1. In this problem we will investigate solvability for a particular matrix group. For a general group G, we say that G is *solvable* if G has a composition series

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

where each factor G_i/G_{i-1} is an abelian group. When G is a finite group our lemma from class shows this is the same as requiring that G has a composition series where each factor is cyclic of prime order. For infinite groups there is no guarantee that there are quotients of finite order, and it turns out that having factors which are abelian is still a useful notion, which is why the definition above is the general one.

Let B be the *Borel subgroup* of $\mathrm{GL}_2(\mathbb{R})$, i.e., B is the subgroup

$$B = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \,\Big|\, a,b,d \in \mathbb{R},\ ad \neq 0 \right\}$$

of upper triangular matrices. Consider the following subgroups of B :

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \subset \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \,\Big|\, b \in \mathbb{R} \right\} \subset \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \,\Big|\, a,b \in \mathbb{R},\ a \neq 0 \right\} \subset B$$

Show that each subgroup is normal in the next (i.e, that they form a composition series) and that each quotient is abelian. Also, identify each quotient group (the quotients are abelian groups which you should know, or at least be able to describe).

Solution. Let us first label the groups :

- $B_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$,
- $B_1 = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \,\Big|\, b \in \mathbb{R} \right\}$,
- $B_2 = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \,\Big|\, a,b \in \mathbb{R},\ a \neq 0 \right\}$, and
- $B_3 = B = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \,\Big|\, a,b,d \in \mathbb{R},\ ad \neq 0 \right\}$.

The group law on B_1 is

$$\begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{bmatrix}$$

In other words, the map $B_1 \longrightarrow \mathbb{R}$ sending $\left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right]$ to b is an isomorphism of groups.

The group B_0 (the identity) is normal in B_1, with factor group $B_1/B_0 = B_1 \cong \mathbb{R}$.

Next, consider the map $\varphi\colon B_2 \longrightarrow \mathbb{R}^*$ given by $\varphi\left(\left[\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right]\right) = a$. Since the multiplication law in B_2 is

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1 \\ 0 & 1 \end{bmatrix}$$

we see that φ is a group homomorphism. It is also surjective, since a may be any element of $\mathbb{R}^*$. The kernel of this map is those $g \in B_2$ for which $\varphi(g) = 1$, i.e.,

$$\operatorname{Ker}(\varphi) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \,\middle|\, a = 1 \right\} = B_1.$$

Thus, B_1 (being the kernel of a homomorphism) is a normal subgroup of B_2, and by the homomorphism theorem, $B_2/B_1 = \operatorname{Im}(\varphi) = \mathbb{R}^*$.

Similarly, define $\psi\colon B_3 \longrightarrow \mathbb{R}^*$ by $\psi\left(\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]\right) = d$. The multiplication law in B_3 is

$$\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{bmatrix},$$

which shows that ψ is a surjective group homomorphism. The kernel of ψ is

$$\operatorname{Ker}(\psi) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \,\middle|\, d = 1 \right\} = B_2,$$

so that B_2 is a normal subgroup of B_3, and $B_3/B_2 \cong \operatorname{Im}(\psi) = \mathbb{R}^*$.

Therefore,

$$B_0 \trianglelefteq B_1 \trianglelefteq B_2 \trianglelefteq B_3 = B$$

is a composition series for B with composition factors $B_1/B_0 \cong \mathbb{R}$, $B_2/B_1 \cong \mathbb{R}^*$, and $B_3/B_2 \cong \mathbb{R}^*$. Since the factors are all abelian, B is a solvable group.

Alternate Solution. Alternatively, we can prove directly that each B_{i-1} is normal in B_i, and compute the quotient. The argument for B_0 in B_1 is unchanged, so we proceed to B_1 in B_2, and start by checking that B_1 is normal in B_2.

For $h = \left[\begin{smallmatrix} 1 & b_1 \\ 0 & 1 \end{smallmatrix}\right] \in B_1$ and $g = \left[\begin{smallmatrix} a & b_2 \\ 0 & 1 \end{smallmatrix}\right] \in B_2$ we have

$$ghg^{-1} = \begin{bmatrix} a & b_2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{a} & -\frac{b_2}{a} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & ab_1 \\ 0 & 1 \end{bmatrix}.$$

Since the conjugate ghg^{-1} is always in B_1, we see that B_1 is normal in B_2.

