ALGEBRA II QR GUIDE

BAILEE ZACOVIC

These notes provide an overview of Galois theory and other relevant content for the University of Michigan's Algebra II Qualifying Review Examination. For further reading, see *Abstract Algebra* by Dummit and Foote, *Algebra* by Hungerford, *Algebra* by Lang, *Abstract Algebra: The Basic Graduate Year* by Ash, *Commutative Algebra* by Zariski and Samuel, *Lectures in Abstract Algebra, Vol. III* by Jacobson, and *Basic Algebra* by Jacobson.

1. Subgroups and Quotients

Let G be a group, and denote $e \in G$ the identity element.

Definition 1.1. A *subgroup* $H \leq G$ is a subset of G which is nonempty and closed under products and inverses.

Definition 1.2. A subgroup H of G is *normal*, denoted $H \trianglelefteq G$ is a self-conjugate group, that is, it satisfies any of the following equivalent conditions:

- $gNg^{-1} \subseteq N$ for all $g \in G$,
- $gN = Ng$ for all $g \in G$,
- $[N, G] \subseteq N$.

Normality is a feature which, in particular, ensures the natural (left) coset multiplication: $gN \cdot hN = (gh)N$. For this reason, we only consider quotients by normal subgroups.

Fact 1.3. *All index-2 subgroups are normal.*

Conjugacy classes provide another useful characterization of normal subgroups.

Definition 1.4. Elements $g, h \in G$ are *conjugate* whenever there exists an element $f \in G$ such that $g = fhf^{-1}$.

Example 1.5. In A_5, there are five conjugacy classes, with representatives given by:

$$e,\ (12345),\ (21345),\ (12)(34),\ (123).$$

On can verify that the orders of these classes are given by $1, 12, 12, 15,$ and 20 respectively.

Lemma 1.6. *A subgroup $H \leq G$ is normal if and only if it is the union of conjugacy classes in G.*

Definition 1.7. A *simple group* G is such that $N \trianglelefteq G$ implies $N = \{e\}$ or $N = G$.

Example 1.8. The alternating group A_n is simple for $n \geq 5$. (A_3 is also simple.)

Simplicity of A_n, $n \geq 5$, allows us to deduce the following additional fact, which we include here for completion.

Lemma 1.9. *For $n \geq 5$, A_n is the unique index-2 subgroup of S_n.*

Proof. Let $H \leq S_n$ be another index-2 subgroup. It is therefore normal in S_n. Then $H \cap A_5 \trianglelefteq A_5$, so it follows that $H \cap A_5 = \{e\}$ by A_5 simple. Considering the sign homomorphism sign : $S_n \to \mathbb{Z}/2\mathbb{Z}$, we realize that $H^2 \subseteq H \cap A_5 = \{e\}$ since sign$(h^2) = 0$ for all $h \in H$. This forces $H = \{e\}$, a contradiction. □

Definition 1.10. Let $N \trianglelefteq G$. The *quotient group* denoted G/N is given by the set of all left cosets of N in G, i.e., $G/N = \{gN : g \in G\}$.

Theorem 1.11. *(Second Isomorphism Theorem) For $S \leq G$ and $N \trianglelefteq G$, $SN/N \cong S/N \cap S$, where SN denotes the subgroup generated by the union of elements $S \cup N$.*

The structure of a group G is unveiled in part by its subgroups. Characterizing subgroups is therefore a central project of group theory.

Theorem 1.12. *(Langrange's Theorem) If G is finite and $H \leq G$, then $|H|\big||G|$.*

Theorem 1.13. *(Cauchy's Theorem) If G is finite and p is a prime satisfying $p\big||G|$, then G contains an element of order p.*

Given some subset $S \subseteq G$, we define the following two subgroups associated to S:

Definition 1.14. The *centralizer* of S in G is $C_G(S) = \{g \in G : gs = sg$ for all $s \in S\}$.

The *center* of a group G is denoted $Z(G) = C_G(G)$.

Example 1.15. For $D_{2n} = \langle r, s : r^n = s^2 = e,\ srs = r^{-1}\rangle$,

$$Z(D_n) = \begin{cases} \{e\} & \text{when } n \text{ is odd} \\ \{e, r^{n/2}\} & \text{when } n \text{ is even.} \end{cases}$$

Example 1.16. The center $Z(A_n)$ (and therefore $Z(S_n)$) is trivial for $n \geq 4$.

The center is particularly interesting when G has prime structure.

Theorem 1.17. *(Burnside's Theorem) If G is a p-group, $Z(G)$ is nontrivial.*

Proof. Let $|G| = p^n$ for p a prime. Consider the class equation of G,

$$p^n = |G| = |Z(G)| + \sum_{g_i} [G : C_G(g_i)],$$

where the g_i are representatives of the disjoint conjugacy classes of G, and $[G : C_G(g_i)]$ divides p^n, hence $[G : Z(G)] \geq [G : C_G(g_i)] = p^i \geq 1$ for some $1 \leq i \leq n$. If $Z(G)$ is trivial, then p divides the left-hand side but not the right, a contradiction. So $Z(G)$ is nontrivial. □

Lemma 1.18. *G is abelian if and only if $G/Z(G)$ is cyclic.*

Proof. If G is abelian, $G/Z(G)$ is trivial. Conversely, if $G/Z(G)$ is cyclic, let $\sigma \in G$ be a generator such that $G/Z(G)$ consists of $Z(G), \sigma Z(G), \ldots, \sigma^n Z(G)$. Then any $g, h \in G$ satisfy $g = \sigma^i s$, $h = \sigma^j t$ for $s, t \in Z(G)$, such that

$$gh = (\sigma^i s)(\sigma^j t) = \sigma^{i+j} st = (\sigma^j t)(\sigma^i s) = hg.$$

□

Definition 1.19. The *normalizer* of S in G is $N_G(S) = \{g \in G : gS = Sg\}$.

Not all groups enjoy the property of being abelian. We can capture a group's deviation from being abelian in the commutator subgroup.

Definition 1.20. For G a group, the *commutator subgroup* is defined as $[G, G] = \{ghg^{-1}h^{-1} : g, h \in G\}$.

When G is abelian, $[G, G] = \{e\}$. It is an exercise to show $[G, G] \trianglelefteq G$. We can always consider an "abelianized" version of any group by taking the quotient by the commutator subgroup.

Definition 1.21. The *abelianization* of a group G is given by $G_{ab} = G/[G, G]$.

The order of G_{ab} is given by the absolute value of its presentation matrix (see Exercise 1.23). We define one final family of subgroups, which are invariant under group automorphism.

