Nine Weeks of Groups, Fields & Galois Theory

April 14, 2024

These are my solutions to weekly exercises for the course on groups, fields & Galois theory, taken during Jan-May, 2024. Most of the problems were from Dummit & Foote and the sentence "*Proof of Question XY.Z, AB*" refers to the Section XY.Z of Dummit Foote, Exercise AB. Some questions, however, are from outside sources, and thus the first line clearly states what we wish to prove.

Contents

1 Week 1 : Basic group theory

Proof of Question 1.6, 4. Suppose there is group isomorphism $\varphi : \mathbb{C} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$. Then $a = \varphi(i)$ is a real number such that

$$a^2 = \varphi(i^2) = \varphi(-1) \tag{$*$}$$

We claim that $\varphi(-1) = -1$. Indeed, as φ is a multiplicative group isomorphism, therefore $\varphi(1) = 1 = \varphi((-1)^2) = \varphi(-1)^2$. It follows that $\varphi(-1) = \pm 1$, but since φ is injective and $\varphi(1) = 1$, therefore $\varphi(-1) = -1$, as required.

It follows from $(*)$ that $a^2 = -1$ where $a \in \mathbb{R}$, a contradiction. □

Proof of Question 1.6, 25. a) Let $p = (x_0, y_0)$ be a point in $\mathbb{R}^2$ and let

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Represent $p = (r\cos\theta_0, r\sin\theta_0)$ for some $\theta_0 \in (0, 2\pi]$ and $r > 0$. We wish to show that $Ap = (r\cos(\theta + \theta_0), r\sin(\theta + \theta_0))$. Indeed, we see that

$$\begin{aligned} Ap &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} r\cos\theta_0 \\ r\sin\theta_0 \end{bmatrix} = \begin{bmatrix} r\cos\theta\cos\theta_0 - r\sin\theta\sin\theta_0 \\ r\sin\theta\cos\theta_0 + r\cos\theta\sin\theta_0 \end{bmatrix} \\ &= \begin{bmatrix} r\cos(\theta + \theta_0) \\ r\sin(\theta + \theta_0) \end{bmatrix}, \end{aligned}$$

as required.

b) We know that elements of D_{2n} are of form

$$D_{2n} = \left\{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}.$$

Hence, it suffices to define the map $\varphi : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ on elements r^k and sr^k so that it satisfies

$$\begin{aligned} \varphi(r^k) &= \varphi(r)^k \\ \varphi(sr^k) &= \varphi(s)\varphi(r^k) \end{aligned} \tag{1.1}$$

for all $0 \le k \le n-1$.

We now construct $\varphi : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$. For $k = 0$, we define $\varphi(e) = I_2$. Fix $0 < k \le n-1$. We define

$$\varphi(r^k) := A^k$$

where

$$A := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Finally for sr^k, we define

$$\varphi(sr^k) := BA^k$$

where

$$B := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The fact that φ satisfies Eqns 1.1 is immediate now.

c) We wish to show that φ above is injective. We follow the notations of part b). Suppose first that $\mathrm{Ker}\,(\varphi)$ contains r^k for $0 < k \leq n-1$. Then $A^k = 0$. Doing the multiplications, we obtain

$$0 = A^k = \begin{bmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{bmatrix}.$$

It follows that $\cos(k\theta) = \sin(k\theta) = 0$. Hence

$$\cos(2\pi k/n) = \sin(2\pi k/n) = 0$$

for $0 < k \leq n-1$. As $\sin(2\pi k/n) = 0$ implies $2k/n$ is an integer, therefore $k = 0$, a contradiction to the assumption that $0 < k \leq n-1$. Consequently, $r^k \notin \mathrm{Ker}\,(\varphi)$.

Suppose $sr^k \in \mathrm{Ker}\,(\varphi)$ for $0 \leq k \leq n-1$. If $k = 0$, then $B = 0$, which it is not, so $s \notin \mathrm{Ker}\,(\varphi)$. Else if $0 < k \leq n-1$, then

$$0 = \varphi(sr^k) = BA^k = \begin{bmatrix} \sin(k\theta) & \cos(k\theta) \\ \cos(k\theta) & -\sin(k\theta) \end{bmatrix}.$$

We thus again have

$$\cos(2\pi k/n) = \sin(2\pi k/n) = 0$$

for $0 < k \leq n-1$, which, as shown above, gives a contradiction. Thus, no non-identity element is in the kernel of φ, hence showing φ is injective. □

Proof of Question 2.2, 7. a) Suppose $Z(D_{2n}) \neq e$. Suppose $r^k \in Z(D_{2n})$ where $0 < k \leq n-1$. Then, $r^k s = sr^k$. As $rs = sr^{-1}$ and $r^{-1} = r^{n-1}$, it follows that

$$r^k s = sr^{-k} = sr^{n-k}.$$

Thus, $sr^{n-k} = sr^k$ from which it follows that $r^{n-k} = r^k$, that is $n = 2k$, a contradiction to the assumption that n is odd.

Now suppose $sr^k \in Z(D_{2n})$ where $0 \leq k \leq n-1$. If $k = 0$, then $sr^{n-1} = r^{n-1}s$. As $sr^{n-1} = rs$, therefore $r^{n-1} = r$ and thus $r^2 = 0$. Since $n \geq 3$ and r is of order n, therefore we have a contradiction. Finally, suppose $0 < k \leq n-1$. Then, $(sr^k)s = s(sr^k)$. Since $sr^k = r^{-k}s = r^{n-k}s$, therefore we get $r^{n-k}ss = sr^{n-k}s = r^k ss$. It follows that $n = 2k$, a contradiction to the fact that n is odd.

Hence we have a contradiction if any non-identity element lies in center, hence the center

is trivial.

b) Let $n = 2k$. If $r^l \in Z(D_{2n})$ for $0 < l \leq n-1$, then $r^l s = sr^l$. As $r^l s = sr^{-l}$, it follows that $r^{2l} = e$. Since $0 < l \leq n-1$ and the order of r is n, we deduce that $2l = n = 2k$ and thus $l = k$. Consequently, the only elements of the form r^l in the center are r^k.

We now show that elements of the form $sr^l \notin Z(D_{2n})$ for all $0 \leq l \leq n-1$. Observe that in proof of a) above, we showed that $s \notin Z(D_{2n})$ by only using the fact that $n \geq 3$, therefore we conclude that $s \notin Z(D_{2n})$. So we may assume $0 < l \leq n-1$. We thus have that $(sr^l)r^{-l} = r^{-l}(sr^l)$ as $sr^l \in Z(D_{2n})$. We may write $r^{-l}sr^l = sr^l r^l$, from which it follows that $sr^l r^{-l} = sr^l r^l$. It follows that $e = r^{2l}$. As $0 < l \leq n-1$ and order of r is n, therefore $2l = n = 2k$ and thus $l = k$. It would thus suffice now to show that sr^k cannot be in the center. Indeed, if $sr^k \in Z(D_{2n})$ then we have that $(sr^k)sr = sr(sr^k)$. It follows that we have $ssr^{-k}r = ssr^{-1}r^k$, from which upon cancelling s, we obtain $r^{-k+1} = r^{k-1}$. Thus, $r^{-k+1-k+1} = e$. Hence $r^{2(k-1)} = e$. It follows that $2(k-1) \mid 2k$. Hence, $k-1 \mid k$, which is not possible as $k \geq 2$ since $n = 2k \geq 3$. This proves that $sr^l \notin Z(D_{2n})$ for any $0 \leq l \leq n-1$ and hence center only contains 1 and r^k, as required. □

Proof of Question 3.1, 36. Let G be a group and let $Z = Z(G)$ be the center. We wish to show that if G/Z is cyclic then $Z = G$, that is G is abelian. Let $G/Z = \{Z, gZ, g^2Z, \ldots, g^{n-1}Z\}$ for some $g \in G$. Consequently, for every $x \in G$, there exists $z \in Z$ such that $x = g^k z$.

Now pick $x, y \in G$. Then $x = g^k z_1$ and $y = g^l z_2$ for $0 \leq k, l \leq n-1$ and $z_1, z_2 \in Z$. Consequently,

$$xy = g^k z_1 g^l z_2 = g^k g^l z_2 z_1 = g^l g^k z_2 z_1 = g^l z_2 g^k z_1 = yx,$$

as needed. □

Proof of Questiuon 3.2, 18. Let G be a finite group, $H \leq G$ and $N \trianglelefteq G$ be a normal subgroup. Suppose $\gcd(|G/N|, |H|) = 1$. We wish to show that $H \leq N$. Suppose there exists $h \in H$ such that $h \notin N$. Then $hN \in G/N$ is a non-zero element. Consider the cyclic subgroup of G/N generated by hN as

$$\langle hN \rangle = \{N, hN, h^2N, \ldots, h^{k-1}N\}$$

of size k. In particular the order of hN in G/N is k. Thus,

$$k \mid |G/N| \tag{$*$}$$

Also consider the subgroup $\langle h \rangle \leq G$ generated by h. We claim that

$$k \mid |h| \tag{$**$}$$

Indeed, if $h^l = e$ for some $l \in \mathbb{N}$, then $h^l \in N$, that is $h^l N = (hN)^l = N$. It follows that $k|l$ and thus that $k \mid |h|$, as needed.

As $|h| \mid |H|$ by Lagrange's theorem, therefore from $(*)$ and $(**)$, it follows that $k \mid |H|$ and $k \mid |G/N|$. From properties of gcd, it further follows that

$$k \mid \gcd(|G/N|, |H|).$$

As the above gcd is 1, we conclude that $k = 1$. We thus deduce that $\langle hN \rangle = \{N\}$, showing that $hN = N$ and thus $h \in N$, as required. $\square$

Proof of Question 3.3, 7. Let $M, N \trianglelefteq G$ such that $G = MN$. We wish to show that $G/M \cap N \cong G/M \times G/N$. This is a generalization of Chinese remainder theorem for groups. Consider the map

$$\begin{aligned} \varphi : G &\longrightarrow G/M \times G/N \\ g &\longmapsto (gM, gN). \end{aligned}$$

Observe that since $g = mn$ for $m \in M$ and $n \in N$, therefore

$$\varphi(g) = (gM, gN) = (nM, mN).$$

We claim that φ is a surjective group homomorphism whose kernel is $M \cap N$.

We first show that φ is a group homomorphism. Indeed, this is immediate as for any $g, h \in G$, we can write

$$\varphi(gh) = (ghM, ghN) = (gM, gN)(hM, hN) = \varphi(g)\varphi(h).$$

We now wish to show that φ is surjective. Indeed, for any $(gM, hN) \in G/M \times G/N$, we may write $g = m_1 n_1$ and $h = m_2 n_2$ for $m_i \in M$ and $n_i \in N$. It follows that $(gM, hN) = (n_1 M, m_2 N)$. Consequently the element $k = m_2 n_1 \in MN = G$ is such that

$$\varphi(k) = (kM, kN) = (m_2 n_1 M, m_2 n_1 N).$$

Since M, N are normal, therefore $m_2 n_1 M = m_2 M n_1 = M n_1 = n_1 M$. Similarly we deduce that $m_2 n_1 N = m_2 N$. Hence

$$\varphi(k) = (n_1 M, m_2 N) = (gM, hN)$$

as needed. This shows that φ is a surjective homomorphism. We now show that $\mathrm{Ker}\,(\varphi) = M \cap N$. Indeed, we see that $g \in \mathrm{Ker}\,(\varphi)$ iff $(gM, gN) = (M, N)$ iff $gM = M$ and $gN = N$ iff $g \in M$ and $g \in N$ iff $g \in M \cap N$, as needed.

This shows that φ is a surjective homomorphism whose kernel is $M \cap N$. By first isomorphism theorem, it follows that

$$G/M \cap N \cong G/M \times G/N,$$

as needed. $\square$

2 Week 2 : Symmetry groups, simple groups, Sylow's theorems

Proof of Question 3.5, 3. Let $X = \{(i\ i+1) \mid 1 \leq i \leq n-1\} \subseteq S_n$. We wish to show that X is a generating set of S_n. As any $\sigma \in S_n$ can be written as a product of disjoint cycles, therefore it suffices to show that any k-cycle for $1 \leq k \leq n$ is generated by elements

of X.

Pick any k-cycle $\sigma = (i_1\ i_2\ \dots\ i_k)$. We may write it as

$$\sigma = (i_1\ i_k) \cdot (i_1\ i_{k-1}) \cdot \dots \cdot (i_1\ i_3)(i_1\ i_2).$$

We now reduce to writing an $(i_1\ i_k)$ as a product of elements of X for any $1 \leq k \leq n$. Indeed, we have

$$(i_1\ i_k) = (i_2\ i_1) \cdot (i_3\ i_2) \cdot \dots (i_{k-1}\ i_{k-2}) \cdot (i_{k-1}\ i_k) \cdot (i_{k-2}\ i_{k-1}) \cdot \dots \cdot (i_2\ i_3) \cdot (i_1\ i_2)$$

where each element in the above factorization is in X, as required. □

Proof of Question 3.5, 12. We wish to show that there exists an injective group homomorphism $\varphi : S_{n-2} \to A_n$. Consider the following map

$$\begin{aligned} \varphi : S_{n-2} &\longrightarrow A_n \\ \sigma &\longmapsto \begin{cases} \sigma & \text{if } \sigma \in A_{n-2} \\ \sigma(n-1\ n) & \text{else.} \end{cases} \end{aligned}$$

We first claim that φ is a group homomorphism. Indeed, pick any $\sigma, \tau \in S_{n-2}$. If $\sigma\tau \in A_{n-2}$, then $\sigma\tau$ is a product of evenly many transpositions. Writing σ and τ individually as product of transpositions, we see that $\sigma\tau$ is a product of evenly many transpositions if and only if any one of the following happens:

1. both σ and τ can be written as evenly many product of transpositions,
2. both σ and τ can be written as odd many product of transpositions.

In case 1, we have $\sigma, \tau \in A_{n-2}$, so that $\varphi(\sigma) = \sigma$ and $\varphi(\tau) = \tau$. It follows that $\varphi(\sigma\tau) = \sigma\tau = \varphi(\sigma)\varphi(\tau)$, as needed. Whereas in case 2, we have $\sigma, \tau \notin A_{n-2}$. It follows that $\varphi(\sigma\tau) = \sigma\tau = \sigma\tau(n-1\ n)(n-1\ n) = \sigma(n-1\ n)\tau(n-1\ n) = \varphi(\sigma)\varphi(\tau)$ where $\tau(n-1\ n) = (n-1\ n)\tau$ because they are disjoint permutations.

Now suppose $\sigma\tau \notin A_{n-2}$. This is possible if and only if $\sigma \in A_{n-2}$ and $\tau \notin A_{n-2}$. It follows that

$$\varphi(\sigma\tau) = \sigma\tau(n-1\ n) = \varphi(\sigma)\varphi(\tau),$$

as needed. This shows that φ is a group homomorphism.

We now show φ is injective. Indeed, if $\varphi(\sigma) = ()$, then either $\sigma = ()$ or $\sigma(n-1\ n) = ()$. In the former, we are immediately done. In the latter, we may multiply both sides on the right by $(n-1\ n)$ to obtain that $\sigma = (n-1\ n)$, which is not possible as σ is a bijection of $\{1, 2, \dots, n-2\}$. This completes the proof. □

Proof of Question 4.1, 8. a) We wish to show that the transitive action of S_n on $A = \{1, 2, \dots, n\}$ is doubly transitive. Indeed, pick any $k \in A$ so that $1 \leq k \leq n$. Denote $G_k = \mathrm{Stab}_{S_n}(k) = \{\sigma \in S_n \mid \sigma(k) = k\}$. We wish to show that G_k acts transitively on $A \setminus \{k\} = \{1, \dots, \hat{k}, \dots, n\}$. We may assume that $n > 2$ as for $n = 2$, the claim is immediate. Pick any two elements $i, j \in A \setminus \{k\}$, which we can as $n > 2$. We wish to show that there exists $\sigma \in G_k$ such that $\sigma(i) = j$. Indeed, we have $\sigma = (i\ j) \in S_n$ is such that $\sigma(k) = k$, so that $\sigma \in G_k$. Further we have $\sigma(i) = j$, as needed.

b) Let G be a group and A be a G-set. We wish to show that if the action of G on A is doubly transitive, then it is primitive. Let $B \subseteq A$ be a block, that is, for all $\sigma \in G$, $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. We wish to show that if $|B| > 1$, then $B = A$. Indeed, pick any $a \in A$. We wish to show that $a \in B$. Let $b \in B$ and $G_b = \mathrm{Stab}_G(b) = \{\sigma \in G \mid \sigma(b) = b\}$.

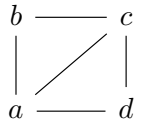
We now claim that for any $\sigma \in G_b$, we have $\sigma(B) = B$. Indeed, as $\sigma(b) = b$ for any $\sigma \in G_b$, it follows that $\sigma(B) \cap B \neq \emptyset$. Since B is a block, therefore $\sigma(B) = B$, as required.

We now complete the proof. As G acts doubly transitive on A, therefore G_b acts transitively on $A \setminus \{b\}$. As $|B| > 1$, therefore there exists $b' \in B \setminus \{b\}$ and thus a $\sigma \in G_b$ such that $\sigma(a) = b' \in B$. Since $G_b \leq G$ is a subgroup, therefore $\sigma^{-1} \in G_b$ as well. By above claim, $\sigma^{-1}(B) = B$. Consequently,

$$a = \sigma^{-1}(\sigma(a)) = \sigma^{-1}(b') \in \sigma^{-1}(B) = B,$$

as needed. This completes the proof.

c) We wish to show that the action of D_8 on square



is not doubly transitive. Indeed if so, then by part b) it has to be primitive. Denote r to be rotation by $\pi/2$ CW and s to be the reflection along the diagonal as shown in the diagram. Let us write $D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. We claim that there is a non-trivial block of D_8 on the square. This will give a contradiction to primitivity. Indeed, consider $B = \{b, d\}$. We claim that B is a block. Then,

$$\begin{aligned} r(B) &= \{c, a\} \\ r^2(B) &= \{b, d\} \\ r^3(B) &= \{c, a\} \\ s(B) &= \{b, d\} \\ sr(B) &= \{a, c\} \\ sr^2(B) &= \{b, d\} \\ sr^3(B) &= \{a, c\}. \end{aligned}$$

In all the above, we see that the $\sigma(B) = B$ for $\sigma(B) \cap B = \emptyset$ for all $\sigma \in D_8$. Hence B is indeed a non-trivial block, showing that action of D_8 on square is not primitive. □

Proof of Question 4.2, 4. We wish to find two elements in S_8 which generate a subgroup isomorphic to Q_8. We interpret S_8 as the group of bijections of the set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Consider the left regular representation of Q_8 in S_8 is given by the homomorphism

$$\begin{aligned} \varphi : Q_8 &\longrightarrow S_8 \\ g &\longmapsto m_g \end{aligned}$$

where $m_g : Q_8 \to Q_8$ mapping as $x \mapsto gx$. By Cayley's theorem, or by direct observation, this map is an injective group homomorphism. Consequently, the $G := \mathrm{Im}\,(\varphi) \leq S_8$ is isomorphic to Q_8. As Q_8 is generated by i and j and φ is an isomorphism onto G, it follows that G is generated by $\varphi(i)$ and $\varphi(j)$, which we calculate as below:

$$\varphi(i) = (1\ 3\ 2\ 4)(5\ 7\ 6\ 8)$$
$$\varphi(j) = (1\ 5\ 2\ 6)(3\ 8\ 4\ 7).$$

Hence the above two permuations generate G, as required. □

Proof of Question 4.2, 8. Let G be a group and $H \leq G$ be a subgroup with $[G : H] = n$. We wish to show that there exists a normal subgroup $K \trianglelefteq G$ such that $K \leq H$ and $[G : K] \leq n!$.

