MATH 830 FALL 2021: HOMEWORK 3 SOLUTIONS

You may work together on these homework problems, but each student in the class must write up the solutions to this assignment entirely on their own. You may use the class notes, previous homework or class supplements, but you may not consult any other sources, including, any algebra textbook, the internet, graduate students not in this class, or any professor except your Math 830 instructor. Please upload a pdf copy of your solutions to Blackboard no later than 10pm on Monday October 19.

1. Let K denote the splitting field of $x^3 - 2$ over $\mathbb{Q}$. In Example 15.2 (b) we illustrated the one-to-one correspondence between the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the intermediate fields $\mathbb{Q} \subseteq E \subseteq K$. Complete this example by verifying parts (i), (ii) and (iii) of the Galois Correspondence Theorem.

Solution. Recall that $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\epsilon, \sqrt[3]{2}\epsilon^2) = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$. From Example 15.2, we have that the only intermediate fields between $\mathbb{Q}$ and K are: $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\epsilon), \mathbb{Q}(\sqrt[3]{2}\epsilon^2)$ and $\mathbb{Q}(\epsilon)$.Though we used part (i) of the Galois Correspondence Theorem to help identify the intermediate fields, we didn't have to. For example, our calculations showed that $\mathbb{Q}(\epsilon)$ is contained in the field field of $\langle\hat{\sigma_1}\rangle$. But $[K : \mathbb{Q}(\epsilon)] = 3$, so there are no fields between $\mathbb{Q}(\epsilon)$ and K, which forces the fixed field of $\langle\hat{\sigma_1}\rangle$ to be $\mathbb{Q}(\epsilon)$ and thus,

$$[K^{\langle\hat{\sigma_1}\rangle} : \mathbb{Q}] = [\mathbb{Q}(\epsilon) : \mathbb{Q}] = 2 = [\mathrm{Gal}(K)/\mathbb{Q}) : \langle\hat{\sigma_1}\rangle].$$

The other equality in indices in part (i) can be shown in a similar manner.

For part (ii), all extensions in question are separable, so we just have to show that K is a splitting field over each intermediate field. If we let E denote any one of the fields, $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\epsilon), \mathbb{Q}(\sqrt[3]{2}\epsilon^2)$, then $K = E(\epsilon)$ is the splitting field of $x^2 + x + 1$ over E. Thus K is Galois over E. If $E = \mathbb{Q}(\epsilon)$, then $K = E(\sqrt[3]{2})$ is the splitting field of $x^3 - 2$ over E, so K is Galois over E.

Finally $\mathbb{Q}(\epsilon)$ is the only intermediate field that is Galois over $\mathbb{Q}$ and $\langle\hat{\sigma_1}\rangle$ is the only subgroup of the Galois group that is a normal subgroup (since the only normal subgroup of S_3 is the subgroup generated by one of the two 3-cycles).

2. Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$.

(a) Use Zorn's Lemma to show there exists a subfield $F \subseteq \overline{\mathbb{Q}}$ maximal with respect to the property of not containing $\sqrt{2}$.

(b) For F as in (a), let K be a finite extension of F. Prove that K is Galois over F and $\mathrm{Gal}(K/F)$ is a cyclic group. (Hint: Reduce to the case that K is Galois over F and use the Galois Correspondence Theorem.)

Note: there is nothing special about $\sqrt{2}$ in this problem. Your argument should work with any $\alpha \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$.

Solution. For (a), let S denote the subfields of $\overline{\mathbb{Q}}$ containing $\mathbb{Q}$, but not containing $\sqrt{2}$. If $\{E_\alpha\}_{\alpha \in A}$ is a chain in S, then, as we have seen before, $\bigcup_{\alpha \in A} E_\alpha$ is a field, certainly contained in $\overline{\mathbb{Q}}$ and it clearly does not contain $\sqrt{2}$. Thus, the chain has an upper bound in S. Therefore, S has a maximal element, F

For (b), suppose that K is a finite extension of F. Let K_0 be a finite extension of F containing K such that K_0 is Galois over F. One way to see this is as follows: Since K is separable over F (F has characteristic zero), $K = F(\alpha)$. Let K_0 be the field obtained by adjoining to F all of the roots of the minimal polynomial for α over F. Then K_0 is a splitting field over F, and thus Galois over F, since separability holds automatically.[1] If $\mathrm{Galois}(K_0/F)$ is cyclic, it is abelian, so that $\mathrm{Galois}(K_0/K)$ is normal in $\mathrm{Galois}(K_0/F)$ and K is Galois over F. In this case $\mathrm{Gal}(K/F)$ is a homomorphic image of $\mathrm{Galois}(K_0/F)$, and thus, is also cyclic. Therefore, replacing K_0 by K, we may begin again, assuming that K is also Galois over F.

