

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet VII: Radical extensions; solution of equations by radicals;
soluble groups (Solutions)

1. Find a normal radical extension of \mathbb{Q} that contains $\mathbb{Q}(\sqrt[3]{2})$.

Solution: Take $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$. Then K is the splitting field of $X^3 - 2$ over \mathbb{Q} , since the roots of this polynomial are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Therefore K is a normal extension of \mathbb{Q} and certainly K contains $\mathbb{Q}(\sqrt[3]{2})$. Consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega). \quad (4)$$

Since $(\sqrt[3]{2})^3 = 2 \in \mathbb{Q}$ and $\omega^3 = 1 \in \mathbb{Q}(\sqrt[3]{2})$, each of the extensions in (4) are simple radical extensions of the previous field. Hence K is also a radical extension of \mathbb{Q} , as required.

2. Find three radical extensions of \mathbb{Q} all containing $\mathbb{Q}(\sqrt{2})$ such that the Galois groups are distinct.

Solution: First note $\mathbb{Q}(\sqrt{2})$ is itself a (simple) radical extension of \mathbb{Q} since $(\sqrt{2})^2 = 2 \in \mathbb{Q}$. It is also a normal extension of \mathbb{Q} , as the splitting field of $X^2 - 2$ over \mathbb{Q} , so the Fundamental Theorem of Galois Theory tells us

$$|\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2.$$

Now consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is the splitting field of $(X^2 - 2)(X^2 - 3)$ over \mathbb{Q} , so is a normal extension of \mathbb{Q} . We observed in Example 2.18 in the lecture notes that the degree $|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = 4$, so the Fundamental Theorem of Galois Theory tells us $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has order 4. We also have a radical extension here because

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

satisfies $(\sqrt{2})^2 = 2 \in \mathbb{Q}$ and $(\sqrt{3})^2 = 3 \in \mathbb{Q}(\sqrt{2})$.

Finally consider $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$. This is the splitting field of $(X^2 - 2)(X^2 - 3)(X^2 + 1)$ over \mathbb{Q} and

$$|\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}(\sqrt{2}, \sqrt{3})| \cdot |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = 8,$$

as $X^2 + 1$ is the minimum polynomial of i over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. (Note $i \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so $X^2 + 1$ does not factorize over this field.) The Fundamental Theorem of Galois Theory then tells us that the Galois group $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)/\mathbb{Q})$ has order 8. We also have a radical extension as

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$$

with $(\sqrt{2})^2 = 2 \in \mathbb{Q}$, $(\sqrt{3})^2 = 3 \in \mathbb{Q}(\sqrt{2})$ and $i^2 = -1 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Hence $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$ are radical extensions of \mathbb{Q} , all of which contain $\mathbb{Q}(\sqrt{2})$, and the Galois groups of these fields over \mathbb{Q} are distinct (as they have different orders).

3. Let $f(X) = X^3 - 3X + 1$ and let K be the splitting field of $f(X)$ over \mathbb{Q} . Show that $|K : \mathbb{Q}| = 3$ and find a radical extension of \mathbb{Q} containing K .

Show that K is not itself a radical extension of \mathbb{Q} .

Solution: First observe

$$\begin{aligned} f(X-1) &= (X-1)^3 - 3(X-1) + 1 \\ &= X^3 - 3X^2 + 3 \end{aligned}$$

is irreducible over \mathbb{Q} by Eisenstein's Criterion. Hence $f(X)$ is irreducible over \mathbb{Q} .

We determine the roots of $f(X)$ in \mathbb{C} by exploiting the trigonometric identity

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta.$$

Consider $\alpha = 2 \cos \theta$. Then

$$\begin{aligned} \alpha^3 - 3\alpha &= 8 \cos^3 \theta - 6 \cos \theta \\ &= 2 \cos 3\theta, \end{aligned}$$

so $f(\alpha) = 0$ if and only if $\cos 3\theta = -\frac{1}{2}$. Thus some solutions are found by taking θ such that $3\theta = 2\pi/3$. Thus two solutions are found by taking $\alpha = 2 \cos \frac{2\pi}{9}$ and $\beta = 2 \cos \frac{8\pi}{9}$. Note that $\alpha \neq \beta$, since, for example, $\alpha > 0$ and $\beta < 0$. The third root of $f(X)$ is determined by noting that the sum of the roots is 0 by the X^2 -coefficient. Thus $\gamma = -\alpha - \beta$ is the third root.