Let X denote the set of all left-cosets of H in G, so that $|X| = n$. We see that G acts on X by left multiplication, that is,

$$G \times X \longrightarrow X$$
$$(g, g'H) \longmapsto gg'H.$$

Consequently, we get a representation

$$\varphi : G \longrightarrow \mathrm{Bij}(X)$$
$$g \longmapsto m_g$$

where $m_g : X \to X$ taking $g'H \mapsto gg'H$. Consider the kernel $K = \mathrm{Ker}\,(\varphi)$ which is a normal subgroup of G. We claim that $K \leq H$. Indeed, for any $k \in K$, we have $m_k(gH) = kgH = gH$. Thus $(kg)g^{-1} = k \in H$, as required. This shows that $K \leq H$ is a normal subgroup of G

By first isomorphism theorem, we have an isomorphism $G/K \cong \mathrm{Im}\,(\varphi)$. Thus, we deduce

$$|G/K| = [G : K] = |\mathrm{Im}\,(\varphi)| \leq n!,$$

as required. □

Proof of Question 4.2, 14. Let G be a finite group of composite order n. Suppose for all $k|n$, there exists a subgroup $H \leq G$ such that $|H| = k$. We wish to show that G cannot be simple.

Suppose to the contrary that G is simple. Fix any proper subgroup $H \lneq G$ and let X_H denote the coset space of H in G. Then, we have an action of $G \circlearrowright X_H$ by left multiplication. This induces a homomorphism

$$\varphi_H : G \longrightarrow \mathrm{Bij}(X_H)$$

into the group of bijections of X_H and since $|X_H| = [G : H]$, therefore $\mathrm{Bij}(X_H) \cong S_{[G:H]}$. Now consider the kernel $\mathrm{Ker}\,(\varphi_H) \leq G$. Note that

$$\begin{aligned}\mathrm{Ker}\,(\varphi_H) &= \{g \in G \mid gg'H = g'H\ \forall\ g'H \in X_H\} \\ &\leq H\end{aligned}$$

since $gg'H = g'H$ implies that $gg' \cdot (g')^{-1} = g \in H$. Now since G is simple and $\mathrm{Ker}\,(\varphi_H) \trianglelefteq G$, therefore either $\mathrm{Ker}\,(\varphi_H) = \{e\}$ or G. If $\mathrm{Ker}\,(\varphi_H) = G$, then by above above it follows that

$$G = \mathrm{Ker}\,(\varphi_H) \leq H \leq G$$

so that $H = G$, but our hypothesis that H be a proper subgroup gives a contradiction. Consequently, $\mathrm{Ker}\,(\varphi_H) = \{e\}$ is the only possible case and hence φ_H is injective.

We have thus shown that for any proper subgroup $H \lneq G$, φ_H is injective. Hence, $\mathrm{Im}\,(\varphi_H) \leq S_{[G:H]}$ and thus $|G| \,|[G:H]!$ for all $H \lneq G$. By hypothesis, there is a subgroup H for each $k|n$, hence it follows that

$$n|k! \;\forall\; k|n. \tag{1}$$

Let p be the smallest prime dividing n. Hence, by Eqn (1), it follows that $n|p!$. As for any $1 \leq k < p$, $\gcd(k, n) = 1$ since p is the smallest factor of n other than 1, therefore $n|p!$ implies that $n|p$. Since $p|n$, so it follows that $n = p$, a contradiction to the assumption that n is composite. □

Proof of Question 4.3, 5. Let G be a group and $Z \trianglelefteq G$ be the center. If $[G : Z] = n$, then we wish to show that every conjugacy class has atmost n elements.

Let $G \circlearrowright G$ by conjugacy and $x \in G$. Denote $C(x) = \mathrm{Orb}_G(x)$ to be the orbit of x under this action, that is, the conjugacy class of $x \in G$. As G/Z is a group of order n, therefore it suffices to construct a surjective function $G/Z \to C(x)$. Indeed, consider the following

$$\begin{aligned} \varphi : G/Z &\longrightarrow C(x) \\ gZ &\longmapsto gxg^{-1}. \end{aligned}$$

Indeed, this is well-defined as if $gh^{-1} \in Z$ (i.e. $gZ = hZ$), then $gh^{-1} = z \in Z$ and thus $g = hz$. Consequently,

$$gxg^{-1} = hzx(hz)^{-1} = hzxz^{-1}h^{-1} = hxzz^{-1}h^{-1} = hxh^{-1},$$

as needed. Now we claim that φ is surjective. Indeed, this is immediate as for any $gxg^{-1} \in C(x)$, we have $gZ \in G/Z$ which maps to gxg^{-1} under φ. □

Proof of Question 4.3, 35. Let p be a prime and $n \in \mathbb{N}$. We wish to find the size of the following set

$$X = \begin{Bmatrix} \text{Conjugacy classes } C(x) \subseteq S_n \\ \text{where } x \in S_n \text{ is of order } p \end{Bmatrix}.$$

We know that if $x \in S_n$, then conjugacy class of x has the following interpretation:

$$C(x) = \begin{Bmatrix} \text{All those permutations in } S_n \text{ which} \\ \text{have the same cycle type as that of} \\ x \in S_n \end{Bmatrix}.$$

It follows that $C(x)$ is uniquely determined by the cycle type of x, so that we are reduced to counting the following

$$|X| = \#\text{ Possible cycle types for elements } x \in S_n \text{ of order } p. \tag{2}$$

Pick an element $x \in S_n$ of order p and consider its disjoint cycle decomposition (where we do not write cycles of length 1):

$$x = x_1 \cdot \cdots \cdot x_r$$

where x_i are disjoint cycles. Since $|x| = \text{lcm}(|x_1|, \ldots, \text{lcm}(x_r)) = p$, therefore $|x_i| \,|p$ for each $i = 1, \ldots, r$. It follows that $|x_i| = 1$ or p. Since $|x_i| > 1$ by assumption, therefore for each $i = 1, \ldots, r$ we have $|x_i| = p$. As x_i are cycles, it follows that each x_i is a cycle of length p.

By Eqn (2), we reduce to counting

$$|X| = \#\text{ Possible non-trivial cycle types only consisting of cycles of length 1 or } p.$$

Since cycle types corresponds to partitions of n, we further reduce to counting

$$|X| = \#\text{ Non-trivial partitions of } n \text{ consisting only of 1 and } p. \tag{3}$$

Now we may partition n non-trivially using 1 and p as follows:

$$n = \underbrace{p + \cdots + p}_{k\text{-times}} + \underbrace{1 + \cdots + 1}_{n-kp\text{-times}}$$

where $1 \leq k \leq N$ where N is the largest positive integer such that

$$Np \leq n.$$

Hence we see from Eqn (3) that

$$|X| = N$$

and by definition of N, we see that

$$N = \left\lfloor \frac{n}{p} \right\rfloor.$$

It follows that

$$|X| = \left\lfloor \frac{n}{p} \right\rfloor,$$

as required. □

Proof of Question 4.5, 16. Let G be a finite group of order pqr where $p < q < r$ are primes. We wish to show that G has a normal Sylow subgroup of order either p, q or r. This shows that any group of order pqr where p, q, r are distinct primes is not simple.

Let n_p, n_q and n_r be the number of Sylow subgroups of order p, q and r in G. Assume to the contrary that $n_p, n_q, n_r > 1$. By Sylow's 3rd theorem we have the following list of relations:

1. $n_p = 1 \mod p$ and $n_p | qr$ thus $n_p = q, r, qr$,
2. $n_q = 1 \mod q$ and $n_q | pr$ thus $n_q = p, r, pr$,
3. $n_r = 1 \mod r$ and $n_r | pq$ thus $n_r = p, q, pq$.

As $p < q < r$, so in item 3, since $n_r = 1 \mod r$, so $n_r \neq p, q$. It follows that $n_r = pq$. Similarly, from item 2 and $p < q$, we deduce that $n_q \neq p$. Thus, $n_q = r, pr$. As p is smallest in p, q, r, therefore $n_p = q, r, qr$.

Now observe that any two distinct cyclic subgroups in G of prime order s, then they intersect trivially, otherwise they both contain a generator of each other. It follows from the fact that $n_r = pq$ that there are $pq(r-1)$ distinct elements of order r in G. Similarly there are $n_q \cdot (q-1)$ distinct elements of order q and $n_p \cdot (p-1)$ distinct elements of order p. As the sum of these three quantities should be less than $|G| = pqr$, it follows that

$$pq(r-1) + n_q \cdot (q-1) + n_p \cdot (p-1) \leq pqr.$$

But since $n_q \geq r$ and $n_p \geq q$, it follows that

$$pq(r-1) + r(q-1) + q(p-1) \leq pqr. \tag{4}$$

But $pq(r-1) + r(q-1) + q(p-1) = pqr + qr - q - r$. Since $q < r$ and $qr > q + r$ as q, r are primes therefore $pqr + qr - q - r > pqr$. This contradicts Eqn (4). This completes the proof. □

Proof of Question 4.5, 23. We wish to show that any group G of order 462 is not simple. Note that $|G| = 462 = 2 \cdot 3 \cdot 7 \cdot 11$. Let n be the number of Sylow 11-subgroups. We claim that $n = 1$. This will complete the proof as G would then have a unique normal Sylow subgroup of order 11 by Sylow's 2nd theorem, and thus be not simple.

By Sylow's 3rd theorem, it follows that $n | 2 \cdot 3 \cdot 7$ and $n = 1 \mod 11$. The former condition yields that

$$n = 1, 2, 3, 7, 6, 14, 21, 42.$$

But none of the above are $1 \mod 11$ except $n = 1$. This completes the proof. □

3 Week 3 : $\mathrm{Aut}\,(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$, semi-direct products

Proof of Question 4.4, 18. a) Let G be a group and $\varphi \in \mathrm{Aut}\,(()G)$ be an automorphism. We wish to show that φ permutes the conjugacy classes of G. Indeed, pick any $\varphi \in \mathrm{Aut}\,(()G)$ and a conjugacy class $C(x) = \{gxg^{-1} \mid g \in G\}$ where $x \in G$. We claim that

$$\varphi(C(x)) = C(\varphi(x)).$$

Indeed, to see ($\subseteq$), pick any element $\varphi(gxg^{-1}) \in \varphi(C(x))$. We see that

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) \in C(\varphi(x)).$$

Conversely, for $h\varphi(x)h^{-1} \in C(\varphi(x))$, we have $h = \varphi(g)$ for some unique $g \in G$ as φ is an isomorphism. Consequently,

$$h\varphi(x)h^{-1} = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(gxg^{-1}) \in \varphi(C(x)).$$

This completes the proof.

b) Let K be the conjugacy class of all transpositions and K' be the conjugacy class of an element $x \in S_n$ of order 2 but not a transposition. We wish to show that $|K| \neq |K'|$. Using this, we further wish to show that any automorphism of S_n sends transpositions to transpositions.

Recall that if $g \in S_n$, then the conjugacy class of g, denoted C, depends only on the cycle type of g and contains exactly all those elements whose cycle type is equal to that of g. As cycle type of a transposition is 2, therefore K consists of all elements of S_n of cycle type 2, hence

$$|K| = \frac{{}^nP_2}{2}.$$

Now, let $x \in S_n$ be an element such that K' is its conjugacy class. It follows from unique decomposition into disjoint cycles of x that

$$x = x_1 \cdot \cdots \cdot x_r$$

where x_i are disjoint cycles and $r \geq 1$. Since $|x| = 2$ and $|x| = \text{lcm}(|x_1|, \ldots, |x_r|)$, it follows that for each $i = 1, \ldots, r$, either $|x_i| = 1, 2$. Since $|x_i| = 1$ implies x_i is identity, hence we may assume by reducing r that $x = x_1 \ldots x_r$ and each x_i is a disjoint cycle of order 2, that is, x_i is a transposition. Hence, the cycle type of x is $\underbrace{2 + 2 + \cdots + 2}_{r\text{-times}}$. It follows that K' consists of all elements of cycle type $2 + \cdots + 2$ r-times. It follows that

$$\left|K'\right| = \frac{{}^nC_2 \cdot {}^{n-2}C_2 \ldots {}^{n-2(r-1)}C_2}{r!}.$$

We claim that the above count is not equal to $|K| = \frac{{}^nP_2}{2} = {}^nC_2$. Fix an $n \geq 7$ and $2 \leq r \leq n/2$. Observe that to show $|K'| \neq |K|$, it suffices to show that

$${}^{n-2}C_2 \ldots {}^{n-2(r-1)}C_2 \neq r!. \tag{1.1}$$

Suppose to the contrary that there exists n and r as above such that in Eqn. (1.1) we have an equality. Observe that

$${}^{n-2}C_2 \ldots {}^{n-2(r-1)}C_2 = \frac{(n-2)!}{2^{r-1}(n-2r)!}.$$

Hence our assumption gives the following equality:

$$(n-2)! = r! \cdot 2^{r-1} \cdot (n-2r)!$$

Now observe that

$$(n-2)! = \underbrace{1 \cdot 2 \cdot 3 \cdot \cdots \cdot r}_{r!} \cdot \underbrace{(r+1) \cdot \cdots \cdot (2r-1)}_{\gneq 2^{r-1}} \cdot \underbrace{2r \cdot (2r+1) \cdot \cdots \cdot (n-2)}_{\gneq (n-2r)!}$$

where $(r+1) \cdot \cdots \cdot (2r-1) \gneq 2^{r-1}$ as $r \geq 2$ so $r + k \gneq 2$ for all $1 \leq k \leq r-1$. Similarly, $2r \cdot (2r+1) \cdot \cdots \cdot (n-2) \gneq 2 \cdot 3 \cdot \cdots \cdot (n-2r)$ as $2r + k \gneq 4 + k \gneq k + 2$ for all $0 \leq k \leq n - 2r - 2$. Hence we have obtained that

$$r! \cdot 2^{r-1} \cdot (n-2r)! = (n-2)! \gneq r! \cdot 2^{r-1} \cdot (n-2r)!$$

which gives the required contradiction.

Now for $n \leq 5$, we see that since $2 \leq r \leq n/2$, therefore $n = 4, 5$ and $r = 2$ is the only possibility. In this case, Eqn. (1.1) is immediately true. For $n = 2, 3$, there is no element of order 2 which is not a transposition. This completes the proof that $|K| \neq |K'|$.

Finally let $\varphi \in \mathrm{Aut}\,(()S_n)$ and K be the set/conjugacy class of all transpositions. We then wish to show that $\varphi(K) = K$. Indeed, in part a), we saw that automorphisms take conjugacy classes to conjugacy classes. Therefore $\varphi(K)$ is a conjugacy class of S_n. In order to show that $\varphi(K) = K$, it would thus suffice to show that $\varphi(K)$ contains a transposition (as $\varphi(K)$ is itself a conjugacy class). Let $x \in K$ be a transposition. As $\varphi : S_n \to S_n$ is an automorphism, therefore we claim that $\varphi(x)$ is also a transposition.

Suppose $\varphi(x) = y_1 \dots y_r$ is the disjoint cycle decomposition of $\varphi(x)$. As φ^{-1} is a homomorphism, therefore we obtain

$$x = \varphi^{-1}(y_1) \dots \varphi^{-1}(y_r).$$

Let $x = x_1 \dots x_s$ be the disjoint cycle decomposition of x obtained by decomposing each $\varphi^{-1}(x_i)$ as a disjoint cycle decomposition. Since x is a transposition, therefore for all except one i_0, $x_i = ()$, so that $x = x_{i_0}$. It thus follows that $x = \varphi^{-1}(y_{i_0}) = x_{i_0}$. Hence $\varphi(x) = y_{i_0}$ where y_{i_0} is a cycle. As $\varphi(x)$ is of order 2 (automorphisms preserves order), therefore y_{i_0} is a cycle of order 2, that is, a transposition, as needed.

c) Let $\sigma \in \mathrm{Aut}\,(()S_n)$. We wish to show that there exists distinct $a, b_2, \dots, b_n \in \{1, 2, \dots, n\}$ such that $\sigma((1\ k)) = (a\ b_k)$ for all $2 \leq k \leq n$.

Observe from part b) that $\sigma((a\ b))$ is also a transposition. We first show that each $\sigma((1\ k))$ and $\sigma((1\ l))$ are not disjoint transpositions for $1 \leq k \neq l \leq n$. Denote

$$\begin{aligned} \sigma((1\ k)) &= (a_k\ b_k) \\ \sigma((1\ l)) &= (a_l\ b_l). \end{aligned} \tag{1.2}$$

Assuming that $(a_k\ b_k)$ and $(a_l\ b_l)$ are disjoint, we deduce that

$$\sigma((1\ l\ k)) = \sigma((1\ k) \cdot (1\ l)) = (a_k\ b_k) \cdot (a_l\ b_l)$$

is a disjoint cycle decomposition of $\sigma((1\ l\ k))$. It follows that $\sigma((1\ l\ k))$ is an order 2 element, but σ is an automorphism and $(1\ l\ k)$ a 3-cycle, so $\sigma((1\ l\ k))$ must have order 3, a contradiction. This shows that in Eqn. (1.2), $(a_k\ b_k)$ and $(a_l\ b_l)$ are not disjoint. Hence we write $\sigma((1\ k)) = (a\ b_k)$ and $\sigma((1\ l)) = (a\ b_l)$. Note that since σ is an automorphism, therefore $b_k \neq b_l$.

We now show that $\sigma((1\ m))$ is also of the form $(a\ b_m)$. Indeed, denote $\sigma((1\ m)) = (a_m\ b_m)$ for $m \neq k, l$. Then, by above $(a_m\ b_m)$ is not disjoint with $(a\ b_k)$ and $(a\ b_l)$. If $a_m = a$ or $b_m = a$, then we are done. If not, then it follows that $a_m = b_k$ and $b_m = b_l$. Consequently, we have $\sigma((1\ m)) = (b_k\ b_l)$. We claim that this implies $(1\ m) = (k\ l)$, which is a contradiction to the fact that $m \neq k, l$. Indeed, we have the following

$$\begin{aligned} \sigma((1\ m)) = (b_k\ b_l) &= (a\ b_k) \cdot (a\ b_l) \cdot (a\ b_k) \\ &= \sigma((1\ k) \cdot (1\ l) \cdot (1\ k)) \\ &= \sigma((k\ l)). \end{aligned}$$

As σ is an automorphism, so it follows that $(1\ m) = (k\ l)$ as required.

This shows that for each $1 \leq k \leq n$, we have

$$\sigma((1\ k)) = (a\ b_k)$$

for some $a, b_k \in \{1, \ldots, n\}$. We now need only show that $b_k \neq b_l$ for $k \neq l$. This is immediate, for if $b_k = b_l$ for some $k \neq l$, then $\sigma((1\ k)) = (a\ b_k) = (a\ b_l) = \sigma((1\ l))$ and thus $(1\ k) = (1\ l)$, a contradiction.

d) We wish to show the following:

1. S_n is generated by the set $X = \{(1\ k) \mid 1 \leq k \leq n\}$.
2. Any $\sigma \in \mathrm{Aut}\,(()S_n)$ is uniquely determined by values on each $(1\ k) \in X$.
3. $\mathrm{Aut}\,(()S_n) = \mathrm{Inn}(S_n)$

1. Indeed, since we know that each element of S_n can be written as a product of transpositions, hence it suffices to show that each transposition $(k\ l)$ is obtained by product of elements from X. This is immediate as

$$(k\ l) = (1\ k)(1\ l)(1\ k).$$

2. Pick any $\sigma \in \mathrm{Aut}\,(()S_n)$. By part c), we conclude that σ defines a permutation of $\{1, 2, \ldots, n\}$. If $\tau \in \mathrm{Aut}\,(()S_n)$ is any other permuation such that $\tau((1\ k)) = \sigma((1\ k))$ for all $2 \leq k \leq n$, then since X generates S_n, therefore $\sigma = \tau$.

