# MATH 601 (DUE 10/30)

HIDENORI SHINOHARA

## Contents



## 1. Factoring Polynomials with coefficients in Finite Fields

**Exercise.** (Problem 1) Consider the Frobenius homomorphism, $F_p : \mathbb{F}_q \to \mathbb{F}_q$. Show that this homomorphism is bijective. If $q = p$, identify it with a familiar homomorphism.

*Proof.* Since $\mathbb{F}_q$ is finite, it suffices to show that $F_p$ is injective. $F_p(a) = 0 \implies a^p = 0$. $a^p = 0 \implies a = 0$ because $\mathbb{F}_q$ contains no zero divisor. If $q = p$, $\mathbb{F}_q \cong \mathbb{Z}/p\mathbb{Z}$, which is a cyclic additive group generated by 1. Since $F_p(1) = 1$, $F_p$ must be the identity homomorphism. □

**Exercise.** (Problem 2) Let $K$ be a field of characteristic $p$. Which polynomials $f(x) \in K[x]$ satisfies $f'(x) = 0$?

*Proof.* $f'(x) = \sum_{i=1}^n i a_i x^i = 0 \iff (\forall i, i \notin (p) \implies a_i = 0)$ since if $i \in (p)$, $i a_i = 0$ regardless of what $a_i$ is. □

**Exercise.** (Problem 3) Suppose that $f(x) \in \mathbb{F}_q[x]$ satisfies $f'(x) = 0$. Show that there exists $g(x) \in \mathbb{F}_q[x]$ with $g^p = f$.

*Proof.* By Problem 2, $f(x)$ with $f'(x) = 0$ can be always written as $\sum_{i=0}^n a_i x^{pi}$.

$$\begin{aligned}
(\sum_{i=0}^n F_p^{-1}(a_i)x^i)^p &= (F_p^{-1}(a_n)x^n + \sum_{i=0}^n F_p^{-1}(a_i)x^i)^p \\
&= a_n x^{pn} + (\sum_{i=0}^{n-1} F_p^{-1}(a_i)x^i)^p \\
&\vdots \\
&= \sum_{i=0}^n a_i x^{pi} = f.
\end{aligned}$$

□

**Exercise.** (Problem 4) Show that there are no inseparable irreducible polynomials, $f(x) \in \mathbb{F}_q[x]$.

*Proof.* If $f$ is inseparable, $\gcd(f, f') \neq F^\times$. If $f' = 0$, then $f$ has a proper factor by Problem 3. Otherwise, $f$ has a factor of degree between 1 and $\deg(f') = \deg(f) - 1$, so $f$ is not irreducible. $\square$

**Exercise.** (Problem 5) Suppose that $f(x) \in \mathbb{F}_q[x]$ and $\gcd(f, f') = f$. How can you reduce the problem of factoring $f$ to a simpler problem?

*Proof.* If $f' \neq 0$, $f \nmid f'$ because $\deg(f') < \deg(f)$. Thus $\gcd(f, f') = f$ implies $f' = 0$. By Problem 3, $f = g^p$ for some $g \in \mathbb{F}_q[x]$, and thus it suffices to factor $g$, whose degree is exactly $\deg(f)/p$. $\square$

**Exercise.** (Problem 6) Let $L$ be a field and $f(x) = \prod_{i=1}^n (x - a_i)^{m_i} \in L[x]$, where the $a_i$'s are pairwise distinct. Compute $d(x) = \gcd(f(x), f'(x))$.

*Proof.* Let $p$ be the characteristic of the finite field $L$. Since $L[x]$ is a UFD, every divisor of $f(x)$ is associate to a product of $(x - a_i)$'s, and so is $d(x)$. Let $j$ be given. Then $f' = m_j(x - a_j)^{m_j - 1} g(x) + (x - a_j)^{m_j} g(x)'$ where $g(x) = \prod_{i \neq j} (x - a_i)^{m_i}$. If $p \mid m_j$, then $(x - a_j)^{m_j}$ divides both $f$ and $f'$. If $p \nmid m_j$, then $b_j = m_j - 1$ is the largest integer such that $(x - a_j)^{b_j}$ divides both $f$ and $f'$. Therefore, $d(x) = \prod_{i=1}^n (x - a_i)^{m_i - c_i}$ where $c_i = 0$ if $p \mid m_i$ and $c_i = 1$ otherwise. $\square$

**Exercise.** (Problem 7) A polynomial, $f(x)$, is said to be square free if it can be written as a product of irreducible factors, no two of which are associate. For $f(x) \in \mathbb{F}_q[x]$, find a criterion in terms of $gcd(f(x), f'(x))$ for $f(x)$ to be square free.

*Proof.* Let $f = \prod f_i$ be square free. Let $j$ be given. $f' = f_j' g + f_j g'$ where $g = \prod_i f_i$. Since $f_j$ is irreducible, $f_j$ is separable by Problem 4. Thus $\gcd(f_j, f_j') = F^\times$, so $f_j \nmid f_j'$. Thus $f_j \nmid f'$.

Since all divisors of $f$ are associate to some product of $f_i$'s, $\gcd(f, f') = 1$.

On the other hand, suppose $f$ is not square free. Then $f = g^2 h$ for some irreducible $g$ and some $h$. $f' = g(2g'h + gh')$, so $g \mid \gcd(f, f')$.

Therefore, $f$ is square free if and only if $\gcd(f, f') = 1$. $\square$

**Exercise.** (Problem 8) Describe how to use repeated computation of gcd's to find a factorization of a given polynomial, $f(x) \in \mathbb{F}_q[x]$, $f = f_1 \cdots f_r$, where each $f_i \in \mathbb{F}_q[x]$ is square free.

