LECTURE NOTES ON GALOIS THEORY

ABSTRACT. This is a condensed summary of the results (mostly without proofs) from Chapter 16 of Artin's book.

1

1.1. **Splitting fields.**

Definition 1. Let F be a field, and let $f(x)$ be a polynomial with coefficients in F. A splitting field for $f(x)$ is a minimal field K such that $f(x)$ decomposes into linear factors in K.

Proposition 2. *A splitting field always exists.*

Proof. Let us decompose $f(x)$ into irreducible factors over F: $f(x) = f_1(x)f_2(x)\cdots f_k(x)$. If all of them are linear, then F is the splitting field for $f(x)$. Otherwise, we can assume that $f_1(x)$ is not linear. Then we can consider the field $K_1 = F[x]/(f_1(x))$, where $f_1(x)$ has a root α. Then $f_1(x) = (x-\alpha)g_1(x)$, and $f(x)$ has at least one (but maybe more) linear factor over K_1. If all irreducible factors over K_1 are linear, stop, otherwise there is an irreducible factor of degree at least 2, and we can repeat the procedure and add its root. Since a polynomial of degree n has at most n roots, the process will eventually stop and all factors will be linear in some extension of F. □

One can prove that the splitting field is unique and does not depend on the order in which we add roots of irreducible factors.

Example 3. Consider the polynomial $f(x) = x^2 + 1$ over $\mathbb{R}$. It is irreducible, so the splitting field should contain $\mathbb{R}[\sqrt{-1}] = \mathbb{C}$. On the other hand, in $\mathbb{C}$ we have $f(x) = (x-i)(x+i)$, so $\mathbb{C}$ is the splitting field for $f(x)$.

Example 4. More generally, if a is not a square in F then $F[\sqrt{a}]$ is the splitting field for $f(x) = x^2 - a$ since $x^2 - a = (x-\sqrt{a})(x+\sqrt{a})$. The degree of the splitting field over F equals 2.

Example 5. Let p be prime, consider the polynomial $f(x) = x^p - 1$ over $\mathbb{Q}$. Let $\zeta = e^{2\pi i/p}$, then ζ is a root of $f(x)$ and we have

$$x^p - 1 = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}),$$

so all roots of $f(x)$ belong to the extension $\mathbb{Q}(\zeta)$. Since the minimal polynomial for ζ equals $x^{p-1}+\ldots+1$, we have $[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$.

Example 6. Consider the polynomial $f(x)=x^3+x+1$ over $\mathbb{Q}$. It has no rational roots, so it is irreducible. Since $f'(x)=3x^2+1>0$, $f(x)$ is increasing on the real line and has exactly one real root α. By the Fundamental Theorem of Algebra, it has two complex roots β and $\overline{\beta}$. Consider the extension $\mathbb{Q}(\alpha)\subset R$, there we have $f(x)=(x-\alpha)g(x)$. Since both roots of $g(x)$ are not real, they do not belong to $\mathbb{Q}(\alpha)$, so $g(x)$ is irreducible over $\mathbb{Q}(\alpha)$. Then we can consider the field $K=\mathbb{Q}(\alpha,\beta)$ where $f(x)$ factors completely. We have

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot 3=6.$$

1.2. **Galois group.**

Definition 7. Let $K\supset F$ be a field extension. The Galois group of K over F is the group of all automorphisms of K which preserve F. The Galois group of a polynomial is defined as the Galois group of its splitting field. It is denoted by $G(K/F)$.

