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 $|xI - M| = x^3 - ax^2 + bx - c$. This implies that $|(-xI) - M| = -x^3 - ax^2 - bx - c$. Since the determinant function preserves multiplication, $|xI - M||-xI - M| = |M^2 - x^2I|$. This implies $|M^2 - x^2I| = -x^6 + (a^2 - 2b)x^4 + (-b^2 + 2ac)x^2 + c^2$. Therefore, $|yI - M^2| = y^3 + (2b - a^2)y^2 + (b^2 - 2ac)y - c^2$.

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 $-4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$. 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.

(ii) Since $\text{Gal}(K/\mathbb{Q}) = A_3$, the degree of extension is 3. First, we claim that $K \subset \mathbb{R}$. If K is not a subset of $\mathbb{R}$, $\sigma(a + bi) = a - bi \in \text{Gal}(K/\mathbb{Q})$. However, this is impossible because $|\sigma| = 2 \nmid 3 = |A_3|$.

Let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be given. Since the degree of extension is 3, there cannot be any intermediate field. Therefore, if $a^{1/n} \notin \mathbb{Q}$, $\mathbb{Q}(a^{1/n}) = K$. Hence, we can uniquely determine σ by checking $\sigma(a^{1/n})$. Since $a^{1/n}$ is a root of $x^n - a$, $\sigma(a^{1/n})$ must be a root of $x^n - a$. Since $K \subset \mathbb{R}$, $\sigma(a^{1/n}) = \pm a^{1/n}$. It is impossible that $\sigma(a^{1/n}) = -a^{1/n}$ since this implies $|\sigma| = 2 \nmid 3$. Therefore, $\sigma = \text{Id}$, but this implies that $\text{Gal}(K/\mathbb{Q})$ is trivial, which is a contradiction.

Thus $a^{1/n} \in \mathbb{Q}$.

Exercise. (Problem 5)

(i) By modifying the code for Problem 4, we obtain that

$$\begin{aligned}&-27s_1^4s_4^2 + 18s_1^3s_2s_3s_4 - 4s_1^3s_3^3 - 4s_1^2s_2^3s_4 + \\ &s_1^2s_2^2s_3^2 + 144s_1^2s_2s_4^2 - 6s_1^2s_3^2s_4 - 80s_1s_2^2s_3s_4 + \\ &18s_1s_2s_3^3 - 192s_1s_3s_4^2 + 16s_2^4s_4 - 4s_2^3s_3^2 - 128s_2^2s_4^2 + \\ &144s_2s_3^2s_4 - 27s_3^4 + 256s_4^3\end{aligned}$$

We are given that $s_1 = s_2 = 0$. Therefore, we are left with $256s_4^3 - 27s_3^4 = 256b^3 - 27a^4$.

(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) $x^n - 1$ cannot split in a field smaller than K because ζ is a root. On the other hand, $\{\zeta^i \mid 0 \leq i \leq n-1\}$ contains n distinct roots of $x^n - 1$. Therefore, K is the splitting field of $x^n - 1$.

(ii) $\phi(n)$ because for any $1 \leq m \leq n-1$ such that $d = \gcd(m, n) \neq 1$, $(\zeta^m)^d = 1$, so ζ^m is not a primitive nth root. On the other hand, $(\zeta^m)^k = 1$ with $1 \leq k \leq n-1$, then $n \mid mk$, so $\gcd(n, m) \neq 1$.

(iii) All the primitive roots are roots of $x^n - 1$. Since $\sigma \in \mathrm{Aut}(K/F)$ permutes the roots of $x^n - 1$, all the primitive roots get mapped to roots of $x^n - 1$. Suppose that $\sigma(\zeta) = \zeta'$ where ζ' is not a primitive root. Then ζ' satisfies $x^m - 1$ where $m < n$. This implies that σ^{-1} sends ζ', a root of $x^m - 1$, to ζ, which is not a root of $x^m - 1$. This is a contradiction, so all the primitive roots must get mapped to primitive roots.

Therefore, any automorphism in $\mathrm{Aut}(K/F)$ sends primitive roots to primitive roots.

(iv) $|(\mathbb{Z}/n)^*| = \phi(n)$ where $\phi(n)$ is Euler's totient function.

(v) $a \mapsto \zeta^a$.

(vi) Let $\Phi : \mathrm{Aut}(K/F) \to (\mathbb{Z}/n)^*$ be defined such that $\Phi(\sigma) = m$ where $\sigma(\zeta) = \zeta^m$.

- Well-defined? Every automorphism in $\mathrm{Aut}(K/F)$ sends a primitive nth root to a primitive nth root as shown in (iii). Therefore, m must be coprime to n, so $\Phi(\sigma) \in (\mathbb{Z}/n)^*$ for all $\sigma \in \mathrm{Aut}(K/F)$.
- Group homomorphism? Let $\sigma_1, \sigma_2 \in \mathrm{Aut}(K/F)$ be given. Let m_1, m_2 be chosen such that $\sigma_1(\zeta) = \zeta^{m_1}, \sigma_2(\zeta) = \zeta^{m_2}$. Then $\sigma_1 \circ \sigma_2$ maps ζ to $\zeta^{m_1 m_2}$. Therefore, $\Phi(\sigma_1 \circ \sigma_2) = m_1 m_2 = \Phi(\sigma_1)\Phi(\sigma_2)$.

- Injective? It suffices to check $\ker(\Phi)$. If $\sigma \in \ker(\Phi)$, then $\sigma(\zeta) = \zeta^1$, so $\sigma = \mathrm{Id}$. Thus the kernel is trivial.

Therefore, Φ is a well-defined, injective group homomorphism.