Observe furthermore that

$$\beta = 2 \cos \frac{8\pi}{9} = -2 \cos \frac{\pi}{9},$$

so

$$\begin{aligned} \alpha &= 2 \cos \frac{2\pi}{9} = 2 \left(2 \cos^2 \frac{\pi}{9} - 1 \right) \\ &= \beta^2 - 2. \end{aligned}$$

Hence $\alpha \in \mathbb{Q}(\beta)$ and therefore $\gamma = -\alpha - \beta \in \mathbb{Q}(\beta)$. We conclude that the splitting field of $f(X)$ over \mathbb{Q} is $K = \mathbb{Q}(\beta)$. Since $f(X)$ is irreducible we deduce

$$|K : \mathbb{Q}| = |\mathbb{Q}(\beta) : \mathbb{Q}| = 3.$$

Let $\varepsilon = e^{2\pi i/3}$ and consider $L = \mathbb{Q}(\beta, \varepsilon)$. Note $\varepsilon^3 = 1 \in \mathbb{Q}$, so $F = \mathbb{Q}(\varepsilon)$ is a simple radical extension of \mathbb{Q} . Also F is the splitting field of $X^3 - 1$ over \mathbb{Q} because the roots of this polynomial are ε , ε^2 and 1.

Consider the extension $L = \mathbb{Q}(\beta, \varepsilon)$ of $F = \mathbb{Q}(\varepsilon)$. By the Tower Law, applied twice,

$$\begin{aligned} |L : \mathbb{Q}| &= |\mathbb{Q}(\beta, \varepsilon) : \mathbb{Q}(\varepsilon)| \cdot |\mathbb{Q}(\varepsilon) : \mathbb{Q}| \\ &= |\mathbb{Q}(\beta, \varepsilon) : \mathbb{Q}(\beta)| \cdot |\mathbb{Q}(\beta) : \mathbb{Q}|. \end{aligned}$$

Hence $|K : \mathbb{Q}| = |\mathbb{Q}(\beta) : \mathbb{Q}| = 3$ divides $|L : \mathbb{Q}|$. Note $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = 2$ because the minimum polynomial of ε over \mathbb{Q} is $X^2 + X + 1$. Therefore $|L : F| = |\mathbb{Q}(\beta, \varepsilon) : \mathbb{Q}(\varepsilon)|$ is divisible by 3. Furthermore, β satisfies $f(X)$, so the minimum polynomial of β over $\mathbb{Q}(\varepsilon)$ is at most 3. We therefore conclude $|L : F| = 3$.

Finally $L = \mathbb{Q}(\varepsilon, \beta)$ is the splitting field of $f(X)$ over $\mathbb{Q}(\varepsilon)$ (because the roots of $f(X)$ are β , $\alpha = \beta^2 - 2$ and $\gamma = -\alpha - \beta$, all of which belong to L). Hence L is a Galois extension of F and the Fundamental Theorem of Galois Theory tells us

$$|\text{Gal}(L/F)| = 3;$$

that is,

$$\text{Gal}(L/F) \cong C_3.$$

We now apply Lemma 7.16 to conclude $L = F(\delta)$ is a simple radical extension of F . Hence

$$\mathbb{Q} \subseteq \mathbb{Q}(\varepsilon) = F \subseteq \mathbb{Q}(\varepsilon, \beta) = L$$

and here L is a radical extension of \mathbb{Q} satisfying $K = \mathbb{Q}(\beta) \subseteq L$, by construction.

Finally suppose K were a radical extension of \mathbb{Q} . Then as $|K : \mathbb{Q}| = 3$, there are no intermediate fields between them so K is a simple radical extension of \mathbb{Q} ; say $K = \mathbb{Q}(\delta)$ where $\delta^p = \lambda \in \mathbb{Q}$ for some prime p . Let $g(X)$ be the minimum polynomial of δ over \mathbb{Q} . Then $g(X)$ has degree 3, since $|K : \mathbb{Q}| = 3$, and $g(X)$ divides $X^p - \lambda$. As K is a normal extension of \mathbb{Q} and $g(X)$ has one root, δ , in K , we conclude $g(X)$ splits in K . Hence $X^p - \lambda$ has at least three roots in K and $p \geq 3$. The roots of $X^p - \lambda$ in \mathbb{C} are

$$\delta\omega^i, \quad \text{for } 0 \leq i \leq p-1,$$

where $\omega = e^{2\pi i/p}$. Notice that $\delta \in \mathbb{R}$ (as $\delta \in K = \mathbb{Q}(\beta)$) but that the other $p-1$ roots are non-real complex numbers. This is impossible as $K \subseteq \mathbb{R}$, so we have a contradiction.

Hence K is not a radical extension of \mathbb{Q} .

