle a \rangle = \langle b \rangle$, $\mathbb{Z}/p[a] = \mathbb{Z}/p[b]$. $\square$

Exercise. (Problem 7) Let K be a field with 81 elements. List all positive integers n which are orders of elements in the group, K^*. Now compute the function $d(n) = [\mathbb{Z}/3[a] : \mathbb{Z}/3]$, where $a \in K^*$ is any element of order n. Present your results in the form of a table with entries n and $d(n)$.

Proof. Problem 6 shows that $d(n)$ is well defined. K^* is a cyclic group with 80 elements. Let α be a generator. Since α^{40} is the only element of order 2 in $\langle \alpha \rangle$, $2 = \alpha^{40}$.

Let $a \in K^*$ be given. Let n be the order of a. By Problem 6, we will assume that $a = \alpha^k$ where $k = 80/n$. This is because $(\mathbb{Z}/3)[a] = (\mathbb{Z}/3)[\alpha^k]$. $\mathbb{Z}/3[a] \leq K$ as additive groups. $(\mathbb{Z}/3[a])^* \leq K^*$ as multiplicative groups. By Lagrange's theorem, $|\mathbb{Z}/3[a]| \mid 81$ and $(|\mathbb{Z}/3[a]| - 1) \mid 81$. Thus $|\mathbb{Z}/3[a]| \in \{3, 9, 81\}$.

- If $n = 1$, then $a = 1$, so $\mathbb{Z}/3[a] = \mathbb{Z}/3$. Thus $d(n) = 1$.
- If $n = 2$, then $a = 2 = \alpha^{40}$, so $\mathbb{Z}/3[a] = \mathbb{Z}/3$. Thus $d(n) = 1$.
- If $n = 4$, then $\mathbb{Z}/3[a]$ must contain at least 4 elements. Thus $|\mathbb{Z}/3[a]| \in \{9, 81\}$. Since $(\alpha^{10})^2 = \alpha^{20} = a$, $\mathbb{Z}/3[a] \subset \mathbb{Z}/3[\alpha^{10}]$. We will show below that if $n = 8$, then $|\mathbb{Z}/3[\alpha^{10}]| = 9$. Thus $|\mathbb{Z}/3[a]| = 9$, so $d(n) = 2$.

- Since $a = \alpha^{16}, 2 = \alpha^{40} \in \mathbb{Z}/3[a]$, $\alpha^8 \in \mathbb{Z}/3[a]$. Therefore, $\mathbb{Z}/3[a]$ must contain at least 10 elements, so $\mathbb{Z}/3[a] = K$. Since $[\mathbb{Z}/3[a] : \mathbb{Z}/3]$ is the dimension of $\mathbb{Z}/3[a]$ as a $\mathbb{Z}/3$-vector space and $|\mathbb{Z}/3[a]| = |\mathbb{Z}/3|^4$, $d(n) = 4$.
- Suppose $n = 8$. Then $a = \alpha^{10}$, so $\{\alpha^{10}, \alpha^{20}, \cdots, \alpha^{70}, \alpha^{80} = 1\} \subset \mathbb{Z}/3[a]$. Moreover, $0 \in \mathbb{Z}/3[a]$. Thus $S = \{0, \alpha^{10}, \alpha^{20}, \cdots, \alpha^{70}, \alpha^{80}\} \subset \mathbb{Z}/3[a]$. We claim that S is a subfield.
  - S is nonempty.
  - Claim: S is closed under subtraction. Every element in S satisfies $x^9 - x = 0$, and S contains 9 elements. Thus $x^9 - x$ can be expressed as the product of 9 linear factors in $S[x]$. Therefore, S contains all the nine roots of $x^9 - x = 0$. Let $r, r' \in S$.

$$\begin{aligned}
(r - r')^9 - (r - r') &= F(F(r + (-r'))) - (r - r') \\
&= F(r^3 + (-r')^3) - (r - r') \\
&= (r^9 + (-r')^9) - (r - r') \\
&= (r^9 - r) - ((r')^9 - r') \\
&= 0.
\end{aligned}$$

    Therefore, $r - r'$ is a root of $x^9 - x = 0$. Since S contains all the roots of $x^9 - x = 0$, $r - r' \in S$.
  - Claim: S is closed under multiplication. $\alpha^k \alpha^l = \alpha^{k+l} \in S$.