Definition 1.22. We call $H \leq G$ a *characteristic subgroup* of G if $\Phi(H) = H$ for all $\Phi \in \mathrm{Aut}(G)$.

Examples of characteristic subgroups include the center $Z(G)$ of a group G, and the commutator subgroup $[G, G]$.

1.1. **Exercises.**

Exercise 1.23. Let G be a group with the following presentation:

$$G = \langle a, b | (a^2 b)^5 = 1,\ a^2 b a^{-1} b^{-2} \rangle,$$

and let $[G, G]$ be the commutator subgroup of G. Compute the order of $G/[G, G]$.

Proof. The abelianization of the free group $F = \langle a, b \rangle$ is $\mathbb{Z}^2$. Denote $\overline{a}$ and $\overline{b}$ the generators. Notice that

$$(a^2 b)^5 = 1 \implies 10\overline{a} + 5\overline{b} = 0,$$
$$a^2 b a^{-1} b^{-2} = 1 \implies \overline{a} - \overline{b} = 0.$$

We obtain an isomorphism

$$G_{ab} = (\mathbb{Z}\overline{a} \oplus \mathbb{Z}\overline{b})/(10\overline{a} + 5\overline{b}, \overline{a} - \overline{b}),$$

i.e. G_{ab} has the presentation matrix

$$\begin{pmatrix} 10 & 1 \\ 5 & -1 \end{pmatrix}$$

whose determinant in absolute value is 15. $\square$

Exercise 1.24. (August 2020 Problem 2) Let G be the group of all invertible upper-triangular 2×2 real matrices (with group law matrix multiplication). Let H be the subset of G consisting of all elements of the form g^2 with $g \in G$. Show that H is a subgroup, and compute its index.

Proof. First, we aim to understand the elements of H. An element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ of G satisfies

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} \sqrt{a} & \frac{b}{\sqrt{a}+\sqrt{c}} \\ 0 & \sqrt{c} \end{pmatrix}^2 \text{ where } \begin{pmatrix} \sqrt{a} & \frac{b}{\sqrt{a}+\sqrt{c}} \\ 0 & \sqrt{c} \end{pmatrix} \in G \iff a, c > 0$$

It is clear now that $H \leq G$, where the coset representatives are given by

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

corresponding to the choice of sign on a and c. This means $[G : H] = 4$. $\square$

Exercise 1.25. (January 2021 Problem 1) Let G be a finite group and let $\Phi : G \to G$ be a group homomorphism. For $n \geq 1$, let $\Phi^n : G \to G$ denote the n-fold composition $\Phi \circ \cdots \circ \Phi$. Set $A = \bigcap_{n=1}^{\infty} \text{Im}(\Phi^n)$ and $B = \bigcup_{n=1}^{\infty} \text{Ker}(\Phi^n)$. Show that B is normal in G, and that G is the semi-direct product of A and B.

Proof. We have $\text{Ker}(\Phi) \subseteq \text{Ker}(\Phi^2) \subseteq \cdots \subseteq G$, which means there exists N such that $\text{Ker}(\Phi^N) = \text{Ker}(\Phi^{N+1}) = \ldots$. This means that $B = \text{Ker}(\Phi^N) \trianglelefteq G$. Moreover, $G \supseteq \text{Im}(\Phi) \supseteq \text{Im}(\Phi^2) \supseteq \ldots$, i.e. there exists M such that $\text{Im}(\Phi^M) = \text{Im}(\Phi^{M+1}) = \ldots$. Thus, $A = \text{Im}(\Phi^M)$. We may assume $M = N$. It remains to show that $G = AB$ and $A \cap B = \{e\}$. Let $g \in A \cap B$. Then there exists $h \in G$ such that $\Phi^M(h) = g$, and so $\Phi^{2M}(h) = e$, i.e. $h \in \text{Ker}(\Phi^{2M}) = \text{Ker}(\Phi^M)$, which implies $g = e$. Next, fix $g \in G$. We aim to show $g = ab$ for $a \in A$ and $b \in B$. Since $\text{Im}(\Phi^M) = \text{Im}(\Phi^{2M})$, there exists some $h \in G$ such that $\Phi^M(g) = \Phi^{2M}(h)$. Denote $a = \Phi^M(h) \in A$. Then $\Phi^M(a^{-1}g) = (\Phi^{2M}(h))^{-1}\Phi^M(g) = e$, i.e. $a^{-1}g \in B$, and the desired decomposition $g = a(a^{-1}g)$ follows. $\square$

Exercise 1.26. (August 2021 Problem 2) Let p be an odd prime number. Form the semi-direct product $G = \mathbb{F}_p \rtimes \mathbb{F}_p^*$ for the standard (scalar multiplication) action of $\mathbb{F}_p^*$ on $\mathbb{F}_p$. Let ℓ be a prime. Calculate the cardinality of the set of all group homomorphisms from G to $\mathbb{Z}/\ell\mathbb{Z}$ in the following cases:

(1) ℓ is a prime number different from p,
(2) $\ell = p$.

Proof. We begin by recalling the fact that $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/\text{gcd}(m, n)\mathbb{Z}$.

(1) When $\ell \neq p$, we know first of all that $\text{Hom}(\mathbb{F}_p, \mathbb{Z}/\ell\mathbb{Z})$ is trivial, i.e. any homomorphism from G to $\mathbb{Z}/\ell\mathbb{Z}$ must factor through $\mathbb{F}_p^*$, which is cyclic of order $p-1$. From this we deduce $\text{Hom}(\mathbb{F}_p^*, \mathbb{Z}/\ell\mathbb{Z}) \cong \mathbb{Z}/\text{gcd}(p-1, \ell)\mathbb{Z}$.

(2) When $\ell = p$, it no longer happens that $\mathrm{Hom}(\mathbb{F}_p, \mathbb{Z}/\ell\mathbb{Z})$ is trivial. On the other hand, since $\mathbb{Z}/\ell\mathbb{Z}$ is abelian, the kernel of an such homomorphism must include $[G, G]$. Since ℓ is odd, any element in $\mathbb{F}_p \rtimes \{e\}$ is of the form $(a, 1) = (a, -1)\cdot(0, -1)$, i.e. any homomorphism must vanish on $\mathbb{F}_p \rtimes \{e\}$, and again factor through the quotient $\mathbb{F}_p^*$. Only this time, $\gcd(p-1, p) = 1$, hence $\mathrm{Hom}(\mathbb{F}_p^*, \mathbb{Z}/\ell\mathbb{Z})$ is trivial.

□

Exercise 1.27. Let F be a field. Prove or disprove: there is an action of $F^\times$ on $\mathrm{SL}_n(F)$ such that $\mathrm{GL}_n(F) = \mathrm{SL}_n(G) \rtimes F^\times$.