[1] Note that more generally, if K is a finite extension of a field F, generated by finitely many α_i over F, if we let K_0 be the field obtained by adjoining to F all of the roots of the minimal polynomials for the α_i then K_0 is a splitting field over F. However, in positive characteristic, this need not be a Galois extension of F.

Now, by the assumption on F, every intermediate field between F and K contains $F(\sqrt{2})$. Therefore, if we let $H := \text{Galois}(K/F(\sqrt{2}))$, then by the Galois Correspondence Theorem, H is a subgroup of $\text{Gal}(K/F)$ containing every proper subgroup of $\text{Gal}(K/F)$. If we take $a \in \text{Gal}(K/F)\backslash H$, then $\langle a \rangle = \text{Gal}(K/F)$, which gives what we want. □

3. Let $K \subseteq H$ be subgroups of the group G and suppose $\{g_\alpha H\}_{\alpha \in A}$ are the distinct left cosets of H in G and $\{h_\beta K\}_{\beta \in B}$ are the distinct left cosets of K in H.

(i) Prove that H is normal in G if for all $\alpha \in A$, $g_\alpha H = Hg_\alpha$.
(ii) Prove that $\{g_\alpha h_\beta K\}_{\alpha \in A, \beta \in B}$ are the distinct left cosets of K in G. Here you may assume that the indexing sets A, B are disjoint.
(iii) Conclude that if $[G : H]$ and $[H : K]$ are finite, then $[G : K] = [G : H] \cdot [H : K]$.

Solution. For (i), let $g \in G$. Then $g \in g_\alpha H$, for some α. Thus, $g \in gH = g_\alpha H = Hg_\alpha$, which implies $Hg = Hg_\alpha$. Thus, $gH = Hg$, which shows that H is normal in G.

For (ii) first note that if $g \in G$, then $g \in g_\alpha H$ for some $\alpha \in A$. Thus, we can write $g = g_\alpha h$ for some $h \in H$. But then $h \in h_\beta K$, for some $\beta \in B$, so that $h = h_\beta k$ for some $k \in K$, so that $g = g_\alpha h_\beta k$, which gives $gK = g_\alpha h_\beta K$, showing that the set $\{g_\alpha h_\beta K\}_{\alpha \in A, \beta \in B}$ accounts for all cosets of K in G. To see that these cosets are distinct, suppose, $g_\alpha h_\beta K = g_{\alpha'} h_{\beta'} K$. If $g_\alpha = g_{\alpha'}$, then we have $h_\beta K = h_{\beta'} K$, which is a contradiction. If $g_\alpha \neq g_{p'}$, we have $g_\alpha h_\beta = g_{\alpha'} h_{\beta'} k$, for some $k \in K$. It follows that $g_{\alpha'}^{-1} g_\alpha = h_{\beta'} k h_\beta^{-1} \in H$. Thus, $g_\alpha H = g_{\alpha'} H$, a contradiction. It follows that the cosets $\{g_\alpha h_\beta K\}_{\alpha \in A, \beta \in B}$ are distinct. Now (iii) follows immediately from (ii). □

4. Let $N \subseteq G$ be a normal subgroup. Let $(G/N)_L$ denote the group of left coset of N in G and $(G/N)_R$ denote the group of right coset of N in G. Either prove that these groups are isomorphic or give a counter-example showing that these groups are not isomorphic.

Solution. Define $\phi : (G/N)_L \to (G/N)_R$ by $\phi(aN) = Na$. Note that if $aN = bN$, then $Na = Nb$, since $aN = Na$ and $bN = Nb$. Moreover,

$$\phi(aNbN) = \phi(abN) = Nab = NaNb = \phi(aN)\phi(bN)$$

so ϕ is a group homomorphism, which is clearly 1-1 and onto. □

Note: If N is a subgroup group of G, but not necessarily a normal subgroup, one can show that the set function ψ defined by $\psi(gN) = Ng^{-1}$ is a 1-1, onto function from the set of distinct left cosets of N in G to the set of distinct right cosets of N in G, even if these sets are infinite.