4. Show that $X^5 - 6X + 3$ is not soluble by radicals over \mathbb{Q} .

Solution: Let $f(X) = X^5 - 6X + 3$. First observe that $f(X)$ is irreducible over \mathbb{Q} , by Eisenstein's Criterion. Also observe

$$f(-2) = -17, \quad f(0) = 3, \quad f(1) = -2, \quad f(2) = 23,$$

so, by the Intermediate Value Theorem, $f(X)$ has at least three roots in \mathbb{R} , namely at least one between -2 and 0 , at least one between 0 and 1 , and at least one between 1 and 2 .

Furthermore, the derivative (as a function $\mathbb{R} \rightarrow \mathbb{R}$) of f is

$$f'(X) = 5X^4 - 6.$$

Hence $f'(X) = 0$ has exactly two solutions in \mathbb{R} , namely $\pm\sqrt{6/5}$. Therefore $f(X)$ has at most three roots in \mathbb{R} , so Rolle's Theorem states that $f'(X) = 0$ has a solution between every pair of roots of $f(X)$.

In conclusion, $f(X)$ has precisely two non-real roots in \mathbb{C} and three real roots. Lemma 7.14 then tells us that the Galois group of $f(X)$ is the symmetric group S_5 of degree 5. This is not soluble, as it contains the non-abelian simple group A_5 . Hence, by Galois's Great Theorem, $f(X)$ is not soluble by radicals.

5. Let F be a field of characteristic zero. Show that a polynomial of the form $X^4 + bX^2 + c$ is soluble by radicals over F .

Solution: The easiest solution is to note that the Galois group of $X^4 + bX^2 + c$ is a subgroup of the symmetric group S_4 of degree 4. This symmetric group is soluble having the following chain of subgroups

$$S_4 > A_4 > V_4 > \langle (1\ 2)(3\ 4) \rangle > \mathbf{1}$$

with quotients $S_4/A_4 \cong C_2$, $A_4/V_4 \cong C_3$, $V_4/\langle (1\ 2)(3\ 4) \rangle \cong C_2$ and $\langle (1\ 2)(3\ 4) \rangle \cong C_2$. Hence the Galois group of our polynomial is a subgroup of a soluble group, so is also soluble.

The following alternative method would also generalize with careful adjustments to some higher degree polynomials which is why I choose to include it.

Let

$$g(X) = X^2 + bX + c$$

and

$$f(X) = g(X^2) = X^4 + bX^2 + c.$$

Let K be the splitting field of $f(X)$ over F . Note that if $\alpha \in K$ is a root of $f(X)$, then $g(\alpha^2) = 0$, so $g(X)$ has a root in K and hence, as a quadratic polynomial, splits in K . Let L be the subfield of K obtained by adjoining the roots of $g(X)$ to F . Thus L is the splitting field of $g(X)$ over F .

Now consider the Galois group $G = \text{Gal}(K/F)$. As K is a Galois extension of F (as a splitting field in characteristic zero) and L is a normal extension of F , L^* is a normal subgroup of G and

$$G/L^* \cong \text{Gal}(L/F),$$

by the Fundamental Theorem of Galois Group. This group, $\text{Gal}(L/F)$, is the Galois group of the quadratic polynomial $g(X)$, so is isomorphic to a subgroup of the symmetric group S_2 of degree 2. Thus $\text{Gal}(L/F)$ is abelian (as $S_2 \cong C_2$).

Consider an element ϕ of $L^* = \text{Gal}(K/L)$. Then ϕ is determined by its effect on the roots of $f(X)$. Consider a root α of $f(X)$ in K . If $\alpha = 0$, then ϕ fixes α . If $\alpha \neq 0$, then $-\alpha$ is also a root of $f(X)$ (after all,

$$f(-\alpha) = g((-\alpha)^2) = g(\alpha^2) = f(\alpha) = 0).$$

Moreover, α^2 , being a root of $g(X)$, belongs to L , so $(\alpha^2)\phi = \alpha^2$; that is, $(\alpha\phi)^2 = \alpha^2$. Hence $\alpha\phi = \pm\alpha$. In conclusion, ϕ either fixes α and $-\alpha$, or ϕ induces a permutation that swaps α and $-\alpha$. This argument applies to all the roots of $f(X)$, so we conclude that any $\phi \in L^*$ is contained in

$$\langle (\alpha \ -\alpha), (\beta \ -\beta) \rangle \tag{5}$$

where α , $-\alpha$, β and $-\beta$ are the distinct roots of $f(X)$ (and where we omit the relevant transposition if α or β equal 0). As transpositions of distinct roots, the group appearing in (5) is abelian (disjoint transpositions commute) and hence L^* is abelian.