Proposition 8. *Let $f(x)$ be a polynomial with coefficients in F which has a root $\alpha\in K$. For any $\phi\in G(K/F)$ the image $\phi(\alpha)$ is also a root of $f(x)$.*

Proof. Indeed, suppose that $f(x)=a_nx^n+\ldots+a_1x+a_0$ and $a_i\in F$. Then

$$f(\phi(\alpha))=a_n(\phi(\alpha))^n+\ldots+a_1\phi(\alpha)+a_0=$$
$$\phi(a_n)(\phi(\alpha))^n+\ldots+\phi(a_1)\phi(\alpha)+\phi(a_0)=$$
$$\phi(a_n\alpha^n+\ldots+a_1\alpha+a_0)=\phi(f(\alpha))=\phi(0)=0.$$

□

Example 9. The complex conjugation has an automorphism of $\mathbb{C}$ which preserves $\mathbb{R}$ (indeed, $\overline{(z+w)}=\overline{z}+\overline{w}$, $\overline{zw}=\overline{z}\overline{w}$). On the other hand, if $\phi\in G(\mathbb{C}/\mathbb{R})$ then $\phi(i)^2+1=0$, so $\phi(i)=i$ or $\phi(i)=-i$. In the first case for all $x,y\in R$ one has $\phi(x+iy)=\phi(x)+\phi(i)\phi(y)=x+iy$, so ϕ is identity automorphism, and in the second case $\phi(x+iy)=\phi(x)+\phi(i)\phi(y)=x-iy$. Therefore $G(\mathbb{C}/\mathbb{R})\simeq\mathbb{Z}_2$ and consists of identity and the conjugation.

Example 10. More generally, suppose that a is not a square in F. Then, similarly to the previous example, one can prove that $G(F[\sqrt{a}]/F)$ has two automorphisms: identity and conjugation $\phi(x+y\sqrt{a})=x-y\sqrt{a}$. If F has characteristic 2 then these automorphisms coincide and the Galois group is trivial. Otherwise $G(F[\sqrt{a}]/F)\simeq\mathbb{Z}_2$.

Proposition 11. *Let p be a prime number, then the Galois group of $f(x) = x^p - 1$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_{p-1}$.*

Proof. As above, let $\zeta = e^{2\pi i/p}$, then $\mathbb{Q}(\zeta)$ is the splitting field of $f(x)$. If $\phi \in G(\mathbb{Q}(\zeta)/\mathbb{Q})$ then by Proposition 8 $\phi(\zeta)$ is also a root of $f(x)$. Since ϕ is a bijection and $\phi(1) = 1$, $\phi(\zeta) \neq 1$. Therefore $\phi(\zeta) = \zeta^k, 1 \leq k \leq p-1$. Since $\mathbb{Q}(\zeta)$ has a basis ζ^i $(i \leq p-2)$, this defines a map $\phi_k : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ by $\phi_k(\zeta^i) = \zeta^{ik}$. More generally, we have $\phi_k(g(\zeta)) = g(\zeta^k)$. Since the minimal polynomials of ζ and ζ^k are the same, the fields $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta^k)$ are isomorphic, so ϕ_k is an automorphism of $\mathbb{Q}(\zeta)$.

Therefore the Galois group has $(p-1)$ elements $\phi_1, \ldots, \phi_{p-1}$. Now $\phi_k \circ \phi_m = \phi_{km}$, so

$$G(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}_p^\times, \cdot) \simeq (\mathbb{Z}_{p-1}, +).$$

□

Theorem 12. *Let $f(x)$ be an irreducible polynomial of degree n over a field F of characteristic 0. Let K be the splitting field for $f(x)$. Then the following facts hold:*

a) All roots of $f(x)$ in K are distinct, we can denote them by $x_1, \ldots, x_n$.

b) The Galois group $G(K/F)$ acts on the set $\{x_1, \ldots, x_n\}$ by permutations.

c) An automorphism $\phi \in G(K/F)$ is completely determined by its values on the roots $\phi(x_1), \ldots, \phi(x_n)$, so $G(K/F)$ is isomorphic to a subgroup of S_n.

d) The size of the Galois group equals the degree of the splitting field: $|G(K/F)| = [K : F]$.

e) The action of $G(K/F)$ on the set of roots is transitive, that is, has one orbit.