5. Let G be a cyclic group.

(i) Prove that every subgroup of G is cyclic.
(ii) Let G be a cyclic group of order $n > 1$. Prove that for each positive integer d dividing n, there exists a unique subgroup H_d of order d. Use this fact to draw a diagram illustrating the subgroup structure of $\mathbb{Z}_{24}$.

Solution. Set $G := \langle a \rangle$ and suppose $H \subseteq G$ is a subgroup. For (i), if we let k denote the least positive integer such that $a^k \in H$, then for $a^j \in H$, write $j = ck + r$, with $0 \leq r < k$. Then $a^j = (a^k)^c \cdot a^r$. Since $a^{kc} \in H$, $a^r \in H$. By the choice of k, $r = 0$. Thus, $a^j \in \langle a^k \rangle$, which shows $H = \langle a^k \rangle$. Note also that k divides n. To see this, write $n = tk + r$, with $0 \leq r < k$. Then $e = a^n = (a^k)^t \cdot a^r$, which shows that $a^r \in H$, so again, $r = 0$, showing k divides n.

For (ii) suppose $n = dk$. Set $H := \langle a^k \rangle$. Then clearly $o(a^k) = d$, which shows $|H| = d$. Suppose that K is a subgroup of order d. Then $K = \langle a^j \rangle$, where j is the least positive integer such that $a^j \in$ and $o(a^j) = d$. Then $a^{jd} = e$. Since $o(a) = n$, $jd \geq n$, If $jd > n$, write $jd = nc + r$, with $0 \leq r < n$. This yields $a^r = e$, which is a contradiction. Thus, $jd = kd$, so that $j = k$. If follows that $H = K$, so that H is the unique subgroup of order d.

A diagram of the subgroups of $\mathbb{Z}_{24}$:

$$\begin{tikzcd}
 & \mathbb{Z}_{24} & \\
\langle 3\rangle \arrow[ur] & & \langle 2\rangle \arrow[ul] \\
\langle 6\rangle \arrow[u] \arrow[urr] & & \langle 4\rangle, \arrow[u] \\
 & \langle 12\rangle \arrow[ul] \arrow[ur] & \langle 8\rangle \arrow[u] \\
 & \langle 0\rangle \arrow[u] \arrow[ur] &
\end{tikzcd}$$

where the diagonal arrow departing from $\langle 6\rangle$ is meant to indicate that $\langle 6\rangle \subsetneq \langle 2\rangle$. □

6. Let G be a group and $H, K \subseteq G$ finite subgroups, prove that $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$. Note that we are not requiring that the set HK be a subgroup of G. Discuss the conditions under which HK is a subgroup.

Solution. Suppose $H = \{h_1, \ldots, h_s\}$ so that $|H| = s$ and $(H \cap K)k_1, \ldots, (H \cap K)k_t$ are the distinct right cosets of $H \cap K$ in K, so that $t = \frac{|K|}{|H\cap K|}$. We need to show that $|HK| = st$. For this, consider the set $X = \{h_ik_j\}$ with $1 \le i \le s$ and $1 \le j \le t$. It suffices to show that $X = HK$ and the elements h_ik_j are distinct. Suppose $h_ik_j = h_ck_d$. Then $h_c^{-1}h_i = k_jk_d^{-1}$ belongs to $H \cap K$. Thus $k_j \in (H \cap K)k_d$, so that $(H \cap K)k_j = (H \cap K)k_d$. Since the cosets are distinct, this forces $k_j = k_d$. From $h_ik_j = h_ck_d$, it follows that $h_i = h_c$. Thus, there are st distinct elements in X. Finally, if $hk \in HK$, then $k \in (H \cap K)k_j$, for some j. Thus, $hk = h(h_0k_j)$, for some $h_0 \in H \cap K$. Therefore $hk = (hh_0)k_j \in X$. Thus, $X = HK$ and we have $|HK| = st$, as required.