Proof. This is true. We may embed $F^\times$ into $\mathrm{GL}_n(F)$ by mapping each $\alpha \in F^\times$ to the matrix $\mathrm{diag}(\alpha, 1 \ldots, 1)$. Notice that $\mathrm{diag}(\alpha, 1 \ldots, 1) \in \mathrm{SL}_n(F)$ if and only if α is the identity, i.e. the image of $F^\times$ in $\mathrm{GL}_n(F)$, isomorphic to $F^\times$, intersects $\mathrm{SL}_n(F)$ only trivially. We also recall that $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$ by the determinant map a homomorphism. In fact, we have the following short exact sequence via the determinant map:

$$e \longrightarrow \mathrm{SL}_n(F) \longrightarrow \mathrm{GL}_n(F) \xrightarrow{\det} F^\times \longrightarrow e$$

Since the embedding above provides a map from $F^\times$ to $\mathrm{GL}_n(F)$, this sequence is right split exact and hence $\mathrm{GL}_n(F) \cong \mathrm{SL}_n(F) \rtimes F^\times$.

□

2. Sylow Theorems

Definition 2.1. A *p-group* is a group in which the order of every element in a power of p.

For fixed p, not all p-groups are isomorphic. For instance, $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. A special feature of p-groups is that their centers are nontrivial.

Fact 2.2. *Any group of order p^2 is abelian.*

The Sylow theorems now provide further machinery to describe certain subgroups of finite groups.

Theorem 2.3. *(Sylow I) Given G such that $|G| = p^e \cdot m$ for p a prime and $\gcd(p, m) = 1$, then there exists a subgroup $H \leq G$ with $|H| = p^e$, called a "Sylow p-subgroup".*

Theorem 2.4. *(Sylow II) Given a Sylow p-subgroup $H \leq G$, any other Sylow p-subgroup $H' \leq G$ is conjugate to H, i.e. $H' = gHg^{-1}$ for some $g \in G$.*

In particular, when $H \leq G$ is the unique Sylow p-subgroup, then $H \trianglelefteq G$. This will be useful in our future discussion of solvability.

Theorem 2.5. *(Sylow III) The number of Sylow p-subgroups n_G of G satisfies $n_G \big| \frac{n}{p^e}$ and $n_G \equiv 1 \pmod{p}$.*

Importantly, the conjugation action of G on the set of Sylow p-subgroups induces a homomorphism $G \to S_{n_G}$.

Example 2.6. Let G be finite with $|G| = 15 = 3 \cdot 5$. Then G admits unique Sylow 3- and 5-subgroups, which are furthemore disjoint by $\gcd(3,5) = 1$. It follows that G is the direct product of its Sylow p-subgroups.

Fact 2.7. *For primes $p < q$, $q \not\equiv 1 \pmod{p}$, and $|G| = p \cdot q$, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*

Definition 2.8. A finite group is *nilpotent* if it is the direct product of its Sylow subgroups.

Example 2.9. All abelian groups and p-groups are nilpotent.

2.1. **Exercises.**

Exercise 2.10. (May 2022 Problem 1) Let G be a simple group. Let $H \trianglelefteq G \times G$. Show that H is isomorphic to the trivial group, G, or $G \times G$.

Proof. Denote π_i the projection onto the ith factor. Consider $H \cap (G \times \{e\}) \trianglelefteq G \times G$, where it follows that $K = H \cap (G \times \{e\})$ is isomorphic to a normal subgroup of G via π_1. Similarly define $L := \pi_2(H)$. We obtain the following short exact sequence:

$$e \longrightarrow K \longrightarrow H \longrightarrow L \longrightarrow e$$

The image of a normal subgroup under a surjective homomorphism is normal, hence $L \trianglelefteq G$. Since $\pi_1(K), L = \{e\}$ or G, it follows from $H/K \cong L$ that $H = \{e\}, G$ or $G \times G$. □

Exercise 2.11. (May 2022 Problem 2) Let p be a prime. Let G be a group such that $|G|$ is divisible by p but not p^2. Show that G contains at most $p - 1$ conjugacy classes of elements of order p.

Proof. By Cauchy's theorem, we are guaranteed an element $\sigma \in G$ of order p, such that $\langle \sigma \rangle \leq G$ is a Sylow p-subgroup. Any other element τ of order p generates the Sylow p-subgroup $\langle \tau \rangle$ which is conjugate to $\langle \sigma \rangle$. In particular, τ is conjugate to one of $\sigma, \sigma^2, \ldots, \sigma^{p-1}$. □

Exercise 2.12. (May 2023 Problem 2) Let G be a finite group with $|G| \equiv 2 \pmod{4}$. Let s and t be two nonidentity elements of G with $s^2 = t^2 = 1$. Show that s and t are conjugate within G.

Proof. Any Sylow 2-subgroup of G has order 2, so $\langle s \rangle = \{1, s\}$ and $\langle t \rangle = \{1, t\}$ are both Sylow 2-subgroups, which are therefore conjugate. Hence $s = gtg^{-1}$ for some $g \in G$. □

Exercise 2.13. (January 2024 Problem 1) Let G be a finite simple group which contains an element of order 55. Prove that the index of any proper subgroup of G is at least 16.

Proof. Fix a proper subgroup $H \leq G$, and denote $n := [G : H]$. Let $\tau \in G$ be of order 55. The action of G on the set of left cosets G/H defines a homomorphism $\rho : G \to S_n$, where $\ker(\rho) \trianglelefteq G$. Since G is simple and H is proper, $\ker(\rho) = \{e\}$. From this it follows that S_n contains an element $\sigma = \rho(\tau)$ of order 55. The order of an element in S_n is the least common multiple of the lengths of the cycles in its cycle decomposition, hence σ

decomposes into disjoint cycles of lengths 5 and 11. This furnishes a lower bound on the size of n, i.e. $n \geq 5 + 11 = 16$. □

Exercise 2.14. (January 2024 Problem 1) Prove that any group G of order $455 = 5 \cdot 7 \cdot 13$ is abelian.