In conclusion, G has a normal subgroup L^* such that L^* and G/L^* is abelian, so G is soluble. Finally, as the Galois group of $f(X)$ is soluble, the polynomial is soluble by radicals.

6. Let G be a soluble group with a chain of subgroups

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_d = 1$$

where, for $i = 1, 2, \dots, d$, G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian.

- (a) If H is a subgroup of G , show that $H \cap G_i$ is a normal subgroup of $H \cap G_{i-1}$ and that $(H \cap G_{i-1})/(H \cap G_i)$ is isomorphic to a subgroup of G_{i-1}/G_i for each i . [Hint: Second Isomorphism Theorem.]

Deduce that subgroups of soluble groups are soluble.

- (b) If A , B and C are subgroups of G with $A \leq B$, show that $A(B \cap C) = AC \cap B$. [This result is known as the *Modular Law*.]

- (c) If N is a normal subgroup of G , show that $G_i N/N$ is a normal subgroup of $G_{i-1} N/N$ and that $(G_{i-1} N/N)/(G_i N/N)$ is isomorphic to a quotient of G_{i-1}/G_i for each i . [Hint: Use the Second and Third Isomorphism Theorems and the Modular Law.]

Deduce that quotients of soluble groups are soluble.

Solution:

- (a) Intersecting the subgroup G_i with H certainly gives a chain of subgroups

$$H = H \cap G_0 \geq H \cap G_1 \geq H \cap G_2 \geq \dots \geq H \cap G_d = \mathbf{1} \quad (6)$$

of H . Consider a particular index i . We know G_i is a normal subgroup of G_{i-1} while $H \cap G_{i-1}$ is certainly a subgroup of G_{i-1} . We can apply the Second Isomorphism Theorem to this situation. It tells us that $(H \cap G_{i-1}) \cap G_i$ is a normal subgroup of $H \cap G_{i-1}$ (that is, $H \cap G_i \trianglelefteq H \cap G_{i-1}$) and

$$\frac{H \cap G_{i-1}}{H \cap G_i} = \frac{H \cap G_{i-1}}{(H \cap G_{i-1}) \cap G_i} \cong \frac{(H \cap G_{i-1})G_i}{G_i}.$$

On the right-hand side, $(H \cap G_{i-1})G_i \leq G_{i-1}$ (as $H \cap G_{i-1}$ and G_i are contained in G_{i-1}), so $(H \cap G_{i-1})G_i / (H \cap G_i)$ is isomorphic to a subgroup of G_{i-1}/G_i , so is abelian. We conclude that (6) is indeed a sequence of subgroups of H , each of which is normal in the previous one and the corresponding quotients are abelian. Thus H is soluble.

- (b) Since $A \leq B$ and $B \cap C \leq B$, we deduce $A(B \cap C) \subseteq B$ (as the subgroup B is closed under multiplication). Also $B \cap C \leq C$, so $A(B \cap C) \subseteq AC$ (though neither of these are necessarily subgroups of G). Putting these together, we have established

$$A(B \cap C) \subseteq AC \cap B.$$

Conversely, if $x \in AC \cap B$, then $x = ac$ for some $a \in A$ and $c \in C$. Now $a, x \in B$, because $a \in A \leq B$ and $x \in B$ by assumption, so

$$c = a^{-1}x \in B.$$

This shows, in fact, $c \in B \cap C$, so $x = ac \in A(B \cap C)$. This establishes the reverse inclusion

$$AC \cap B \subseteq A(B \cap C).$$

In conclusion,

$$A(B \cap C) = AC \cap B.$$

- (c) Note that if H is a subgroup of a group G and N is a normal subgroup of G , then HN is a subgroup of G . (This can be deduced directly and is also part of the statement of the Second Isomorphism Theorem.) Applying this with $H = G_i$, we deduce that $G_i N$, for $i = 0, 1, \dots, d$, are subgroups of G , each of which contain N . Now

$$G = G_0 N \geq G_1 N \geq G_2 N \geq \dots \geq G_d N = N$$

(with $G_d N = \mathbf{1} N = N$ at the last stage) and then, by the Correspondence Theorem, we have a chain of subgroups of G/N :

$$G/N = G_0 N/N \geq G_1 N/N \geq G_2 N/N \geq \dots \geq G_d N/N = \mathbf{1}. \quad (7)$$

Furthermore, observe that $G_i N/N$ is a normal subgroup of $G_{i-1} N/N$ as follows: if $g \in G_{i-1}$ and $x \in G_i$, then $g^{-1}xg \in G_i$ (as $G_i \trianglelefteq G_{i-1}$), so when we conjugate a typical element Nx of $G_i N/N$ by a typical element Ng of $G_{i-1} N/N$ we obtain

$$(Ng)^{-1}(Nx)(Ng) = Ng^{-1}xg \in G_i N/N.$$

Therefore $G_i N/N$ is a normal subgroup of $G_{i-1} N/N$ and then $G_i N \trianglelefteq G_{i-1} N$, using the Correspondence Theorem.