For the second statement, it is not difficult to show that HK is a subgroup of G if and only if $HK = KH$. □

7. Treating $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ as abelian groups under addition, consider the abelian group $\mathbb{Q}/\mathbb{Z}$. Prove :

(i) Every element of $\mathbb{Q}/\mathbb{Z}$ is a coset of the form $q + \mathbb{Z}$, with $0 \le q < 1$.
(ii) Every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, but there are elements in $\mathbb{Q}/\mathbb{Z}$ of arbitrarily large order.
(iii) $\mathbb{Q}/\mathbb{Z}$ is the subgroup of $\mathbb{R}/\mathbb{Z}$ of elements of finite order.

Proof. For (i), suppose $r + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. We may write $r = r_0 + n$, where n is an integer and $0 \le r_0 < 1$. But then $r + \mathbb{Z} = (r_0 + n) + \mathbb{Z} = r_0 + \mathbb{Z}$.

For (ii), if $r + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, write $r = \frac{a}{b}$, with $a, b \in \mathbb{Z}$, and $b > 0$. Then $b \cdot r$, which is r added to itself b times, is an element of $\mathbb{Z}$. This shows that in $\mathbb{Q}/\mathbb{Z}$, $r + \mathbb{Z}$ added to itself finitely many times is $0 + \mathbb{Z}$. Thus, $r + \mathbb{Z}$ has finite order. For $n \ge 1$, $\frac{1}{n} + \mathbb{Z}$ clearly has order n, so that $\mathbb{Q}/\mathbb{Z}$ has elements of arbitrarily large order.

For (iii), let $\alpha + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ have finite order. Then $n(\alpha + \mathbb{Z}) = n\alpha + \mathbb{Z} = 0 + \mathbb{Z}$, for some integer $n \ge 1$. Thus, $n\alpha \in \mathbb{Z}$, so that $n\alpha = m$, for some $m \in \mathbb{Z}$. But this implies $\alpha \in \mathbb{Q}$, and therefore, $\mathbb{Q}/\mathbb{Z}$ is the set of elements of finite order in $\mathbb{R}/\mathbb{Z}$. □

8. Let G be a group and $x, y \in G$. Set $[x, y] := xyx^{-1}y^{-1}$, the *commutator* of x and y. Note that $[x, y]^{-1}$ is also a commutator. Let $G^{(1)}$ denote the subgroup of G consisting of all finite products of $[x, y]$ such that $x, y \in G$. $G^{(1)}$ is called the *commutator subgroup* of G. Prove the following statements:

(i) $G^{(1)}$ is a (not necessarily proper) normal subgroup of G.
(ii) For a normal subgroup $N \subseteq G$, G/N is abelian if and only if $G^{(1)} \subseteq N$.

Solution. For (i), by what we have mentioned in the statement of the problem, we just have to check the normal property. If $[x_1, y_1] \cdot [x_2, y_2] \cdots [x_n, y_n] \in G^{(1)}$, then for any $a \in G$, we have

$$a^{-1}[x_1, y_1] \cdot [x_2, y_2] \cdots [x_n, y_n]a = a^{-1}[x_1, y_1]a \cdot a^{-1}[x_2, y_2]a \cdots a^{-1}[x_n, y_n]a,$$

so it suffices to show that any conjugate of a commutator belongs to $G^{(1)}$. For this, we have

$$\begin{aligned} a^{-1}[x,y]a &= a^{-1}x^{-1}y^{-1}xya \\ &= (xa)^{-1}y^{-1}xya \\ &= (xa)^{-1}y^{-1}x(ayy^{-1}a^{-1})ya \\ &= \{(xa)^{-1}y^{-1}(xa)y\} \cdot y^{-1}a^{-1}ya, \end{aligned}$$

which is a product of two commutators and therefore belongs to $G^{(1)}$.

For part (ii), suppose $N \subseteq G$ is a normal subgroup. Then G/N is abelian if and only if $xNyN = yNxN$ for all $x, y \in G$, which happens if and only if $xyN = yxN$ if and only if $(yx)^{-1}xy \in N$ if and only if $x^{-1}y^{-1}yx \in N$. Since this is true for all x, y, and N is a subgroup, the latter happens if and only if $G^{(1)} \subseteq N$. □

9. Let G be a group. For $i \geq 2$, set $G^{(i)} := (G^{(i-1)})^{(1)}$, the commutator subgroup of $G^{(i-1)}$. Use the previous problem to prove that G is solvable if and only if $G^{(n)} = \{e\}$, for some $n \geq 1$.

