Galois theory - Problem Set 6 solutions

Solved on Thursday 02.05

Chapter 18.3

Problem 1. Is the polynomial $f(x) = x^5 - x^4 - x + 1$ solvable by radicals?

Solution. We have

$$f(x) = (x-1)(x^4-1) = (x-1)(x-1)(x^3+x^2+x+1) = (x-1)^2(x+1)(x^2+1) = (x-1)^2(x+1)(x+i)(x-i)$$

and hence the splitting field of $f(x)$ is $E = \mathbb{Q}(-i, i) = \mathbb{Q}(i)$. Then the Galois group of $f(x)$ has order equal to $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Therefore the Galois group of $f(x)$ is $\mathbb{Z}_2$ which is solvable. By Theorem 16.7 we conclude that $f(x)$ is solvable by radicals.

Problem 2. (Exercise 18.3.1 in the book.) Show that the following polynomials are not solvable by radicals over $\mathbb{Q}$:

(a) $x^5 - 9x + 3$.

(b) $2x^5 - 5x^4 + 5$.

(c) $x^5 - 8x + 6$.

(d) $x^5 - 4x + 2$.

Solution.

(a) Set $f(x) = x^5 - 9x + 3$. Then $f(x)$ is monic and is irreducible by Eisenstein's criterion for $p = 3$. We have

$$f(-2) = -11, f(0) = 3, f(1) = -5, f(2) = 17.$$

Hence by the intermediate value theorem, $f(x)$ has three real roots $r_1 \in (-2, 0)$, $r_2 \in (0, 1)$ and $r_3 \in (1, 2)$. We compute

$$f'(x) = 5x^4 - 9 = 5(x^4 - \tfrac{9}{5}) = 5(x - \sqrt[4]{\tfrac{9}{5}})(x + \sqrt[4]{\tfrac{9}{5}})(x - i\sqrt[4]{\tfrac{9}{5}})(x + i\sqrt[4]{\tfrac{9}{5}}).$$

Hence $f'(x)$ has two real roots and so $f(x)$ has exactly two local minima/maxima. It follows that $f(x)$ has exactly two roots in $\mathbb{C}\setminus\mathbb{R}$. By Theorem 16.12 we conclude that $\mathrm{Gal}(f) \cong S_5$. Since S_5 is not solvable, $f(x)$ is not solvable by radicals.

(b) Set $f(x) = 2x^5 - 5x^4 + 5$. Since this polynomial is not monic, we perform the change of variables $x = \frac{y}{2}$. Then

$$f(x) = f(\tfrac{y}{2}) = 2\frac{y^5}{32} - 5\frac{y^4}{16} + 5 = \frac{1}{16}(y^5 - 5y^4 + 80).$$

Set $g(y) = y^5 - 5y^4 + 80$. Then $g(r) = 0$ if and only if $f(\frac{r}{2}) = 0$ and so $g(y)$ is solvable by radicals if and only if $f(x)$ is solvable by radicals (since the roots of $f(x)$ differ from the roots of $g(y)$ only by a division by 2.) Then $g(y)$ is monic and irreducible by Eisenstein's criterion for $p = 5$. We have

$$g(-2) = -32, g(-1) = 74, g(4) = -176, g(5) = 80.$$

Hence by the intermediate value theorem, $g(y)$ has three real roots $r_1 \in (-2,-1)$, $r_2 \in (-1,4)$ and $r_3 \in (4,5)$. We compute

$$g'(y) = 5y^4 - 20y^3 = 5y^3(y-4).$$

Hence $g'(y)$ has two real roots and so $g(y)$ has exactly two local minima/maxima. It follows that $g(y)$ has exactly two roots in $\mathbb{C}\setminus\mathbb{R}$. By Theorem 16.12 we conclude that $\mathrm{Gal}(g) \cong S_5$. Since S_5 is not solvable, $g(y)$ and hence $f(x)$ is not solvable by radicals.

(c) Set $f(x) = x^5 - 8x + 6$. Then $f(x)$ is monic and is irreducible by Eisenstein's criterion for $p = 2$. We have

$$f(-2) = -10, f(-1) = 13, f(1) = -1, f(2) = 22.$$

Hence by the intermediate value theorem, $f(x)$ has three real roots $r_1 \in (-2,-1)$, $r_2 \in (-1,1)$ and $r_3 \in (1,2)$. We compute

$$f'(x) = 5x^4 - 8 = 5(x^4 - \tfrac{8}{5}) = 5(x - \sqrt[4]{\tfrac{8}{5}})(x + \sqrt[4]{\tfrac{8}{5}})(x - i\sqrt[4]{\tfrac{8}{5}})(x + i\sqrt[4]{\tfrac{8}{5}}).$$

Hence $f'(x)$ has two real roots and so $f(x)$ has exactly two local minima/maxima. It follows that $f(x)$ has exactly two roots in $\mathbb{C}\setminus\mathbb{R}$. By Theorem 16.12 we conclude that $\mathrm{Gal}(f) \cong S_5$. Since S_5 is not solvable, $f(x)$ is not solvable by radicals.