Example 13. Consider again the polynomial $f(x) = x^3 + x + 1$ over $\mathbb{Q}$. As explained above, its splitting field K has degree 6, so $|G(K/\mathbb{Q})| = 6$. On the other hand, $G(K/\mathbb{Q})$ is a subgroup of S_3 and $|S_3| = 6$. Therefore $G(K/\mathbb{Q}) = S_3$. This is the first example of a non-commutative Galois group.

The following theorem is one of the most fundamental results in Galois theory. Let $K \supset L \supset F$ be a chain of field extensions. Any automorphism of K preserving L is automatically preserving F, so $G(K/L) \subset G(K/F)$.

Theorem 14. *Let K be a splitting field of some irreducible polynomial over F. If $K \supset L \supset F$ then K is a splitting field (of some other polynomial) over L and $G(K/L) \subset G(K/F)$. Conversely, for every*

subgroup $H \subset G(K/F)$ there is a unique intermediate field L such that $G(K/L) = H$. This defines a bijective correspondence between the subgroups of the Galois group $G(K/F)$ and intermediate fields L.

1.3. **Construction of the 17-gon.** In this section we use Galois theory to prove the celebrated theorem of Gauss about the construction of regular polygons with the straightedge and compass.

Theorem 15. *Let $p > 2$ be a prime number. Then a regular p-gon can be constructed using straightedge and compass if and only if $p = 2^n + 1$ for some integer n.*

Corollary 16. *One can construct the 17-gon using straightedge and compass since $17 = 2^4 + 1$. On the other hand, it is impossible to construct a 7-gon.*

Proof. One can construct a regular p-gon if and only if the complex number $\zeta_p = e^{2\pi i/p}$ is constructible, or, equivalently, its real and imaginary parts $\cos(2\pi/p), \sin(2\pi/p)$ are constructible.

Recall (see section 15.5 of the book for details) that a number α is constructible if and only if there is a chain of fields

$$\mathbb{Q}(\alpha) = F_n \supset F_{n-1} \supset \dots F_2 \supset F_1 = \mathbb{Q}$$

such that $[F_k : F_{k-1}] = 2$ for all k.

Suppose that ζ_p is constructible, then the degree of the minimal polynomial of ζ_p equals $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2 \cdots 2 = 2^n$. On the other hand, the minimal polynomial for ζ_p equals $x^{p-1} + \dots + 1$ and has degree $p - 1$. Therefore $p - 1 = 2^n$, and $p = 2^n + 1$.

Conversely, suppose that $p = 2^n + 1$, we need to construct a chain of subfields:

$$\mathbb{Q}(\zeta_p) = F_n \supset F_{n-1} \supset \dots F_2 \supset F_1 = \mathbb{Q}.$$

By proposition 11 we have $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{Z}_{p-1} = \mathbb{Z}_{2^n}$. It has a chain of subgroups

$$\mathbb{Z}_{2^n} \supset \mathbb{Z}_{2^{n-1}} \supset \dots \mathbb{Z}_2.$$

By Main Theorem 14 there is a field $\mathbb{Q}(\zeta_p) \supset F_2 \supset \mathbb{Q}$ such that $G(\mathbb{Q}(\zeta_p)/F_2) = \mathbb{Z}_{2^{n-1}}$ and $\mathbb{Q}(\zeta_p)$ is a splitting field over F_2. This means that $[\mathbb{Q}(\zeta_p) : F_2] = |G(\mathbb{Q}(\zeta_p)/F_2)| = 2^{n-1}$, and

$$[F_2 : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : F_2]} = \frac{2^n}{2^{n-1}} = 2.$$

By the same theorem, there is a field $\mathbb{Q}(\zeta_p) \supset F_3 \supset F_2$ such that $G(\mathbb{Q}(\zeta_p)/F_3) = \mathbb{Z}_{2^{n-2}}$ and $\mathbb{Q}(\zeta_p)$ is a splitting field over F_3. This means

that $[\mathbb{Q}(\zeta_p) : F_3] = |G(\mathbb{Q}(\zeta_p)/F_3)| = 2^{n-2}$, and

$$[F_3 : F_2] = \frac{[\mathbb{Q}(\zeta_p) : F_2]}{[\mathbb{Q}(\zeta_p) : F_3]} = \frac{2^{n-1}}{2^{n-2}} = 2.$$

By continuing this procedure, we can construct the desired chain of quadratic extensions. □

1.4. **Solvable groups and solvable equations.** We need to recall the notion of the normal subgroup and of the quotient group.