Solution. We first note that if $A \subseteq B$ are subgroups of G, then $A^{(1)} \subseteq B^{(1)}$. Now suppose G is solvable, with solvable series

$$\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_{r-1} \subseteq N_r = G.$$

Since G/N_{r-1} is abelian, by the previous problem, $G^{(1)} \subseteq N_{r-1}$. Since N_{r-1}/N_{r-2} is abelian, $N_{r-1}^{(1)} \subseteq N_{r-2}$. By the comment above, $G^{(2)} = (G^{(1)})^{(1)} \subseteq N_{r-1}^{(1)} \subseteq N_{r-2}$. Continuing inductively, it follows that for all $1 \leq i \leq r$, $G^{(i)} \subseteq N_{r-i}$. Therefore $G^{(r)} \subseteq N_r = \{e\}$, which shows $G^{(r)} = \{e\}$.

Conversely, if $G^{(n)} = \{e\}$ for some n, then

$$\{e\} = G^{(n)} \subseteq G^{(n-1)} \subseteq \cdots \subseteq G^{(1)} \subseteq G,$$

is a solvable series. □

10. For $n \geq 2$, set $\sigma := (1,2)$, $\tau := (1,2,\ldots,n) \in S_n$. Show that no proper subgroup of S_n contains both σ and τ. In other words, $S_n = \langle \sigma, \tau \rangle$. Does this generalize to any 2-cycle and any n-cycle?

Solution. It is easy to check that for any any 2-cycle (a,b) and $\gamma \in S_n$, that $\gamma(a,b)\gamma^{-1} = (\gamma(a), \gamma(b))$. Thus, since $\tau^{i-1}(1) = i$ and $\tau^{i-1}(2) = i+1$, it follows that $\tau^{i-1}(1,2)\tau^{-(i-1)} = (i, i+1)$ belongs to the subgroup generated by σ and τ. Since S_n is generated by 2-cycles, it suffices to show that any 2-cycle is a product of 2-cycles with adjacent entries. Let (a,b) be a 2-cycle, and we assume $a < b$. Say , $b = a + i$, with $i \geq 1$. Then,

$$(a,b) = (a,a+1)(a+1,a+2)\cdots(a+i-2,a+i-1)(a+i-1,b)(a+i-2,a+i-1)\cdots(a+1,a+2)(a,a+1).$$

For the second statement, in S_4 if we take $\sigma = (2,4)$ and $\tau = (1,2,3,4)$, an easy calculation shows that $\tau\sigma = (1,2)(3,4) = \sigma\tau^3$. It follows that, any finite product involving σ and τ can be written in the form $\sigma^i\tau^j$, with $0 \leq i \leq 1$ and $0 \leq j \leq 3$. Thus, the subgroup of S_4 generated by σ and τ has at most eight elements. Therefore, σ and τ do not generate S_4. □

Bonus Problem. . Let $K := F(x)$ denote the rational function field in one variable over $F$and $\sigma : K \to K$ be a field homomorphism.

(i) Prove that σ is an automorphism of K fixing F if and only if σ is a fractional linear transformation, i.e., σ fixes F and $\sigma(x) = \frac{ax+b}{cx+d}$, where $a, b, c, d \in F$ satisfy, $ad - bc \neq 0$. Hint: Note that σ is determined by its value on x and use problem 10 from Homework 1.

(ii) Since the degree of K over F is infinite, let us say that K is Galois over F if the fixed field of $\mathrm{Gal}(K/F)$ is F. Prove that K is Galois over F if and only if F is infinite. (Again problem 10 from Homework 1 might be useful.)