3. By item 2, it follows that every $\sigma \in \mathrm{Aut}\,(()S_n)$ gives a unique permutation of $\{1, 2, \ldots, n\}$. Hence there are atmost n! automorphisms of S_n, i.e $|\mathrm{Aut}\,(()S_n)| \leq n!$. But since $\mathrm{Inn}(S_n) \leq \mathrm{Aut}\,(()S_n)$ and $\mathrm{Inn}(S_n) \cong S_n/Z(S_n)$ where $Z(S_n)$ is trivial, therefore $|\mathrm{Inn}(S_n)| = |S_n| = n!$. Consequently, $n! \leq \mathrm{Aut}\,(()S_n) \leq n!$. Hence, it follows that $\mathrm{Aut}\,(()S_n) = \mathrm{Inn}(S_n) \cong S_n$ if $n \neq 6$. □

Proof of Question 5.4, 19. a) We wish to show that any simple non-abelian group is perfect. Indeed, let G be such a group. It would suffice to show that $G' \leq G$ is a normal subgroup. Denote

$$X = \{ghg^{-1}h^{-1} \mid g, h \in G\} \subseteq G.$$

Pick any $k \in G$. We wish to show that $kG'k^{-1} = G'$. Denote

$$I := \{H \leq G \mid H \supseteq X\}.$$

Since $G' = \bigcap_{H \in I} H$. Thus,

$$kG'k^{-1} = \bigcap_{H \in I} kHk^{-1}. \tag{2.1}$$

Hence we reduce to showing that $G' = \bigcap_{H \in I} kHk^{-1}$. To this end, it is sufficient to show that

$$I = \{kHk^{-1} \mid H \in I\}, \tag{2.2}$$

that is, conjugating with k permutes I. Indeed for $(\supseteq)$, pick $H \in I$. We first claim that $kHk^{-1} \in I$. We must show that $kHk^{-1} \supseteq X$ if $H \supseteq X$. Indeed, pick $ghg^{-1}h^{-1} \in X$. Write

$$ghg^{-1}h^{-1} = k \cdot \underbrace{(k^{-1}gk) \cdot (k^{-1}hk) \cdot (k^{-1}gk)^{-1} \cdot (k^{-1}hk)^{-1}}_{\in X \subseteq H} \cdot k^{-1}.$$

It follows that $ghg^{-1}h^{-1} \in kHk^{-1}$. This shows $X \subseteq kHk^{-1}$, that is, $kHk^{-1} \in I$.

For $(\subseteq)$, pick $H \in I$. We wish to show that $H = kMk^{-1}$ for some $M \in I$. Since $k^{-1}Hk \in I$ by above, therefore $k(k^{-1}Hk)k^{-1} = H$. This shows the claim in Eqn. (2.2) and thus completes the proof.

b) Let $H, K \leq G$ be a perfect subgroups of G. We wish to show that $\langle H, K\rangle \leq G$ is also a perfect subgroup. We first observe the following fact that we know.

Lemma 3.0.1. *Let G be a group and $S \subseteq G$ be a subset. Then the subgroup $\langle S\rangle \leq G$ generated by S consists of finite product of elements from S and S^{-1}. That is,*

$$\langle S\rangle = \{s_1 \dots s_n \in G \mid s_i \in S \text{ or } s_i^{-1} \in S\}.$$

Now consider the commutator subgroup of $\langle H, K\rangle$ denoted $D^1\langle H, K\rangle$. We wish to show that

$$D^1\langle H, K\rangle = \langle H, K\rangle.$$

We already have $D^1\langle H, K\rangle \subseteq \langle H, K\rangle$. For the converse, pick $a_1b_1 \dots a_nb_n \in \langle H, K\rangle$ where $a_i \in H$ and $b_i \in K$ by Lemma 1. Now observe that a commutator element of either H or K is a commutator element of $\langle H, K\rangle$. As we wish to show that $a_1b_1 \dots a_nb_n \in D^1\langle H, K\rangle$, therefore it suffices to write it as a product of commutators of $\langle H, K\rangle$.

Indeed, since we have the following as H and K are perfect:

$$a_i = h_ih_i'h_i^{-1}h_i'^{-1}$$
$$b_i = k_ik_i'k_i^{-1}k_i'^{-1}$$

for each $1 \leq i \leq n$ where $h_i \in H$ and $h_i \in K$. Consequently, we may write

$$a_1b_1 \dots a_nb_n = (h_1h_1'h_1^{-1}h_1'^{-1})(k_1k_1'k_1^{-1}k_1'^{-1}) \dots (h_nh_n'h_n^{-1}h_n'^{-1})(k_nk_n'k_n^{-1}k_n'^{-1})$$

where the product in each bracket is in $D^1\langle H, K\rangle$. Hence, $a_1b_1 \dots a_nb_n \in D^1\langle H, K\rangle$, as needed.

We now wish to show that subgroup generated by any collection of perfect subgroups is perfect. Indeed, let $\{H_\alpha\}_{\alpha \in I}$ be a collection of perfect subgroups of G. We claim that $H = \langle H_\alpha \mid \alpha \in I\rangle$ is perfect. Indeed, pick any element $a_{\alpha_1} \dots a_{\alpha_n}$ of H where $a_{\alpha_i} \in H_{\alpha_i}$. We wish to show that $a_{\alpha_1} \dots a_{\alpha_n} \in D^1H$. As each H_{α_i} is perfect, therefore $a_{\alpha_i} = g_{\alpha_i}g'_{\alpha_i}g_{\alpha_i}^{-1}g'^{-1}_{\alpha_i}$ for each $i \in I$ and $g_{\alpha_i}, g'_{\alpha_i} \in H_{\alpha_i}$. As every commutator element of H_α is a commutator element of H, therefore by writing

$$a_{\alpha_1} \dots a_{\alpha_n} = \prod_{i=1}^{n} g_{\alpha_i}g'_{\alpha_i}g_{\alpha_i}^{-1}g'^{-1}_{\alpha_i}$$

we deduce that $a_{\alpha_1} \dots a_{\alpha_n} \in D^1 H$, as needed. This completes the proof.

c) We wish to show that any conjugate of a perfect subgroup is perfect. Let $g \in G$ and $H \leq G$ be a perfect subgroup. We wish to show that gHg^{-1} is also perfect. It suffices to show that if $H \leq G$ is a subgroup then $D^1(gHg^{-1}) = gD^1(H)g^{-1}$. Indeed, this is immediate from the following expression for any $h, k \in H$:

$$(ghg^{-1})(gkg^{-1})(ghg^{-1})^{-1}(gkg^{-1})^{-1} = g(hkh^{-1}k^{-1})g^{-1}.$$

This completes the proof.

d) We wish to show that any group G has a unique maximal perfect subgroup and this subgroup is normal.

Indeed, let $J = \{H \leq G \mid H \text{ is a perfect subgroup}\}$. Consider the subgroup $\tilde{H} = \langle H \leq G \mid H \in J \rangle$ generated by all perfect subgroups. By part b), $\tilde{H}$ is a perfect subgroup of G. It is also maximal perfect subgroup as if there is any perfect subgroup $H \leq G$, then $H \leq \tilde{H}$. Uniqueness is also clear as if there is another maximal perfect subgroup say $K \leq G$, then $K \in J$ and thus $K \leq \tilde{H}$. Since K is maximal, therefore $K = \tilde{H}$, as needed.

We now show that $\tilde{H}$ is normal. Pick any $g \in G$ and consider the conjugate $g\tilde{H}g^{-1}$. As $\tilde{H}$ is perfect, therefore by part c), so is $g\tilde{H}g^{-1}$. Consequently, $g\tilde{H}g^{-1} \in J$ and thus $g\tilde{H}g^{-1} \leq \tilde{H}$. We now wish to show that $\tilde{H} \leq g\tilde{H}g^{-1}$. Pick $h \in \tilde{H}$. Since $k\tilde{H}k^{-1} \leq \tilde{H}$ for each $k \in G$, therefore $g^{-1}\tilde{H}g \leq \tilde{H}$ as well. It follows that $g^{-1}hg \in \tilde{H}$ and thus $h = g(g^{-1}hg)g^{-1} \in g\tilde{H}g^{-1}$. This shows that $\tilde{H} = g\tilde{H}g^{-1}$ for all $g \in G$, and thus $\tilde{H}$ is normal. □

Proof of Question 5.5, 6. Let K be a cyclic group and H be a group. Consider two homomorphisms

$$\varphi_1, \varphi_2 : K \to \mathrm{Aut}\,(()H),$$

which we may assume to be injective if K is infinite. Suppose $\mathrm{Im}\,(\varphi_1)$ and $\mathrm{Im}\,(\varphi_2)$ are conjugate subgroups in $\mathrm{Aut}\,(()H)$. We then wish to show that then there is an isomorphism

$$H \ltimes_{\varphi_1} K \cong H \ltimes_{\varphi_2} K.$$

By assumption, there exists $\sigma \in \mathrm{Aut}\,(()H)$ such that $\sigma \mathrm{Im}\,(\varphi_1)\sigma^{-1} = \mathrm{Im}\,(\varphi_2)$. As K is cyclic, therefore let $k \in K$ be the generator of K. Consequently, there exists $n \in \mathbb{Z}$ such that

$$\sigma \circ \varphi_1(k) \circ \sigma^{-1} = \varphi_2(k)^n. \tag{3.1}$$

Now consider the function

$$\begin{aligned} \psi : H \ltimes_{\varphi_1} K &\longrightarrow H \ltimes_{\varphi_2} K \\ (h, k^a) &\longmapsto (\sigma(h), k^{an}). \end{aligned}$$

We first show that ψ is a group homomorphism. Let $(h_1, k^a), (h_2, k^b) \in H \ltimes_\varphi K$ be two elements where $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}
\psi((h_1, k^a) \cdot (h_2, k^b)) &= \psi\left((h_1\varphi_1(k^a)(h_2), k^{a+b})\right) \\
&= \psi\left((h_1 \cdot \sigma^{-1} \circ \varphi_2(k^{an}) \circ \sigma(h_2), k^{a+b})\right) \\
&= \left(\sigma\left(h_1 \cdot (\sigma^{-1} \circ \varphi_2(k^{an}) \circ \sigma(h_2))\right), k^{(a+b)n}\right) \\
&= \left(\sigma(h_1) \cdot \varphi_2(k^{an})(\sigma(h_2)), k^{(a+b)n}\right) \\
&= (\sigma(h_1), k^{an}) \cdot (\sigma(h_2), k^{bn}) \\
&= \psi\left((h_1, k^a)\right) \cdot \psi\left((h_2, k^b)\right),
\end{aligned}$$

as needed. We now construct an inverse of ψ. We divide this in two cases for K. First suppose that K is infinite cyclic with generator k. Then since $\sigma^{-1}\mathrm{Im}\,(\varphi_2)\sigma = \mathrm{Im}\,(\varphi_1)$, therefore we get some $m \in \mathbb{Z}$ such that

$$\sigma^{-1} \circ \varphi_2(k) \circ \sigma = \varphi_1(k)^m.$$

Hence, we have that $\varphi_2(k) = \sigma \circ \varphi_1(k^m) \circ \sigma^{-1} = \varphi_2(k)^{nm}$. Consequently, $k^{mn-1} \in \mathrm{Ker}\,(\varphi_2)$. Since φ_2 is injective by our hypothesis, therefore $k^{mn} = k$.

Now consider the following map

$$\begin{aligned}
\kappa : H \ltimes_{\varphi_2} K &\longrightarrow H \ltimes_{\varphi_1} K \\
(h, k^a) &\longmapsto (\sigma^{-1}(h), k^{am}).
\end{aligned}$$

We claim that this map is an inverse for ψ. Indeed we first show that $\kappa \circ \psi = \mathrm{id}$. Indeed, pick $(h, k^a) \in H \ltimes_{\varphi_1} K$. Then $\kappa(\psi((h, k^a))) = \kappa((\sigma(h), k^{an})) = (h, k^{anm}) = (h, (k^{nm})^a) = (h, k^a)$. Similarly, it follows that $\psi \circ \kappa = \mathrm{id}$.

Finally, assume that $K = \langle k \rangle$ is a finite cyclic group of order l. Consider the following map (it suffices to define the map only on the generator of K):

$$\begin{aligned}
\kappa : H \ltimes_{\varphi_2} K &\longrightarrow H \ltimes_{\varphi_1} K \\
(h, k) &\longmapsto (h, k^m)
\end{aligned}$$

where $m \in \mathbb{N}$ is a positive integer such that $k^{mn} = k$. We show the existence of such an integer m later. Let us otherwise complete the proof. Indeed, $\kappa \circ \psi = \mathrm{id}$ as for any $(h, k^a) \in H \ltimes_{\varphi_1} K$, we get $\kappa(\psi((h, k^a))) = \kappa((\sigma(h), k^{an})) = (\sigma^{-1}\sigma(h), k^{anm}) = (h, (k^{mn})^a) = (h, k^a)$. Similarly, one sees the other direction.

Now we show the existsence of m. We wish to find $m \in \mathbb{N}$ such that $l | mn - 1$. This is equivalent to showing that $\gcd(n, l) = 1$. We will show that by approriately replacing n so that the new induced map ψ still is a homomorphism, this can be achieved. Observe that $\varphi_2(k) \in \mathrm{Aut}\,(()H)$ is an element of order coprime to n as $\varphi_2(k)^n$ is a generator of $\mathrm{Im}\,(\varphi_2) = \langle \varphi_2(k) \rangle$. Denoting $a = |\varphi_2(k)|$, we have $\gcd(a, n) = 1$. Moreover, we know in general that $a | l$. Now observe the following lemma:

Lemma 3.0.2. *Let $a, n, l \in \mathbb{Z}$ be integers such that $\gcd(a, n) = 1$ and $a | l$. Then there exists $n' \in \mathbb{Z}$ such that $n' = n \mod a$ and $\gcd(n', l) = 1$.*

Proof. Consider $n' = n + q_1 \dots q_k \cdot a$ where q_i is a prime such that $q_i | l$ and $q_i \nmid n$. Pick any prime $p|l$. If $p|n$, then $p \nmid q_1 \dots q_k a$. Similarly, if $p \nmid n$, then $p | q_1 \dots q_k a$. This shows in both cases that $p \nmid n'$, as required. □

Finally, using Lemma 3.0.2, we claim that we can replace n by n' and the map ψ thus obtained would still be a homomorphism. Indeed, in Eqn. (3.1), one observes that $\varphi_2(k)^n = \varphi_2(k)^{n'}$ as $n' = n \mod a$, where $a = |\varphi_2(k)|$. This completes the proof. □

Proof of Question 5.5, 8. a) We first wish to find a non-trivial group of order $75 = 3 \cdot 5^2$. By general results on semi-direct products, we need only construct a non-trivial map $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$ to construct a group $(\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\varphi \mathbb{Z}_3$, which would thus be non-abelian. Indeed, we further reduce to showing that $\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$ has an element of order 3. It thus remains to be seen that what is the order of $\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$. Observe that automorphisms of $\mathbb{Z}_p \times \mathbb{Z}_p$ are just invertible $\mathbb{Z}_p$-linear transformations $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$, for any prime p. It follows that $\mathrm{Aut}\,(()\mathbb{Z}_p \times \mathbb{Z}_p) = \mathrm{GL}_2(\mathbb{Z}_p)$. Since $|\mathrm{GL}_2(\mathbb{Z}_p)| = (p^2-1)(p^2-p)$, therefore we see that

$$|\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)| = |\mathrm{GL}_2(\mathbb{Z}_5)| = 480 = 2^3 \cdot 3 \cdot 5.$$

Hence, there is an element of order 3 in $\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$ by Cauchy's theorem, as required.

We now construct an explicit element matrix $A \in \mathrm{GL}_2(\mathbb{Z}_5)$ of order 3, which we then use to construct the map $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$. Indeed, observe that the matrix

$$A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_5)$$

is of order 3. Indeed, one constructs this as the companion matrix of $p(x) = x^2 + x + 1$ where $p(x) \in \mathbb{Z}_5[x]$. Then since $x^3 - 1 = (x-1)p(x)$, therefore $A^3 - I = 0$, as required. Hence, the map

$$\begin{aligned} \varphi : \mathbb{Z}_3 &\longrightarrow \mathrm{GL}_2(\mathbb{Z}_5) \\ 1 &\longmapsto A \end{aligned}$$

gives the required map φ. Hence, the operation of group $(\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\varphi \mathbb{Z}_3$ is given as follows. Consider two elements $((a_1, b_1), c_1)$ and $((a_2, b_2), c_2)$ in $(\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\varphi \mathbb{Z}_3$. We showcase their product as follows:

$$((a_1, b_1), c_1) \cdot ((a_2, b_2), c_2) = \begin{cases} ((a_1, b_1) \cdot (a_2, b_2), 0) & \text{if } c_1 = 0 \\ ((a_1, b_1) \cdot (-b_2, a_2 - b_2), c_2) & \text{if } c_1 = 1 \\ ((a_1, b_1) \cdot (-a_2 + b_2, -a_2), 2c_2) & \text{if } c_1 = 2. \end{cases}$$

The above multiplication on the set $(\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_3$ hence defines a group which is non-abelian of order 75, as needed.

b) We wish to classify all groups of order 75. Indeed, we claim that upto isomorphism, there are only three groups of order 75, out of which two are abelian and only one is non-abelian:

1. $\mathbb{Z}_{75}$,
2. $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$,
3. $(\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\varphi \mathbb{Z}_3$,

where φ is as constructed in part a). The first two follows from structure theorem for finitely generated abelian groups and the fact that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ is $\gcd(m,n) = 1$. The non-trivial part is to show that any non-abelian group G of order 75 is isomorphic to $(\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\varphi \mathbb{Z}_3$. We show this now.

We first claim that there is a unique Sylow 5-subgroup of G. Indeed, let n_5 be the no. of Sylow 5-subgroups of G. Then by Sylow's third theorem, it follows that $n_5 = 1 \mod 5$ and $n_5 | 3$. The only solution to this is $n_5 = 1$. Hence, there is a unique Sylow 5-subgroup $K \cong \mathbb{Z}_{25}$ of order 25. By Sylow's second theorem, K is a normal subgroup. Moreover, observe by Cauchy's theorem that there exists an element of order 5 in K. This means that K is not cyclic of order 25. Hence, every element in K is of order 5. Pick two disjoint subgroups of order 5 in K, which exists as every non-identity element in a group of order 5 is a generator. It follows that $K \cong \mathbb{Z}_5 \times \mathbb{Z}_5$.

Observe that there are subgroups of order 3 by either Cauchy or Sylow. Pick any one and call it H. Note $H \cong \mathbb{Z}_3$. We claim that $H \cap K = e$ and $H \cdot K = G$. Indeed, this follows from size arguments as $|H \cdot K| = \frac{|H||K|}{|H \cap K|} = 75$. Hence, we deduce that G is an internal semi-direct product of H and K. It follows that under the conjugation map $\psi : H \to \mathrm{Aut}\,(()K)$, we have $G = K \ltimes_\psi H \cong (\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\psi \mathbb{Z}_3$. Observe that $\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5) \cong \mathrm{GL}_2(\mathbb{Z}_5)$ and thus is of order $480 = 2^5 \cdot 3 \cdot 5$.

Since the images of ψ and φ are both subgroups of order 3 in $\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$, therefore they are both Sylow 3-subgroups of $\mathrm{Aut}\,(()\mathbb{Z}_5 \times \mathbb{Z}_5)$. It thus follows by Sylow's second theorem that $\mathrm{Im}\,(\psi)$ and $\mathrm{Im}\,(\varphi)$ are conjugate. By Question 5.5, 6, it follows that $G \cong (\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\psi \mathbb{Z}_3 \cong (\mathbb{Z}_5 \times \mathbb{Z}_5) \ltimes_\varphi \mathbb{Z}_3$, as needed.

□

Proof of Question 5.5, 24. Let $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be a positive integer where p_i are distinct primes. We wish to show that the following are equivalent:

1. Every group of order n is abelian.
2. Each $\alpha_i = 1$ or 2 and $p_i \nmid p_j^{\alpha_j} - 1$ for all i, j.

(1. $\Rightarrow$ 2.) Suppose to the contrary that statement 2 is not true. In each case, we then construct a non-abelian group of order n, taking help of semi-direct products.

If statement 2 is not true, then either for some $i_0 = 1, \dots, r$, $\alpha_{i_0} \geq 3$ or for some $i_0, j_0 = 1, \dots, r$, we get $p_{i_0} | p_{j_0}^{\alpha_{j_0}} - 1$. Before proving both the cases, we state the following claims.