To determine the quotient B_2/B_1, we look for a complete set of coset representatives. We claim that the subset (and subgroup)

$$Q_2 = \left\{ \begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix} \,\middle|\, a \in \mathbb{R},\, a \neq 0 \right\}$$

is a complete set of coset representatives. First, every coset $g\mathrm{B}_1$ with $g \in B_2$ contains an element of Q_2. Given $g = \left[\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right] \in B_2$ then choosing $g_1 = \left[\begin{smallmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{smallmatrix}\right] \in B_1$ we get

$$g \cdot g_2 = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$$

which is in Q_2 and (by construction) in the coset $g_2 B_1$. Second, no two elements of Q_2 are in the same left B_1 coset : given $h_1 = \left[\begin{smallmatrix} a_1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $h_2 = \left[\begin{smallmatrix} a_2 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, trying to solve

$$\begin{bmatrix} a_2 & 0 \\ 0 & 1 \end{bmatrix} = h_2 = h_1 g_1 = \begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 & a_1 b \\ 0 & 1 \end{bmatrix}$$

gives $a_1 = a_2$ and $b = 0$. Finally, the group law on Q_2 is

$$\begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 1 \end{bmatrix}.$$

This shows that the map $Q_2 \longrightarrow \mathbb{R}^*$ given by $\left[\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right] \mapsto a$ is an isomorphism of groups. Therefore $B_2/B_1 \cong Q_2 \cong \mathbb{R}^*$.

Now let's check that B_2 is normal in B_3. Given $h = \left[\begin{smallmatrix} a_1 & b_1 \\ 0 & 1 \end{smallmatrix}\right] \in B_2$ and $g = \left[\begin{smallmatrix} a_2 & b_2 \\ 0 & d_2 \end{smallmatrix}\right] \in B_3$, we have

$$ghg^{-1} = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2 d_2} \\ 0 & \frac{1}{d_2} \end{bmatrix} = \begin{bmatrix} a_1 & \frac{1}{d_2}(a_2 b_1 - a_1 b_2 + b_2) \\ 0 & 1 \end{bmatrix}.$$

Since $ghg^{-1} \in B_2$ (and since $g \in B_3$ and $h \in B_2$ are arbitrary), we see that B_2 is normal in B_3. To understand the quotient B_3/B_2 we again look for a set of coset representatives. This time we claim that the subgroup

$$Q_3 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \,\Big|\, d \in \mathbb{R},\, d \neq 0 \right\}$$

is a complete set of coset representatives for the cosets of B_2 in B_3. We first check that every coset gB_2 with $g \in B_3$ contains an element of Q_3. Given $g = \left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] \in B_3$, choosing $g_2 = \left[\begin{smallmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{smallmatrix}\right] \in B_2$ we get

$$gg_2 = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix},$$

so that every left coset of B_2 contains an element of Q_3. No two elements of Q_3 are in the same left coset of B_2 : trying to solve

$$\begin{bmatrix} 1 & 0 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

gives $a = 1$, $b = 0$, and $d_1 = d_2$. Finally, as a group $Q_3 \cong \mathbb{R}^*$, and so $B_3/B_2 = Q_3 \cong \mathbb{R}^*$.

We conclude as before that $B_0 \trianglelefteq B_1 \trianglelefteq B_2 \trianglelefteq B_3$ is a composition series with abelian quotients.

2. In this problem we will prove part (b) of the lemma on radical extensions from class. That is, we will show that if M is a field of characteristic zero which contains a primitive m-th root of unity ζ, and β and element such that $\beta^m \in M$, then the extension $M(\beta)/M$ is Galois with abelian Galois group.

Set $\gamma = \beta^m$. Then β is a root of $f(x) = x^m - \gamma \in M[x]$.

(a) Find the roots of f and explain why they are all in $M(\beta)$. (Hint: Don't forget that $\zeta \in M$.)

(b) Let $q(x)$ be the minimal polynomial polynomial of β over M. Explain why $q(x) \mid f(x)$.

(c) Explain why $q(x)$ splits completely in $M(\beta)$.

(d) Explain why $M(\beta)/M$ is a Galois extension.

Let $G = \text{Gal}(M(\beta)/M)$. Since β is a generator of $M(\beta)/M$, to understand how $\sigma \in G$ acts on $M(\beta)$ it is enough to understand what σ does to β.