Definition 17. A subgroup $H \subset G$ is called normal, if for all $g \in G$ and $h \in H$ one has $ghg^{-1} \in H$.

Recall that $H \subset G$ defines two equivalence relations on G:

$$x \sim_L y \text{ if } x = yh \text{ for some } h \in H,$$

$$x \sim_R y \text{ if } x = hy \text{ for some } h \in H.$$

Theorem 18. *Let $H \subset G$ be a normal subgroup. Then $x \sim_L y$ if and only if $x \sim_R y$, and the set of equivalence classes for $\sim$ is a group. It is called the quotient group G/H.*

Proof. Suppose that $x \sim_L y$, then $x = yh$ for some $h \in H$. Since $yhy^{-1} = h' \in H$, we can write $yh = h'y$, so $x = h'y \sim_R y$. Therefore two equivalence relations coincide and we can denote them just by $\sim$. Now suppose that $x \sim y$ and $z \sim w$, then

$$x = yh,\ z = wh'' \ \Rightarrow xz = yhwh'' = ywh'h'' \sim yw,$$

where $h' = w^{-1}hw$, so $hw = wh'$. This means that the equivalence class of the product of two elements depends only on the equivalence classes of these elements, and the product of equivalence classes is defined correctly. This defines the group structure on the set of equivalence classes. □

For more details, see section 2.12 of the book.

Example 19. The subgroup $A_n \subset S_n$ consisting of all even permutations is normal, since a conjugate of an even permutation is even. Odd permutations and even permutations form two conjugacy classes, and $S_n/A_n \simeq \mathbb{Z}_2$.

Definition 20. A group G is called solvable if there is a chain of subgroups

$$G = H_1 \supset H_2 \supset H_3 \supset \ldots \supset H_n = e$$

such that H_{k+1} is normal in H_k and H_k/H_{k+1} is a cyclic group.

Definition 21. A group G is called solvable if there is a chain of subgroups

$$G = H_1 \supset H_2 \supset H_3 \supset \ldots \supset H_n = e$$

such that H_{k+1} is normal in H_k and H_k/H_{k+1} is abelian.

Proposition 22. *For finite groups, definitions 20 and 21 are equivalent.*

Proof. Every cyclic group is abelian, so Definition 20 implies Definition 21. Conversely, suppose that there is a chain of subgroups such that H_k/H_{k+1} is abelian. By Fundamental Theorem of Abelian Groups one can write

$$H_k/H_{k+1} = \mathbb{Z}_{n_1} \oplus \ldots \mathbb{Z}_{n_l}$$

for some $n_1, \ldots, n_l$ (in fact, we can choose n_i to be prime). Let $p : H_k \to H_k/H_{k+1}$ be the natural projection. Consider the chain of subgroups

$$H_k/H_{k+1} \supset (\mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_l}) \supset (\mathbb{Z}_{n_3} \oplus \ldots \oplus \mathbb{Z}_{n_l}) \supset \ldots \mathbb{Z}_{n_l},$$

since H_k/H_{k+1} is abelian, all of them are normal. Now

$$H_k \supset p^{-1}(\mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_l}) \supset p^{-1}(\mathbb{Z}_{n_3} \oplus \ldots \oplus \mathbb{Z}_{n_l}) \supset \ldots p^{-1}(\mathbb{Z}_{n_l}) \supset H_{k+1}$$