(d) Set $f(x) = x^5 - 4x + 2$. Then $f(x)$ is monic and is irreducible by Eisenstein's criterion for $p = 2$. We have

$$f(-2) = -22, f(-1) = 5, f(1) = -1, f(2) = 26.$$

Hence by the intermediate value theorem, $f(x)$ has three real roots $r_1 \in (-2,-1)$, $r_2 \in (-1,1)$ and $r_3 \in (1,2)$. We compute

$$f'(x) = 5x^4 - 4 = 5(x^4 - \tfrac{4}{5}) = 5(x - \sqrt[4]{\tfrac{4}{5}})(x + \sqrt[4]{\tfrac{4}{5}})(x - i\sqrt[4]{\tfrac{4}{5}})(x + i\sqrt[4]{\tfrac{4}{5}}).$$

Hence $f'(x)$ has two real roots and so $f(x)$ has exactly two local minima/maxima. It follows that $f(x)$ has exactly two roots in $\mathbb{C}\setminus\mathbb{R}$. By Theorem 16.12 we conclude that $\mathrm{Gal}(f) \cong S_5$. Since S_5 is not solvable, $f(x)$ is not solvable by radicals.

Problem 3. (a) Let G be an abelian group. Show that G is simple if and only if it is cyclic of prime order.

(b) Show that finite abelian groups are solvable. (*Hint*: you may use Problem 13(d), that is that the direct product of two solvable groups is solvable.)

Solution.

(a) Assume first that G is simple. Let $x \in G\setminus\{e\}$. Since G is abelian, the subgroup $\langle x\rangle \triangleleft G$ is normal. Since G is simple and $x \neq e$, we conclude that $G = \langle x\rangle$ is cyclic. It remains to show that x has prime order. If x has infinite order, then $\langle x^2\rangle$ is a normal subgroup of $\langle x\rangle = G$ with $\{e\} \neq \langle x^2\rangle \neq \langle x\rangle$, contradicting the fact that G is simple. Hence x has finite order, say n. If p is a prime with $p \mid n$, then $\langle x^p\rangle$ is a subgroup of $\langle x\rangle$ of order $\frac{n}{p}$. Hence if $p \neq n$, there exists a nontrivial normal subgroup of $\langle x\rangle$. We conclude that $p = n$ is prime.

Assume now that G is a cyclic group of prime order p. Let $H \triangleleft G$ be a normal subgroup and assume that $H \neq \{e\}$. Then there exists $x \in H \setminus \{e\}$. Then $\mathrm{o}(x) \mid p$ and since $x \neq e$ we obtain that $\mathrm{o}(x) = p$. Hence $\langle x\rangle \triangleleft H \triangleleft G$ and $|\langle x\rangle| = p = |G|$ give that $|H| = p$ and so $H = G$. Hence the only normal subgroups of G are $\{e\}$ and G and so G is simple.

(b) Let G be a finite abelian group. Then there exist prime numbers $p_1, \ldots, p_k$ and positive integers $m_1, \ldots, m_k$ such that

$$G \cong \mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}.$$

By Problem 13(d) it is enough to show that $\mathbb{Z}_{p_i^{m_i}}$ is solvable for each $1 \leq i \leq k$. Consider the composition series

$$\{e\} \triangleleft \mathbb{Z}_{p_i} \triangleleft \cdots \triangleleft \mathbb{Z}_{p_i^{m_i-1}} \triangleleft \mathbb{Z}_{p_i^{m_i}}.$$

Each succesive quotient in this series is isomorphic to $\mathbb{Z}_{p_i}$ which is cyclic of prime order. Hence $\mathbb{Z}_{p_i^{m_i}}$ is solvable, as required.

Chapter 18.5

Problem 4. Find for which $n \in \mathbb{Z}_{\geq 1}$ is $\sqrt[n]{2}$ constructible.

Solution. The minimal polynomial of $\sqrt[n]{2}$ is $x^n - 2$ (it is monic, has $\sqrt[n]{2}$ as a root and is irreducible by Eisenstein's criterion for $p = 2$). Hence

$$\left[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] = \deg\left(x^n - 2\right) = n.$$

We claim that $\sqrt[n]{2}$ is constructible if and only if $n = 2^t$ for some $t \geq 0$.

Assume first that $\sqrt[n]{2}$ is constructible. Then by Theorem 17.9 we have that $\left[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] = 2^t$ for some $t \geq 0$. Hence $n = 2^t$ as required.

Assume now that $n = 2^t$. We use induction on $t \geq 0$ to show that $\sqrt[2^t]{2}$ is constructible. If $t = 0$, then $\sqrt[2^t]{2} = 2 \in \mathbb{Q}$ is constructible. For the induction step assume that $\sqrt[2^t]{2}$ is constructible. By Lemma 17.8 we have that $\sqrt{\sqrt[2^t]{2}}$ is constructible. Hence $\sqrt{\sqrt[2^t]{2}} = \sqrt[2^{t+1}]{2}$ is constructible, as required.

Problem 5. (Exercise 18.3.4 in the book.) Prove that the regular 17-gon is constructible with ruler and compass.

Solution. We have $\phi(17) = 16 = 2^4$. It follows by Corollary 17.14 that the regular 17-gon is constructible.

Problem 6. (Exercise 18.5.1 in the book.) Show that the angle $\frac{2\pi}{5}$ can be trisected using ruler and compass.