Proof. By the Sylow theorems, G contains exactly one or 91 Sylow 5-subgroups, exactly one Sylow 7-subgroup, and exactly one Sylow 13-subgroup. Denote N_7 and N_{13} the (normal) Sylow 7- and 13-subgroups. Since $N_7 \cap N_{13} = \{e\}$ homomorphism $\varphi : G \to G/N_7 \times G/N_{13}$ is injective, and in fact each of G/N_7 and G/N_{13} are abelian since $G/N_7 \cong C_5 \times C_{13}$ and $G/N_{13} \cong C_5 \times C_7$. Since subgroups of solvable groups remain solvable, and the direct product of solvable groups is solvable, the result follows. The key idea here was to break the factors 7 and 13 over two quotient groups. □

Exercise 2.15. Let G be a finite group of order n. Let G act on itself by left multiplication, and let $\Phi : G \to S_n$ be the homomorphism associated to this action. Show that $\text{im}(G) \subseteq A_n$ if and only if (1) n is odd, or (2) n is even and the 2-Sylow subgroups of G are not cyclic.

Proof. Let $|G| = 2^k m$, for m odd. First, suppose n is even, i.e. $k \geq 1$, and that the 2-Sylows are cyclic. We have at least one cyclic Sylow subgroup, then, of order 2^k, call it C_{2^k} and let b be a generator of this subgroup. Next, recall that the any cycle of even length in the symmetric group has sign -1. Then the order of $|\Phi(b)|\big|2^k$ (where $\Phi(b)$ generates a cyclic subgroup in S_n), in particular it is even, hence the sign of $\Phi(b)$ is odd, and so $\text{im}(\Phi) \nsubseteq A_n$.

Conversely, if n is odd, then the order of every $g \in G$ is odd, hence the order of $\Phi(g)$ is odd, i.e. consists of a product of cycles of odd length. Since any odd cycle has sign $+1$, it follows that $\Phi(g) \in A_n$. Now let n be even, and suppose the 2-Sylows are not cyclic. Then $g \in G$ has order $2^a b$, b odd. It follows that g^b has order 2^a and is contained in a 2-Sylow subgroup. Since the 2-Sylow subgroups are not cyclic, $a < k$. Then g acts on G by $2^{k-a} \cdot \frac{m}{b}$ cycles of length $2^a b$, and since $2^{k-a} \cdot \frac{m}{b}$ is even, the sign of $\Phi(g)$ is $(-1)^{2^{k-a} \cdot \frac{m}{b}} = +1$. In all cases, $\text{im}(\Phi) \subseteq A_n$. □

Exercise 2.16. (January 2022 Problem 1) Let p be a prime number. Let G be a group of order p^k for $k \geq 1$ and let H be the subgroup of G generated by elements of the form g^p. Show that $H \neq G$.

Proof. All p-groups are nilpotent, and therefore G admits some nontrivial abelian quotient G/ξ. Since G/ξ is a p-group, it admits a surjective group homomorphism $G/\xi \to \mathbb{Z}/p\mathbb{Z}$. In particular, $H \subseteq \text{Ker}(G/\xi \to \mathbb{Z}/p\mathbb{Z})$, and so $H \neq G$. □

3. Solvability

It is natural to ask when certain polynomial equations are solvable by radicals. To answer this question, Galois theory provides the necessary bridge between group theory

and field theory. The polynomials which are solvable by radicals turn out to be exactly those which correspond to certains groups of solvable type under this identification.

Definition 3.1. A group G is *solvable* if there exists a sequence of subgroups $H_1, \ldots, H_k \leq G$ such that

- $H_j \trianglelefteq H_{j-1}$,
- the *factor groups* H_{j-1}/H_j are abelian, and
- $H_k = \{e\}$.

We obtain the following chain:

$$G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_k = \{e\}.$$

Example 3.2. All abelian groups, dihedral groups $D_{2n} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$, p-groups, and nilpotent groups are solvable.

Non-Example 3.3. Simple, nonabelian groups (like A_n) and symmetric groups S_n (for $n \geq 5$) are not solvable.

We can define a slightly relaxed version of this series, which exists for all finite groups.

Definition 3.4. A *composition series* of G is a finite chain of subgroups $G_1, \ldots, G_n \leq G$ such that

- $G_i \trianglelefteq G_{i-1}$,
- the *factor groups* G_{i-1}/G_i are simple, and
- $G_n = \{e\}$.

We obtain the following chain:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}.$$

Definition 3.5. The *length* of a composition series is the number of subgroups in the chain not including the identity.

Theorem 3.6. *(Jordan-Hölder Decomposition Theorem) Every finite group G has a composition series, and any two composition series of G has the same length.*

The solvable groups are precisely those finite groups whose simple factor groups in its composition series are abelian, and so necessarily prime-order cyclic. We proceed to a few nice properties of solvable groups:

Lemma 3.7. *Let G be a solvable group. Then,*

- *For $H \leq G$, H is solvable,*
- *For $N \trianglelefteq G$, G/N is solvable,*
- *For G, H solvable, $G \times H$ is solvable,*
- *For any surjective group homomorphism $\varphi : G \to H$, H is solvable.*

We even obtain the following converse:

Lemma 3.8. *For $N \trianglelefteq G$, G is solvable if and only if N and G/N are solvable.*

Theorem 3.9. *(Feit-Thompson Theorem) Every group of odd order is solvable.*

3.1. **Exercises.**

Exercise 3.10. Let G be a group of order $4 \cdot 3^n$. Show that G is solvable.

Proof. From the Sylow theorems, G has either 1 or 4 Sylow 3-subgroups. If it has only one, call it H, we are done, since p-groups are solvable and $|H| = 3^n$, $|G/H| = 2^2$.

Suppose G has 4 Sylow 3-subgroups. The conjugation action of G on the set of Sylow 3-subgroups defines a homomorphism $\varphi : G \to S_4$. In particular, $|G/\ker(\varphi)|$ divides $24 = 2^3 \cdot 3$ and $4 \cdot 3^n$, so it is either $2, 3, 4, 2 \cdot 3$ or $3 \cdot 4$. If it is 4 or $3 \cdot 4$, then $\ker(\varphi)$ is a p-group and therefore solvable. If it is $2 \cdot 3$, then $\ker(\varphi)$ contains an index-2 p-group, and is therefore solvable. It cannot be 2 or 3, else this contradicts that there are 4 distinct Sylow 3-subgroups. In all cases, $\ker(\varphi)$ is solvable, and $\mathrm{im}(\varphi)$ is solvable since S_4 is solvable. It follows that G is solvable. □

Exercise 3.11. Let k be a positive integer. The group $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ consists of matrices with entries in the ring $\mathbb{Z}/2^k\mathbb{Z}$ whose determinant in a unit of $\mathbb{Z}/2^k\mathbb{Z}$. Show that $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is a solvable group. You may use without proof that $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ is solvable.