*Proof.*

(1) Calculate $d = \gcd(f, f')$.
(2) If $d = 1$, $f$ is square free by Problem 7, and we are done.
(3) If $d = f$, then $f' = 0$, so $f = g^p$ for some $g$ by Problem 2. Let $f = g$, and go back to Step 1.
(4) Otherwise, we can factor both $d$ and $f/d$ further by going back to Step 1.

This process must terminate finitely because the degree of a polynomial continues to decrease. $\square$

## 2. Modules

**Exercise.** (Problem 6) Take four $4 \times 4$ matrices with integer entries and check if the abelian group presented by the matrix is cyclic.

*Proof.*

$$\begin{bmatrix} -166 & -74 & 254 & 347 \\ 140 & -93 & 246 & 425 \\ -196 & 57 & -363 & 202 \\ 325 & 257 & 314 & -389 \end{bmatrix} \to \begin{bmatrix} 18444530375 & 1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 237 & -81 & 332 & -132 \\ 95 & 268 & 229 & 498 \\ 387 & 213 & 46 & 55 \\ 88 & -126 & -380 & -447 \end{bmatrix} \to \begin{bmatrix} 2610768268 & 1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} -275 & -22 & -207 & -276 \\ -469 & -342 & 240 & -101 \\ -41 & 455 & 51 & -151 \\ 267 & -450 & 98 & -40 \end{bmatrix} \to \begin{bmatrix} 33644517767 & 1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 48 & 29 & 22 & -481 \\ 388 & -468 & -137 & -491 \\ 84 & -352 & 85 & -384 \\ -226 & -486 & 102 & -156 \end{bmatrix} = \begin{bmatrix} 13267264454 & 1 & 1 & 1 \end{bmatrix}$$

Each of the groups contains 4 generators, so none of them are cyclic. □

## 3. Galois Theory

**Exercise.** (Problem 1) Let $F = \mathbb{Q}$. Let $L = \mathbb{Q}(\sqrt{7}, \sqrt{-11})$. To what familiar group is $\mathrm{Aut}(L/F)$ is isomorphic?

*Proof.* $[K : \mathbb{Q}(\sqrt{7})] = [K : \mathbb{Q}(\sqrt{-11})] = 2$. Since the characteristic of $K$ is not 2, by the argument presented on P.3 of the Galous Theory handout, $\mathrm{Aut}(K/\mathbb{Q}(\sqrt{7}))$ and $\mathrm{Aut}(K/\mathbb{Q}(\sqrt{-11}))$ have 2 elements. For instance, $\alpha = \sqrt{7}$ and the minimal monic polynomial is $x^2-7$. This gives $D = 28$ and two automorphisms in $\mathrm{Aut}(K/\mathbb{Q}(\sqrt{7}))$, the identity map, and $\sigma : \sqrt{D} \mapsto -\sqrt{D}$ as discussed in the handout. Similarly, $\mathrm{Aut}(K/\mathbb{Q}(\sqrt{-11}))$ contains the identity map and $\sigma : \sqrt{D} \mapsto -\sqrt{D}$ where $D = -44$.

Finish this proof.

□

**Exercise.** (Problem 2) Let $F \subset K$ be a field extension.

(1) Prove in at most two sentences that each $\sigma \in \mathrm{Aut}(K/F)$ is an $F$-linear transformation of the $F$-vector space, $K$.
(2) Does the same condition hold in general for $\sigma \in \mathrm{Aut}(K)$? Prove or give a counterexample.

*Proof.*

(1) For any $a \in F$ and $v, w \in K$, $\sigma(av + w) = \sigma(a)\sigma(v) + \sigma(w) = a\sigma(v) + \sigma(w)$, so $\sigma$ is indeed an $F$-linear transformation.

(2) Let $F = \mathbb{Q}(\sqrt{7})$ and $K = \mathbb{Q}(\sqrt{7}, \sqrt{-11})$. Let $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ such that $\sigma(\sqrt{7}) = -\sqrt{7}, \sigma(\sqrt{-11}) = -\sqrt{-11}$. The existence of such an automorphism is shown in the solution to Problem 1. $K$ is an $F$-vector space. However, $\sigma(\sqrt{7} \cdot 1) = -\sqrt{7} \neq \sqrt{7} = \sqrt{7}(\sigma(1))$, so $\sigma$ is not an $F$-linear transformation.

□

**Exercise.** (Problem 3) Let $\zeta = \exp(2\pi i/3) \in \mathbb{C}$. Consider the following subfields of $\mathbb{C}$. Let $F = \mathbb{Q}(\zeta)$. For $i \in \{0, 1, 2\}$, let $K_i = \mathbb{Q}(\zeta^i 7^{1/3})$. Let $L = \mathbb{Q}(7^{1/3}, \zeta 7^{1/3}, \zeta^2 7^{1/3})$.

*Proof.*

(1) $[F : \mathbb{Q}] = 2$ since $\zeta^2 + \zeta + 1 = 0$.

(2) $\mathrm{Aut}(F/\mathbb{Q})$ permutes the roots of $x^2 + x + 1 = 0$. Thus it contains two maps, namely, the identity map and another map that swaps $\zeta$ and $\zeta^2$.

(3) $[K_i : \mathbb{Q}] = 3$ for each $i$ because $\{1, \zeta^i 7^{1/3}, (\zeta^i 7^{i/3})^2\}$ is a $\mathbb{Q}$-basis.

(4)

□