Solution. To show that the angle $\frac{2\pi}{5}$ can be trisected using ruler and compass we need to show that the angle of measure $\frac{2\pi}{15}$ is constructible. This is equivalent to constructibility of a regular 15-gon. Since $\phi(15) = 8 = 2^3$, the regular 15-gon is constructible by Corollary 17.14.

Problem 7. (Exercise 18.3.2 in the book.) Show that it is impossible to construct a regular 9-gon or 7-gon using ruler and compass.

Solution. We have $\phi(9) = 6$ and $\phi(7) = 6$. Since 6 is not a power of 2, it follows by Corollary 17.14 that a regular 9-gon and a regular 7-gon are both not constructible using ruler and compass.

Problem 8. (Exercise 18.3.3 in the book.) Show that it is possible to trisect $54°$ using ruler and compass.

Solution. We transform $54°$ to radians by multiplying with $\frac{\pi}{180°}$:

$$54° \frac{\pi}{180°} = \frac{3\pi}{10}.$$

Hence trisecting $54°$ is equivalent to constructing an angle of measure $\frac{\pi}{10} = \frac{2\pi}{20}$. This is equivalent to constructing a regular 20-gon. Since $\phi(20) = 8 = 2^3$, it follows by Corollary 17.4 that a regular 20-gon is constructible. We conclude that it is possible to construct an angle of measure $\frac{\pi}{10}$ and so trisecting $54°$ is possible using ruler and compass.

Problem 9. Let $\mathbb{K}$ be the set of constructible numbers and $\mathbb{A}$ be the set of algebraic numbers.

(a) Does $\mathbb{K} \subseteq \mathbb{A}$ hold?

(b) Does $\mathbb{A} \subseteq \mathbb{K}$ hold?

Solution.

(a) Let $z \in \mathbb{K}$. By Theorem 17.9 we have that $[\mathbb{Q}(z) : \mathbb{Q}] = 2^t$ for some $t \geq 0$. In particular the field extension $\mathbb{Q} \subseteq \mathbb{Q}(z)$ is finite and so algebraic. Hence z is algebraic over $\mathbb{Q}$ and so $z \in \mathbb{A}$. We conclude that $\mathbb{K} \subseteq \mathbb{A}$.

(b) Consider $\sqrt[3]{2}$. Then $\sqrt[3]{2} \in \mathbb{A}$ since it is a root of $x^3 - 2$. Moreover, we have $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $x^3 - 2$ is irreducible. Since 3 is not a power of 2, we conclude by Theorem 17.9 that $\sqrt[3]{2} \notin \mathbb{K}$ and so $\mathbb{A}$ is not a subset of $\mathbb{K}$.

Problem 10. (Exercise 18.3.5 in the book.) Find which of the following numbers are constructible:

(i) $\sqrt{3}+1$.

(ii) π^2+1.

(iii) $\sqrt{\sqrt{3}-1}+1$.

(iv) $\sqrt[3]{2}+1$.

(v) $\sqrt[4]{\sqrt{2}+\sqrt{5}}$.

Solution.

(i) Since $\mathbb{Q} \subseteq \mathbb{K}$, by Lemma 17.8 we have that $\sqrt{3} \in \mathbb{K}$. Since $\mathbb{K}$ is a field, we conclude that $\sqrt{3}+1$ is constructible.

(ii) Since

$$\pi^2 = (\pi^2+1)-1$$

and $-1 \in \mathbb{K}$, it follows that $\pi^2+1 \in \mathbb{K}$ if and only if $\pi^2 \in \mathbb{K}$. We claim that π^2 is not algebraic. We have field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\pi^2) \subseteq \mathbb{Q}(\pi)$. Moreover, $[\mathbb{Q}(\pi) : \mathbb{Q}(\pi^2)] \leq 2$ since π is a root of $x^2 - \pi^2 \in \mathbb{Q}(\pi^2)[x]$. Assume to a contradiction that π^2 is algebraic. Then $[\mathbb{Q}(\pi^2) : \mathbb{Q}]$ is finite. Hence

$$[\mathbb{Q}(\pi) : \mathbb{Q}] = [\mathbb{Q}(\pi) : \mathbb{Q}(\pi^2)][\mathbb{Q}(\pi^2) : \mathbb{Q}] < \infty,$$

which contradicts π being transcedental. Hence $\pi^2 \notin \mathbb{A}$. Since $\mathbb{K} \subseteq \mathbb{A}$ by Problem 9, it follows that $\pi^2 \notin \mathbb{K}$. We conclude that π^2+1 is not constructible.

(iii) Since $\mathbb{Q} \subseteq \mathbb{K}$, by Lemma 17.8 we have that $\sqrt{3} \in \mathbb{K}$. Since $\mathbb{K}$ is a field, we have that $\sqrt{3}-1 \in \mathbb{K}$. Again by Lemma 17.8 we obtain that $\sqrt{\sqrt{3}-1} \in \mathbb{K}$. Since $\mathbb{K}$ is a field, we conclude that $\sqrt{\sqrt{3}-1}+1 \in \mathbb{K}$ and so $\sqrt{\sqrt{3}-1}+1$ is constructible.