Proof. We proceed by induction on $k \geq 1$. When $k = 1$, we are done. When $k > 1$, let $\pi_k : \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2^{k-1}\mathbb{Z})$ denote the entry-wise reduction modulo 2^{k-1} group homomorphism. As this map is surjective, it suffices to show $\ker(\pi_k)$ is solvable. The matrices occupying $\ker(\pi_k)$ are those of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2^{k-1} \begin{pmatrix} i & j \\ m & n \end{pmatrix},$$

where $in - jm \in (\mathbb{Z}/2^k\mathbb{Z})^*$. One can check that all matrices of this form commute in $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$, hence $\ker(\pi_k)$ is abelian and therefore solvable. □

4. Field Extensions

Recall the notion of a field extension E/F. We review a few classical facts before proceeding to Galois theory.

Definition 4.1. Let E/F be a field extension. An element $\alpha \in E$ is called *algebraic* over F whenever there exists a non-zero polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$.

We can always assume such a polynomial f is monic.

Definition 4.2. A field extension E/F is an *algebraic extension* if every element $\alpha \in E$ is algebraic over F.

Definition 4.3. The *degree* of a field extension E/F is the dimension of E regarded as a vector space over the field of scalars F. We denote the degree by $[E : F]$.

We obtain the following simple "tower relation".

Lemma 4.4. *For a chain of field extensions $E/K/F$, $[E : F] = [E : K] \cdot [K : F]$. In particular, $[E : F]$ is finite if and only if both $[E : K]$ and $[K : F]$ are finite.*

Lemma 4.5. *Let E/F and K/F be finite field extensions, and denote EK the smallest field containing both E and K. Then $[EK : F] \leq [E : F] \cdot [K : F]$, with equality whenever $[E : F]$ and $[K : F]$ are coprime.*

Proof. set $n := [E : F]$ and $m := [K : F]$. Let $\alpha_1, \ldots, \alpha_n$ be a F-basis for E, and $\beta_1, \ldots, \beta_m$ be a F-basis fo K. Then $\{\alpha_i \beta_j : 1 \leq i \leq n,\ 1 \leq j \leq m\}$ is a F-spanning set for EK. Moreover, both $[E : F]$ and $[K : F]$ divide $[EK : F] = [EK : E] \cdot n = [EK : K] \cdot m$. When $\gcd(n, m) = 1$, nm divides $[EK : F]$, i.e. $[EK : F] \geq [E : F] \cdot [K : F]$, hence equality follows. □

Lemma 4.6. *Let E/F be a field extension. Then for any $\alpha \in E$, $deg(m_\alpha(X)) \leq [E : F]$ where $m_\alpha \in F[X]$ is the minimal polynomial of α.*

Proof. Say $n = [E : F]$, and consider the list $1, \alpha, \ldots, \alpha^n$. These elements must be linearly dependent by L a vector space of dimension n over K, which guarantees some $b_0, \ldots, b_{n-1} \in F$ such that $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Since α is a solution of $h(X) = X^n + b_{n_1}X^{n-1} + \cdots + b_1 X + b_0 \in F[X]$, $m_\alpha | h(X)$ and so $\deg(m_\alpha(X)) \leq n$. □

In particular, if α is the root of some irreducible polynomial $f(X) \in \mathbb{Q}[X]$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f)$.

Example 4.7. Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and $\mathbb{Q}(\omega\sqrt[3]{2})/\mathbb{Q}$, for $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}) \cdot \mathbb{Q}(\omega\sqrt[3]{2})$, and

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3$$

because ω is a solution of $X^2 + X + 1$. We notice that

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] < [\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Lemma 4.8. *Let E/F be a field extension of the form $F(\alpha)/F$, where the minimal polynomial $m_\alpha(X)$ of α has odd degree. Then $F(\alpha) = F(\alpha^2)$.*

Proof. Let $\deg(m_\alpha(X)) = 2k + 1$, and notice that $[F(\alpha) : F(\alpha^2)] \leq 2$. The lemma follows by the observation

$$[F(\alpha) : F(\alpha^2)] \cdot [F(\alpha^2) : F] = [F(\alpha) : F] = 2k + 1,$$

which forces $[F(\alpha) : F(\alpha^2)] = 1$. □

Lemma 4.9. *For E/F an algebraic extension, and $F \subseteq R \subseteq E$ a subring of E, R is a field.*

Definition 4.10. If E is an extension of F and $f \in F[X]$, we say f *splits* over E if $f(x) = \lambda \cdot \prod_{1 \leq i \leq k}(X - \alpha_i)$ for $\lambda \in F, \alpha_i \in E$.

Definition 4.11. If $F \leq K$ and $f \in F[X]$, we say that K is a *splitting field* for f over F if f splits over K but any proper subfield of K containing F.

Definition 4.12. An irreducible $f \in F[X]$ is *separable* if f has no repeated roots in a splitting field; an arbitrary $f \in F[X]$ is separable if its irreducible factors are separable.

Example 4.13. Every polynomial over a field of characteristic zero is separable.

Non-Example 4.14. Let $f(X) = X^p - \alpha^p \in \mathbb{F}_p[\alpha^p]$. Then f is not separable because $f(X) = (X - \alpha)^p \in \mathbb{F}_p[\alpha] \geq \mathbb{F}_p[\alpha^p]$, where $\mathbb{F}_p[\alpha]$ is a splitting field for $\mathbb{F}_p[\alpha^p]$.

Fact 4.15. *For $F \leq K \leq E$, E/F is separable if and only if E/K and K/F are separable.*

Definition 4.16. An algebraic extension E/F is *normal* if every irreducible over F that has at least one root in E splits entirely over E.

When encountered in the wild, separable field extensions may not be so easy to detect. The following fact provides a more practical characterization.

Fact 4.17. *E/F is normal if and only if E is a splitting field for some polynomial $f \in F[X]$.*

Fact 4.18. *For $F \leq K \leq E$, E/F normal implies E/K normal.*

Lemma 4.19. *All index-2 subgroups are normal.*

Definition 4.20. A finite extension E/F is *Galois* if it is (1) normal, and (2) separable, where $[E : F] = \#\{\text{automorphisms of } E \text{ that fix } F\}$.

Up to isomorphism, there is exactly one finite field consisting of p^n elements, and we denote it GF(p^n). All finite fields are of this type. It is a splitting field for the separable polynomial $X^{p^n} - X$ over $\mathbb{F}_p$, hence GF(p^n)/GF(p) is a Galois extension. The generator of GL$(p^n) \setminus \{0\}$, the multiplicative group of order $p^n - 1$, is called a *primitive element*.

Example 4.21. The element 2 is primitive for GF(3) and GF(5), but not for GF(7) since $2^3 \cong 1 \pmod 7$, i.e. it does not generate all six elements.

