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: $(x^4 + 4x^2 + 5x + 3)(x^4 + 15x^3 - 16x^2 - 27x - 26)(x^4 - 3x^3 + 9x^2 - 23x + 1)$.

I used the following Python code to factorize. The idea is to use the methods developed in Problem 11 and Problem 17. Later, I noticed that I should have added code to check if $f(x)$ is square free, but for some reason, the code was still able to factorize the polynomial for Problem 18.

```
from sympy import *
from random import *

x = symbols('x')

# Find a random polynomial of degree <= deg in Z_{mod}.
def randpoly(deg, mod):
    p = poly(0, x, modulus = mod)
```

```
    for d in range(deg):
        p = x * p + randint(0, mod - 1)
    return poly(p, x, modulus = mod)

# Find f^exp % modf in Z_{mod}.
def polypow(f, exp, modf, mod):
    res = poly(1, x, modulus = mod)
    while exp > 0:
        if exp % 2 == 1:
            quotient, res = div(res * f, modf, modulus = mod)
        quotient, f = div(f * f, modf, modulus = mod)
        exp = exp // 2
    return res

# Calculate x^(p^n) - x % modf.
def xqd(p, n, modf):
    res = polypow(x, p**n, modf, p)
    res -= poly(x, x, modulus = p)
    return res


def factor(f, p, originaldegree, factors):
    # Problem 11
    for n in range(2, originaldegree):
        g = xqd(p, n, f)
        d = gcd(f, g)
        if 1 <= d.degree() < f.degree():
            # We found a proper factor.
            # Factorize further.
            factor(d, p, originaldegree, factors)
            quotient, remainder = div(f, d, modulus = p)
            factor(quotient, p, originaldegree, factors)
            return

    # Problem 17
    for r in range(2, f.degree()):
        if f.degree() % r != 0: continue
        for i in range(10):
            h = randpoly(r, p)
            # Raise h to the power of (p^r - 1)/2.
            h = polypow(h, (p**r - 1) // 2, f, p)
            h = h - poly(1, x, modulus = p)
```

```
            d = gcd(f, h)
            if d.degree() == 0 or d.degree() == f.degree():
                continue
            else:
                # We found a proper factor.
                # Factorize further.
                factor(d, p, originaldegree, factors)
                quotient, remainder = div(f, d)
                factor(quotient, p, originaldegree, factors)
                return
    factors.append(f)

def factorizepoly(f, mod):
    print("Factorize %s" % f)
    factors = []
    factor(f, mod, f.degree(), factors)
    prod = poly(1, x, modulus = mod)
    for fac in factors:
        prod *= fac
        print(latex(fac))
    if prod != f:
        print("******ERROR!******")
    print()
    return

f = poly(x**8 + x**7 - x**6 + x**5 + x**4 - x**3 - x**2 - x + 1, x, modul
factorizepoly(f, 3)

f = poly((x**12+48*x**11+42*x**10+58*x**9+11*x**8+25*x**7+22*x**6+30*x**5
factorizepoly(f, 73)

f = poly((x**12+12*x**11 +25*x**10 + 40*x**9 + 6*x**8 + 15*x**7 + 24*x**6
factorizepoly(f, 73)
```

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, $\phi \in g\,\mathrm{Aut}(L/K)g^{-1}$.