(vii) We showed earlier that $\{\zeta^0, \zeta^1, \cdots, \zeta^{n-1}\}$ are the n distinct roots of $x^n - 1$. Thus $x^n - 1$ is separable. By Theorem 8 of the Galois Theory II handout, $\mathrm{Aut}(K/F) = [K : F]$ Therefore, this is a Galois extension. Moreover, $\mathrm{Aut}(K/F)$ can be embedded in $(Z/n)^*$, which is clearly an abelian group. Therefore, $\mathrm{Aut}(K/F)$ is abelian.

(viii) Let $\zeta = e^{2\pi i/5}$ and $K = \mathbb{Q}(\zeta)$. Then ζ is a primitive 5th root. $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. Thus ζ is a root of $f(x) = x^4 + x^3 + x^2 + x + 1$. By substituting $x = x + 1$, we obtain $x^4 + 5x^3 + 10x^2 + 10x + 5$, which is irreducible by Eisenstein. Therefore, $f(x)$ must be irreducible.

By the argument above, $\mathrm{Aut}(K/F)$ can be embedded in $(\mathbb{Z}/5)^* = \langle 2 \rangle$. This implies that $\mathrm{Aut}(K/F)$ either contains 1, 2, 4 elements. Since $\mathrm{Aut}(K/F)$ has to be transitive, it cannot be trivial. Suppose $\mathrm{Aut}(K/F)$ has two elements. Let $r_1, \cdots, r_4$ denote the 4 distinct roots of $x^4 + x^3 + x^2 + x + 1$. There must be a $\sigma \in \mathrm{Aut}(K/F)$ such that $r_2 = \sigma(r_1)$. However, σ must be the only nontrivial element in $\mathrm{Aut}(K/F)$. Then there is no automorphism in $\mathrm{Aut}(K/F)$ that sends r_1 to r_3. Therefore, $\mathrm{Aut}(K/F)$ is not transitive if it only contains two elements.

Therefore, $\mathrm{Aut}(K/F)$ must contain 4 elements, and thus $\mathrm{Aut}(K/F) \cong (\mathbb{Z}/5)^* = \langle 2 \rangle$.

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.

Exercise. (Problem 3) Figure 1 shows all the subgroups of G where $a = (1325), b = (1435), c = (1243), d = (1254), e = (2354)$. By the fundamental theorem of Galois theory, there is a bijective correspondence between intermediate groups and intermediate fields, and the inclusion is reversed. The degree of extension corresponds to the index. By Lagrange's theorem, it is clear that, between any two groups connected by an edge in the figure, there cannot be any proper subgroups between them.

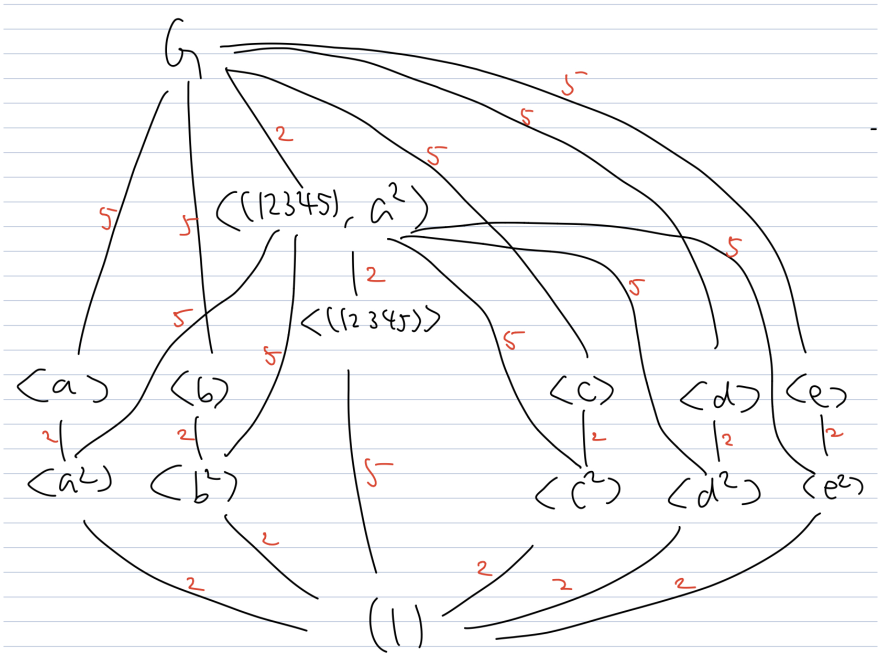

Figure 1. Subgroups

The number of subgroups of order 4 and 5 must be 5 and 1 by Sylow's theorem. By writing out all the 20 elements

$$(1), (12)(35), (12345), (1243), (1254), (13)(45), (1325), (1342), (13524), (14)(23),$$
$$(14253), (1435), (1452), (15)(24), (1523), (1534), (15432), (2354), (2453), (25)(34),$$

we conclude that the number of elements of order 2 is 5. Thus the number of subgroups of order 2 is 5. Finally, $G/\langle(12345)\rangle$ is isomorphic to $\mathbb{Z}/4$. Therefore, there can be only one subgroup of order 10 between G and $\langle(12345)\rangle$. Conversely, since every subgroup of order 10 must contain a subgroup of order 5, $\langle(12345), a^2\rangle$ is the only subgroup of order 10.

In order to check which intermediate fields are Galois, it suffices to check normality. By the index, $\langle(12345), a^2\rangle$ is normal in G. Clearly, $\langle(1)\rangle$ and G are normal in G. $\langle(12345)\rangle$ is normal since it is only subgroup of order 10. The other subgroups are not normal. For instance, $b\,\langle a^2\rangle\, b^{-1} \neq \langle a^2\rangle$.