Definition 4.22. The minimal polynomial of a generator of GF(p^n) with coefficients in GF$(p) = \mathbb{F}_p$ is called the *primitive polynomial*.

Non-Example 4.23. The polynomial $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ is not primitive for GF(2^4) because it divides $X^5 - 1$, that is, its roots have order 5 and will not generate all 15 field elements.

Theorem 4.24. *(Primitive Element Theorem) Every finite, separable field extension is simple, i.e. generated by a single element.*

Example 4.25. One can check that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

The Galois group of this finite field extension has particularly simple structure.

Proposition 4.26. *The Galois group Gal(GF(p^n)/GF(p)) is cyclic of order n and generated by the Frobenius endomorphism $\sigma : \alpha \mapsto \alpha^p$.*

The theory of finite fields furnishes an additional interesting result.

Lemma 4.27. *All algebraically closed fields are infinite.*

Proof. Let K be an algebraically closed field. If K has characteristic zero, then $\mathbb{Q} \subseteq K$, hence K is infinite. Otherwise, $\mathrm{GF}(p) \subseteq K$ for some prime p. Since K is algebraically closed, $X^{p^{n+1}} - X$ factors into linear terms for all $n \in \mathbb{N}$, and so K must be infinite. □

For the sake of convenience, we will denote $\mathbb{F}_p := \mathrm{GF}(p)$. We now consider a special case of groups involving finite fields, namely $\mathrm{GL}_n(\mathbb{F}_p)$, and elucidate a bit of its structure.

Fact 4.28. *The order of the group $GL_n(\mathbb{F}_p)$ is given by $|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.*

Proof. Count the number of linearly independent column vectors. □

Fact 4.29. *The order of the group $SL_n(\mathbb{F}_p)$ is given by $|SL_n(\mathbb{F}_p)| = \frac{|GL_n(\mathbb{F}_p)|}{p-1}$.*

When $n = 2$, this yields $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = p(p+1)(p-1)^2$. Let's consider only $\mathrm{GL}_2(\mathbb{F}_p)$ for the moment, for which we highlight a few important subgroups.

Definition 4.30.

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{F}_p,\ ac \in \mathbb{F}_p^\times \right\},$$
$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\},$$
$$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{F}_p,\ ab \in \mathbb{F}_p^\times \right\}.$$

Lemma 4.31. *For the subgroups as above, $N \trianglelefteq U$, $U = TN$, and $T \cap N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hence $U \cong N \rtimes T$.*

4.1. **Exercises.**

Exercise 4.32. (August 2022 Problem 3) Let L/F be a field extension and let K_1 and K_2 be two distinct subfields with $F \subseteq K_1, K_2 \subseteq L$ such that $L = K_1K_2$ and $[K_1 : F] = [K_2 : F] = 3$. Show that $[L : F]$ is either 6 or 9, and give examples to show that both values can occur.

Proof. Let $\alpha_1, \alpha_2, \alpha_3$ be a F basis for K_1. Then $[K_1K_2 : K_2] \leq 3$. By K_1 and K_2 distinct, we know $[K_1K_2 : K_2] > 1$, hence $[L : F] = [L : K_2] \cdot [K_2 : F] = 2 \cdot 3$ or $3 \cdot 3$.

For example, we notice $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$, for ω the third root of unity, where $[\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\omega\sqrt[3]{2}) \cdot \mathbb{Q}(\sqrt[3]{2})$. On the other hand, consider $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}] = 9$, where $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$, and $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2}) \cdot \mathbb{Q}(\sqrt[3]{3})$.

□

Exercise 4.33. (August 2021 Problem 4) Fix a prime number p. Describe a p-Sylow subgroup in each of the following groups:

(1) $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

(2) $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$

Proof. (1) Recall that $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p) = p(p^2-1)(p-1)$. Any p-Sylow subgroup therefore has order p, and one example includes $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\}$, $|N| = p$.

(2) The key object here is the short exact sequence

$$1 \to \mathrm{Ker}(r) \to \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{r} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1,$$

where r is given by reduction modulo p. Since $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ maps into $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ via $1 \mapsto p$, the SES is right split. Note that $\mathrm{Ker}(r)$ contains matrices of the form

$$\begin{pmatrix} 1+ap & bp \\ cp & 1+dp \end{pmatrix}$$

for $a, b, c, d \in \{0, 1, \ldots, p-1\}$, hence $|\mathrm{Ker}(r)| = p^4$. It follows that $|\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})| = p^4 \cdot |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = p^p 4(\mathrm{p}^2 - 1)(p^2 - p) = p^5(p^2-1)(p-1)$, so we might take this p-Sylow subgroup.

□

Exercise 4.34. (January 2021 Problem 3) Let K be a nontrivial extension field of $\mathbb{C}$. Show that K does not have a countable basis as a $\mathbb{C}$-vector space.

Proof. Fix $t \in K \setminus \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, t generates the purely transcendental extension $\mathbb{C}(t)$. We notice, then, that elements of the form $\frac{1}{t-\alpha}$, for $\alpha \in \mathbb{R}$, generate an uncountably infinite family. We aim to show they are linearly independent. Suppose for some nonzero $a_1, \ldots, a_n \in \mathbb{C}$, $\sum_{i=1}^n a_i \cdot \frac{1}{t-\alpha_i} = 0$. This would imply that

$$\sum_{i=1}^{n} a_i \cdot \prod_{j \neq i} (t - \alpha_j) = 0,$$

contradicting t transcendental over $\mathbb{C}$. □

Exercise 4.35. (August 2021 Problem 5) Let L/K be an algebraic extension of fields of characteristic zero. Assume that for every $\alpha \in L$, the extension $K(\alpha)/K$ has degree at most 2. Show that $[L : K] \leq 2$.

Proof. If $[L : K] > 2$, then we can find elements $\alpha \notin K$ and $\beta \notin K(\alpha)$ such that $[K(\alpha, \beta) : K] > 2$. By the primitive element theorem, for $K(\alpha, \beta)/K$ a finite, separable field extension, there exists $\gamma \in K(\alpha, \beta) \subseteq L$ such that $K(\gamma) = K(\alpha, \beta)$, contradicting that $[K(\alpha) : K] \leq 2$ for all $\alpha \in L$. □

Exercise 4.36. (January 2022 Problem 2) Let K/F be a field extension of degree n. Show that there is a subgroup of $\mathrm{GL}_n(F)$ which is isomorphic to $K^\times$.