(iv) We have that $\mathbb{Q}(\sqrt[3]{2}+1) = \mathbb{Q}(\sqrt[3]{2})$. Moreover the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2 (it is monic, irreducible by Eisenstein's criterion for $p=2$, and has $\sqrt[3]{2}$ as a root.) Hence

$$[\mathbb{Q}(\sqrt[3]{2}+1) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3-2) = 3.$$

By part (3) of Theorem 17.9 we conclude that $\sqrt[3]{2}+1$ is not constructible.

(v) Since $\mathbb{Q} \subseteq \mathbb{K}$, by Lemma 17.8 we have that $\sqrt{2}, \sqrt{5} \in \mathbb{K}$. Since $\mathbb{K}$ is a field, we have that $\sqrt{2}+\sqrt{5} \in \mathbb{K}$. Again by Lemma 17.8 we obtain that $\sqrt{\sqrt{2}+\sqrt{5}} \in \mathbb{K}$. One more application of Lemma 17.8 gives $\sqrt{\sqrt{\sqrt{2}+\sqrt{5}}} \in \mathbb{K}$ and so $\sqrt[4]{\sqrt{2}+\sqrt{5}}$ is constructible.

Problem 11. Let L be a line and P be a point in $\mathbb{C}$.

(a) Using ruler and compass, show that we may draw the line that goes through P and is perpendicular to L.

(b) Using ruler and compass, show that we may draw the line that goes through P and is parallel to L.

Solution.

(a) If $P \in L$ then there is nothing to show. Otherwise pick any point X in L. Construct the circle C with center P and radius $|P-X|$. This circle C intersects L in at least the point X. If C intersects L at exactly X, then it is tangent at X and so we can construct the line through P and X which will be the required perpendicular line.

Otherwise, assume that C intersects L in two points: one will be the point X and we call the other point Y. Draw the circle C_1 with center X and radius $|X-Y|$ and the circle C_2 with center Y and radius $|Y-X|$. These circles intersect in two points: by Euclidean geometry, both of these points are in the line perpendicular to L that goes through P. Since we have two points in that line, we can construct it as required.

(b) By part (a) we can construct the line L' that goes through P and is perpendicular to L. Now by part (a) again we can construct the line L'' that goes through P and is perpendicular to L'. Since L'' and L are both perpendicular to L', we have that L'' and L are parallel and since $P \in L''$, we have that L'' is the required line.

Problem 12. Let $0 \leq \theta < 2\pi$. We say that an angle of measure θ is *constructible* if there exist constructible $O, P, Q \in \mathbb{C}$ such that the segments (OP) and (OQ) form an angle of measure θ. Show that the following are equivalent.

(a) An angle of measure θ is constructible.

(b) The number $\cos(\theta)$ is constructible.

(c) The number $\sin(\theta)$ is constructible.

Solution. First we claim that it is enough to consider the case $0 \leq \theta \leq \frac{\pi}{2}$. Indeed, since

$$\cos(\theta + \frac{\pi}{2}) = -\sin(\theta), \;\; \cos(\theta + \pi) = -\cos(\theta), \;\; \cos(\theta + \frac{3\pi}{2}) = \sin(\theta)$$

and

$$\sin(\theta + \frac{\pi}{2}) = \cos(\theta), \;\; \sin(\theta + \pi) = -\sin(\theta), \;\; \sin(\theta + \frac{3\pi}{2}) = -\cos(\theta),$$

we have that if the claim is true for $0 \leq \theta \leq \frac{\pi}{2}$, then we may construct the rest of the sines and cosines since $-x$ is constructible if and only if x is constructible. We only show the equivalence of (a) and (b) in the case $0 \leq \theta \leq \frac{\pi}{2}$; the equivalence of (a) and (c) in the same case is similar.

The case $\theta = 0$ is clear since $\cos(0) = 1$ is constructible, while an angle of measure 0 is just a point. The case $\theta = \frac{\pi}{2}$ is also clear since $\cos(0) = 1$ is constructible and an angle of measure $\frac{\pi}{2}$ is constructible since $0, 1, i \in \mathbb{C}$ are constructible. Hence we may assume that $0 < \theta < \frac{\pi}{2}$.

Assume first that (a) holds. Without loss of generality we may assume that we have two segments (OP) and (OQ) intersecting at the point $O = (0, 0)$ and such that P is in the x-axis and the angle formed has measure $\theta \in (0, \frac{\pi}{2})$ and is in the first quadrant. We draw the circle C with center $(0, 0)$ and radius 1 and the line L going through $(0, 0)$ and Q. Then C and L intersect at two points and we call X the point of intersection at the first quadrant. By Problem 11 we may draw the perpendicular from X to the x-axis and call the point of intersection Y. Then $Y = cos(\theta)$ since the orthogonal triangle OXY has hypotenuse of length 1 and the angle formed by (OX) and (OY) is of measure θ. Hence $\cos(\theta)$ is constructible.

Assume now that (b) holds, that is $P = \cos(\theta)$ is constructible. Then $Q = \cos(\theta) + 1$ is also constructible since constructible numbers form a field. Hence we may draw a circle C with center at P and going through Q. In particular, C has radius 1. By Problem 11 we may draw the line L that goes through 0 and is perpendicular to the x-axis. Let X be the point of intersection of C and L with positive imaginary part. Then the right triangle OXP has a side of size $\cos(\theta)$ and a hypotenuse of size 1 and hence the angle formed by the intersection of (OX) and (OP) has measure θ, as required.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 13. (Chapter 18.3) Assume all groups in this exercise are finite.