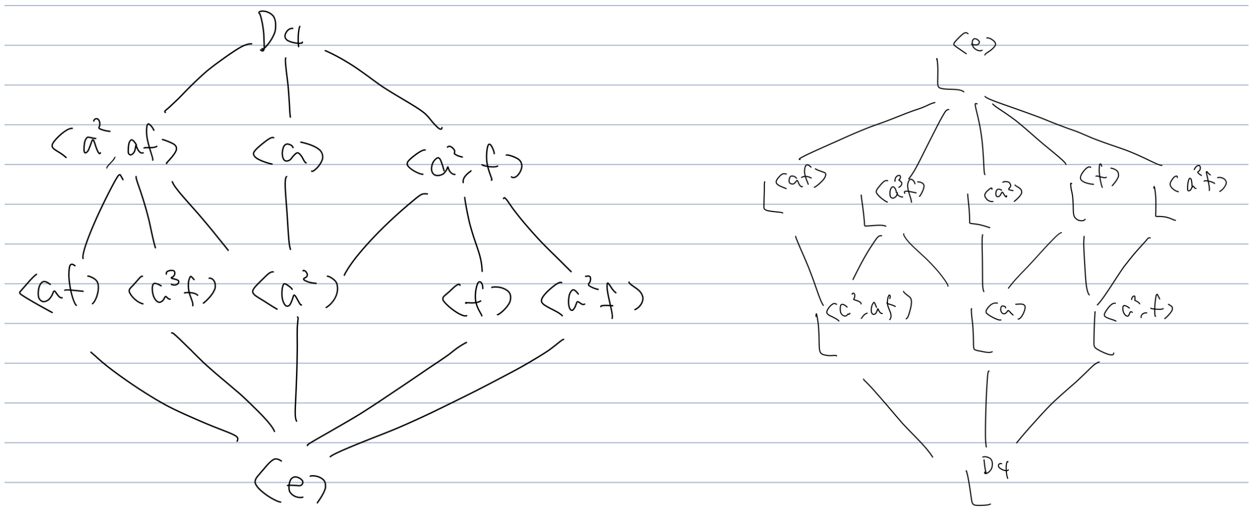

Figure 1. Problem 3

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.

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 $G_2 = \{e, af, a^2, a^3f\}$ 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. $\square$

Exercise. (Problem 5) Let $F \subset M$ be a Galois extension with Galois group isomorphic to the symmetric group S_4. Let $H = \langle(123)\rangle \subset S_4$. Make a list of the intermediate fields in the extension, $F \subset M^H$. For each intermediate field L indicate whether or not $F \subset L$ is Galois and whether or not $L \subset M^H$ is Galois.

Proof. There are only 4 subgroups of S_4 that contain S_3. They are H, S_3, A_4, S_4. The smallest subgroup containing H and an element in S_3 is clearly either H or S_3. We will consider the smallest subgroup containing H and an element σ in $S_4 \setminus S_3$. If σ is an even permutation, $\langle H, \sigma \rangle$ is a subgroup of A_4. By Figure 8 on P.111 (Dummit and Foote), $\langle H, \sigma \rangle = A_4$. Suppose σ is an odd permutation. Since $\sigma \notin S_3$, σ sends 4 to 1, 2, or 3. Then $\sigma^{-1}(123)\sigma$ is an even permutation that sends 4 to 1, 2, or 3. In other words, $\langle H, \sigma \rangle$ contains an even permutation that is not in H. Consider the group H_e that consists of all the even permutation sin $\langle H, \sigma \rangle$. $H \subsetneq H_e \subset A_4$. By Figure 8 on P.111 (Dummit and Foote), $H_e = A_4$. Since H properly contains A_4, it must be S_4. Therefore, we showed that $\langle H, \sigma \rangle$ is either S_3, A_4, S_4 for any $\sigma \notin H$.

Clearly, there is no subgroup between A_4 and S_4. Similarly, there is no subgroup between S_3 and S_4. If there is one, $|S_3| = 6$ and $|S_4| = 24$ imply that the subgroup has order 12. However, the only subgroup of order 12 in S_4 is A_4, which does not contain S_3.

Clearly, $M^H \subset M^H$ and $M^{S_4} \subset F$ are Galois. H is not a normal subgroup of S_4 because $(14)(12)(14) \notin H$. Therefore, $F \subset M^H$ is not Galois.

$S_3 = \{e, (12), (13), (23), (123), (132)\}$ is a proper subgroup of S_4 that contains H properly. Therefore, $F \subsetneq M^{S_3} \subsetneq M^H$. Since $[S_3 : H] = 2$, H is a normal subgroup of S_3. Therefore, $M^{S_3} \subset M^H$ is Galois. S_3 is not a normal subgroup of S_4 because $(14)(12)(14) \notin S_3$. Therefore, $F \subset M^{S_3}$ is not Galois.

A_4 is a normal subgroup of H because the index is 2. Therefore, $F \subset M^{A_4}$ is Galois. H is not a normal subgroup of A_4 because $((12)(34))(23)((12)(34)) = (14) \notin H$. Therefore, $M^{A_4} \subset M_h$ is not Galois. $\square$