Lemma 3.0.3. *There is a non-abelian group of order:*

1. p^3,
2. p^α *for each* $\alpha \geq 3$,
3. pq *where* $p | q - 1$,
4. pq^2 *where* $p | q^2 - 1$,
5. $p^\alpha q^\beta$ *where* $1 \leq \alpha, \beta \leq 2$ *and* $p | q^\beta - 1$.

Proof. Items 1 and 3 are done in Dummit & Foote. For item 2, consider any group of order $p^{\alpha-3}$, say H and let K be a non-abelian group of order p^3 as constructed in item 1.

Then, $H \times K$ is a non-abelian group of order p^α, as it contains a non-abelian subgroup. For item 4, since $p|q^2-1$, $\mathrm{Aut}\,(()\mathbb{Z}_q \times \mathbb{Z}_q) = \mathrm{GL}_2(\mathbb{F}_q)$ and $|\mathrm{GL}_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$, therefore $p|\,|\mathrm{Aut}\,(()\mathbb{Z}_q \times \mathbb{Z}_q)|$. It follows by Cauchy's theorem that there exists a non-trivial map $\varphi : \mathbb{Z}_p \to \mathrm{Aut}\,(()\mathbb{Z}_q \times \mathbb{Z}_q)$. As any non-trivial (the underlying map is non-trivial) semi-direct product yields a non-abelian group, therefore $(\mathbb{Z}_q \times \mathbb{Z}_q) \ltimes_\varphi \mathbb{Z}_p$ is a non-abelian group of order pq^2, as needed. Using item 4, one can prove item 5 as follows. We proceed by considering various cases on α and β.

1. If $\alpha = 1 = \beta$. Then, by item 3, we are done.
2. If $\alpha = 1$ and $\beta = 2$. Then, by item 4, we are done.
3. If $\alpha = 2$ and $\beta = 1$. Then $p|q-1$ and thus by item 3, we have a non-abelian group of order pq, say H. Take the group of order p, say K, and consider $H \times K$, which is thus a non-abelian group of order p^2q.
4. If $\alpha = 2$ and $\beta = 2$. Then, by item 4, there is a non-abelian group of order pq^2. We may multiply it by the group of order p to get a non-abelian group of order p^2q^2.

This completes the proof of the lemma. □

We now use Lemma 3.0.3 to complete this direction. Indeed, if $\alpha_{i_0} \geq 3$, then by the above lemma, we have a group H of order $p_{i_0}^{\alpha_{i_0}}$. Let K be a group of order $\prod_{j \neq i_0} p_j^{\alpha_j}$. Then $H \times K$ is a group of order n which is not abelian, a contradiction.

Finally, if there exists $i_0, j_0 \in \{1, \ldots, r\}$ such that $p_{i_0} | q_{j_0}^{\alpha_{j_0}} - 1$, then we proceed as follows. We may first assume that all $1 \leq \alpha_i \leq 2$ as if not, then we are in previous case and we would be done. By Lemma 3.0.3, 5, there is a non-abelian group H of order $p_{i_0}^{\alpha_{i_0}} q_{j_0}^{\alpha_{j_0}}$. Let K be any group of order $\prod_{k \neq i_0, j_0} p_k^{\alpha_k}$. Then $H \times K$ is a non-abelian group of order n, a contradiction. This completes the proof of forward direction.

(2. $\Rightarrow$ 1.) we proceed by strong induction on n. The case for $n = 1, 2$ is immediate. Now suppose that every group of order $m = \prod_{i=1}^r p_i^{\alpha_i} < n$ such that $\alpha_i = 1$ or 2 and $p_i \nmid p_j^{\alpha_j} - 1$ for all i, j is abelian. Let G be a group of order n. By inductive hypothesis, every proper subgroup of G is abelian. We wish to show that G is abelian. The proof of this is complicated and hence we first state all the steps we need in the following proposition.

Proposition 3.0.4. *Let G be of order $n = \prod_{i=1}^r p_i^{\alpha_i}$ such that $\alpha_i = 1$ or 2 and $p_i \nmid p_j^{\alpha_j} - 1$ for all i, j . Suppose further that every proper subgroup of G is abelian. Then the following statements are true:*

1. *G is solvable.*
2. *There exists a proper normal subgroup $N \trianglelefteq G$ such that G/N is prime cyclic.*
3. *The center ZG is equal to G. That is, G is abelian.*

The proof of (2. $\Rightarrow$ 1.) would then follow from item 4 in above proposition.

Proof of Proposition 1.

1. This follows from item 1 and Exercise 56 of §4.5 of Dummit-Foote.
2. By item 2, G is solvable. Then, by one of the equivalent criterion of solvability, it follows that there is a composition series with prime cyclic factors. Therefore there is a normal proper subgroup $N \trianglelefteq G$ such that $G/N \cong \mathbb{Z}_p$, where p is a prime, as required.

3. By item 3, there is a normal subgroup $N \trianglelefteq G$ of index prime p_1 (WLOG) where p_1 is a prime dividing $|G| = n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Now consider the action of G/N as automorphisms of N by conjugation, that is,

$$\begin{aligned} G/N \times N &\longrightarrow N \\ (gN, n) &\longmapsto gng^{-1}. \end{aligned}$$

This determines a homomorphism

$$\varphi : G/N \to \mathrm{Aut}\,(()N). \tag{5.1}$$

Observe that

$$|N| = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

where $1 \leq \alpha_i \leq 2$. Observe that N is abelian by item 1. In particular, N is an abelian group of order $p_1^{\alpha_1-1}p_2^{\alpha_2} \dots p_r^{\alpha_r}$. It follows by structure theorem of finitely generated abelian groups that either N is isomorophic to $\mathbb{Z}_{p_1} \times N'$ or to N', where N' is some abelian group of order $p_2^{\alpha_2} \dots p_r^{\alpha_r}$.
Now since $\mathrm{Aut}\,(()K_1 \times K_2) \cong \mathrm{Aut}\,(()K_1) \times \mathrm{Aut}\,(()K_2)$ by pre and post composing with inclusions and surjections of factors, we deduce that

$$\mathrm{Aut}\,(()N) \cong \begin{cases} \mathrm{Aut}\,(()\mathbb{Z}_{p_1}) \times \mathrm{Aut}\,(()N') \text{ or,} \\ \mathrm{Aut}\,(()N'). \end{cases}$$

Thus, $|\mathrm{Aut}\,(()N)| = (p_1 - 1) \times |\mathrm{Aut}\,(()N')|$ or $|\mathrm{Aut}\,(()N)| = |\mathrm{Aut}\,(()N')|$. Observe that since $p_1 \nmid p_j^{\alpha_j} - 1$ for all $j = 2, \dots, r$, therefore we claim that $p_1 \nmid |\mathrm{Aut}\,(()N')|$. Indeed, by another use of structure theorem, for each $j = 2, \dots, r$, either N' will have $\mathbb{Z}_{p_j}$ as a factor or $\mathbb{Z}_{p_j^2}$ as a factor or $\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j}$ as a factor. Consequently, $|\mathrm{Aut}\,(()N')|$ will have either $p_j - 1$ as a factor $p_j^2 - p_j$ as a factor, $(p_j^2 - 1)(p_j^2 - p_j)$ as a factor. As p_1 does not divide any of the three, therefore we conclude that the map φ in Eqn. (5.1) is trivial. That is, the conjugation action of G/N on N is trivial. Therefore for every $gN \in G/N$, $gng^{-1} = n$ for all $n \in N$. It follows that $N \leq ZG$. If $N = ZG$, then G/ZG is cyclic and thus G is abelian, so we are done. If $N \lneq ZG$, then ZG/N determines a non-trivial subgroup of $G/N \cong \mathbb{Z}_{p_1}$. It then also follows that $ZG = G$, as required.

This completes the proof of the proposition. □

This completes the proof of the result. □

4 Week 4 : Free groups, irreducibility

Proof of Question 6.3, 3. We wish to show that the commutator subgroup $H = [G : G]$ of $G = \mathbb{Z} * \mathbb{Z}$ is not finitely generated. Recall that

$$H = \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle.$$

Suppose that H is finitely generated. We first claim that there is a finite subset of $S = \{ghg^{-1}h^{-1} \mid g, h \in G\}$ which generates H. Indeed, since there is a finite generating set, say $T = \{t_1, \ldots, t_n\} \subseteq H$, therefore we may write each $t_i \in T$ as a finite product of elements from S. Let $F \subseteq S$ be the finite subset obtained by taking all elements of S which appear in factorization of each $t_i \in T$. Thus F generates H, as required.

Let $F = \{g_k h_k g_k^{-1} h_k^{-1} \mid k = 1, \ldots, L\}$ and furthermore, denote

$$g_k = a^{m_{k_1}} b^{m_{k_2}} \ldots a^{m_{k_{l_k-1}}} b^{m_{k_{l_k}}}$$
$$h_k = a^{n_{k_1}} b^{n_{k_2}} \ldots a^{n_{k_{l_k-1}}} b^{n_{k_{l_k}}}$$

where $a, b \in G$ are the two generating elements of G. Now observe the following for each $1 \leq k \leq L$:

$$g_k h_k g_k^{-1} h_k^{-1} = a^{m_{k_1}} b^{m_{k_2}} \ldots\ldots\ldots b^{-n_{k_2}} a^{-n_{k_1}}.$$

Now let $M = \sum_{k=1}^{L} m_{k_1}$ and $N = \sum_{k=1}^{L} n_{k_1}$. Further, denote

$$H' = \langle g_k h_k g_k^{-1} h_k^{-1} \mid k = 1, \ldots, L \rangle$$

which is equal to H by assumption. Since any element in H' is obtained by finite product of elements from F. Thus, every element in H' will be of form $a^{m_{k_1}} b^{m_{k_2}} \ldots\ldots b^{-n_{l_2}} a^{-n_{l_1}}$ for some $1 \leq k, l \leq L$. Pick any $\kappa > \max\{M, N\}$. Then the element $a^\kappa b^\kappa a^{-\kappa} b^{-\kappa}$ is in H, but not in H'. This shows that $H' \neq H$, a contradiction. Thus H is not finitely generated, as required. □

Proof of Question 6.3, 10. Consider S_6 and the following five elements t_i' in S_6:

$$t_1' = (1\ 2)(3\ 4)(5\ 6)$$
$$t_2' = (1\ 4)(2\ 5)(3\ 6)$$
$$t_3' = (1\ 3)(2\ 4)(5\ 6)$$
$$t_4' = (1\ 2)(3\ 6)(4\ 5)$$
$$t_5' = (1\ 4)(2\ 3)(5\ 6).$$

We wish to show the following three statements:

1. $(t_i')^2 = 1$ for each $i = 1, \ldots, 5$, $(t_i' t_j')^2 = 1$ for $|i - j| \geq 2$ and $(t_i' t_{i+1}')^3 = 1$ for each $1 \leq i \leq 4$.
2. S_6 is generated by t_i', $1 \leq i \leq 5$.
3. The map $\varphi : S_6 \to S_6$ given on generators by $(i\ i+1) \mapsto t_i'$ for each $i = 1, \ldots, 5$ is an automorphism.

1. Let $i \in \{1, \ldots 5\}$. Then since each t_i' is a product of disjoint transpositions, therefore $t_i' t_i' = 1$. For the next, observe that all the pairs (i, j) such that $|i - j| \geq 2$ are $(1,3), (1,4), (1,5), (2,4), (2,5), (3,1), (3,5), (4,1), (4,2), (5,1), (5,2), (5,3)$. We show this only for one pair from the above, the rest follows exactly similarly. Let $(i, j) = (5, 3)$. Then

$$\begin{aligned} t_5' t_3' &= (1\ 4)(2\ 3)(5\ 6) \cdot (1\ 3)(2\ 4)(5\ 6) \\ &= (1\ 2)(3\ 4). \end{aligned}$$

Then since $t_5't_3'$ is a product of disjoint transpositions, therefore $(t_5't_3')^2 = 1$, as required. Finally, to show that $(t_i't_{i+1}')^3 = 1$ for each $i = 1, \ldots, 4$, we show this again only for one i, the rest following in the exact same manner. Indeed, let $i = 4$. Then

$$\begin{aligned} t_4't_5' &= (1\ 2)(3\ 6)(4\ 5) \cdot (1\ 4)(2\ 3)(5\ 6) \\ &= (1\ 5\ 3)(2\ 6\ 4). \end{aligned}$$

As $t_4't_5'$ is a product of disjoint 3-cycles, hence it follows at once that $(t_4't_5')^3 = 1$, as required. This completes the proof of item 1.

2. Recall the following presentation of S_n:

$$S_n = \langle t_1, \ldots, t_{n-1} \mid t_i^2 = 1,\ (t_it_{i+1})^3 = 1\ \forall i \text{ and } t_it_j = t_jt_i\ \forall\, |i-j| \geq 2 \rangle.$$

By item 1, we already have five elements $t_1', \ldots, t_5'$ which satisfies $(t_i')^2 = 1 = (t_i't_{i+1}')^3$ for all i. Now since $t_i't_j't_i't_j' = 1$ for each $|i-j| \geq 2$, and since each $t_i' = t_i'^{-1}$, therefore $t_i't_j't_i'^{-1}t_j'^{-1} = t_i't_j't_i't_j' = 1$, as needed.

Thus we have found the required five elements in S_6 which satisfies the relations the generators have to satisfy. Hence, $S_6 = \langle t_1', \ldots, t_5' \rangle$.

3. Let $t_i := (i\ i+1)$. Observe that $\{t_i\}$ and $\{t_i'\}$ both are generating sets of S_6 which satisfy the same relations, that is, both of them gives a presentation of S_6. The φ defined on t_i as $t_i \mapsto t_i'$ gives a unique group homomorphism. Similarly we may define $\psi : S_6 \to S_6$ on the generating set $\{t_i'\}$ as $t_i' \mapsto t_i$. Now it is immediate that $\psi \circ \varphi$ on generating set $\{t_i\}$ maps as $t_i \mapsto t_i$. Thus $\psi \circ \varphi = \mathrm{id}$. Similarly, $\varphi \circ \psi = \mathrm{id}$. Hence, $\varphi : S_6 \to S_6$ is an isomorphism, as required. □

Proof of Question 13.1, 5. Let $\alpha \in \mathbb{Q}$ be a root of a monic polynomial $p(x) \in \mathbb{Z}[x]$. We wish to show that α is an integer.

Let us write $\alpha = \frac{a}{b}$ where we may assume $\gcd(a, b) = 1$. Recall that $\mathbb{Z}$ is a UFD, so the results surrounding Gauss' lemma holds here. As $p(x) \in \mathbb{Q}[x]$ has a zero in $\mathbb{Q}$ given by α, it follows that $bx - a | p(x)$ in $\mathbb{Q}[x]$. As $\gcd(a, b) = 1$, therefore $bx - a$ is a primite polynomial in $\mathbb{Z}[x]$. Hence by general results around Gauss' lemma, we deduce that $bx - a | p(x)$ in $\mathbb{Z}[x]$. Consequently, there exists $q(x) \in \mathbb{Z}[x]$ such that

$$p(x) = (bx - a) \cdot q(x).$$

As $p(x)$ is monic, it follows that the leading coefficient on LHS is 1. Thus, there exists $c \in \mathbb{Z}$ such that $bc = 1$, showing that b is a unit in $\mathbb{Z}$. As the only units of $\mathbb{Z}$ are ± 1, therefore we have $b = \pm 1$. It follows that $\alpha = \frac{a}{b}$ is an integer, as required. □

Proof of Question 13.1, 8. We wish to show that if $a \neq 0, 2, -1$, then the polynomial $p(x) = x^5 - ax - 1 \in \mathbb{Z}[x]$ is irreducible.

First observe that if $q(x) \in \mathbb{Z}[x]$ divides $p(x)$ then $p(x) = q(x) \cdot r(x)$ for some $r(x) \in \mathbb{Z}[x]$. It follows that $q(x)$ and $r(x)$ are monic. It thus suffices to show that there are no linear or

quadratic monic factors of $p(x)$. Indeed, suppose $q(x) = x - n \in \mathbb{Z}[x]$ is a linear factor of $p(x)$. Then, we yield

$$n^5 - an - 1 = 0.$$

We may write this as $n(n^4 - a) = 1$. As n and $n^4 - a$ are integers, therefore we deduce that either $n = 1$ and $n^4 - a = 1$, or $n = -1$ and $n^4 - a = -1$. In both cases, $a = 0$ or $a = 2$, which we assumed to not be the case, hence a contradiction. This shows that $p(x)$ has no linear factors.

In the other case, if $p(x)$ has $x^2 + bx + c$ as a factor, then we may write

$$p(x) = (x^2 + bx + c) \cdot (x^3 + dx^2 + ex + f)$$

for $d, e, f \in \mathbb{Z}$. Expanding the RHS, we deduce that

$$p(x) = x^5 - ax - 1 = x^5 + (b + d)x^4 + (c + bd + e)x^3 + (cd + be + f)x^2 + (bf + ce)x + cf.$$

From this, it follows that

$$\begin{aligned} b + d &= 0 \\ c + bd + e &= 0 \\ cd + be + f &= 0 \\ bf + ce &= -a \\ cf &= -1. \end{aligned}$$

The last equality in particular implies that $c = 1$ and $f = -1$ or $c = -1$ and $f = 1$. Suppose the former is true, that is $c = 1, f = -1$. By fourth equality, we get $-b + e = -a$. Solving the rest, we obtain $d(1 - e) = 1$ and $e = 1 + d^2$. Solving these two yields $d = 1$. It follows that $e = 0$, but then $d^2 = -1$, not possible.

Now suppose the latter is true, that is $c = -1$, $f = 1$. One can then derive from above equations that $d(2 + d^2) = 1$. It follows that $d > 0$. But there is no solution to the above, a contradiction.

This proves that $p(x)$ has a no linear or quadratic factors, hence is irreducible. □

Proof of Question 13.2, 4. We wish to find degree of $\alpha = 2 + \sqrt{3}$ over $\mathbb{Q}$. Observe that for $p(x) = x^2 - 4x + 1 \in \mathbb{Q}[x]$ is such that $p(\alpha) = 0$. Therefore $m_{\alpha,\mathbb{Q}}(x) | p(x)$. As $m_{\alpha,\mathbb{Q}}(x)$ is not linear as $\alpha \notin \mathbb{Q}$, it follows that $m_{\alpha,\mathbb{Q}}(x) = p(x)$.

Next, we wish to find degree of $\beta = 1 + 2^{1/3} + 2^{2/3}$. Observe first that

$$\frac{1}{2^{1/3} - 1} = \frac{(2^{1/3})^3 - 1}{2^{1/3} - 1} = 1 + 2^{1/3} + 2^{2/3} = \beta$$

It follows from above that $\beta \in \mathbb{Q}(2^{1/3})$, so that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(2^{1/3})$. We now claim that $\mathbb{Q}(2^{1/3}) \subseteq \mathbb{Q}(\beta)$. Indeed, as $\beta = (2^{1/3} - 1)^{-1}$, therefore this is immediate. We thus deduce that $\mathbb{Q}(2^{1/3}) = \mathbb{Q}(\beta)$, and thus $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$, as required. □

Proof of Question 13.2, 5. We wish to show that x^3-2 and x^3-3 are irreducible over $F=\mathbb{Q}(i)$. Indeed, it suffices to show that $F[x]/\langle x^3-2\rangle$ and $F[x]/\langle x^3-3\rangle$ are prime ideals (or, equivalently by PID condition, maximal ideals). We first prove this for x^3-2. We wish to show that $F[x]/\langle x^3-2\rangle$ is a domain. Indeed, since $F\cong\mathbb{Q}[y]/\langle y^2+1\rangle$, therefore we get that

$$\frac{F[x]}{x^3-2}\cong\frac{\frac{\mathbb{Q}[y]}{y^2+1}[x]}{x^3-2}\cong\frac{\mathbb{Q}[x,y]}{x^3-2,y^2+1}.$$

Now observe that $\langle x^3-2,y^2+1\rangle$ is a prime ideal in $\mathbb{Q}[x,y]$ as it is the kernel of the following map

$$\begin{aligned}\theta:\mathbb{Q}[x,y]&\longrightarrow\mathbb{C}\\ f(x,y)&\longmapsto f(2^{1/3},i).\end{aligned}$$

Indeed, it is clear that $\langle x^3-2,y^2+1\rangle\subseteq\operatorname{Ker}(\theta)$. Conversely, if $f(x,y)\in\operatorname{Ker}(\theta)$, then the image of $f(x,y)$ in $Q[x,y]/\langle y^2+1\rangle\cong Q(i)[x]$ is $\overline{f(x,y)}$ and is in the ideal $\langle x^3-2\rangle$. Thus, $\overline{f(x,y)}=p(x)\cdot(x^3-2)$ in $Q(i)[x]$. Going back to $\mathbb{Q}[x,y]$, we obtain that $f(x,y)=p(x)\cdot(x^3-2)+q(x,y)\cdot(y^2+1)$, as required. This shows that $\operatorname{Ker}(\theta)=\langle x^3-2,y^2+1\rangle$. Thus, $\langle x^3-2,y^2+1\rangle$ is prime, as required. This completes the proof. One can show that x^3-3 is irreducible in $F[x]$ in the exact same manner. □

Proof of Question 13.2, 17. Let F be a field and $f(x)\in F[x]$ be an irreducible polynomial of degree n. Let $g(x)\in F[x]$. We wish to show that if $p(x)\in F[x]$ is an irreducible factor of $f(g(x))\in F[x]$, then $\deg p(x)$ is a multiple of n.