Proof. Fix a basis $e_1, \ldots, e_n$ for K over F. For each $\alpha \in K$, multiplication by α is an F-linear map from K to K, which can be represented as the matrix $\alpha \cdot \mathrm{Id}_n$ in the basis $e_1, \ldots, e_n$. Since $\alpha, \beta \in K^\times$ satisfy $(\alpha \cdot I_n) \cdot (\beta \cdot I_n) = \alpha\beta \cdot I_n$, and since $(\alpha \cdot I_n)(k) = k$ for

al $k \in K$ if and only if α is the identity in $K^\times$, it follows that $K^\times$ is isomorphic to the subgroup consisting of matrices of the form $\alpha \cdot I_n$ for $\alpha \in K^\times$. □

5. Galois Theory

Galois theory finds its genesis and motivation in algebraic number theory, in particular the study of polynomial roots. It distills field theoretic problems such as solvability by radicals down to group theory, rendering them amenable classical machinery.

Theorem 5.1. *(Galois' Theorem) A field extension $E/\mathbb{Q}$ contains only elements expressible by radicals if and only if Gal$(E/\mathbb{Q})$ is solvable.*

Corollary 5.2. *A polynomial $f(X)$ is solvable by radicals if and only if it has a solvable Galois group.*

Broadly, the Galois group encodes how the roots of a polynomial may be permuted without detection by the polynomial. Concretely, the Galois group $\text{Gal}_{\mathbb{Q}}(f)$ of a polynomial f with n roots is a subgroup of S_n.

We recall a few equivalent conditions of E/F Galois:

Theorem 5.3. *A finite extension E/F is a Galois field extension if one of the following hold:*

- *E/F is a normal and separable extension,*
- *E is the splitting field of a separable polynomial with coefficients in F,*
- *$|Aut(E/F)| = [E : F]$,*
- *Every irreducible polynomial in $F[X]$ with at least one root in E splits over E and is separable,*
- *$|Aut(E/F)| \geq [E : F]$.*

Question 5.4. For which f containing n roots is $\text{Gal}_{\mathbb{Q}}(f) = S_n$?

We present a family of Galois groups which coincide with the symmetric group.

Theorem 5.5. *Let p be a prime, and $G \leq S_p$ such that G acts transitively on $\{1, \ldots, p\}$, and G contains a transposition (ij). Then $G = S_p$.*

Proof. By the orbit-stabilizer theorem, $|G| = p \cdot |\text{Stab}(\{1, \ldots, p\})|$, hence G contains an element σ of order p by Cayley's theorem. Without loss of generality, $\sigma = (12 \cdots p)$, and let the transposition be (12). Then any transposition (ij) may be written as follows:

$$(ij) = ((12)\sigma)^{j-i-1}(\sigma^{-1}(12))^{j-1}\sigma^{i-1}.$$

□

Corollary 5.6. *Let p be a prime. If $f \in \mathbb{Q}[X]$ is irreducible, deg$(f) = p$, and f has exactly $p - 2$ real roots, then if E is its splitting field, Gal$(E/F) = S_p$.*

Example 5.7. For p a prime and ξ the pth root of unity, $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Theorem 5.8. *(Fundamental Theorem of Galois Theory) Let E/F be a finite Galois extension. There is an inclusion-reversing bijection between subgroups $H \leq G := Gal(E/F)$ and intermediate fields $F \leq K \leq E$. For K corresponding to H:*

(1) E/K is always normal (hence Galois)
(2) K/F is normal iff $H \trianglelefteq G$
(3) $[K : F] = [G : H]$, and $[E : K] = |H|$.

5.1. **Exercises.**

Exercise 5.9. (January 2024 Problem 5) Prove that $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is a Galois field extension of $\mathbb{Q}$, and compute its Galois group.

Proof. First, observe that $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is the splitting field of the separable polynomial $f(X) = (X^2-2)^2 - 2 = X^4 - 4X^2 + 2$ over $\mathbb{Q}$. The polynomial f has roots $\pm\alpha, \pm\beta$ where $\alpha = \sqrt{2+\sqrt{2}},\ \beta = \sqrt{2-\sqrt{2}}$, and $\alpha\beta = \sqrt{2}$ hence $\beta = \frac{\alpha^2-2}{\alpha} \in \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ as well. So $\left|\text{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)/\mathbb{Q}\right)\right| = 4$, and we claim it is $\mathbb{Z}/4\mathbb{Z}$. It suffices to demonstrate an element $\sigma \in \text{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)/\mathbb{Q}\right)$ of order 4. Consider the automorphism σ given by $\alpha \mapsto \beta$, then $\beta \mapsto \frac{\beta^2-2}{\beta}$ In particular, $\sigma^2(\alpha) = \sigma(\beta) = -\frac{\sqrt{2}}{\beta} = -\alpha \neq \alpha$. □

Exercise 5.10. (August 2024 Problem 4) Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $E = F(\alpha)$ for $\alpha = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}$. You may use without proof that $[F : \mathbb{Q}] = 4$.

(1) Prove that $[E : F] = 2$, and that $E/\mathbb{Q}$ is a degree-8 extension.
(2) Prove that E is Galois over $\mathbb{Q}$ and $\text{Gal}(E/\mathbb{Q})$ has two non-commuting elements of order 4.

Proof. (1) The element α solves the polynomial $X^2 - (\sqrt{2}+2)(\sqrt{3}+3) \in F[X]$, hence $[E : F] \leq 2$. Since $\alpha \notin F$, $[E : F] = 2$. Therefore, $[E : \mathbb{Q}] = [E : F] \cdot [F : \mathbb{Q}] = 8$ by the tower law.

(2) We note that the roots of m_α as written above are given by

$$\begin{array}{ll} r_1 = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)} & -r_1 = -\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)} \\ r_2 = \sqrt{(-\sqrt{2}+2)(\sqrt{3}+3)} & -r_2 = -\sqrt{(-\sqrt{2}+2)(\sqrt{3}+3)} \\ r_3 = \sqrt{(\sqrt{2}+2)(-\sqrt{3}+3)} & -r_3 = -\sqrt{(\sqrt{2}+2)(-\sqrt{3}+3)} \\ r_4 = \sqrt{(-\sqrt{2}+2)(-\sqrt{3}+3)} & -r_4 - \sqrt{(-\sqrt{2}+2)(-\sqrt{3}+3)} \end{array}$$

.

Now consider the automorphism $\sigma : r_1 \mapsto -r_2$ and $\tau : r_1 \mapsto -r_3$. Then notice

$$\sigma^4 : r_1 \mapsto -r_2 \mapsto -r_1 \mapsto r_2 \mapsto r_1,$$

and

$$\tau^4 : r_1 \mapsto -r_3 \mapsto -r_1 \mapsto r_3 \mapsto r_1.$$

Moreover, $\sigma \circ \tau : r_1 \mapsto -r_3 \mapsto -r_3$, while $\tau \circ \sigma : r_1 \mapsto -r_2 \mapsto -r_2$.