  Therefore, S is a subring of K. Since S is a finite integral domain, it must be a field. (Corollary 3, P.228, Dummit and Foote) $2 = \alpha^{40} \in \mathbb{Z}/3[a]$, so S contains both a and $\mathbb{Z}/3$. Thus S is a subfield containing $\mathbb{Z}/3$ and a. Moreover, S is the smallest subfield with such properties because a subfield must be closed under multiplication. Hence, $S = \mathbb{Z}/3[a]$. Thus $|\mathbb{Z}/3[a]| = 9$, so $d(n) = 2$.
- If $n \geq 10$, then $\langle \mathbb{Z}/3[a] \rangle \geq 10$, so $\mathbb{Z}/3[a] = K$.

  Since $[\mathbb{Z}/3[a] : \mathbb{Z}/3]$ is the dimension of $\mathbb{Z}/3[a]$ as a $\mathbb{Z}/3$-vector space and $|\mathbb{Z}/3[a]| = |\mathbb{Z}/3|^4$, $d(n) = 4$.

n	$d(n)$
1	1
2	1
4	2
5	4
8	2
10	4
16	4
20	4
40	4
80	4

$\square$

2. Factorization in Integral Domain

Exercise. (Problem 7) Define $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid p\}$. Now $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$ and $p\mathbb{Z}_{(p)}$ is a maximal ideal.

(i) Prove that there is a ring isomorphism, $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$.

(ii) Suppose given $f \in \mathbb{Z}_{(p)}[x, y]$ such that when viewed as an element of $\mathbb{Q}(x)[y]$, f has content 1 and degree n in y. Prove that if the reduction mod p of f, $f_0 \in \mathbb{Z}/p[x, y]$ is irreducible and of degree n in y, then f is irreducible in $\mathbb{Q}[x, y]$.

Proof.

(i) Define $\phi : \mathbb{Z}_{(p)} \to \mathbb{Z}/p\mathbb{Z}$ such that $a/b \mapsto ab^{-1}$.
- Claim: ϕ is well-defined. If $p \nmid b$, then $b \notin \mathbb{Z}/p\mathbb{Z}$, so b^{-1} exists. Moreover, if $a/b = c/d \in \mathbb{Z}(p)$, then $ad = bc$, so $ab^{-1} = cd^{-1}$.
- Claim: ϕ is surjective. For all $a \in \mathbb{Z}/p\mathbb{Z}$, $\phi(a/1) = a$.
- Claim: $\ker(\phi) = p\mathbb{Z}_{(p)}$.

$$\begin{aligned} \frac{a}{b} \in \ker(\phi) &\iff ab^{-1} = 0 \\ &\iff p \mid a \\ &\iff \frac{a}{b} \in p\mathbb{Z}_{(p)}. \end{aligned}$$

By the first isomorphism theorem for rings (Theorem 7, P.243, Dummit and Foote), $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$.

(ii) Suppose, on the contrary, that $f(x, y)$ is not irreducible in $\mathbb{Q}[x, y]$. This implies the existence of non-unit polynomials $f_1(x, y), f_2(x, y) \in \mathbb{Q}[x, y]$ such that $f = f_1 f_2$. Since f_1 is not a unit, if $\deg_y(f_1) = 0$, then $\deg_x(f_1) \geq 1$. This implies that $f(x, y)$ has a factor that is a non-constant polynomial in x. However, this is not possible because the content of f when viewed as an element of $\mathbb{Q}(x)[y]$ is 1. Therefore, $\deg_y(f_1) \geq 1$. Similarly, $\deg_y(f_2) \geq 1$.

Let $f_{1,0}, f_{2,0}$ be the reduction mod p of f_1, f_2, respectively. Then $f_0 = f_{1,0} f_{2,0}$. This is because the reduction map $a/b \mapsto ab^{-1}$ is a ring homomorphism as shown in Part (i). Since $f_0 \in \mathbb{Z}/p[x, y]$ is irreducible, one of $f_{1,0}$ or $f_{2,0}$ must be a unit. Without loss of generality, suppose that $f_{1,0}$ is a unit. Then $\deg_y(f_{1,0}) = 0$. $\deg_y(f_{2,0}) \leq \deg_y(f_2)$ because the reduction map maps 0 to 0. This implies that $\deg_y(f_0) = \deg_y(f_{1,0}) + \deg_y(f_{2,0}) < \deg_y(f_1) + \deg_y(f_2) = \deg(f)$. However, this is a contradiction because f_0 must have the same degree in y as f. Therefore, $f(x, y)$ must be irreducible in $\mathbb{Q}[x, y]$.

$\square$

Exercise. (Problem 10) Prove that $x^4 + x^3 + x^2 + x + 3 \in \mathbb{Q}[x]$ is irreducible.

