MATH 601 (DUE 11/22)

HIDENORI SHINOHARA

Contents

1. THE THEOREM ON SYMMETRIC POLYNOMIALS

Exercise. (Problem 1) By substituting $u_4 = 0$, we get $u_1^2u_2u_3 + u_1u_2^2u_3 + u_1u_2u_3^2 = s_3s_1$. s_3s_1 with 4 variables expands to $u_1^2u_2u_3 + u_1^2u_2u_4 + u_1^2u_3u_4 + u_1u_2^2u_3 + u_1u_2^2u_4 + u_1u_2u_3^2 + 4u_1u_2u_3u_4 + u_1u_2u_4^2 + u_1u_3^2u_4 + u_1u_3u_4^2 + u_2^2u_3u_4 + u_2u_3^2u_4 + u_2u_3u_4^2$. Then $s_3s_1 - f$ where f is the original polynomial gives us $4u_1u_2u_3u_4 = 4s_4$. Therefore, $f = s_3s_1 - 4s_4$.

Exercise. (Problem 2) We are given that $|M - xI| = x^3 - ax^2 + bx - c$. This implies that $|M - (-x)I| = -x^3 - ax^2 - bx - c$. Since the determinant function preserves multiplication, $|M - xI||M - (-x)I| = |M^2 - x^2I|$. This implies $|M^2 - x^2I| = -x^6 + (a^2 - 2b)x^4 + (-b^2 + 2ac)x^2 + c^2$. Therefore, the characteristic polynomial of M is $-x^3 + (a^2 - 2b)x^2 + (-b^2 + 2ac)x + c^2$.

$|xI - M|$ is what I need to calculate.

2. Galois Theory VI

Exercise. (Problem 3)

(i) $\{(123), (132), e\}$ is clearly a subgroup of the stabilizer group S_v of v. Since $(12) \notin S_v$, $3 \leq |S_v| \leq 5$. By Lagrange's Theorem, $S_v = \langle (123) \rangle$.

(ii) By (i), S_3v contains only $[S_3 : S_v] = 2$ elements. Thus $v' = (12) \cdot v = u_2u_1^2 + u_1u_3^2 + u_3u_2^2$.

(iii) By substituting $u_3 = 0$ for $v + v'$, we get $u_1u_2^2 + u_2u_1^2 = s_1s_2$. Then $v + v' - s_1s_2 = -3u_1u_2u_3 = -3s_3$. Therefore, $v + v' = s_1s_2 - 3s_3$.

(iv) We will use the fundamental theorem of Galois Theory. $F(v) = K^{\langle (123) \rangle}$, so $|\langle (123) \rangle| = 3 = [K : F(v)]$. Moreover, $|\langle \mathrm{Gal}(K/F) \rangle| = [K : F]$. Therefore, $[F(v) : F] = [K : F]/[K : F(v)] = |\mathrm{Gal}(K/F)|/3$.

(v) Calculation shows that $vv' = 9s_3^2 + s_3s_1^3 - 6s_3s_1s_2 + s_2^3$. By substituting $s_1 = 0, s_2 = p, s_3 = q$, we get $9q^2 + p^3$.

(vi) Since A_3 is the only proper transitive subgroup of S_3, $\mathrm{Gal}(K/F) = S_3$ if and only if $\sigma \in \mathrm{Gal}(K/F)$ where σ corresponds to the permutation (12). (i.e., $u_1 \mapsto u_2, u_2 \mapsto u_1$.)

v, v' are not fixed by σ, so $v, v' \notin F$ if $\mathrm{Gal}(K/F) = S_3$. v, v' are fixed by every permutation if $\mathrm{Gal}(K/F) = A_3$ because it is generated by σ' that corresponds to (123). Therefore, we can conclude that $\mathrm{Gal}(K/F) \neq S_3$ if and only if $v, v' \in F$. $v, v' \in F$ if and only if $(y-v)(y-v')$ factors in F. Therefore, $h(y) = y^2 - (v+v')y + vv' = y^2 + 3qy + (9q^2 + p^3)$ is the desired polynomial.

(vii) The discriminant is $(3q)^2 - 4(9q^2 + p^3) = 9q^2 - 36q^2 - 4p^3 = -27q^2 - 4p^3$.