□

Exercise 5.11. (August 2021 Problem 1) Let K be a subfield of $\mathbb{C}$ such that K is a Galois extension of $\mathbb{Q}$ with $[K : \mathbb{Q}]$ odd. Show that $K \subset \mathbb{R}$.

Proof. The key observation is that for complex conjugation σ, the order of $\sigma \leq 2$ but must divide $\text{Gal}(K/\mathbb{Q}) = [K : \mathbb{Q}]$, hence it is 1 and so $\sigma = \text{Id}$, i.e. σ acts trivially on K. □

Exercise 5.12. (August 2020 Problem 5) Let p be a prime number and let K be a field of characteristic p. Let $a, b \in K$, $a \neq 0$, and let L be the splitting field of $X^p - aX - b$ over K. Show that L/K is Galois and that its Galois group is solvable.

Proof. Notice first that $f'(X) = a \neq 0$, hence f is separable and so L/K is Galois. Let u and w be distinct roots of f. Then $f(u) - f(w) = (u - w)^p - a(u - w) = (u - w) \cdot ((u - w)^{p-1} - a) = 0$ implies $\delta := u - w$ is such that $\delta^{p-1} = a$. This means that $w + m\delta$ for $m = 0, 1, 2 \ldots, p - 1$ comprise all roots of f, since $m^p \equiv m$.

We aim to decompose $\text{Gal}(L/K)$ into abelian pieces, by which it will become solvable. Consider the following short exact sequence:

$$e \longrightarrow \text{Gal}(L/K(\delta)) \longrightarrow \text{Gal}(L/K) \longrightarrow \text{Gal}(K(\delta)/K) \longrightarrow e$$

We note that $K(\delta)/K$ is the splitting field of the polynomial $X^{p-1} - a \in K[X]$, whose roots are precisely $\delta, 2\delta, \ldots, (p-1)\delta$, hence $K(\delta)/K$ is normal. Both $L/K(\delta)$ and $K(\delta)/K$ are Galois by the Galois correspondence, as $K \leq K(\delta) \leq L$. Since K contains $\mathbb{F}_p^\times$ and therefore all $(p-1)$st roots of unity, $\text{Gal}(K(\delta)/K) \leq \mathbb{Z}/(p-1)\mathbb{Z}$, hence it is abelian. Similarly $\text{Gal}(L/K(\delta))$ consists of all automorphisms of L fixing δ, so any $\sigma : w + m\delta \mapsto w + (m + \ell)\delta$ for all $m = 0, 1, 2 \ldots, p - 1$. Therefore, $\text{Gal}(L/K(\delta))$ is a subgroup of $\mathbb{Z}/p\mathbb{Z}$ and hence also abelian. Since $\text{Gal}(K(\delta)/K) \cong \text{Gal}(L/K)/\text{Gal}(L/K(\delta))$ and $\text{Gal}(L/K(\delta)$ are both abelian, i.e. solvable, $\text{Gal}(L/K)$ is solvable.

□

Exercise 5.13. (January 2021 Problem 4) Let p and q be distinct primes and let $K/\mathbb{Q}$ be a Galois field extension of degree $p^a q^b$ with $a, b \geq 1$. Show that there are linearly disjoint proper subfields E and F of K such that K is the compositum EF.

Proof. We know that $|\text{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = p^a q^b$, which means we are guaranteed p- and q-Sylow subgroups. Let H be a p-Sylow and G be a q-Sylow. Then $H \cap G = \{e\}$ since their orders are distinct prime powers. By the fundamental theorem of Galois theory, H and G correspond to proper subfields E and F of K, respectively. It happens that $K = EF$ because $H \cap G$ is trivial. □

Exercise 5.14. (January 2021 Problem 5) Let n be a positive integer, let $K = \mathbb{Q}(x_1, x_2, \ldots, x_n)$, and let $F \subseteq K$ be the subfield of functions that are symmetric in $x_1, x_2, \ldots, x_n$. Set

$$p = x_1^2 x_2 + x_2^2 x_3 + \cdots + x_{n-1}^2 x_n + x_n^2 x_1$$

$$q = x_1x_2^2 + x_2x_3^2 + \cdots + x_{n-1}x_n^2 + x_nx_1^2.$$

Show that q belongs to $F(p)$, the subfield of K generated by p.

Proof. First, we note that F is the fixed field of the action of S_n on K. Observe that p is fixed by $\langle(12\cdots n)\rangle \leq S_n$, and q, too. The stabilizer of $F(p)$ in S_n is exactly $\langle(12\cdots n)\rangle$ by the fundamental theorem of Galois theory, and the fact that $F(p)$ is the smallest field containing F and p. Since $\langle(12\cdots)\rangle$ is contained in the stabilizer of q, it must happen that $F(q) \subseteq F(p)$, i.e. q belongs to $F(p)$. □

Exercise 5.15. (May 2021 Problem 3) Let n be a positive integer. Show that $\mathbb{C}(t)/\mathbb{R}(t^n)$ is a Galois extension, and determine its Galois group. Here t is an indeterminate and $\mathbb{C}(t)$ is the rational function field.

Proof. Denote ξ the nth root of unity. We claim that $\sigma : t \mapsto \xi t$ and complex conjugation $c : z \mapsto \overline{z}$ generate $\mathrm{Gal}(\mathbb{C}(t)/\mathbb{R}(t^n))$. These generate a group isomorphic to the dihedral group D_{2n}, since $\sigma^n = c^2 = \sigma c \sigma^{-1} c = e$. Notice that σ and c are automorphisms of $\mathbb{C}(t)$ which fix $\mathbb{R}(t^n)$, and $[\mathbb{C}(t) : \mathbb{R}(t^n)] = [\mathbb{C}(t) : \mathbb{R}(t)] \cdot [\mathbb{R}(t) : \mathbb{R}(t^n)] = 2n$, so $\langle \sigma, c\rangle$ generates all symmetries and is Galois by the fifth characterization in Theorem 5.3. □

Exercise 5.16. (January 2022 Problem 4) Let $K/\mathbb{Q}$ be a Galois extension with degree 9 and at least 2 distinct subfields $\mathbb{Q} \subsetneq L_1, L_2 \subsetneq K$. What is $\mathrm{Gal}(K/\mathbb{Q})$?

Proof. The only two groups of order 9 are $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Since $\mathbb{Z}/9\mathbb{Z}$ contains only one nontrivial proper subgroup, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ by the Galois correspondence. □