Now apply the Second Isomorphism Theorem to the subgroup G_{i-1} and the normal subgroup $G_i N$ of $G_{i-1} N$, to conclude that $G_{i-1} \cap G_i N$ is a normal subgroup of G_{i-1} and

$$\frac{G_{i-1}(G_i N)}{G_i N} \cong \frac{G_{i-1}}{G_{i-1} \cap G_i N};$$

that is,

$$\frac{G_{i-1} N}{G_i N} \cong \frac{G_{i-1}}{G_{i-1} \cap G_i N}.$$

Finally apply the Modular Law (part (b)) with $A = G_i$, $B = G_{i-1}$ and $C = N$ to conclude

$$G_i(G_{i-1} \cap N) = G_i N \cap G_{i-1}.$$

Putting the above together, we can now establish the quotient groups in (7) are abelian. We already know that $G_i N/N \trianglelefteq G_{i-1} N/N$ and then

$$\begin{aligned} \frac{G_{i-1} N/N}{G_i N/N} &\cong \frac{G_{i-1} N}{G_i N} && \text{by the Third Isomorphism Theorem} \\ &= \frac{G_{i-1}(G_i N)}{G_i N} \\ &= \frac{G_{i-1}}{G_{i-1} \cap G_i N} && \text{by the Second Isomorphism Theorem, as above} \\ &= \frac{G_{i-1}}{G_i(G_{i-1} \cap N)} && \text{by the Modular Law} \\ &\cong \frac{G_{i-1}/G_i}{G_i(G_{i-1} \cap N)/G_i} && \text{by the Third Isomorphism Theorem.} \end{aligned}$$

Note at the last stage, $G_i(G_{i-1} \cap N)$ is a subgroup of G_{i-1} and contains G_i , so we can form the quotient $G_i(G_{i-1} \cap N)/G_i$. In conclusion

$$\frac{G_{i-1} N/N}{G_i N/N}$$

is isomorphic to a quotient of the abelian group G_{i-1}/G_i and hence is abelian.

Thus (7) has the correct form to conclude that G/N is soluble.

7. Let G be a group and N be a normal subgroup of G .

(a) If G/N is soluble, show that there is a chain of subgroups

$$G = G_0 \geq G_1 \geq \dots \geq G_k = N$$

such that G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian for $i = 1, 2, \dots, k$. [Hint: Correspondence Theorem.]

(b) Deduce that if G/N and N are soluble, then G is soluble.

Solution:

(a) Suppose G/N is soluble. Then there is a sequence of subgroups of G/N from G/N down to the trivial subgroup, each normal in the previous and with abelian quotients. The Correspondence Theorem says each subgroup of G/N has the form G_i/N with $N \leq G_i \leq G$. Thus our sequence of subgroups of the quotient groups is

$$G/N = G_0/N \geq G_1/N \geq \dots \geq G_k/N = 1.$$

The Correspondence Theorem then yields

$$G = G_0 \geq G_1 \geq \dots \geq G_k = N$$

and, as $G_i/N \trianglelefteq G_{i-1}/N$ for each i , necessarily $G_i \trianglelefteq G_{i-1}$. Moreover, by the Third Isomorphism Theorem,

$$\frac{G_{i-1}}{G_i} \cong \frac{G_{i-1}/N}{G_i/N}$$

is abelian. Thus we have the required chain of subgroups from G down to N .

(b) First use part (a) to find subgroups

$$G = G_0 \geq G_1 \geq \dots \geq G_k = N$$

with $G_i \trianglelefteq G_{i-1}$ and G_{i-1}/G_i abelian for each i . As N is soluble we know

$$N = N_0 \geq N_1 \geq \dots \geq N_\ell = \mathbf{1}$$

with $N_i \trianglelefteq N_{i-1}$ and N_{i-1}/N_i abelian for each i . Putting these together,

$$G = G_0 \geq G_1 \geq \dots \geq G_k = N = N_0 \geq N_1 \geq \dots \geq N_\ell = \mathbf{1}$$

and each subgroup is normal in the previous one with the corresponding quotient being abelian. Hence G is soluble.