(a) Let G be a solvable group and $H < G$ be a subgroup. Show that H is solvable.

(b) Let G be a solvable group and $H \triangleleft G$ be a normal subgroup. Show that G/H is solvable.

(c) Let G be a group and $H \triangleleft G$ be a normal subgroup. Show that if H and G/H are solvable, then G is also solvable.

(d) Show that if G_1 and G_2 are solvable groups, then $G_1 \times G_2$ is a solvable group.

Solution.

(a) Let

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

be a composition series of G. Let $H_i = G_i \cap H$ for $0 \leq i \leq n$. Notice that since $H < G$ and $G_i \lhd G_{i+1}$, we have that $H_i = H \cap G_i \lhd H$. We obtain a sequence

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H \tag{1}$$

of subgroups of H. In general this is not a composition series since it may happen that $H_i = H_{i+1}$. However, we may refine (1) by removing consecutive subgroups when they are actually equal. Hence to show that H is solvable, it is enough to show that if $H_i \neq H_{i+1}$, then H_{i+1}/H_i is a cyclic group of prime order. Using the second isomorphism theorem of groups we have

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

Since $H_{i+1} < G_{i+1}$ and $G_i \lhd G_{i+1}$, we obtain $H_{i+1}G_i < G_{i+1}$. Hence we have that

$$\frac{H_{i+1}}{H_i} = \frac{H_{i+1}G_i}{G_i} < \frac{G_{i+1}}{G_i}.$$

Since by assumption we have that $\frac{G_{i+1}}{G_i}$ is cyclic of prime order, and since $H_i \neq H_{i+1}$, we conclude that $\frac{H_{i+1}}{H_i} = \frac{G_{i+1}}{G_i}$ is also a cyclic group of prime order, as required.

(b) Since $H \lhd G$ and $G_i < G$, we obtain that $H \lhd G_iH$. Hence we may set $L_i = \frac{G_iH}{H}$. Since $H \lhd G_{i+1}H$ and $G_i < G_{i+1}H$, we also have $G_iH \lhd G_{i+1}H$ and so

$$L_i = \frac{G_iH}{H} \lhd \frac{G_{i+1}H}{H} = L_{i+1}.$$

We obtain a sequence

$$\{e\} = L_0 \lhd L_1 \lhd \cdots \lhd L_n = G/H \tag{2}$$

of subgroups of H. As above, it is enough to show that if $L_i \neq L_{i+1}$, then $\frac{L_{i+1}}{L_i}$ is a cyclic group of prime order. By the third isomorphism theorem for groups we have

$$\frac{L_{i+1}}{L_i} = \frac{\frac{G_{i+1}H}{H}}{\frac{G_iH}{H}} \cong \frac{G_{i+1}H}{G_iH}.$$

Using the second isomorphism theorem for groups we have

$$\frac{L_{i+1}}{L_i} \cong \frac{G_{i+1}H}{G_iH} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iH)}.$$

Applying the third isomorphism theorem for groups once more we have

$$\frac{L_{i+1}}{L_i} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iH)} \cong \frac{\frac{G_{i+1}}{G_i}}{\frac{G_{i+1} \cap (G_iH)}{G_i}}.$$

Hence $\frac{L_{i+1}}{L_i}$ is isomorphic to a quotient of the group $\frac{G_{i+1}}{G_i}$. Since $\frac{G_{i+1}}{G_i}$ is cyclic of prime order and $L_i \neq L_{i+1}$, it follows that $\frac{L_{i+1}}{L_i} \cong \frac{G_{i+1}}{G_i}$ is cyclic of prime order as well.

(c) Since G/H is solvable, there exists a composition series

$$\{e\} = \overline{G}_0 \lhd \overline{G}_1 \lhd \cdots \lhd \overline{G}_n = G/H \tag{3}$$

of G/H with each factor $\frac{\overline{G}_{i+1}}{\overline{G}_i}$ being a cyclic group of prime order. By the correspondence theorem for subgroups it follows that there exist subgroups

$$\{e\} = G_0 < G_1 < \cdots < G_n < G$$

such that $\overline{G_i} \cong \frac{G_i}{H}$. In particular, since $\frac{G_i}{H} \lhd \frac{G_{i+1}}{H}$ is a strict subgroup, we have that $G_i \lhd G_{i+1}$ is also a strict subgroup. Furthermore, we have

$$G/H = \overline{G}_n \cong \frac{G_n}{H} \implies G_n = G,$$

and

$$\{e\} = \overline{G}_0 \cong \frac{G_0}{H} \implies G_0 = H.$$

Now since H is solvable there exists a composition series

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_k = H \tag{4}$$

of H with each factor $\frac{H_{i+1}}{H_i}$ being a cyclic group of prime order. Then we obtain a sequence

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_k = H = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

of subgroups of G. By construction every two consecutive subgroups are different. Moreover, H_{i+1}/H_i is a cyclic group of prime order by assumption, while by the third isomorphism theorem for groups we obtain that

$$\frac{G_{i+1}}{G_i} \cong \frac{\frac{G_{i+1}}{H}}{\frac{G_i}{H}} \cong \frac{\overline{G}_{i+1}}{\overline{G}_i}$$

is also a cyclic group of prime order by assumption. Hence G is solvable.