(e) Explain why $\sigma(\beta) = \beta \cdot \zeta^n$ for some $n \in \{0, \dots, m-1\}$.

Let us use σ_n to name an element such that $\sigma_n(\beta) = \beta \cdot \zeta^n$. (So $\sigma_3(\beta) = \beta \cdot \zeta^3$, $\sigma_4(\beta) = \beta \cdot \zeta^4$, $\sigma_0(\beta) = \beta \cdot \zeta^0 = \beta$, etc.) Note we are not claiming that $\sigma_n \in G$ for every possible n, just that this gives a consistent way of giving a name to the elements of G.

(f) Suppose that $\sigma_{n_1}, \sigma_{n_2} \in G$. Show that $\sigma_{n_1}\sigma_{n_2} = \sigma_{n_2}\sigma_{n_1}$ by computing what each side does to β. (Hint: ζ is in M.)

Since σ_{n_1} and σ_{n_2} were arbitrary, this means that G is abelian, proving this part of the lemma.

Solution.

(a) The roots of f are β, $\beta \cdot \zeta$, $\beta \cdot \zeta^2$,..., $\beta \cdot \zeta^{m-1}$. Since $\zeta \in M$ and $\beta \in M(\beta)$, all of the roots are in $M(\beta)$.

(b) One of the properties of the minimal polynomial of β over M is that it divides any other polynomial with coefficients in M with β as a root. Since $f(x) \in M[x]$ and $f(\beta) = 0$ we then have $q(x) \mid f(x)$.

(c) Since $q(x) \mid f(x)$ the roots of $q(x)$ are a subset of the roots of $f(x)$. Since all the roots of $f(x)$ are in $M(\beta)$ (by part (a)), all the roots of $q(x)$ are in $M(\beta)$, so $q(x)$ splits completely in $M(\beta)$.

(d) $M(\beta)$ is generated over M by β, with minimal polynomial $q(x)$. By part (c) $q(x)$ splits completely in $M(\beta)$ and so $M(\beta)/M$ is a normal extension. Since we are in characteristic zero, separability is automatic, and therefore $M(\beta)/M$ is a Galois extension.

(e) Given any $\sigma \in G$, $\sigma(\beta)$ is a root of $q(x)$. From parts (a) and (c) we see that the roots of $q(x)$ are all of the form $\beta \cdot \zeta^n$ for some $n \in \{0, \ldots, m-1\}$. Thus $\sigma(\beta) = \beta \cdot \zeta^n$ for some n, $0 \leqslant m \leqslant m-1$.

(f) Since $\zeta \in M$, $\sigma(\zeta) = \zeta$ for all $\sigma \in G$. Therefore

$$\sigma_{n_1}\sigma_{n_2}(\beta) = \sigma_{n_1}(\sigma_{n_2}(\beta)) = \sigma_{n_1}(\beta{\cdot}\zeta^{n_2}) = \sigma_{n_1}(\beta){\cdot}\sigma_{n_1}(\zeta^{n_2}) = (\beta{\cdot}\zeta^{n_1}){\cdot}\zeta^{n_2} = \beta{\cdot}\zeta^{n_1+n_2}.$$

Similarly, $\sigma_{n_2}(\sigma_{n_1}(\beta)) = \beta \cdot \zeta^{n_1+n_2}$.

Remark. The proof actually shows that G is isomorphic to a subgroup of $\mathbb{Z}/m\mathbb{Z}$ (the subgroup being whichever n show up as $\sigma_n \in G$). Since every subgroup of a cyclic group is cyclic, we conclude that G is cyclic. That is, the proof shows that $\mathrm{Gal}(M(\beta)/M)$ is a cyclic group, and not just abelian.

3. In this problem we will see what the general constructions from class mean in two examples we have already computed. In each of the examples we had $K = \mathbb{Q}$, and L the splitting field of a polynomial of the form $f(x) = x^m - \gamma$, with $\gamma \in K$ (i.e, in $\gamma \in \mathbb{Q}$).

