MATH 601 (DUE 11/13)

HIDENORI SHINOHARA

Contents

1. Factoring Polynomials with Coefficients in Finite Fields

Exercise. (Problem 14) For $a \in \mathbb{F}_q$, what are the possible values for $a^{(q-1)/2}$? How many different a take each value?

Proof. Let $\langle \alpha \rangle = (\mathbb{F}_q)^*$. Let $k \in \mathbb{Z}$. If k is even, then $(\alpha^k)^{(q-1)/2} = (\alpha^{k/2})^{q-1} = 1$. If $k = 2l+1$ for some l, then $(\alpha^k)^{(q-1)/2} = \alpha^{l(q-1)} \cdot \alpha^{(q-1)/2} = \alpha^{(q-1)/2} = -1$ because -1 has degree 2 and $\alpha^{(q-1)/2}$ is the only element in $\langle \alpha \rangle$ of degree 2. Therefore,

$$a^{(q-1)/2} = \begin{cases} 0 & (a = 0) \\ 1 & (\exists l \in \mathbb{Z}, a = \alpha^{2l}) \\ -1 & (\exists l \in \mathbb{Z}, a = \alpha^{2l+1}). \end{cases}$$

This is well defined because every nonzero element in $\mathbb{Z}_q$ is in $\langle \alpha \rangle$ and $2 \mid |\langle \alpha \rangle| = q-1$, so the parity of the exponent does not depend on the choice of k. Hence, 1 value gives 0, $(q-1)/2$ values give 1, and $(q-1)/2$ values give -1. $\square$

Exercise. (Problem 15) Let $f(x)$ be as in problem 13 and let $h \in \mathbb{F}_q[x]$ be a randomly chosen polynomial. What is the probability that $h^{(q^r-1)/2} = \pm 1$ in the ring $\mathbb{F}_q[x]/(f(x))$.

Proof. As shown in Problem 13 last week, there exists an isomorphism $\Phi : \mathbb{F}_q[x]/(f(x)) \to \mathbb{F}_q[x]/(f_1(x)) \times \cdots \times \mathbb{F}_q[x]/(f_m(x))$ by the Chinese Remainder Theorem. For any $h \in \mathbb{F}_q[x]$, $\Phi(h + (f)) = (h + (f_1), \cdots, h + (f_m))$. Moreover, $\Phi(h^{(q-1)/2} + (f)) = (h^{(q-1)/2} + (f_1), \cdots, h^{(q-1)/2} + (f_m))$. Therefore, $h^{(q-1)/2} + (f) = 1$ if and only if $h^{(q-1)/2} + (f_1), \cdots, h^{(q-1)/2} + (f_m)$ all equal 1.

Let $\alpha_1, \cdots, \alpha_m$ be generators of $(\mathbb{F}_q[x]/(f_1(x)))^*, \cdots, (\mathbb{F}_q[x]/(f_m(x)))^*$. For each i, $h^{(q-1)/2} + (f_i) = 1$ if and only if $h \in \langle \alpha_i^2 \rangle$ by Problem 14. Therefore, $h^{(q-1)/2} + (f) = 1$ if and only if $(h + (f_1), \cdots, h + (f_m)) \in \langle \alpha_1^2 \rangle \times \cdots \times \langle \alpha_m^2 \rangle$. There are exactly $((q^r-1)/2)^m$ elements that satisfy that. Therefore,

$$\frac{(\frac{q^r-1}{2})^m}{(q^r)^m} = \left(\frac{q^r - 1}{2q^r} \right)^m = \left(\frac{1}{2} - \frac{1}{2q^r} \right)^m.$$

is the probability that $h^{(q^r-1)/2} = 1$ in $\mathbb{F}_q[x]/(f(x))$.

Using the exact same argument, we can derive that the probability that $h^{(q^r-1)/2} = -1$ is exactly the same value. $\square$

Exercise. (Problem 16) With $f(x)$ as in problem 13, write $f(x) = g_1(x) \cdots g_m(x)$ for the factorization into irreducible factors. Express $\gcd(f(x), h^{(q^r-1)/2} - 1)$ in terms of the $g_i(x)$'s.