(d) We have that both $G_1 \cong G_1 \times \{e\} \lhd G_1 \times G_2$ and $\frac{G_1 \times G_2}{G_1 \times e} \cong G_2$ are solvable by assumption. The claim follows by part (c).

Problem 14. (Chapter 18.3) Show that the symmetric group S_n is solvable if and only if $n \leq 4$. (*Hint:* consider the cases $n = 1, 2, 3, 4$ and $n \geq 5$ separately.)

Solution. We have that $S_1 = \{e\}$ is a trivial group and so it is trivially solvable (it has no composition factors).

We have that $S_2 = \mathbb{Z}_2$ and so it is solvable as it is a finite abelian group.

Consider the alternating group $A_3 \lhd S_3$. If $S_3 = \{e, (12), (13), (23), (12)(13), (12)(23)\}$, then the alternating group A_3 is $A_3 = \{e, (12)(13), (12)(23)\}$. Then $A_3 \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$ are both simple. Then the composition series $\{e\} \lhd A_3 \lhd S_3$ gives the composition factors $A_3 \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$ which are both cyclic of prime order. Hence S_3 is solvable.

Consider the alternating group $A_4 \lhd S_4$. We have $|S_4| = 24$ and $|A_4| = 12$. Consider also the subgroup $V = \{e, (12)(34), (13)(24), (14)(23)\}$ of S_4. Notice the elements of V are the only even permutations of type $(2, 2)$ (that is, consisting of two disjoint transpositions). Since conjugation in S_4 does not change the cycle structure, we have that $gVg^{-1} \subseteq V$ for any $g \in S_4$ and hence for any $g \in A_4$. This shows that $V \lhd A_4$. Consider the sequence

$$\{e\} \lhd \{e, (12)(34)\} \lhd V \lhd A_4 \lhd S_4.$$

By a counting argument we have $S_4/A_4 \cong \mathbb{Z}_2$, $A_4/V \cong \mathbb{Z}_3$, $V/\{e, (12)(34)\} \cong \mathbb{Z}_2$ and $\{e, (12)(34)\} \cong \mathbb{Z}_2$. Hence all the composition factors of S_4 are cyclic groups of prime order and so S_4 is solvable.

Now assume that $n \geq 5$. First we claim that A_n is the subgroup of S_n generated by all 3-cycles. To see this, notice that if i, j, k, l are distinct, then

$$(ij)(kl) = (ikj)(kjl) \text{ and } (ij)(ik) = (ijk). \tag{5}$$

In particular, $(ij)(ik) = (ijk)$ implies that A_n contains all 3-cycles. Now let $\sigma \in A_n$. We may write $\sigma = (i_1 i_2)(i_3 i_4) \cdots (i_{4k-1} i_{4k})$ as a product of an even number of transpositions. Using (5) we may write each product of two consecutive transpositions in σ as a product of 3-cycles. Hence the set of 3-cycles generates A_n.

Next let $N \lhd A_n$ and assume that $N \neq \{e\}$. We claim that if N contains at least one 3-cycle, then $N = A_n$. Since A_n is generated by 3-cycles, it is enough to show that if N contains a 3-cycle, then N contains all 3-cycles. Let $(ijk) \in N$ and let $(i'j'k') \in S_n$ be an arbitrary 3-cycle. It is enough to show that $(i'j'k') \in N$. Since

elements with the same cycle structure are conjugate in S_n, there exist $\sigma \in S_n$ such that $(i'j'k') = \sigma^{-1}(ijk)\sigma$. If $\sigma \in A_n$, then $(i'j'k') \in N$ since N is a normal subgroup of A_n. If $\sigma \notin A_n$ then σ is an odd permutation. Then $\sigma^{-1}(ijk)\sigma = \sigma^{-1}(xy)^{-1}(ijk)(xy)\sigma$, where i, j, k, x and y are disjoint (which is possible since $n \geq 5$). Then $(xy)\sigma$ is even and so again $(i'j'k') \in N$, as required.

Now we claim that A_n is simple. In view of the previous paragraph, it is enough to show that if $N \triangleleft A_n$ with $N \neq \{e\}$, then N contains a 3-cycle. We may write the elements of N as products of disjoint cycles and let us consider the longest such disjoint cycle $(i_1 \cdots i_s)$ that may appear. Then there exists an element $\sigma = \rho(i_1 \cdots i_s) \in N$ such that ρ acts as the identity on $i_1, \ldots, i_s$. We consider several cases and in each case we either reach a contradiction or we show that a 3-cycle belongs to N.

Case $s \geq 4$. Then $(i_1i_2i_3)\sigma(i_1i_2i_3)^{-1} \in N$ since $N \triangleleft A_n$ and $(i_1i_2i_3) \in A_n$. We have

$$\sigma^{-1}(i_1i_2i_3)\sigma(i_1i_2i_3)^{-1} = (i_1 \cdots i_s)^{-1}\rho^{-1}(i_1i_2i_3)\rho(i_1 \cdots i_s)(i_1i_2i_3)^{-1} = (i_s \cdots i_1)(i_1i_2i_3)(i_1 \cdots i_s)(i_3i_2i_1) = (i_1i_3i_s) \in N,$$

where we used the fact that ρ acts as the identity on $i_1, \ldots, i_s$. Hence we have found a 3-cycle in N.