We translate this problem into finite degree field extensions and their properties. Denote

$$K=\frac{F[x]}{\langle f(x)\rangle}$$

and

$$L=\frac{F[x]}{\langle p(x)\rangle}.$$

Both are field extensions of finite degree over F with $[K:F]=\deg f(x)=n$ and $[L:F]=\deg p(x)$. We claim the following two statements:

1. There is an injective homomorphism $K\hookrightarrow L$.
2. The extension L/K is finite.

This would complete the proof as then we would have

$$\deg p(x)=[L:F]=[L:K]\cdot[K:F]=[L:K]\cdot n,$$

as required. Hence we reduce to proving the above two claims.

For item 1, observe the map

$$\begin{aligned}\theta:F[x]&\longrightarrow F[x]\\ x&\longmapsto g(x).\end{aligned}$$

Consider the ideal $\langle p(x)\rangle \leq F[x]$. We have

$$\begin{aligned}\theta^{-1}(\langle p(x)\rangle) &= \{r(x) \in F[x] \mid p(x) \text{ divides } r(g(x))\} \\ &\supseteq \langle f(x)\rangle.\end{aligned}$$

But since $f(x)$ is irreducible, therefore $\langle f(x)\rangle$ is maximal and since θ is non-trivial, it follows that

$$\theta^{-1}(\langle p(x)\rangle) = \langle f(x)\rangle.$$

We now at once conclude that θ induces the following injection:

$$K = \frac{F[x]}{\langle f(x)\rangle} \hookrightarrow \frac{F[x]}{p(x)} = L,$$

as needed.

We now prove item 2. As finite extensions are equivalent to finitely generated algebraic extensions, therefore we reduce to showing that L/K is finitely generated and algebraic. Since L/F is algebraic and $K \supseteq F$, therefore we immediately, deduce that L/K is algebraic. We hence need only show that L/K is a finitely generated K-algebra.

To this end, we first observe that L is generated by one element over F as we have a surjection $F[y] \twoheadrightarrow L$ given by $y \mapsto \bar{x}$. We also have an injection $F[y] \hookrightarrow K[y]$ given by $y \mapsto y$, which extends the inclusion $F \hookrightarrow K$. Now consider the map $F[y] \to L$ given by $y \mapsto \bar{x}$. We have the following comutative diagram:

$$\begin{array}{ccc} K[y] & & \\ \uparrow & \searrow & \\ F[y] & \twoheadrightarrow & L \end{array} .$$

The commutativity of the above triangle immediately forces the map $K[y] \to L$ to be surjective. This shows that L is generated by a single image as a K-algebra, as needed. This completes the proof. □

5 Week 5 : Degree, splitting fields & normal extensions

Proof of Question 13.2, 22. Let K/F be a field and $K \supseteq K_1, K_2 \supseteq F$ be two subfields. We wish to show that the following are equivalent:

1. $K_1 \otimes_F K_2$ is a field.
2. $[K_1K_2 : F] = [K_1 : F] \cdot [K_2 : F]$.

(1. $\Rightarrow$ 2.) We first show that $K_1 \otimes_F K_2 \cong K_1K_2$. This would suffice as $\dim_F(K_1 \otimes_F K_2) = \dim_F K_1 \cdot \dim_F K_2$, which is equivalent to thus $[K_1K_2 : F] = [K_1 : F][K_2 : F]$. Indeed, consider the bilinear mapping $f : K_1 \times K_2 \to K_1K_2$ given by $(k_1, k_2) \mapsto k_1k_2$. Consequently, we get a map $\varphi : K_1 \otimes_F K_2 \to K_1K_2$ which maps on simple tensors as $k_1 \otimes k_2 \mapsto k_1k_2$. As $K_1 \otimes_F K_2$ is a field, it suffices to show that φ is a surjection. Indeed, it suffices to show that $K_1, K_2 \subseteq \mathrm{Im}\,(\varphi)$. Indeed, as $\varphi(k_1 \otimes 1) = k_1$ and $\varphi(1 \otimes k_2) = k_2$, therefore $\mathrm{Im}\,(\varphi) \supseteq K_1K_2$,

thus $\mathrm{Im}\,(\varphi) = K_1K_2$, as required.

($2. \Rightarrow 1.$) Consider the above map $\varphi : K_1 \otimes_F K_2 \to K_1K_2$ which we showed to be surjective. Considering φ as an F-linear map, we see that $\dim_F K_1 \otimes_F K_2 = \dim_F K_1 \cdot \dim_F K_2 = [K_1 : F] \cdot [K_2 : F] = [K_1K_2 : F] = \dim_F K_1K_2$. It follows that φ is an isomorphism, thus showing that $K_1 \otimes_F K_2$ is a field as K_1K_2 is a field. □

Proof of Question 13.4, 3. We wish to find the splitting field of $p(x) = x^4 + x^2 + 1$ and its degree. Indeed, observe that we can write

$$p(x) = (x+1)(x-1)(x-\omega^2)(x+\omega^2)(x-\omega)(x+\omega).$$

Then the splitting field is $\mathbb{Q}(\omega)$ and its degree is 2. □

Proof of Question 13.4, 4. We wish to find splitting field of $p(x) = x^6 - 4$ and its degree. Indeed, observe that we can write

$$p(x) = (x - 2^{1/3})(x - \omega 2^{1/3})(x - \omega^2 2^{1/3})(x + 2^{1/3})(x + \omega 2^{1/3})(x + \omega^2 2^{1/3}).$$

Then the splitting field is $\mathbb{Q}(\omega, 2^{1/3})$ and its degree 6 as $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$ have gcd 1. □

Proof of Question 13.4, 5. Let K/F be a finite extension. Then the following are equivalent:

1. K/F is a splitting field.
2. For every irreducible polynomial $g(x) \in F[x]$ which has a root in K, $g(x)$ has all roots in K.

($1. \Rightarrow 2.$) Pick any irreducible $g(x) \in F[x]$ such that it has a root $\alpha \in K$. Let β be another root of $g(x)$ in the algebraic closure. We wish to show that β is in K. Observe that since β is a root of $g(x)$, therefore we can lift $\mathrm{id} : F \to F$ to an isomorphism $F(\alpha) \to F(\beta)$ which fits in the following diagram:

$$\begin{array}{ccc} F(\alpha) & \xrightarrow[\psi]{\cong} & F(\beta) \\ \uparrow & & \uparrow \\ F & \xrightarrow[\mathrm{id}]{} & F \end{array} .$$

Observe that $\psi(f(x)) = f(x)$. Now, we can further lift ψ to an isomorphism of the splitting fields of $f(x)$ over $F(\alpha)$ and $F(\beta)$ as

$$\begin{array}{ccc} L_1 & \xrightarrow[\cong]{\theta} & L_2 \\ \uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\psi]{\cong} & F(\beta) \end{array}$$

where L_1 is the splitting field of $f(x)$ over $F(\alpha)$ and L_2 is the splitting field of $f(x)$ over $F(\beta)$.

We now claim that $L_1 = K(\alpha)$. Indeed, as L_1 contains all roots of $f(x)$, therefore

$L_1 \supseteq K$ and thus $L_1 \supseteq K(\alpha)$. Conversely, $L_1 \subseteq K(\alpha)$ as $K(\alpha)$ contains all roots of $f(x)$ over $F(\alpha)$, therefore $L_1 \subseteq K(\alpha)$. Hence $L_1 = K(\alpha)$. Similarly, we get that $L_2 = K(\beta)$.

As $\alpha \in K$, it follows that $K(\alpha) = K$. Hence $\theta : K \cong K(\beta)$. As both K and $K(\beta)$ are both 1-dimensional K-vector spaces, therefore $\beta \in K$, as required.

(2. $\Rightarrow$ 1.) We construct a polynomial $f(x) \in F[x]$ such that K is the splitting field of F. Indeed, as K/F are finite, therefore $K = F(\alpha_1, \ldots, \alpha_n)$ is a finitely generated algebraic extension over F. Let $p_1, \ldots, p_n \in F[x]$ be minimal polynomials of $\alpha_1, \ldots, \alpha_n$ respectively. Define

$$f(x) = p_1(x) \cdot \cdots \cdot p_n(x) \in F[x].$$

We claim that K is the splitting field of $f(x)$ over F. Indeed, let L/F be the splitting field of $f(x)$ over F. As each $p_i(x) \in F[x]$ is irreducible and has a root in K, namely α_i, it follows by our hypothesis that $p_i(x)$ splits into linear factors over K, for each $i = 1, \ldots, n$. Thus, $f(x)$ is split into linear factors over K and thus $L \subseteq K$. For the converse, as L contains α_i as α_i is a root of $p_i(x)$, and also contains F, thus L contains $K = F(\alpha_1, \ldots, \alpha_n)$. Thus $L = K$, as required. This completes the proof. $\square$

6 Week 6 : Irreducible & separable polynomials, perfect fields

Proof of Question 9.4, 16. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ be a polynomial and consider the reverse polynomial $f_!(x) := x^n f(1/x)$. We first wish to find coefficients of $f_!$ in terms of coefficients of f. Observe that

$$\begin{aligned} f_!(x) &= x^n f(1/x) \\ &= x^n \left(a_n \frac{1}{x^n} + \cdots + a_1 \frac{1}{x} + a_0 \right) \\ &= a_n + a_{n-1} x + \cdots + a_1 x^{n-1} + a_0 x^n. \end{aligned}$$

Thus, if $c_k(f_!)$ denotes the coefficient of x^k in $f_!(x)$ for $0 \leq k \leq n$, then we have

$$c_k(f_!) = a_{n-k}$$

for each $0 \leq k \leq n$.

We next wish to show that $f(x)$ is irreducible if and only if $f_!(x)$ is irreducible. Indeed, first observe that $f_{!!} I(x) = f(x)$, so we need only show that $f(x)$ is irreducible implies $f_!(x)$ is irreducible. To this end, suppose $f_!(x)$ is not irreducible so that we have

$$f_!(x) = g(x)h(x)$$

where $g, h \in F[x]$ and $1 \leq \deg g(x), \deg h(x) \leq n$ with $\deg g(x) = m_1$ and $\deg h(x) = m_2$ clearly with $m_1 + m_2 = n$. Now,

$$\begin{aligned} f(x) = f_{!!}(x) &= x^n g(1/x) h(1/x) \\ &= x^{m_1+m_2} g(1/x) x^{m_2} h(1/x) \\ &= x^{m_1} g(1/x) x^{m_2} h(1/x) \\ &= g_!(x) h_!(x) \end{aligned}$$

where $1 \leq \deg g_!(x), \deg h_!(x) \leq n$. Hence, this shows that $f(x)$ is not irreducible, a contradiction. □

Proof of Question 13.5, 2. We wish to first find all irreducible polynomials of degrees 1, 2 and 4 over $\mathbb{F}_2$.

1. For degree 1, we have the following two irreducibles : $x, x+1$.
2. For degree 2, we first find degree 2 reducibles by multiplying all degree 1 irreducibles: $x(x+1) = x^2 + x, x^2, (x+1)^2 = x^2 + 1$. Thus, any polynomial in $\mathbb{F}_2$ of degree 2 which is not one of the above has to be irreducible. As there are only four degree 2 polynomials, it follows that there is only one degree 2 irreducible polynomial, namely $x^2 + x + 1$.
3. For degree 4, we again first find all degree 4 reducibles. Indeed if $p(x) \in \mathbb{F}_2[x]$ is a degree 4 reducible, then $p(x) = f(x)g(x)$ for $f(x), g(x) \in \mathbb{F}_2[x]$ with $1 \leq \deg f(x), \deg g(x) \leq 3$ and $\deg f(x) + \deg g(x) = 4$. Let us state all the eight degree 3 polynomials as well here: $x^3, x^3+1, x^3+x, x^3+x^2, x^3+x+1, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1$. Thus, we have the following cases for degrees of f and g:
   (a) If $\deg f(x) = \deg g(x) = 2$. In this case, the degree 4 reducibles we get by multiplying two degree 2 polynomials are: $x^4+x^2, x^4+x^3, x^4+x^3+x^2+x, x^4, x^4+1$.
   (b) If $\deg f(x) = 1$ and $\deg g(x) = 3$. In this case, $p(x)$ is obtained by multiplying a degree 3 polynomial with either x or $x+1$. Thus we get following degree 4 reducibles corresponding to this case which are not already in item (a): $x^4 + x, x^4 + x^3 + x + 1, x^4 + x^2 + x, x^4 + x^3 + x^2 + 1, x^4 + x^3 + x, x^4 + x^2 + x + 1, x^4 + x^3 + x^2, x^4 + x$.

   Using these two cases, we get total twelve reducible degree 4 polynomials. Consequently, the rest four are going to be the only degree 4 irreducible polynomials and they are:
   - $x^4 + x + 1$
   - $x^4 + x^2 + 1$
   - $x^4 + x^3 + 1$
   - $x^4 + x^3 + x^2 + x + 1$.

   This completes the proof.

□

Proof of Question 13.2, 5. Pick any prime p and any non-zero element $a \in \mathbb{F}_p$. We wish to show that $f(x) = x^p - x + a \in \mathbb{F}_p[x]$ is irreducible and separable over $\mathbb{F}_p$.

We first immediately see that $f(x)$ is separable as $f'(x) = -1$, so has no roots and

thus $f(x)$ and $f'(x)$ have no roots in common. It follows that $f(x)$ has p distinct roots in $\overline{\mathbb{F}_p}$. We now show irreducibility of $f(x)$. Our main idea is to show that $f(x)$ is a minimal polynomial of some element in the algebraic closure, namely a root of $f(x)$.

Let $K/\mathbb{F}_p$ be the splitting field of $f(x)$. As $K = \mathbb{F}_p(\alpha_1, \ldots, \alpha_p)$, where $\alpha_i \in \overline{\mathbb{F}_p}$ are roots of $f(x)$. Observe that if α is a root of $f(x)$, then so is $\alpha + 1$ as $(\alpha+1)^p - (\alpha+1) + a = \alpha^p + 1 - \alpha - 1 + a = \alpha^p + 1 - \alpha - 1 + a = 1 - 1 = 0$. Hence, denoting $\alpha = \alpha_1$, we see that all roots of $f(x)$ are $S = \{\alpha, \alpha+1, \ldots, \alpha+(p-1)\}$. Consequently, $K = \mathbb{F}_p(\alpha_1, \ldots, \alpha_p) = \mathbb{F}_p(\alpha)$.

Now, the splitting field $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a finite extension where the minimal polynomial $m_{\alpha,\mathbb{F}_p}(x) \in \mathbb{F}_p[x]$ divides $f(x)$. We claim that $\deg m_{\alpha,\mathbb{F}_p}(x) = \deg f(x)$. This will imply that $f(x) = m_{\alpha,\mathbb{F}_p}(x)$ and since the latter is irreducible, therefore so is $f(x)$ and we would be done. To see that $\deg m_{\alpha,\mathbb{F}_p}(x) = \deg f(x)$, let us assume to the contrary that $m_{\alpha,\mathbb{F}_p}(x)$ has degree atleast 1 lower than that of $f(x)$. Thus $m_{\alpha,\mathbb{F}_p}$ doesn't have every element in S as its zero. Consequently, the sum of roots of $m_{\alpha,\mathbb{F}_p}(x)$ would become $k\alpha + r$ where $1 \leq k \leq p-1$ and $r \in \mathbb{F}_p$. As sum of roots is a coefficient of $m_{\alpha,\mathbb{F}_p}$, therefore $k\alpha + r \in \mathbb{F}_p$. It follows that $k\alpha \in \mathbb{F}_p$, but k is invertible in $\mathbb{F}_p$, so $\alpha \in \mathbb{F}_p$, a contradiction. This completes the proof. □

Proof of Question 13.5, 11. Let K/F be a field extension such that F is perfect and $f(x) \in F[x]$ has no repeated irreducible factors in $F[x]$. We wish to show that $f(x)$ has no repeated irreducible factors in $K[x]$.

Let $f(x) = p_1(x) \ldots p_k(x)$ for $p_i(x) \in F[x]$ irreducible. As F is perfect, therefore $p_i(x)$ are further separable. Consequently, write $p_i(x) = q_{i1}(x) \ldots q_{il_i}(x)$ where $q_{ij} \in K[x]$ are irreducible for each $1 \leq i \leq k$. Thus we obtain a decomposition of $p(x)$ into product of irreducibles $q_{ij}(x)$ over K. We claim that none of $q_{ij}(x)$ repeat. Suppose they do, then we have two cases.

1. Suppose $q_{ij}(x) = q_{ij'}(x)$ for $j \neq j'$. It follows that $p_i(x)$ has a repeated irreducible factor in $K[x]$. To get a contradiction it would suffice to show that a separable polynomial $p(x) \in F[x]$ remains separable in $K[x]$. This is what we prove now.
   Indeed, suppose $p(x)$ is inseparable over K. Thus, there exists $\alpha \in \overline{K}$ which is a repeated root of $p(x)$ where $\overline{K}$ is an algebraic closure of K containing F. Thus, $\alpha \in \overline{F} \subseteq \overline{K}$. It follows that $p(x)$ has a repeated root in $\overline{F}$, which is a contradiction to the separability of $p(x)$ over F.
2. Suppose $q_{ij}(x) = q_{kj'}(x)$ for $i \neq k$. We thus have that $p_i(x)$ and $p_j(x)$ share a common factor in $K[x]$ for some $i \neq j$, thus a common root α in an algebraic closure $\overline{K}$ of K which contains F. Hence, $m_{\alpha,F}(x) \in F[x]$ divides both $p_i(x)$ and $p_j(x)$. Since $p_i(x)$ and $p_j(x)$ are irreducible, therefore $p_i(x) = m_{\alpha,F}(x) = p_j(x)$, a contradiction to the assumption that $p_i(x)$ and $p_j(x)$ are distinct.

This shows that all $q_{ij}(x)$ are distinct irreducible over K. By unique factorization of $K[x]$, we conclude the proof. □

Proof of Question 14.1, 4. We wish to show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic fields. Indeed, suppose $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ is a field isomorphism. Since

$$n = n\varphi(1) = \varphi(n) = \varphi\left(\frac{n}{m} \cdot m\right) = m\varphi\left(\frac{n}{m}\right),$$

thus $\varphi(n/m) = n/m$ for all $n/m \in \mathbb{Q}$. It follows that φ is $\mathbb{Q}$-linear. Now, we see that

$$2 = \varphi(2) = \varphi((\sqrt{2})^2) = \varphi(\sqrt{2})^2.$$

Thus, $\varphi(\sqrt{2})$ is an element in $\mathbb{Q}(\sqrt{3})$ whose square is 2. We show that there is no element in $\mathbb{Q}(\sqrt{3})$ whose square is 2. Indeed, if $a+b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ for $a, b \in \mathbb{Q}$ such that $(a+b\sqrt{3})^2 = 2$, thus

$$(a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3} = 2.$$

Hence,

$$\begin{aligned} a^2 + 3b^2 &= 2 \\ 2ab &= 0. \end{aligned}$$

It thus follows that either a or b is 0, so we may assume (WLOG) that $a = 0$. Hence $3b^2 = 2$, thus $b^2 = 2/3$ and $b = \pm\frac{\sqrt{2}}{\sqrt{3}}$, a contradiction to the fact that $a, b \in \mathbb{Q}$. □

Proof of Question 14.1, 6. a) Let k be a field and $f : k[t] \to k[t]$ be defined by $t \mapsto at+b$ for fixed $a, b \in k$ with $a \neq 0$. We wish to show that f is an automorphism of $k[t]$.