Proof. By the third properties of the content from the factorization in integral domains handout, $f(x) = x^4 + x^3 + x^2 + x + 3$ is primitive. By Corollary 1(ii) of the factorization in integral domains handout, it suffices to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Since $\deg(f(x)) = 4$, if $f(x)$ is not irreducible it must have a factor of degree 1 or 2.

If there exists a factor of degree 1, then $f(x)$ must have a root in $\mathbb{Z}[x]$. If $x(x^3+x^2+x^1+1) = -3$, x must divide 3. In other words, the only values that may be a root of $f(x)$ are $\pm 1, \pm 3$.

However, none of them are actually roots because $f(3) = 123, f(-3) = 63, f(1) = 7, f(-1) = 3$.

If there exists a factor of degree 2, then $f(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b + ac + d)x^2 + (bc + ad)x + bd$ for some $a, b, c, d \in \mathbb{Z}$. Then $bd = 3$. This implies that $(b, d) = (1, 3), (-1, -3), (3, 1), (-3, -1)$. By symmetry, it suffices to only check $(1, 3), (-1, -3)$.

- If $(b, d) = (1, 3)$, then we have a system of equations

  $$\begin{cases} a + c &= 1 \\ c + 3a &= 1. \end{cases}$$

  Thus $a = 0, c = 1$. However, $b + ac + d = 1 + 0 + 3 = 4 \neq 1$.
- If $(b, d) = (-1, -3)$, then we have a system of equations

  $$\begin{cases} a + c &= 1 \\ -c - 3a &= 1. \end{cases}$$

  Thus $a = -1, c = 2$. However, $b + ac + d = -1 + -2 + -3 = -6 \neq 1$.

Therefore, there exist no such a, b, c, d, so $f(x)$ must be irreducible. $\square$

Exercise. (Problem 11) Let R be a commutative ring and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ a nonzero polynomial of degree d. Suppose that $a_n \in R^*$. Show that $R[x]/(f(x))$ is a free R-module with basis, $1, x, x^2, \cdots, x^{n-1}$. In other words, using the notation, $I := (f(x))$, show that every element of $R[x]/I$ may be written as an R-linear combination of $1 + I, \cdots, x^{n-1} + I$ in exactly one way.

Proof. First, we will show the uniqueness. Suppose $\sum_{i=0}^{n-1} b_i(x^i + I) = \sum_{i=0}^{n-1} c_i(x^i + I)$.

$$\begin{aligned} \sum_{i=0}^{n-1} b_i(x^i + I) = \sum_{i=0}^{n-1} c_i(x^i + I) &\implies (\sum_{i=0}^{n-1}(b_i - c_i)x^i) + I = 0 \\ &\implies \sum_{i=0}^{n-1}(b_i - c_i)x^i \in (f(x)) \\ &\implies \exists g(x) \in R[x], \sum_{i=0}^{n-1}(b_i - c_i)x^i = g(x)f(x). \end{aligned}$$

If $g(x) = 0$, then $b_i - c_i = 0$ for each i, so we are done. Suppose $g(x) \neq 0$. Since the leading coefficient of $f(x)$ is a unit, $\deg(g(x)f(x)) \geq \deg(f(x)) = n$. However, this is a contradiction because the left hand side is either 0 or a polynomial of degree $\leq n - 1$.

Next, we will show the existence by induction. Let $P(m)$ be the statement "$\sum_{i=0}^{m} b_i x^i + I \in R/I$ may be written as an R-linear combination of $1 + I, \cdots, x^{n-1} + I$." $P(m)$ is clearly true when $m \leq n-1$. Suppose that $P(m)$ is true for some $m \geq n-1$. We will show that $P(m+1)$ is true. Let $h(x) = \sum_{i=0}^{m+1} b_i x^i + I$. Let $h'(x) = h(x) - \frac{b_{m+1}}{a_n} f(x) x^{m+1-n}$.

- This is possible because a_n is a unit and $m + 1 - n \geq (n-1) + 1 - n = 0$.
- $h'(x)$ can be written now as $\sum_{i=0}^{m} c_i x^i + I$ for some $c_i \in R$.
- $h(x) + I = h'(x) + I$ because $h(x) - h'(x) \in I = (f(x))$.

By the inductive hypothesis, $h(x) + I$ can be written as an R-linear combination of $1 + I, \cdots, x^{n-1} + I$.

By induction, $P(m)$ is true for any non-negative integer m. $\square$