Case $s = 3$ and there exists a 3-cycle in ρ. Hence $\rho = \rho'(i_4i_5i_6)$ with $i_1, \ldots, i_6$ all disjoint and ρ' acts as the identity on $i_1, \ldots, i_6$. Then $\sigma = \rho'(i_4i_5i_6)(i_1i_2i_3)$ and $(i_1i_2i_4)\sigma(i_1i_2i_4)^{-1} \in N$ since $N \triangleleft A_n$ and $(i_1i_2i_4) \in A_n$. We have

$$\sigma^{-1}(i_1i_2i_4)\sigma(i_1i_2i_4)^{-1} = (i_3i_2i_1)(i_6i_5i_4)\rho'^{-1}(i_1i_2i_4)\rho'(i_4i_5i_6)(i_1i_2i_3)(i_4i_2i_1) = (i_1i_4i_2i_6i_3) \in N,$$

where we used the fact that ρ' acts as the identity on $i_1, \ldots, i_6$. But this contradicts $s = 3$ since we found a 5-cycle in N.

Case $s = 3$ and there exists no 3-cycle in ρ. Then $\sigma = \rho(i_1i_2i_3)$ and ρ is a product of transpositions. In particular, $\rho^2 = e$. We have

$$\sigma^2 = \rho(i_1i_2i_3)\rho(i_1i_2i_3) = \rho^2(i_1i_2i_3)(i_1i_2i_3) = (i_1i_3i_2) \in N,$$

where we used the fact that ρ acts as the identity on i_1, i_2, i_3. Hence we found a 3-cycle in N.

Case $s = 2$. In this case $\sigma = \rho(i_1i_2)$ is a product of transpositions. Since $\sigma \in N \subseteq A_n$, we have that ρ is a product of an odd number of transpositions. In particular, $\rho = \rho'(i_3i_4)$ and $\sigma = \rho'(i_3i_4)(i_1i_2)$ with $i_1, \ldots, i_4$ distinct and ρ' acts as the identity on $i_1, \ldots, i_4$. Then $(i_1i_2i_3)\sigma(i_1i_2i_3)^{-1} \in N$ since $N \triangleleft A_n$ and $(i_1i_2i_3) \in A_n$. We have

$$\sigma^{-1}(i_1i_2i_3)\sigma(i_1i_2i_3)^{-1} = (i_2i_1)(i_3i_4)\rho'^{-1}(i_1i_2i_3)\rho'(i_3i_4)(i_1i_2)(i_3i_2i_1) = (i_1i_3)(i_2i_4) \in N.$$

Let i_5 be different from $i_1, \ldots, i_4$. Then

$$N \ni (i_1i_3i_5)^{-1}(i_1i_3)(i_2i_4)(i_1i_3i_5)(i_1i_3)(i_2i_4) = (i_1i_3i_5),$$

contradicting $s = 2$ since we found a 3-cycle in N.

Hence we have shown that A_n is simple for $n \geq 5$. Since $S_n/A_n \cong \mathbb{Z}_2$, it follows that $\{e\} \triangleleft A_n \triangleleft S_n$ is a composition series of S_n and so its composition factors are $\{\mathbb{Z}_2, A_n\}$. But A_n is not a cyclic group of prime order, since the order of A_n is $\frac{n!}{2}$, which is not a prime number for $n \geq 5$. Therefore, we conclude that S_n is not solvable for $n \geq 5$.

Problem 15. (Chapter 18.5) This problem aims to demonstrate that the last sentence of Theorem 18.5.9 in the book is wrong. That is, we show that there exists α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ but α is not constructible.

Assume that $z \in \mathbb{K}$ is a constructible number.

(a) Show that there exists a normal field extension $\mathbb{Q} \subseteq N$ such that $z \in N$ and $[N : \mathbb{Q}] = 2^n$ for some $n \geq 0$. (*Hint:* Use Theorem 17.9 to obtain a sequence of field extensions and use induction to show that each of the fields in that sequence is included in another field as part of a normal extension of degree some power of 2.)

(b) Show that the splitting field of the minimal polynomial of z over $\mathbb{Q}$ has degree 2^n for some $n \geq 0$.

(c) Show that the Galois group of the minimal polynomial of z over $\mathbb{Q}$ has degree 2^n for some $n \geq 0$.

(d) Assume that we are given a monic polynomial $f(x) \in \mathbb{Q}[x]$ which is irreducible over $\mathbb{Q}$, of degree 4 and such that the Galois group of $f(x)$ is S_4[1]. Let α be a root of $f(x)$. Show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ but α is not constructible.

Solution.

(a) By Theorem 17.9 there exists a sequence of field extensions

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$$

with $z \in K_m$ and such that $[K_i : K_{i-1}] = 2$, $K_i = K_{i-1}(z_i)$ for some $z_i^2 \in K_{i-1}$. We claim that for every $0 \leq i \leq m$ there exists a normal field extension $K_i \subseteq N_i$ with $[N_i : \mathbb{Q}] = 2^{m_i}$ for some $m_i \geq 0$. We show this claim using induction on i.