Indeed, consider the map $g : k[t] \to k[t]$ defined by $t \mapsto \frac{1}{a}(t - b)$. This is a homomorphism. We wish to show that this is the inverse of f. Indeed, we see that $f \circ g(t) = f(g(t)) = f(\frac{1}{a}(t-b)) = a \cdot \frac{1}{a}(t-b) + b = t = \mathrm{id}(t)$. For the other side, $g \circ f(t) = g(at + b) = \frac{1}{a}(at + b) - b = t = \mathrm{id}(t)$. Thus f is an isomorphism. Moreover, $f(c) = c$ for all $c \in k$, thus f is a k-algebra isomorphism.

b) Let $\varphi : k[t] \to k[t]$ be a k-algebra isomorphism. We wish to show that $\varphi(t) = at + b$ for some $a, b \in k$ and $a \neq 0$.

Indeed, let $\varphi(t) = a_n t^n + \cdots + a_1 t + a_0$, $a_i \in k$. Suppose $\mathrm{char} k = p$. Fix $m > 1$ in $\mathbb{Z}$ such such that $m \neq p$ and choose any $m > 1$ if $\mathrm{char} k = 0$. As $m = 1 + \cdots + 1$ m-times in k and $\varphi(mt) = m\varphi(t)$ since φ is k-linear, therefore we deduce that

$$a_n m t^n + \cdots + a_1 m t + a_0 m = a_n m^n t^n + \cdots + a_1 m t + a_0.$$

Now, if $a_i \neq 0$ for some $i \geq 2$, then we would have

$$a_i m = a_i m^i$$

in k, from which it follows that $a_i = a_i m^{i-1}$ and since $i - 1 \geq 1$, it follows that

$$m^{i-1} = 1,$$

a contradiction as $m > 1$ in $\mathbb{Z}$. □

Proof of Question 14.1, 7. We wish to show that $\mathrm{Aut}\,(()\mathbb{R}/\mathbb{Q})$ is a singleton. We will do this by showing that any $\sigma \in \mathrm{Aut}\,(()\mathbb{R}/\mathbb{Q})$ necessarily fixes $\mathbb{Q}$ and is continuous. We will then show that any continuous function $\mathbb{R} \to \mathbb{R}$ which is id on $\mathbb{Q}$ is itself id.

First let us see that any $\sigma \in \mathrm{Aut}\,((\,)\mathbb{R}/\mathbb{Q})$ fixes $\mathbb{Q}$. Indeed, we need only observe the following for any $m, n \in \mathbb{Z}$.

$$n = n\sigma(1) = \sigma(n) = \sigma\left(\frac{n}{m} \cdot m\right) = m\sigma\left(\frac{n}{m}\right),$$

which thus shows that $\sigma(n/m) = n/m$.

Next, we show that σ is continuous. To this end, we first show that σ is order preserving. Indeed, if $a > 0$ in $\mathbb{R}$, then $a = c^2$ for some $c > 0$. As $\sigma(a) = \sigma(c)^2 > 0$ where $\sigma(c) \neq 0$ as σ is an isomorphism, therefore σ takes positive real number to positive reals. Consequently, if $a - b > 0$, then $\sigma(a - b) > 0$ and thus $\sigma(a) > \sigma(b)$, as required.

To conclude that σ is continuous, we wish to show that for all every $x_0 \in \mathbb{R}$ and for all $\epsilon > 0$, there exists $\delta > 0$ such that $|x - x_0| < \delta \implies |\sigma(x) - \sigma(x_0)| < \epsilon$. Indeed, we see that for any $m \in \mathbb{Z}$ such that $0 < \frac{1}{m} < \epsilon$, we have that if

$$\sigma(x) - \sigma(x_0) = \sigma(x - x_0) < \frac{1}{m}$$

for some $x \in \mathbb{R}$, then applying σ^{-1} yields $x - x_0 < \frac{1}{m}$ as σ^{-1} is also $\mathbb{Q}$-linear. This conclusion can be reversed and we thus see that,

$$\sigma(x) - \sigma(x_0) < \frac{1}{m} \iff x - x_0 < \frac{1}{m}.$$

This shows that we may take δ to be $1/m$. Hence, σ is continuous.

Finally to complete the proof, we see that σ is id on $\mathbb{Q}$ and is continuous. Pick any irrational $r \in \mathbb{R}$ and let $q_n \to r$ be a sequence of rationals converging to r. Using continuity of σ and id on $\mathbb{Q}$, we conclude that $\sigma(q_n) = q_n \to \sigma(r)$. As $\mathbb{R}$ is Hausdorff, so limits are unique. We conclude that $\sigma(r) = r$. This completes the proof. □

7 Week 7 : Direct computations of Galois groups, norm and trace, cyclotomic & Kronecker-Weber

Proof of Question 13.6, 3. Let F be a field and $n \in \mathbb{N}$ be odd. Let F contain all n^{th}-roots of unity, μ_n. We wish to show that F contains $2n^{\text{th}}$-roots of unity as well.

Indeed, let $\zeta \in F$ be a primitive n^{th}-root of unity. Note that $-1 \notin \mu_n$ as $(-1)^n \neq 1$ as n is odd. Consequently, we claim that $-\zeta_n$ is a primitive $2n^{\text{th}}$-root of unity. Indeed, we see that $-\zeta_n$ is a $2n^{\text{th}}$-root of unity as $(-\zeta)^{2n} = (-1)^{2n} \cdot \zeta^{2n} = (\zeta^n)^2 = 1$. Thus $-\zeta \in \mu_{2n}$. Furthermore, $-\zeta$ is a primitive root of unity as if the order of $-\zeta$ is $k|2n$ in μ_{2n}, then either $k = 2l$ for some $l|n$ or $k|n$. If the former, then $(-\zeta)^{2l} = 1$, from which it follows that $\zeta^{2l} = 1$. Thus $2l|n$ as ζ is an element of order n in μ_{2n}, which is a contradiction as n is odd, so no even number can divide it.

If the latter, then $k|n$. Thus, $(-\zeta)^k = 1$ from which it follows that $\zeta^k = (-1)^k$. Clearly, $k \neq n$ as otherwise $\zeta^n = (-1)^n \neq 1$, a contradiction to the fact that $\zeta \in \mu_n$. Thus, $k < n$. As n is odd, therefore k is odd. Consequently we have that $\zeta^k = -1$ for some $k|n$, $k < n$. It follows that μ_n contains -1. This is a contradiction as -1 is not an n^{th}-root of unity since n is odd.

Hence, we have shown that $-\zeta \in F$ is a primitive $2n^{\text{th}}$-root of unity in F, as required. □

Proof of Question 13.6, 9. a) Let $A \in M_n(\mathbb{C})$ be an $n \times n$ matrix such that $A^k = I$ for some $k \geq 1$, that is, A is nilpotent. We first wish to show that A is diagonalizable.

By general theory of linear algebra, we need only show that the minimal polynomial of A is split into distinct linear factors over $\mathbb{C}$ in order to conclude that A is diagonalizable. Let $m(x) \in \mathbb{C}[x]$ be the minimal polynomial of A. Then, $m(x)|x^k - 1$ as $A^k - I = 0$. As $\mathbb{C}$ is algebraically closed, it follows that $m(x)$ has all roots which are k^{th}-roots of unity in $\mathbb{C}$. As all k^{th}-roots of unity are distinct, thus, $m(x)$ is split into distinct linear factors, as required.

b) Consider the matrix

$$A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$$

for $\alpha \in \mathbb{F}_p$ and $\alpha \neq 0$ where $p \in \mathbb{Z}$ is a prime. We first wish to show that $A^p = I$. Indeed, observe that

$$A^n = \begin{bmatrix} 1 & n\alpha \\ 0 & 1 \end{bmatrix}.$$

As $\text{char}\mathbb{F}_p = p$, therefore $A^p = I$.

We next wish to show that A cannot be diagonalized. Indeed, we need only show that the minimal polynomial $p(x) \in \mathbb{F}_p[x]$ of A is not split into distinct roots over $\mathbb{F}_p[x]$. Observe that $p(x)|(x-1)^2$ as $(A-I)^2 = 0$. Consequently, $p(x) = x - 1$ or $(x-1)^2$. Since $A \neq I$, therefore $p(x) = (x-1)^2$, thus $p(x)$ is not split into distinct linear factors, as required. $\square$

Proof of Question 14.2, 6. Let $K = \mathbb{Q}(2^{1/8}, i)$, $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(2^{1/2})$ and $F_3 = \mathbb{Q}(i2^{1/2})$. We wish to show the following three computations:

1. $\text{Gal}\,(K/F_1) \cong \mathbb{Z}/8\mathbb{Z}$.
2. $\text{Gal}\,(K/F_2) \cong D_8$.
3. $\text{Gal}\,(K/F_3) \cong Q_8$.

Before beginning, we show that all three extensions are Galois. Indeed, observe that

1. $m_{2^{1/8},F_1}(x) = x^8 - 2$ and $m_{i,F_1}(x) = x - i$,
2. $m_{2^{1/8},F_2}(x) = x^4 - 2^{1/2}$ and $m_{i,F_2}(x) = x^2 + 1$,
3. $m_{2^{1/8},F_3}(x) = x^8 - 2$ and $m_{i,F_3}(x) = x^2 + 1$.

All three are separable (as seen by taking derivatives) and is split into linear factors in K. Thus they are all Galois. Note that each K/F_i has degree 8, thus, each has Galois group of size 8. Further observe that the polynomial $x^8 - 2$ splits over K as

$$x^8 - 2 = (x - \sqrt{i}2^{1/8})(x + \sqrt{i}2^{1/8})(x - i2^{1/8})(x + i2^{1/8})(x - 2^{1/8})(x + 2^{1/8})(x - i^{3/2}2^{1/8})(x + i^{3/2}2^{1/8}).$$

1. Consider the F_1-automotphism of K which on $2^{1/8}$ obtained by extending $\text{id} : F_1 \to F_1$ to $K \to K$ mapping

$$\sigma : 2^{1/8} \mapsto \sqrt{i}2^{1/8}.$$

This is because $2^{1/8}$ and $\sqrt{i}2^{1/8}$ are F_1-conjugates. Then we see that

$$\begin{aligned}
\sigma^2 &: 2^{1/8} \mapsto i2^{1/8} \\
\sigma^3 &: 2^{1/8} \mapsto i^{3/2}2^{1/8} \\
\sigma^4 &: 2^{1/8} \mapsto -2^{1/8} \\
\sigma^5 &: 2^{1/8} \mapsto -i^{1/2}2^{1/8} \\
\sigma^6 &: 2^{1/8} \mapsto -i2^{1/8} \\
\sigma^7 &: 2^{1/8} \mapsto -i^{3/2}2^{1/8} \\
\sigma^8 &: 2^{1/8} \mapsto 2^{1/8}.
\end{aligned}$$

Thus, we get that $\sigma \in \mathrm{Gal}\,(K/F_1)$ is an element of order 8, thus $\mathrm{Gal}\,(K/F_1)$ is a cyclic group isomorphic to $\mathbb{Z}/8\mathbb{Z}$.

2. We first show that there exists $\sigma, \tau \in \mathrm{Gal}\,(K/F_2)$ of order 4 and 2 respectively. Indeed, any $\kappa \in \mathrm{Gal}\,(K/F_2)$ is completely determined by its values on $2^{1/8}$ and i. Furthermore, any such κ has to map $2^{1/8}$ and i to its F_2-conjugates. Thus, consider the following maps

$$\begin{aligned}
\sigma : 2^{1/8} &\longmapsto i2^{1/8} \\
i &\longmapsto i
\end{aligned}$$

and

$$\begin{aligned}
\tau : 2^{1/8} &\longmapsto 2^{1/8} \\
i &\longmapsto -i.
\end{aligned}$$

Observe that $\sigma, \tau \in \mathrm{Gal}\,(K/F_2)$ since $\sigma : K \to K$ is a $\mathbb{Q}$-automorphism such that $\sigma(2^{1/2}) = \sigma(2^{1/8})^4 = (i2^{1/8})^4 = 2^{1/2}$. Thus, σ is also a $\mathbb{Q}(2^{1/2})$-automorphism. Similarly, $\tau : K \to K$ is a $\mathbb{Q}$-automorphism and since $\tau(2^{1/2}) = \tau(2^{1/8})^4 = (2^{1/8})^4 = 2^{1/2}$, therefore τ is a $\mathbb{Q}(2^{1/2})$-automorphism of K.

Now, observe that $\sigma, \tau \in \mathrm{Gal}\,(K/F_2)$ are order 4 and 2 elements respectively. It now suffices to show that $\tau\sigma\tau^{-1} = \sigma^{-1}$. Indeed, we need to check the equality only for elements $2^{1/8}$ and i. To this end, we have

$$\tau\sigma\tau^{-1}(2^{1/8}) = \tau\sigma(2^{1/8}) = \tau(i2^{1/8}) = -i2^{1/8}$$

and

$$\sigma^{-1}(2^{1/8}) = \sigma^{-1}(-i^2 2^{1/8}) = \sigma^{-1}(-i)\sigma^{-1}(i2^{1/8}) = -i2^{1/8},$$

as required. Similarly,

$$\tau\sigma\tau^{-1}(i) = \tau\sigma(-i) = \tau(-i) = i$$

and

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

This completes the proof that $\mathrm{Gal}\,(K/F_2) \cong D_8$.

3. To show that $\mathrm{Gal}\,(K/F_3) \cong Q_8$, we have to find four elements $e, \alpha, \beta, \gamma \in \mathrm{Gal}\,(K/F_3)$ such that $\alpha^2 = \beta^2 = \gamma^2 = \alpha\beta\gamma = e$ and $e^2 = \mathrm{id}$. Note that any $\kappa \in \mathrm{Gal}\,(K/F_3)$ is determined by its value on $2^{1/8}$ and i. We thus consider the following maps:

$$\begin{aligned} e : 2^{1/8} &\mapsto -2^{1/8} \\ i &\mapsto i \\ \alpha : 2^{1/8} &\mapsto i2^{1/8} \\ i &\mapsto i \\ \beta : 2^{1/8} &\mapsto i^{3/2}2^{1/8} \\ i &\mapsto -i \\ \gamma : 2^{1/8} &\mapsto \sqrt{i}2^{1/8} \\ i &\mapsto -i. \end{aligned}$$

It is immediate that $e^2 = \mathrm{id}$. Further, one checks immediately that $\alpha^2 = \beta^2 = \gamma^2 = e$ and $\alpha\beta\gamma = e$. Thus, we need only show that each one of the above is a $\mathbb{Q}(i2^{1/2})$-automorphism, that is, we wish to show that they take $i2^{1/2}$ to $i2^{1/2}$. Indeed, for any automorphism $\kappa : K \to K$, we have

$$\kappa(i2^{1/2}) = \kappa(i) \cdot \kappa(2^{1/8})^4.$$

Using this, one immediately sees that each e, α, β, γ fixes $i2^{1/2}$, as needed. □

Proof of Question 14.2, 12. We wish to find the Galois group of polynomial $f(x) = x^4 - 14x^2 + 9 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

We claim that the Galois group of $f(x)$ is isomorphic to V_4, the Klein 4-group. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. We wish to find the Galois group of $K/\mathbb{Q}$. To this end, we first need to find K. Indeed, we first see that over $\bar{\mathbb{Q}}$, we can write (let $\alpha = \sqrt{7 + 2\sqrt{10}}$ and $\beta = \sqrt{7 - 2\sqrt{10}}$)

$$x^4 - 14x^2 + 9 = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta).$$

Moreover, observe that $\beta = 9 \cdot \alpha^{-1}$. Thus, we claim that

$$K = \mathbb{Q}(\alpha).$$

Indeed, as $\mathbb{Q}(\alpha)$ by above has both α and β, therefore $\mathbb{Q}(\alpha) \supseteq K$. To show equality, it suffices to show that $[\mathbb{Q}(\alpha) : K] = 1$. Indeed, we have

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : K] \cdot [K : \mathbb{Q}].$$

Note that $f(x) \in \mathbb{Q}[x]$ is irreducible as is clear from its splitting in K above. Thus, $f(x) = m_{\alpha,\mathbb{Q}}(x)$. It follows that

$$4 = \deg f(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

We further claim that $[K : \mathbb{Q}] \geq 4$. Indeed, as $f(x)$ is separable since it has no common root with its degree and K is splitting field of $f(x)$, it follows that $K/\mathbb{Q}$ is Galois and thus finite normal in particular. Consequently, $\mathrm{Gal}\,(K/\mathbb{Q})$ has same size $[K : \mathbb{Q}]$ and has to act transitively on the roots of $f(x)$ in K. But there are four roots of $f(x)$ in K and thus there are atleast four elements in $\mathrm{Gal}\,(K/\mathbb{Q})$ and thus $[K : \mathbb{Q}] \geq 4$. This proves that $[\mathbb{Q}(\alpha) : K] = 1$, as required.

Having found the splitting field K as $\mathbb{Q}(\alpha)$ which is a degree 4 extension of $\mathbb{Q}$, we now need only find its Galois group. As $|\mathrm{Gal}\,(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4$, therefore $\mathrm{Gal}\,(K/\mathbb{Q})$ is a group of order 4. We now consider following maps $K \to K$, which we prescribe to be identity on $\mathbb{Q}$ and thus define only on α:

$$\begin{aligned} \sigma &: \alpha \mapsto \beta \\ \tau &: \alpha \mapsto -\beta. \end{aligned}$$

Observe that $\sigma^2(\alpha) = \sigma(\beta) = \sigma(9\alpha^{-1}) = 9\sigma(\alpha)^{-1} = 9(\beta)^{-1} = 9(9\alpha^{-1})^{-1} = \alpha$. Similarly, $\tau^2(\alpha) = \alpha$. Hence, σ and τ are automorphisms of $K = \mathbb{Q}(\alpha)$ and both are order 2 elements in $\mathrm{Aut}\,(()K)$. Since both σ and τ fix $\mathbb{Q}$, thus $\sigma, \tau \in \mathrm{Gal}\,(K/\mathbb{Q})$ are order 2 elements. Now consider $\sigma\tau \in \mathrm{Gal}\,(K/\mathbb{Q})$. We can see that $(\sigma\tau)^2(\alpha) = \alpha$, thus showing that $(\sigma\tau)^2 = \mathrm{id}$. Hence, we have shown that $\mathrm{Gal}\,(K/\mathbb{Q})$ has two elements σ, τ such that $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{id}$. This shows that

$$\mathrm{Gal}\,(K/\mathbb{Q}) \cong V_4,$$

where V_4 is the Klein 4-group. □

Proof of Question 14.2, 31. Let K/F be a finite extension of degree n and $\alpha \in K$. We wish to show the following three items:

1. Element α acting by left multiplication on K is an F-linear transformation, which we denote by $T_\alpha : K \to K$.
2. The minimal polynomial of element $\alpha \in K$, denoted $m_{\alpha,F}(x)$ is same as the minimal polynomial of the F-linear map $T_\alpha : K \to K$, denoted $p(x) \in F[x]$.
3. The norm $N_{K/F}(\alpha)$ and trace $\mathrm{Tr}_{K/F}(\alpha)$ are respectively the determinanat and trace of the F-linear map T_α.