All these subgroups are normal in H_k and by the isomorphism theorem

$$H_k/p^{-1}(\mathbb{Z}_{n_2} \oplus \ldots \mathbb{Z}_{n_l}) \simeq \mathbb{Z}_{n_1},$$
$$p^{-1}(\mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_l})/p^{-1}(\mathbb{Z}_{n_3} \oplus \ldots \oplus \mathbb{Z}_{n_l}) \simeq \mathbb{Z}_{n_2}, \ldots,$$
$$p^{-1}(\mathbb{Z}_{n_l})/H_{k+1} \simeq \mathbb{Z}_{n_l}.$$

Therefore between each pair $H_k \supset H_{k+1}$ one can include a chain of normal subgroups so that all successive quotients are cyclic, and Definition 20 holds. □

Example 23. The group S_3 has a chain of normal subgroups $S_3 \supset A_3 \supset \{e\}$. One has $S_3/A_3 \simeq \mathbb{Z}_2, A_3/\{e\} = A_3 \simeq \mathbb{Z}_3$, so S_3 is solvable.

Example 24. The group S_4 has a chain of normal subgroups $S_4 \supset A_4 \supset K_4 \supset \{e\}$, where

$$K_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

By Example 19, $S_4/A_4 \simeq \mathbb{Z}_2$. The group A_4/K_4 has $12/4 = 3$ elements and hence is isomorphic to Z_3. The group $K_4/\{e\} = K_4$ is abelian, in fact, it is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Therefore S_4 is solvable.

Proposition 25. *A subgroup of a solvable group is solvable.*

Definition 26. A group G is called simple, if it has no nontrivial normal subgroups.

We will use the following fact from group theory without proof.

Theorem 27. *The group A_5 is simple. The only nontrivial normal subgroup of S_5 is A_5. As a consequence, S_5 is not solvable.*

The importance of solvable groups in Galois theory is emphasized by the following theorem.

Theorem 28. *A polynomial $f(x)$ over a field F of characteristic zero can be solved in radicals if and only if its Galois group is solvable.*

Proposition 29. *Every polynomial equation of degree at most 4 can be solved in radicals.*

The corresponding formulas were found by Cardano in degree 3 and by Ferrari in degree 4, long before the Galois theory.

Proof. The Galois group of a degree 3 equation is a subgroup of S_3, the Galois group of a degree 4 equation is a subgroup of S_4. Since both S_3 and S_4 are solvable and a subgroup of a solvable group is solvable, the Galois groups of these equations are always solvable. By Theorem 28 the equations can be solved in radicals. □

Theorem 30. *There are equations of degree 5 which cannot be solved in radicals.*

Proof. One can prove (see below) that there exists an equation of degree 5 with Galois group S_5. Since S_5 is not solvable, this equation cannot be solved in radicals. □

The following example was not discussed in class, but we include it for completeness.

Theorem 31. *Let $f(x)$ be an irreducible polynomial of degree 5 with rational coefficients, which has exactly 3 real roots. Then the Galois group of $f(x)$ is isomorphic to S_5.*

Proof. Let K be the splitting field of $f(x)$. The Galois group $G(K/\mathbb{Q})$ is a subgroup of S_5. Since $f(x)$ has exactly 3 real roots, it also has 2 complex conjugate roots. The complex conjugation is an automorphism of K which preserves real roots and swaps complex ones, so it acts as a transposition in S_5.

Since the action of the Galois group on the roots is transitive, it has an orbit of length 5. By the Orbit-Stabilizer formula, the order of $G(K/\mathbb{Q})$ is divisible by 5. By Sylow theorem, $G(K/\mathbb{Q})$ must have an element of order 5. Since $G(K/\mathbb{Q}) \subset S_5$, this element of order 5 must be a 5 -cycle.

Therefore $G(K/\mathbb{Q})$ contains both a transposition and a 5-cycle. One can check that these two permutations generate S_5, so $G(K/\mathbb{Q}) = S_5$. □