Proof. $\gcd(f(x), h^{(q^r-1)/2} - 1)$ is the product of $g_i(x)$'s that divide $h^{(q^r-1)/2} - 1$. It is divisible by $g_i(x)$ if and only if $h \in \langle \alpha_i^2 \rangle$ from Problem 15. $\square$

Exercise. (Problem 17) Describe a probabilistic factoring algorithm which has a very high probability of finding the irreducible factors of a polynomial $f(x) \in \mathbb{F}_q[x]$, provided one knows ahead of time that $f(x)$ is a product of m distinct irreducible polynomials of degree r.

Proof. Let i_0 be fixed. Given a random $h(x) \in \mathbb{F}_q[x]$, the probability that $h^{(q-1)/2} - 1 \in (f_{i_0})$ is $1/2 - 1/(2q^r)$, which is slightly smaller than 50%. Therefore, it is likely that given a random $h(x) \in \mathbb{F}_q[x]$, the probability that $h^{(q-1)/2} - 1 \in (f_i)$ for *some* i's is high. However, the probability that $h^{(q-1)/2} - 1 \in (f_i)$ in *all* i's is low.

In other words, the probability that $h^{(q-1)/2} - 1$ is a proper divisor of f is high. Therefore, we can expect to factor $f(x)$ by

- Step 1: Generate a random polynomial $h(x) \in \mathbb{F}_q[x]/(f(x))$.
- Step 2: Calculate $h^{(q^r-1)/2} - 1$. This step can be done efficiently by exponentiation by squaring.
- Step 3: Calculate $d(x) = \gcd(f(x), h^{(q^r-1)/2} - 1)$. This step can be done efficiently by the Euclid algorithm.
- Step 4: If $1 \leq \deg(d(x)) < \deg(f(x))$, then factorize $f(x)/d(x)$ and $d(x)$ further by going back to Step 1 unless it is degree r. Otherwise, we were unlucky, so we go back to Step 1.

$\square$

Exercise. (Problem 18, 19, 20)

- Problem 18: $(x^2 + x - 1)^4$
- Problem 19: $(x^3 - 25x^2 - 35x + 3)(x^4 + 4x^2 + 5x + 3)(x^5 + 4x^2 + 8x + 3)$.
- Problem 20: $(x^4 + 4x^2 + 5x + 3)(x^4 + 15x^3 - 16x^2 - 27x - 26)(x^4 - 3x^3 + 9x^2 - 23x + 1)$.

2. Galois Theory III

Exercise. (Problem 1) Prove Proposition 23 part (ii).

Proof. Clearly, $F \subset gK \subset L$ because $g \in \mathrm{Aut}(L/F)$. gK is a subfield because g preserves addition, multiplication and multiplicative inverse, so gK is closed under addition, multiplication and multiplicative inverse.

Let $\phi \in \mathrm{Aut}(L/gK)$. Then clearly, $g^{-1}\phi g \in \mathrm{Aut}(L)$. $g^{-1}\phi g$ fixes K because $\forall x \in K, (g^{-1}\phi g)(x) = g^{-1}(g(x)) = x$. Therefore, $\phi \in g \,\mathrm{Aut}(L/K) g^{-1}$.

Let $g\psi g^{-1} \in g\,\mathrm{Aut}(L/K)g^{-1}$. Then $g\psi g^{-1} \in \mathrm{Aut}(L)$. For all $g(k) \in g(K)$, $(g\psi g^{-1})(g(k)) = g(\psi(k)) = g(k)$. Therefore, $g\psi g^{-1} \in \mathrm{Aut}(L/gK)$. $\square$

Exercise. (Problem 2) Show that the Galois correspondence is order reversing.