1. Indeed, $T_\alpha : K \to K$ is given by $x \mapsto \alpha x$ which F-linear as $T_\alpha(x + cy) = \alpha(x + cy) = \alpha x + c\alpha y = T_\alpha(x) + cT_\alpha(y)$ where $c \in F$.

2. As $m_{\alpha,F}(x)$ is irreducible, we need only show that $p(x)|m_{\alpha,F}(x)$. Note that $m_{\alpha,F}(T_\alpha) = 0$ since for any $z \in K$, we have

$$m_{\alpha,F}(T_\alpha)(z) = m_{\alpha,F}(\alpha)z = 0.$$

Hence $p(x)|m_{\alpha,F}(x)$, as required.

3. Let $m_{\alpha,F}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ in $F[x]$ and $[K : F] = n$. By item 2, the minimal polynomial $p(x)$ of T_α is also $m_{\alpha,F}(x)$. Determinant of T_α is the product of

all eigenvalues (with repetitions) and trace of T_α is the sum of all eigenvalues. By Questions 17 and 18 of Section 14.2 of DF, it follows that

$$N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$$

and

$$\mathrm{Tr}_{K/F}(\alpha) = \frac{-n}{d} a_{d-1}.$$

As K/F is separable, therefore we may write $p(x) = m_{\alpha,F}(x) = (x-\lambda_1)\cdot\cdots\cdot(x-\lambda_d)$ where λ_i are distinct eigenvalues of T_α or equivalently, F-conjugates of α. It is now sufficient to show that each eigenvalue λ_i has algebraic multiplicity n/d.

Let $\Phi(x) \in F[x]$ be the characteristic polynomial of T_α. Since $p(x)$ and $\Phi(x)$ have same irreducible factors and $p(x)$ is irreducible, it follows that $\Phi(x) = p(x)^k$ for some $k \geq 1$. As $\Phi(x)$ has degree n and $p(x)$ has degree d, therefore we conclude that $k = n/d$, as required. □

Proof of Question 14.3, 8. We wish to find the splitting field of $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0$ in $\mathbb{F}_p$ and then the Galois group of it.

In Question 13.2, 5, we showed that $f(x)$ is irreducible in $\mathbb{F}_p[x]$. Let $\alpha \in \overline{\mathbb{F}_p}$ be a root of $f(x)$. Then, we see that

$$f(\alpha+1) = (\alpha+1)^p - (\alpha+1) - a = \alpha^p + 1 - \alpha - 1 - a = 0.$$

Consequently, if α is a root of $f(x)$, then $\alpha+1$ is a root of $f(x)$. It follows that in $\overline{\mathbb{F}_p}$, we have the following roots:

$$\alpha, \alpha+1, \ldots, \alpha+(p-1).$$

Thus we have found p distinct roots of $f(x)$ in $\overline{\mathbb{F}_p}$ and all are of the form as above. This shows that $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is the splitting field of $f(x)$ over $\mathbb{F}_p$. As $f(x)$ is a separable polynomial, thus $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a Galois extension.

Next, we wish to find the Galois group $\mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$. Indeed, we first claim that $|\mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)| \geq p$. As $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \leq p$ since α is a root of $f(x)$ where $\deg f(x) = p$, therefore it would follow that $|\mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)| = p$, thus showing that it is cyclic.

We thus reduce to showing that $|\mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)| \geq p$. Indeed, we can extend $\mathrm{id} : \mathbb{F}_p \to \mathbb{F}_p$ to $\sigma : \mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha+1)$ mapping $\alpha \mapsto \alpha+1$ as minimal polynomial of α is $f(x)$ and $\alpha+1$ is also a root of $f(x)$. Thus $\sigma \in \mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$. Now consider $\sigma^k : \mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha+k)$ for each $1 \leq k \leq p-1$. We see that each $\sigma^k \in \mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$. This shows that $\mathrm{Gal}\,(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ has atleast p-elements, as required. □

Proof of Question 14.4, 1. We wish to find the Galois closure of $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$. To this end, we first have to show that $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is a finite separable extension. Indeed this is finite as it is simple and $\alpha := \sqrt{1+\sqrt{2}}$ is algebraic over $\mathbb{Q}$. Furthermore, consider the polynomial

$$f(x) = x^4 - 2x^2 - 1 \in \mathbb{Q}[x].$$

Observe that $f(\alpha) = 0$ and over $\mathbb{C}$, we may factor it as (let $\beta = \sqrt{\sqrt{2}-1}$ and observe $\alpha \cdot \beta = 1$):

$$f(x) = (x-\alpha)(x+\alpha)(x-i\beta)(x+i\beta).$$

It follows that $m_{\alpha,\mathbb{Q}}(x)|f(x)$. Moreover, $f(x)$ is irreducible in $\mathbb{Q}[x]$ since the factorization in $\mathbb{C}$ shows that it cannot have any degree 2 factor. Since $f(x)$ is separable as $f'(x)$ has no common roots with $f(x)$, we deduce that $m_{\alpha,\mathbb{Q}}(x)$ is separable as well, showing that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is finite separable, as required. Thus there is a Galois closure, say $E/\mathbb{Q}$ of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Note that $E \neq \mathbb{Q}(\alpha)$ as $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois as it doesn't have all conjugates of α.

We now claim that $\mathbb{Q}(i,\alpha)/\mathbb{Q}$ is the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Indeed, we first show that $\mathbb{Q}(i,\alpha)/\mathbb{Q}$ is a Galois extension. As $m_{i,\mathbb{Q}}(x) = x^2+1$ and $m_{\alpha,\mathbb{Q}}(x) = f(x)$. As both x^2+1 and $f(x)$ are separable and have all roots in $\mathbb{Q}(i,\alpha)$, it follows that $\mathbb{Q}(i,\alpha)/\mathbb{Q}$ is Galois.

By minimality of E, it follows that $E \subseteq \mathbb{Q}(i,\alpha)$. We claim that $E = \mathbb{Q}(i,\alpha)$. Indeed, by tower law, we have

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}].$$

Since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ and $[E:\mathbb{Q}(\alpha)] \geq 2$ since $E \neq \mathbb{Q}(\alpha)$, thus, $[E:\mathbb{Q}] \geq 8$. Furthermore, we have

$$[\mathbb{Q}(i,\alpha):\mathbb{Q}] = [\mathbb{Q}(i,\alpha):\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}].$$

Since $[\mathbb{Q}(i,\alpha):\mathbb{Q}(\alpha)] = 2$ as $m_{i,\mathbb{Q}(\alpha)}(x) = x^2+1$, therefore we get that $[\mathbb{Q}(i,\alpha):\mathbb{Q}] = 8$. As $E \subseteq \mathbb{Q}(i,\alpha)$, the fact that $[\mathbb{Q}(i,\alpha):\mathbb{Q}] = 8$ and $[E:\mathbb{Q}] \geq 8$ implies that $E = \mathbb{Q}(i,\alpha)$, as required. □

Proof of Question 14.5, 5. Let $\epsilon_1, \ldots, \epsilon_{p-1}$ be primitive p^{th}-roots of unit. Denote for any $n \in \mathbb{N}$ the following quantity:

$$p_n = \epsilon_1^n + \cdots + \epsilon_{p-1}^n.$$

Note that $\epsilon_i \in \mathbb{Q}(\epsilon_1)$ where $\mathbb{Q}(\epsilon_1)$ is a cyclotomic extension. We wish to show that

$$p_n = \begin{cases} -1 & \text{if } p \nmid n \\ p-1 & \text{if } p|n. \end{cases}$$

Indeed, if $p|n$, then $\epsilon_i^n = 1$ for all i, so this case is immediate. So now suppose that p does not divide n. As the following map

$$\begin{aligned} \varphi : (\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}\,(\mathbb{Q}(\epsilon_1)/\mathbb{Q}) \\ \bar{a} &\longmapsto \epsilon_1 \mapsto \epsilon_1^a \end{aligned}$$

is an isomorphism and that if $n' = n \mod p$ with $2 \leq n' \leq p-1$, then $\epsilon_i^n = \epsilon_i^{n'}$, we get that

$$p_n = \epsilon_1^{n'} + \cdots + \epsilon_{p-1}^{n'}$$

Moreover, $\varphi(\bar{n})(\epsilon_i) = \epsilon_i^{n'}$ for each $1 \leq i \leq p-1$. It follows that

$$\begin{aligned} p_n &= \varphi(\bar{n})(\epsilon_1 + \cdots + \epsilon_{p-1}) \\ &= \varphi(\bar{n})(p_1). \end{aligned}$$

As $p_1 = -1$ since p_1 is the sum of roots of $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, so we get by above that

$$p_n = \varphi(\bar{n})(-1) = -1,$$

as required. □

Proof of Question 14.5, 10. We wish to show that $\mathbb{Q}(2^{1/3})$ is not a subfield of any cyclotomic extension.

By Kronecker-Weber, $\mathbb{Q}(2^{1/3})$ is a subfield of some cyclotomic extension if and only if $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is a finite abelian extension. It is clearly finite, we claim that it is not abelian. To this end, it is sufficient to show that $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois. Indeed, it is separable since $m_{2^{1/3},\mathbb{Q}}(x) = x^3 - 2$ is separable. But $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not normal as $x^3 - 2$ does not have all roots in $\mathbb{Q}(2^{1/3})$; roots of $x^3 - 2$ are $2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}$. Thus $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois and thus is not abelian in particular. □

8 Week 8 : Discriminants & Galois groups, polynomial with S_p Galois group

Proof of Question 14.6, 3. Let $a, b \in \mathbb{F}_{p^n} = F$. We wish to show that if the polynomial $f(x) = x^3 + ax + b$ is irreducible, then $D = -4a^3 - 27b^2$ is square in $\mathbb{F}_{p^n}$.

Indeed, as finite fields are perfect, therefore $f(x)$ is separable. Let K/F be the splitting field of $f(x)$. Note that D is just the discriminant of $f(x)$. We wish to show discriminant is a square. It is equivalent to showing that $\mathrm{Gal}\,(K/F)$ is a subgroup of A_3. Let $\alpha \in K$ be a root of $f(x)$. Then $[K : F] = [K : F(\alpha)][F(\alpha) : F]$ where $F(\alpha)/F$ is a degee 3 extension. It follows that $[K : F]$ is a multiple of 3. Now $\mathrm{Gal}\,(K/F) \hookrightarrow S_3$ and $|S_3| = 6$, therefore $\mathrm{Gal}\,(K/F) = A_3$ or S_3.

Let $\alpha, \beta, \gamma \in K$ be the three distinct roots so that $K = F(\alpha, \beta, \gamma)$. We claim that $K = F(\alpha)$. Now, $K = F(\alpha)$ as $F(\alpha)/F$ is a finite extension of a finite field, and thus Galois. Consequently, $F(\alpha)$ has all other roots β, γ by normality. Thus the splitting field K is equal to $F(\alpha)$, as required.

It follows that $[K : F] = 3$, thus $|\mathrm{Gal}\,(K/F)| = 3$. Thus, $\mathrm{Gal}\,(K/F) = A_3$, as required. □

Proof of Question 14.6, 7. We wish to determine the Galois group of $f(x) = x^4 + 2x^2 + x + 3$ over $\mathbb{Q}$. We first observe that $f(x)$ is irreducible. Indeed, going mod 2, we get the polynomial $\bar{f}(x) = x^4 + x + 1$. We claim that this is irreducible so by mod p-test we will be done. Indeed, suppose that $\bar{f}(x)$ is reducible. Then as $\bar{f}(x)$ has no zeroes in $\mathbb{F}_2$, it implies that $\bar{f}(x)$ has no linear factors. It follows that $\bar{f}(x)$ only has quadratic factors. One easily checks that the only quadratic polynomial with no linear factors is $x^2 + x + 1$. But $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq \bar{f}(x)$. Thus, $\bar{f}(x)$ is irreducible, as required. This shows that

$f(x)$ is irreducible over $\mathbb{Q}$.

Now observe that as $f(x)$ is irreducible and $\mathbb{Q}$ is characteristic 0 (i.e. perfect), therefore $f(x)$ is separable. It follows that $\mathrm{Gal}\,(K/\mathbb{Q})$ is a doubly transitive subgroup of S_4, where we are assuming that

$$\mathrm{Gal}\,(K/\mathbb{Q}) \hookrightarrow S_4$$

by permuting the four distinct roots of $f(x)$. Now, the only doubly transitive subgroup of S_4 is A_4 and S_4. It follows that $\mathrm{Gal}\,(K/F)$ can either be A_4 or S_4. To this end, it suffices to check whether $\mathrm{Gal}\,(K/F)$ is a subgroup of A_4 or not. It is equivalent to checking that whether the discriminat D of $f(x)$ is a square or not. Since discriminant of $f(x)$ is same as the discriminant of the resolvent cubic $h(x) = x^3 - 4x^2 - 8x + 1$, which on calculation yields 3877, which is not a square. Hence we deduce that $\mathrm{Gal}\,(K/F)$ is not a subgroup of A_4, hence it is S_4. □

Proof of Question 14.6, 12. Let $F/\mathbb{Q}$ be an extension of degree 4. We wish to show that the following are equivalent:

1. $F = \mathbb{Q}(\alpha)$ where α is a root of an irreducible $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$.
2. There is an intermediate quadratic extension as in $F/\mathbb{Q}(\sqrt{c})/\mathbb{Q}$ where $\sqrt{c}$ is an element whose square is in $\mathbb{Q}$.

(1. $\Rightarrow$ 2.) Let $g(y) = y^2 + ay + b$. Observe that $g(x^2) = f(x)$. We first claim that $g(y)$ is irreducible. If not, then $g(y) = h(y)k(y)$. where $h(y), k(y) \in \mathbb{Q}[x]$ are linear non-constant polynomials. Then, $f(x) = g(x^2) = h(x^2)k(x^2)$, where $h(x^2), k(x^2)$ are quadratic non-constant polynomials. This gives a contradiction to the irreducibility of $f(x)$. This show that $g(y)$ is irreducible.

Roots of $g(y)$ are given by

$$y = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

where $a^2 - 4b$ is not a square as $g(y)$ is irreducible. Now roots of $f(x)$ in $\mathbb{C}$ are given by

$$x = \pm\sqrt{\frac{-a \pm \sqrt{a^2 - 4b}}{2}}.$$

Let α be one of the above four roots. It follows that $\sqrt{a^2 - 4b} \in F$. Thus,

$$\mathbb{Q}(\sqrt{a^2 - 4b}) \subseteq F,$$

where $\mathbb{Q}(\sqrt{a^2 - 4b})/\mathbb{Q}$ is a quadratic extension, as required.

(2. $\Rightarrow$ 1.) Observe that by tower law we have that $F/\mathbb{Q}(\sqrt{c})$ is a degree 2 extension. Thus, $F = \mathbb{Q}(\sqrt{c})(\sqrt{d})$, for some $d \in \mathbb{Q}(\sqrt{c})$. Note $m_{\sqrt{c},\mathbb{Q}}(x) = x^2 - c$ and $m_{\sqrt{d},\mathbb{Q}(\sqrt{c})} = x^2 - d$. Let $d = a + b\sqrt{c}$, $a, b \in \mathbb{Q}$. It follows that $\sqrt{d} = \sqrt{a + b\sqrt{c}}$. Thus, $F = \mathbb{Q}(\sqrt{a + b\sqrt{c}})$. Consider the polynomial $f(x) = (x^2 - a)^2 - b^2c$. Observe that this is in $\mathbb{Q}[x]$. Moreover, its zeroes

are $\pm\sqrt{a \pm b\sqrt{c}}$, that is, one of its roots is $\sqrt{d}$. We need only show that $f(x)$ is irreducible. We may first write

$$f(x) = \left(x - \sqrt{a + b\sqrt{c}}\right)\left(x + \sqrt{a + b\sqrt{c}}\right)\left(x - \sqrt{a - b\sqrt{c}}\right)\left(x + \sqrt{a - b\sqrt{c}}\right)$$

Indeed, if $f(x)$ is not irreducible, then either it has two quadratic factors or has a linear factor. Clearly, latter cannot happen as all roots of $f(x)$ are distinct and not rational. Furthermore, if it has two quadratic factors, then by above factorization one can see that no pairing of roots will lead to a quadratic whose coefficients are in $\mathbb{Q}$. This completes the proof. □

Proof of Question 14.7, 7. Let F be a characteristic $p > 0$ field and $\zeta_n \in F$ where ζ_n is a primitive n^{th}-root of unity where $\gcd(n, p) = 1$. Let K/F be a cyclic extension of degree d, where $d|n$. By Kummer's theorem, we will have $K = F(a^{1/n})$ for some $a \in F$. Let $\sigma \in \mathrm{Gal}\,(K/F)$ be a generator. We wish to show the following three items:

1. $\sigma(a^{1/n}) = \zeta_d a^{1/n}$ for some primitive d^{th}-root of unity.
2. Let $K = F(a^{1/n}) = F(b^{1/n})$. We wish to show that element $\frac{a^{1/n}}{\left(b^{1/n}\right)^k}$ for some $k \in \mathbb{Z}$ with $\gcd(k, d) = 1$, is in F.
3. The following are equivalent:
   (a) $K = F(a^{1/n}) = F(b^{1/n})$.
   (b) There exists $c, d \in F$ such that $a = b^k c^n$ and $b = a^l d^n$.

1. First note that since $\mu_d \hookrightarrow \mu_n$, it follows that $\mu_d \subseteq F^\times$. Now recall from the proof of Kummer's theorem that we constructed an injective group homomorphism $\varphi : \mathrm{Gal}\,(K/F) \hookrightarrow \mu_n$ whose image is μ_d. This was given by $\varphi(\sigma) = \frac{\sigma(a^{1/n})}{a^{1/n}} = \frac{\zeta_n^{k_\sigma} a^{1/n}}{a^{1/n}} = \zeta_n^{k_\sigma}$. As σ is the generator and group isomorphisms map generators to generators, therefore $\varphi(\sigma) = \zeta_n^{k_\sigma}$ is a generator of μ_d, that is, $\zeta_n^{k_\sigma}$ is a primitive d^{th}-root, as required.

2. Recall that map $\varphi : \mathrm{Gal}\,(K/F) \hookrightarrow \mu_n$ with image μ_d which we used in item 1. By fundamental theorem, it suffices to show that

$$\sigma\left(\frac{a^{1/n}}{b^{k/n}}\right) = \frac{a^{1/n}}{b^{k/n}}.$$

We first find the required k. We first claim that

$$\frac{\sigma(a^{1/n})}{a^{1/n}} = \left(\frac{\sigma(b^{1/n})}{b^{1/n}}\right)^k \tag{1}$$

for some $\gcd(k, n) = 1$. Indeed, the map φ takes σ to $\frac{\sigma(a^{1/n})}{a^{1/n}}$ in μ_d. As σ is a generator of $\mathrm{Gal}\,(K/F)$, therefore $\varphi(\sigma) = \frac{\sigma(a^{1/n})}{a^{1/n}}$ is the generator of μ_d. Similarly, writing $K = F(b^{1/n})$, we get $\varphi(\sigma) = \frac{\sigma(b^{1/n})}{b^{1/n}}$ is a generator in μ_d. As μ_d is cyclic of order d, therefore there exists $k \in \mathbb{Z}$ with $\gcd(k, d) = 1$ such that Eqn. (1) holds.

Having found the required k, we observe that

$$\sigma\left(\frac{a^{1/n}}{b^{k/n}}\right) = \frac{\sigma(a^{1/n})}{\sigma(b^{k/n})} = \frac{a^{1/n}}{b^{k/n}},$$

as required.

3. ((a) $\Rightarrow$ (b)) By item 2, we deduced that $a^{1/n} = b^{k/n}c$, $c \in F$. Raising n^{th}-power, we get the result. Replacing a by b, we get the desired result for b as well.

((b) $\Rightarrow$ (a)) As $a^{1/n} = b^{k/n}c$, therefore $F(a^{1/n}) \subseteq F(b^{1/n})$. As $b^{1/n} = a^{l/n}d$, therefore $F(b^{1/n}) \subseteq F(a^{1/n})$, as required.