For $i = 0$ we have $K_0 = \mathbb{Q}$ and we may take, for example, $N_0 = \mathbb{Q}(\sqrt{2})$. For the induction step assume that $K_{i-1} \subseteq N_{i-1}$ is a normal field extension and $[N_{i-1} : \mathbb{Q}] = 2^{m_i}$. Let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of z_i over $\mathbb{Q}$ (z_i is algebraic since the extension $\mathbb{Q} \subseteq K_{i-1}(z_i) = \mathbb{Q}(z_1, \ldots, z_i)$ is finite). Let $p_i(x) \in \mathbb{Q}[x]$ be the minimal polynomial of z_i over $\mathbb{Q}$ and let $q_i(x) \in \mathbb{Q}[x]$ be the minimal polynomial of z_i^2 over $\mathbb{Q}$. Let $w_1, w_2, \ldots, w_s$ be the roots of $p_i(x)$ in $\overline{\mathbb{Q}}$, where we may assume $z_i = w_1$. Let $\sigma^j : \mathbb{Q}(w_1) \to \mathbb{Q}(w_j)$ be the isomorphism defined by $\sigma^j(w_1) = w_j$ and $\sigma^j\big|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Then

$$\sigma^j(z_i^2) = \sigma^j(w_1^2) = \sigma^j(w_1)^2 = w_j^2$$

and

$$q_i(w_j^2) = q_i(\sigma^j(z_i^2)) = \sigma^j(q_i(z_i^2)) = 0.$$

Hence $w_1^2, w_2^2, \ldots, w_s^2$ are all roots of $q_i(x)$. Since $w_1^2 = z_i^2 \in K_{i-1} \subseteq N_{i-1}$, we have that $w_1^2 \in N_{i-1}$. Since $K_{i-1} \subseteq N_{i-1}$ is normal, we conclude that $w_1^2, w_2^2, \ldots, w_s^2 \in N_{i-1}$. Now consider the sequence of field extensions

$$N_{i-1} \subseteq N_{i-1}(w_1) \subseteq N_{i-1}(w_1, w_2) \subseteq \cdots \subseteq N_{i-1}(w_1, w_2, \ldots, w_s).$$

Then $w_i^2 \in N_{i-1}$ and hence $w_i^2 \in N_{i-1}(w_1, \ldots, w_{i-1})$. Hence we obtain that

$$[N_{i-1}(w_1, \ldots, w_i) : N_{i-1}(w_1, \ldots, w_{i-1})] \leq 2$$

for $1 \leq i \leq s$. In particular we have that

$$[N_{i-1}(w_1, \ldots, w_i) : N_{i-1}(w_1, \ldots, w_{i-1})] = 1 \text{ or } 2.$$

Set $N_i = N_{i-1}(w_1, \ldots, w_s)$. Then we compute

$$[N_i : N_{i-1}] = [N_{i-1}(w_1, \ldots, w_s) : N_{i-1}(w_1, \ldots, w_{s-1})] \cdot \ldots \cdot [N_{i-1}(w_1) : N_i] = 2^l$$

for some $0 \leq l \leq s$. On the other hand we have $K_{i-1} \subseteq N_{i-1} \subseteq N_i$ and $z_i = w_1 \in N_i$. Hence

$$K_i = K_{i-1}(z_i) \subseteq N_i.$$

For the induction step it remains to show that $K_i \subseteq N_i$ is a normal extension. We have that N_i is a normal extension of $\mathbb{Q}$ since it is the splitting field of $p(x)$ over $\mathbb{Q}$. Since $\mathbb{Q} \subseteq K_i \subseteq N_i$ and $\mathbb{Q} \subseteq N_i$ is normal, we conclude that $K_i \subseteq N_i$ is also normal by Problem 12 in Problem Set 2. This proves the induction step. Then N_m is by construction a normal extension of $\mathbb{Q}$ with $[N_m : \mathbb{Q}] = 2^n$ for some $n \geq 0$, as required.

(b) Let E be the splitting field of the minimal polynomial of z and let N be as in part (a). Since $z \in N$ and $\mathbb{Q} \subseteq N$ is a normal field extension, we have that $\mathbb{Q} \subseteq E \subseteq N$. Since $[N : \mathbb{Q}] = 2^n$ for some $n \geq 0$, we have

$$2^n = [N : \mathbb{Q}] = [N : E][E : \mathbb{Q}],$$

and the claim follows.

[1]Example: $x^4 - x - 1$ is one such polynomial, although with our tools it is not easy to see that this polynomial satisfies these requirements. One needs the notions of *resolvent* and *discriminant* to show this.

(c) Let E be the splitting field of the minimal polynomial of z over $\mathbb{Q}$. By the FTGT we have that

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 2^n,$$

for some $n \geq 0$, where the last equality follows by part (b).

(d) We have that

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

since $f(x)$ is irreducible. On the other hand, let E be the splitting field of $f(x)$. By assumption we have that

$$|\mathrm{Gal}(E/\mathbb{Q})| = |S_4| = 4! = 24,$$

which is not a power of 2. Since $f(x)$ is the minimal polynomial of α, it follows by part (c) that α is not constructible.