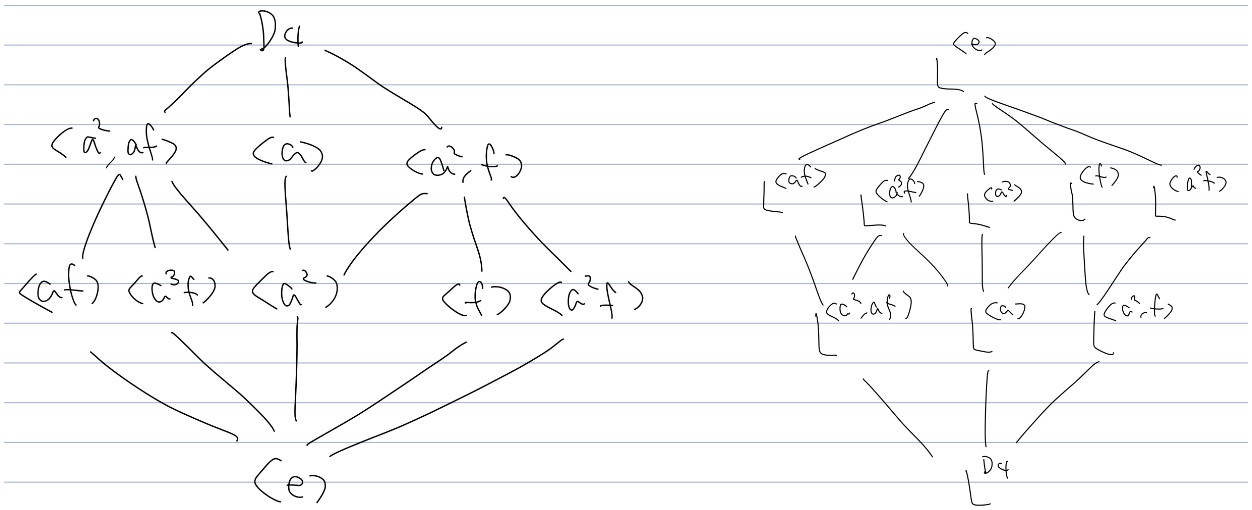

FIGURE 1. Problem 3

Proof. Let $H_1 \subset H_2$ be given. Let $x \in K^{H_2}$. Then x is fixed by every element in H_2. Then x is clearly fixed by every element in H_1. Thus $x \in K^{H_1}$.

Let $K_1 \subset K_2$. Let $\sigma \in \mathrm{Aut}(L/K_2)$. Then σ clearly fixes K_1. Thus $\sigma \in \mathrm{Aut}(L/K_1)$. $\square$

Exercise. (Problem 3) Draw a picture showing all the subgroups of the dihedral group with eight elements, $D4 := \langle a, f : a^4 = 1 = f^2, faf = a^{-1} \rangle \simeq \langle (1234), (12)(34) \rangle \subset S_4$ showing which are contained in which. Now draw a diagram of the corresponding intermediate fields in a Galois extension, $F \subset L$, with Galois group isomorphic to D_4 indicating which are ontained in which.

Proof. Figure 1. $\square$

Exercise. (Problem 4) Let $F \subset M$ be a Galois extension with Galois group isomorphic to the dihedral group with eight elements (denoted D 4 in class). Show that there is a tower of intermediate fields, $F \subset K \subset L$ such that $F \subset K$ is Galois and $K \subset L$ is Galois, but $F \subset L$ is not Galois.

Proof. $G_1 = \langle af \rangle$ is a normal subgroup of $G_2 = \{e, af, a^2, a^3 f\}$ because the index is 2. Similarly, G_2 is a normal subgroup of D_4 because the index is 2. However, G_1 is not a normal subgroup of D_4. (For instance, $f \langle af \rangle f^{-1} = \langle fa \rangle$,but $af \neq fa$.) By the Fundamental Theorem of Galois Theory, L^{G_1} and L^{G_2} are intermediate fields. By Proposition 23(iii), $L^{G_2} \subset L^{G_1}$ and $L^{D_4} \subset L^{G_2}$ is Galois, but $L^{D_4} \subset L^{G_1}$ is not Galois. $\square$