This completes the proof. □

Proof of Question 14.7, 12. Let $\mathbb{Q}(\alpha)/\mathbb{Q}$ be a finite extension. This is separable as well since $m_{\alpha,\mathbb{Q}}(x)$ is irreducible in a characteristic 0 field. Let $L/\mathbb{Q}$ be the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$. It follows that L is the splitting field of $m_{\alpha,\mathbb{Q}}(x)$. Let $G = \text{Gal}\,(L/\mathbb{Q})$. Suppose $p \in \mathbb{Z}$ is a prime such that $p|\,|G|$. We wish to show that there exists a subfield F as in $L/F/\mathbb{Q}$ such that L/F is a degree p-extension and $L = F(\alpha)$.

Indeed, by fundamental theorem and Cauchy's theorem, we have a subgroup of order p of G and thus an intermediate extension $F/\mathbb{Q}$ with $|\text{Gal}\,(L/F)| = p$. We wish to show that there exists a field $F'/\mathbb{Q}$ such that L/F' is of degree p. Assuming to the contrary we get that for all intermediate fields L/F of degree p, $L \neq F(\alpha)$. As

$$p = [L : F] = [L : F(\alpha)] \cdot [F(\alpha) : F]$$

and $L \neq F(\alpha)$, therefore $\alpha \in F$. Hence we have that for each L/F of degree p, $\alpha \in F$. Pick any such F. Observe that if F contains all conjugates of α then $L = F$, a contradiction. So $L = F(\beta_1, \ldots, \beta_k)$ where $\beta_i \in L$ are some conjugates of α. But since there is no intermediate extension in L/F, it follows that $k = 1$ and thus $L = F(\beta)$ for some $\mathbb{Q}$-conjugate β of α. Let $\sigma \in \text{Gal}\,(L/\mathbb{Q})$ be such that $\sigma(\alpha) = \beta$. Then $\tau = \sigma^{-1} \in \text{Gal}\,(L/\mathbb{Q})$ is such that $\sigma^{-1}(\beta) = \alpha$. Now, $\tau(F)$ is also an intermediate extension such that $L/\tau(F)$ is degree p as $[F : \mathbb{Q}] = [\tau(F) : \mathbb{Q}]$. It follows that $\alpha \in \tau(F)$. Now observe that $[\tau(L) : \tau(F)] = p$, where $\tau(L) = L$. But since $\tau(L) = \tau(F(\beta)) = \tau(F)(\tau(\beta)) = \tau(F)(\alpha) = L$. Thus, $\tau(F)(\alpha)/\tau(F)$ is a degree p extension. By our hypothesis, $\alpha \in \tau(F)$, but then $\tau(F)(\alpha) = \tau(F)$, a contradiction to the fact that $\tau(F)(\alpha)/\tau(F)$ is degree p. □

Proof of Question 14.7, 17. Let $a \in \mathbb{Q}$ be non-zero rational and $D \in \mathbb{Z}$ be a square-free integer. We wish to show that $K = \mathbb{Q}(\sqrt{a\sqrt{D}})$ cannot be a degree 4 cyclic extension over $\mathbb{Q}$.

Suppose $K/\mathbb{Q}$ is a cyclic extension of degree 4. Observe that $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is a degree 2 intermediate extension of $K/\mathbb{Q}$. Now, by Question 14.6, 12, $K = \mathbb{Q}(\alpha)$ where α is a root of irreducible $f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$. As $K/\mathbb{Q}$ is Galois (as it is cyclic), therefore K has all roots of $f(x)$. Thus, K is the splitting field of $f(x)$ and has all the four roots of $f(x)$

listed below:

$$\alpha_1 = \sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}$$
$$\alpha_2 = \sqrt{\frac{-b-\sqrt{b^2-4c}}{2}}$$
$$\alpha_3 = -\sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}$$
$$\alpha_4 = -\sqrt{\frac{-b-\sqrt{b^2-4c}}{2}}.$$

Let us assume that $\alpha = \alpha_1$, wlog. Moreover, as we have $K = \mathbb{Q}(\alpha)$, therefore we may also write $K = \mathbb{Q}(\alpha_i)$ for each $i = 1, \ldots, 4$. Note that in a cyclic group of order 4, there is only one element of order 2. We claim that $\mathrm{Gal}\,(K/\mathbb{Q})$ has two elements of order 2, thus yielding us a contradiction.

Indeed, consider the following two maps in $\mathrm{Gal}\,(K/\mathbb{Q})$ where since $K = \mathbb{Q}(\alpha_1)$, they are determined by their values on any of the α_i (we choose α_1 for below):

$$\sigma : \alpha_1 \mapsto \alpha_3$$
$$\tau : \alpha_1 \mapsto \alpha_2.$$

Indeed, $\sigma^2(\alpha_1) = \sigma(\alpha_3) = \sigma(-\alpha_1) = -\sigma(\alpha_1) = -(\sigma_3) = \alpha_1$. We next show the same for τ. Indeed, we first show that $\tau(\sqrt{b^2-4c}) = 0$. Indeed, this follows by squaring both sides in the equation $\tau(\alpha_1) = \alpha_2$. Thus, we get

$$\tau(\tau(\alpha_1)) = \tau(\alpha_2).$$

Now, observe that

$$\alpha_2^2 = \alpha_1^2 - \sqrt{b^2-4c}.$$

Thus, $\tau(\alpha_2)^2 = \tau(\alpha_1)^2 = \alpha_2^2$. Thus, we have

$$\tau(\alpha_2) = \pm\alpha_2.$$

If $\tau(\alpha_2) = -\alpha_2 = \alpha_4$, then $\tau^2(\alpha_2) = \tau(-\alpha_2) = -(-\alpha_2) = \alpha_2$. As $K = \mathbb{Q}(\alpha_2)$ as well, therefore τ is determined by its value on α_2. It follows that $\tau^2 = \mathrm{id}$. However, above calculation shows that $\tau^2(\alpha_1) = -\alpha_2 \neq \alpha_1$, a contradiction. Hence $\tau(\alpha_2) \neq -\alpha_2$. Hence $\tau(\alpha_2) = \alpha_2$, thus showing that $\tau^2(\alpha_1) = \alpha_1$, that is, $\tau^2 = \mathrm{id}$.

We have thus exhibited two order 2 elements of $\mathrm{Gal}\,(K/F)$, where $\mathrm{Gal}\,(K/F)$ is cyclic of order 4, thus a contradiction. □

Proof of Question 7. a) We wish to show that a subgroup H of S_p containing a p-cycle and a transposition is S_p. We first show that H is a transitive subgroup. As we have seen in class, a transitive subgroup of S_p containing a transposition is S_p, therefore we will be done.

Pick any $k, l \in \{1, \ldots, p\}$. Assume $l > k$. Then observe that $(1\ 2\ \ldots\ p)^{l-k}$ is an element of H which takes k to $k + (l - k) = l$, as required.

b)[1] Let p be a prime. Construct a polynomial $f(x) \in \mathbb{Z}[x]$ of degree p such that if $K/\mathbb{Q}$ is the splitting field of $f(x)$, then $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}\,(K/\mathbb{Q}) = S_p$.

Clearly, we need $f(x)$ to be irreducible, so that $K/\mathbb{Q}$ is Galois and Galois group being transitive. Now, $f(x)$ must have one pair of complex roots and $p - 2$ real roots so that $G := \mathrm{Gal}\,(K/\mathbb{Q})$ atleast has a conjugation. Consider $q(x) = (x^2 + 1)\prod_{i=1}^{p-2}(x - i)$ which is in $\mathbb{Z}[x]$ and has exactly two complex roots. Define for each $k \in \mathbb{N}$ the following:

$$p_k(x) = q(x) + \frac{x^p + p}{kp^2} \in \mathbb{Q}[x]$$

where $p \in \mathbb{Z}$ is some prime. It can be checked that this is an Eisenstein polynomial for prime p. Hence $p_k(x)$ is irreducible in $\mathbb{Q}[x]$.

Observe that the roots of $q(x)$ are

$$V(q(x)) = \{i, -i, 1, 2, \ldots, p - 3, p - 2\}.$$

Let $a \in V(q(x))$ be any zero. We wish to show that $p_k(x)$ for some k has exactly one root in $B_{1/2}(a)$ in $\mathbb{C}$. To this end we apply Rouché's theorem as follows. One can observe that on the circle $C_{1/2}(a)$, we have for some large k the following:

$$|p_k(x) - q(x)| = \left|\frac{x^p + p}{kp^2}\right| \leq q(x).$$

Thus $p_k(x)$ for some k has exactly one root in $B_{1/2}(a)$ in $\mathbb{C}$. By taking maximum of ks obtained by $a \in V(q(x))$, we get that $p_k(x)$ has one root in $B_{1/2}(a)$ for each $a \in V(q(x))$. But since $p_k(x)$ only has real coefficients, so all complex roots must occur in pairs. If the roots are purely complex, then we can derive a contradiction to uniqueness of roots in $B_{1/2}(a)$. Thus all roots in $B_{1/2}(a)$ must be real, thus we get $p - 2$ real roots of $p_k(x)$. Now since for $a = \pm i$, we have one roots in $B_{1/2}(\pm i)$ each and since these balls don't intersect $\mathbb{R}$ nor each other, hence we have exactly two purely complex roots and they therefore must be conjugates of each other.

Now $\mathrm{Gal}\,(K/\mathbb{Q})$ has a transposition and since $p|\mathrm{Gal}\,(K/\mathbb{Q})$, therefore it also has an order p-element. As $\mathrm{Gal}\,(K/\mathbb{Q}) \hookrightarrow S_p$, it follows that the only order p-element is a p-cycle. By item 1, we thus deduce that $p_k(x)$ has Galois group S_p, as required. □

9 Week 9 : Constructible reals, pure inseparability, more on norm & trace

Proof of Question 13.3, 2. Consider the Archimedes' construction to trisect an angle with a ruler and a compass (see Figure 1 below).

We wish to show that $\alpha = \theta/3$. Indeed, as $OB = OC = 1$, therefore triangle OBC is isosceles, that is $\beta = \gamma$. Similarly, since $OB = AB$, thus triangle ABO is isosceles, that is

[1] Solution primarily from Shubham Sharma.

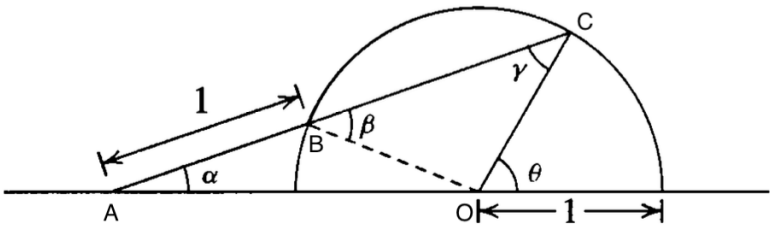


Figure 1: Archimedes' construction for trisecting an angle.

$\alpha = \angle BOA$. It follows that $\angle OBA = \pi - 2\alpha$. Thus, $\beta + \pi - 2\alpha = \pi$, from which we deduce that $\beta = 2\alpha = \gamma$. Hence $\angle BOC = \pi - 4\alpha$. As $\angle BOA + \angle BOC + \theta = \pi$, it follows that $\alpha + \pi - 4\alpha + \theta = \pi$, that is $\theta = 3\alpha$, as required. □

Proof of Question 13.3, 4. We wish to show that $\alpha = \cos(2\pi/7)$ is not constructible by straightedge and compass. Observe that α satisfies the polynomial $f(x) = x^3 + x^2 - 2x - 1$. We need only show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \neq 2^n$ for some $n \in \mathbb{N}$. Consider $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$. As $m_{\alpha,\mathbb{Q}}(x) | f(x)$, therefore $\deg m_{\alpha,\mathbb{Q}}(x) = 2$ or 3. It follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ or 3. We claim that $f(x)$ is irreducible over $\mathbb{Q}$, this would show that $m_{\alpha,\mathbb{Q}}(x) = f(x)$ and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. This will complete the proof.

Indeed, going modulo 2, we get that $\bar{f}(x) = x^3 + x^2 - 1$. As it is a cubic, to check that it is irreducible it suffices to show whether $\bar{f}(x)$ has roots in $\mathbb{F}_2$ or not. We immediately see that $\bar{f}(0) = 1 = \bar{f}(1)$. It follows that $\bar{f}(x)$ has no roots, thus, $\bar{f}(x)$ is irreducible in $\mathbb{F}_2[x]$ and thus is irreducible in $\mathbb{Q}[x]$, as required. □

Proof of Question 3. Let $b \in \mathbb{R}$ be constructible by straightedge and compass. We wish to show that the Galois closure of $\mathbb{Q}(b)/\mathbb{Q}$ is a solvable extension.

Observe that if $K/\mathbb{Q}$ is the Galois closure of $\mathbb{Q}(b)/\mathbb{Q}$, then $K/\mathbb{Q}$ is the splitting field of $f(x) := m_{b,\mathbb{Q}}(x)$. Consequently, we need only show that $f(x)$ is a polynomial which is solvable by radicals, that is, every root of $f(x)$ in K is solvable by radicals. Indeed, we may write

$$f(x) = (x - b)(x - \sigma_1(b)) \dots (x - \sigma_{n-1}(b))$$

where $\sigma_i \in \mathrm{Gal}\,(K/\mathbb{Q})$. Consequently, we reduce to showing that for any $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$, element $\sigma(b) \in K$ is also solvable by radicals. Indeed, since we have the following series

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i \subseteq K_{i+1} \subseteq \cdots \subseteq K_n \subseteq K$$

where $K_{i+1} = K_i(a_i^{1/2})$ where $a_i \in K_i$, therefore applying σ, we get

$$\mathbb{Q} = K_0 \subseteq \sigma K_1 \subseteq \cdots \subseteq \sigma K_i \subseteq \sigma K_{i+1} \subseteq \cdots \subseteq \sigma K_n \subseteq \sigma K = K$$

where we claim that $\sigma K_{i+1} = (\sigma K_i)(\sigma(a_i)^{1/2})$. Indeed, as $a_i^{1/2} \in K_{i+1}$ satisfies $x^2 - a_i$, therefore $\sigma(a_i^{1/2})$ satisfies $x^2 - \sigma(a_i)$. Thus, denoting $\sigma(a_i)^{1/2}$ as a root of $x^2 - \sigma(a_i)$, we see that $\sigma K_{i+1} \supseteq (\sigma K_i)(\sigma(a_i)^{1/2})$. Converse is immediate by observing that any element of

K_{i+1} is of form $c + da_i^{1/2}$, where $c, d \in K_i$. This proves the claim.

As $\sigma(b) \in \sigma K_n \subseteq K$, therefore the above claim shows that $\sigma(b)$ is solvable by radicals, as required. □

Proof of Question 4. a) Let K/F be a field extension where $\text{char}(F) = p > 0$. We wish to show that the following two are equivalent:

1. K/F is purely inseparable.
2. $\left|\hom_F(K, \bar{F})\right| = 1$.

(1. $\Rightarrow$ 2.) As $[K : F]_s = \left|\hom_F(K, \bar{F})\right|$, thus it suffices to show that $[K : F]_s = 1$. As K/F is finite, therefore by tower law for separable degree, it suffices to show that $[F(\alpha) : F]_s = 1$. Since $[F(\alpha) : F]_s$ = number of distinct roots of $m_{\alpha,F}(x)$, therefore it suffices to show that $m_{\alpha,F}(x)$ has only one distinct root. Indeed, as K/F is purely inseparable, therefore $m_{\alpha,F}(x) | x^{p^n} - a$ for $a \in F$ where $a = \alpha^{p^n}$. However, in K, we can write $x^{p^n} - a = (x - \alpha)^{p^n}$, showing that $x^{p^n} - a$ has only one root. Hence, so does $m_{\alpha,F}(x)$, as required.

(2. $\Rightarrow$ 1.) We have $[K : F]_s = \left|\hom_F(K, \bar{F})\right| = 1$. By tower law, it follows that each element $\alpha \in K$ is such that $m_{\alpha,F}(x)$ has only one distinct root. As K/F is finite where F is characteristic p, therefore the minimal polynomial $m_{\alpha,F}(x)$ has each root of same multiplicity which is some p^n. Consequently, we can in write in K, $m_{\alpha,F}(x) = (x - \alpha)^{p^n}$ for $\alpha \in K$. But then

$$m_{\alpha,F}(x) = x^{p^n} - \alpha^{p^n}$$

over F. It follows that $\alpha^{p^n} \in F$, as required.

b) We wish to show that K/F a purely inseparable extension is normal. Indeed, as $\alpha \in K$ is such that $m_{\alpha,F}(x) | x^{p^n} - a$ for some $a = \alpha^{p^n} \in F$, therefore all distinct roots of $m_{\alpha,F}(x)$ are distinct roots of $x^{p^n} - a$ as well. However, over K we have $x^{p^n} - a = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$. Thus, $x^{p^n} - a$ has only one distinct root, it follows that $m_{\alpha,F}(x)$ has only one distinct root, $\alpha \in K$. Since $\alpha \in K$ is arbitrary, hence K/F is normal, as required. □

Proof of Question 5. Let $L/K/F$ be a finite extension. We wish to show the transitivity of trace and norm, that is,

$$\begin{aligned} \text{Tr}_{K/F}(\text{Tr}_{L/K}(\alpha)) &= \text{Tr}_{L/F}(\alpha) \\ N_{K/F}(N_{L/K}(\alpha)) &= N_{L/F}(\alpha). \end{aligned}$$

We know that if E/D is a finite extension, then for any $\alpha \in E/D$

$$\text{Tr}_{E/D}(\alpha) = [E : D]_i \cdot \sum_{\sigma \in \hom_D(E, \bar{D})} \sigma(\alpha).$$

Applying this in our case, we get

$$\text{Tr}_{L/K}(\alpha) = [L : K]_i \cdot \sum_{\sigma \in \hom_K(L, \bar{K})} \sigma(\alpha).$$

Applying $\mathrm{Tr}_{K/F}$ onto above, we yield (note that $\bar{F} = \bar{K}$ as K/F is finite):

$$\begin{aligned}
\mathrm{Tr}_{K/F}\left(\mathrm{Tr}_{L/K}(\alpha)\right) &= \mathrm{Tr}_{K/F}\left([L:K]_i \cdot \sum_{\sigma \in \hom_K(L,\bar{K})} \sigma(\alpha)\right) \\
&= [L:K]_i[K:F]_i \cdot \sum_{\tau \in \hom_F(K,\bar{F})} \tau\left(\sum_{\sigma \in \hom_K(L,\bar{K})} \sigma(\alpha)\right) \\
&= [L:F]_i \cdot \sum_{\tau \in \hom_F(K,\bar{F})} \sum_{\sigma \in \hom_K(L,\bar{K})} \tilde{\tau}(\sigma(\alpha))
\end{aligned}$$

where $\tilde{\tau}$ is an extension of $\tau : K \to \bar{F}$ to $\tilde{\tau} : \bar{K} \to \bar{F}$. We now define a bijection

$$\begin{aligned}
\varphi : \hom_K(L,\bar{K}) \times \hom_F(K,\bar{F}) &\longrightarrow \hom_F(L,\bar{F}) \\
(\sigma,\tau) &\longmapsto \tilde{\tau} \circ \sigma. \qquad (5.1)
\end{aligned}$$

Note that $\tilde{\tau} \circ \sigma$ is id on F and τ on k. This is injective as if $\tilde{\tau} \circ \sigma = \tilde{\tau_1} \circ \sigma_1$, then restricting to K we get $\tau = \tau_1$ and thus, $\sigma = \sigma_1$. Moreover, this is surjective as the size of domain is $[L:K]_s \cdot [K:F]_s$ which is same as the size of codomain $[L:F]_s$. It follows that φ is a bijection.

We can now write Eqn. (5.1) as

$$\begin{aligned}
\mathrm{Tr}_{K/F}(\mathrm{Tr}_{L/K}(\alpha)) &= [L:F]_i \cdot \sum_{\kappa \in \hom_F(L,\bar{F})} \kappa(\alpha) \\
&= \mathrm{Tr}_{L/F}(\alpha),
\end{aligned}$$

as required. One can follow exact same procedure to show that

$$N_{K/F}(N_{L/K}(\alpha)) = N_{L/F}(\alpha),$$

as required. □