Exercise. (Problem 4)

(i) The discriminant can be expressed as $-4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3 - 4s_2^3 - 27s_3^2$. By substituting $s_1 = 1, s_2 = -2, s_3 = -1$, we get 49.

```
from sympy.polys.polyfuncs import symmetrize
from sympy import *

u1, u2, u3 = symbols('u1 u2 u3')

u = [u1, u2, u3]

discriminant = 1
for i in range(3):
    for j in range(i + 1, 3):
        discriminant *= (u[i]   u[j]) * (u[i]   u[j])

print(latex(symmetrize(discriminant, formal = True)[0]))
```

Since the discriminant is a square, the Galois group is isomorphic to A_3.

Exercise. (Problem 5)

(i)

(ii) $x^4 + x + 1$ is irreducible because

- It does not have a linear factor by the rational root theorem.
- If it factors into two rational quadratic polynomials, they will factor into two monic integer quadratic polynomials, namely, $x^2 + ax + b$ and $x^2 - ax + 1/b$ based on the coefficients. This implies $b = \pm 1$. Since the coefficient of x is 1, $-ab + a/b = 1$, but this implies $b \neq \pm 1$.

We will use the discussion presented in the Galois Theory IV handout. By (i), the discriminant is 229, so $h(y) = y^2 - 229$. Also, $g(y) = y^3 - 4y - 1$ since $a = b = 0, c = -1, d = 1$. Therefore, both $h(y)$ and $g(y)$ are irreducible, so the Galois group is S_4.

(iii) It does not have a linear factor by the rational root theorem. Based on coefficients, if it factors into quadratic polynomials, it will be $(x^2 + ax + b)(x^2 - ax + c)$ for some $a, b, c \in \mathbb{Z}$ by Gauss' lemma. This gives $bc = 12$ and $-ab + ac = -8$, so $a(c - 12/c) = -8$. This is a quadratic polynomial in c with the discriminant $64 - 48a$. This must be a square for c to exist. By checking each possible value of a, we get $64 - 48 \cdot -8 = 448, 64 - 48 \cdot -4 = 256, 64 - 48 \cdot -2 = 160, 64 - 48 \cdot -1 = 112, 64 - 48 \cdot 1 = 16$. (For other a, $64 - 48a < 0$.) Thus the only two possible values are $a = 1, -4$. $a = 1$ gives $c - b = -8$ and $bc = 12$, which we can confirm to be impossible by examining the divisors of 12. Similarly, $a = -4$ gives $c - b = 2$ and $bc = 12$ and this is impossible to satisfy. Therefore, $x^4 - 8x + 12$ is irreducible over $\mathbb{Q}$.

(iv) Again, we will use the discussion presented in the Galois Theory IV handout. By calculating the discriminant, we have $h(y) = h(y) = y^2 - 331776$ and $g(y) = y^3 - 48y - 64$. $h(y)$ factors as $576^2 = 331776$. $g(y)$ does not factor by the rational root theorem. Therefore, the Galois group is A_4.

3. Galois Theory V(Further exercises)

Exercise. (Problem 3)

(i)

4. Galois Theory V

Exercise. (Problem 1)

(i) D_4 is a subgroup of S_4 and the Galois Theory V handout states that S_4 is solvable and any subgroup of a finite solvable group is solvable.

(ii) If S_5 is solvable, $A_5 \leq S_5$ is solvable. However, as stated in the handout, A_5 is not solvable.

Exercise. (Problem 2)

(i) Let $a = (12345)$ and $b = (2354)$. Since $|a| = 5$ and $|b| = 4$, $20 \mid |G|$. On the other hand, every element can be written as $a^i b^j$ because of the relation $ab = (1243) = ba^3$. Since every element can be written as $a^i b^j$ where $0 \leq i \leq 4$ and $0 \leq j \leq 3$, G contains exactly 20 elements.

(ii) G has a subgroup $G_1 = \{(1), (12)(35), (12345), (13)(45), (13524), (14)(23), (14253), (15)(24), (15432), (25)(34)\}$. of index 2. G_1 has a subgroup $G_2 = \{(1), (12345), (13524), (14253), (15432)\}$ of index 2. G_2 is abelian, so we can pick $G_3 = \{(1)\}$. Then $G_3 \subset G_2 \subset G_1 \subset G$ is a filteration.