(a) On February 22nd and 24th ("An example", and "An example continued") we computed the Galois group of the splitting field of $f(x) = x^3 - 2$. (The answer was that the Galois group is $S_3 = D_3$.) Let L be this splitting field, i.e., $L = \mathbb{Q}(2^{\frac{1}{3}}, \omega)$ where $\omega = e^{\frac{2\pi i}{3}}$. The tower of fields

$$\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\omega, 2^{\frac{1}{3}}) = L$$

is a radical tower. Identify the subgroups of $\mathrm{Gal}(L/K)$ corresponding to each of the fields in the tower, and compute the factors of the resulting composition series. (By our lemma from class, they should all be abelian.)

(b) On February 26th ("A more complicated example") we computed the Galois group of the splitting field of $f(x) = x^4 - 5$. (The answer was that the Galois group is D_4.) Let $L = \mathbb{Q}(5^{\frac{1}{4}}, i)$ be the splitting field. The tower of fields

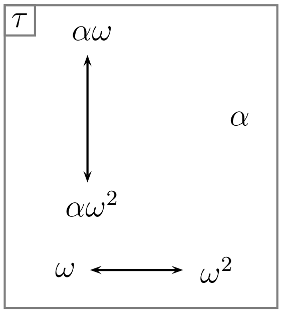
$$\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, 5^{\frac{1}{4}}) = L$$

is a radical tower. Identify the subgroups of $\mathrm{Gal}(L/K)$ belonging to each of the fields in the tower, and compute the factors of the resulting composition series. (They should again all be abelian.)

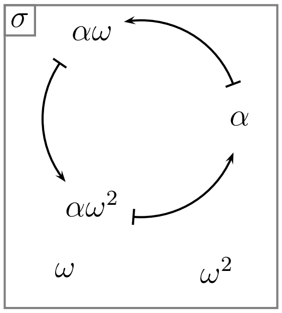
In this question you can freely use the details we computed in class (e.g., the Galois correspondence) — there is no need to work it out again from scratch.

Solution.

(a) In class we had found the following generators of the Galois group :



and



.

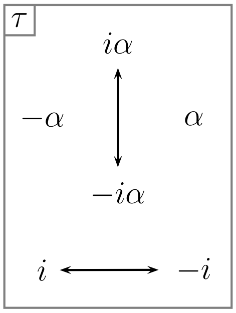
(As a reminder, τ was complex conjugation, and we constructed σ using the lifting lemma.)

$$\begin{tikzcd}
L \arrow[d, dash, "3"] \\
\mathbb{Q}(\omega) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

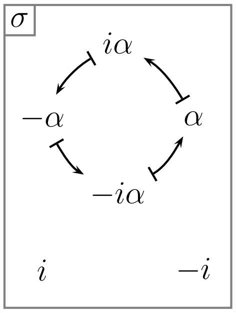
The tower of field extensions is shown to the right. Let $H \subset G$ be the Galois group associated to the intermediate field $\mathbb{Q}(\omega)$, i.e., $H = \mathrm{Gal}(L/\mathbb{Q}(\omega))$. From the tower we see that $|H| = 3$. Since σ fixes ω, $\sigma \in H$, and since σ has order e, we conclude that $H = \langle\sigma\rangle = \{\mathrm{Id}_L, \sigma, \sigma^2\}$.

The associated composition series is $\{\mathrm{Id}_L\} \trianglelefteq H \trianglelefteq G$ with composition factors $H/\{\mathrm{Id}_L\} = H = C_3$ and $G/H = \mathrm{C}_2$. (Since G/H has order 2, this is the only possibility for the quotient.)

(b) In class we found the following generators for the Galois group :



and



.

In this example, τ was again complex conjugation, and σ constructed from the lifting lemma.

The tower of field extensions is shown to the right. Let $H \subset G$ be the Galois group associated to the extension $\mathbb{Q}(i)$. From the tower we see that $|H| = 4$. Since $\sigma \in H$, and since σ has order 4, we have $H = \langle \sigma \rangle = \{\mathrm{Id}_L, \sigma, \sigma^2, \sigma^3\}$.

Therefore we have the composition series $\{\mathrm{Id}_L\} \trianglelefteq H \trianglelefteq G$ with composition factors $H/\{\mathrm{Id}_L\} = H = C_4$ and $G/H = C_2$.

$$\begin{tikzcd}
L \arrow[d, dash, "4"] \\
\mathbb{Q}(i) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

The composition factors are all cyclic, as predicted by the lemma from class.