Solution. This is a difficult problem, if one is not used to working with the rational function field in one variable over F. For one direction, suppose σ is an automorphism of K fixing F and set $\sigma(x) := \frac{f(x)}{g(x)}$. Then, since σ is an automorphism of K fixing F, $F(\sigma(x)) = \sigma(F(x)) = F(x)$. Thus, $[K : F(\sigma(x))] = 1$. By Homework 1, problem 10, the maximum of the degrees of $f(x)$ and $g(x)$ equals 1. Therefore, we may write $\sigma(x) = \frac{ax+b}{cx+d}$, where $a, b, c, d \in F$, and a, b not both 0. Suppose $ad - bc = 0$. Then the second row of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over F is a multiple of the first row. Therefore, there exists $0 \neq \lambda \in F$ such that $cx + d = \lambda(ax + b)$. Therefore $\lambda\sigma(x) = \lambda \cdot \frac{ax+b}{cx+d} = 1$. It follows that

$$\sigma(\lambda x - 1) = \lambda \cdot \sigma(x) - 1 = 0,$$

which contradicts σ being an automorphism. Therefore, $ad - bc \neq 0$.

Conversely, suppose $\sigma : K \to K$ is defined by $\sigma(x) = \frac{ax+b}{cx+d}$, where $a, b, c, d \in F$ satisfy, $ad - bc \neq 0$. Note that σ extends to all of K by defining $\sigma(\frac{f(x)}{g(x)}) := \frac{f(\sigma(x))}{g(\sigma(x))}$, for all $\frac{f(x)}{g(x)} \in K$. It is straightforward to check that σ is a field homomorphism as long as $\sigma(x)$ is not algebraic over F. Indeed, if we set $\sigma(x) := u$, then we can think of u as a variable over F, and then $\sigma(\frac{f(x)}{g(x)}) = \frac{f(u)}{g(u)}$, for all $\frac{f(x)}{g(x)} \in K$, and this is easily seen to be a field homomorphism. So, assume for the moment that $\sigma(x)$ is not algebraic over F, and thus σ is a field homomorphism. Since $ad - bc \neq 0$, there exists a matrix equation over F:

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then, using the matrix equation above, we have

$$\sigma(\frac{ex+f}{gx+h}) = \frac{e\sigma(x)+f}{g\sigma(x)+h} = \frac{e(\frac{ax+b}{cx+d})+f}{g(\frac{ax+b}{cx+d})+h} = \frac{(ea+cf)x+(eb+df)}{(ga+hc)x+(gb+hd)} = x.$$

This implies σ is surjective, since the image of σ equals $F(\sigma(x))$ which is a subfield of K, and since x is in the image of σ, $F(x)$ is in the image of σ, so σ is onto. Therefore σ is an automorphism of K.

Finally, suppose $\sigma(x) = \frac{ax+b}{cx+d}$ were algebraic over F. First, assume $c \neq 0$. Using the division algorithm, $\sigma(x) = \frac{d}{c} + \frac{b - \frac{ad}{c}}{cx+d}$, where by assumption, $b - \frac{ad}{c} \neq 0$. Then, using that sums, products and inverses of algebraic elements are algebraic, we get that $\frac{1}{cx+d}$ is algebraic over F, and thus $cx + d$ is algebraic over F, and then x is algebraic over F, which is a contradiction. Therefore, $\sigma(x)$ is not algebraic over F. A similar, though simpler, argument shows that if $c = 0$, then $\sigma(x) = \frac{ax+b}{d}$ is not algebraic over F.

For part (ii), by part (i) we have that $\mathrm{Gal}(K/F)$ is the set of all automorphisms of K with $\sigma(x) = \frac{ax+b}{cx+d}$, where $a, b, c, d \in F$ satisfy, $ad - bc \neq 0$. Now, suppose F is finite. Then, there are only finitely many expressions of the form $\frac{ax+b}{cx+d}$ where $a, b, c, d \in F$ (satisfy, $ad - bc \neq 0$). Thus, $\mathrm{Gal}(K/F)$ is finite, say $\mathrm{Gal}(K/F) = \{id, \sigma_2, \ldots, \sigma_n\}$. Then clearly, any elementary symmetric function in $x, \sigma_2(x), \ldots, \sigma_n(x)$ belongs to the fixed field F_0 of $\mathrm{Gal}(K/F)$. Thus,

$$f(t) := (t - x)(t - \sigma_2(x)) \cdots (t - \sigma_n(x)) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n,$$

belongs to $F_0[t]$. Here $s_1, \ldots, s_n$ are the elementary symmetric functions in $x, \sigma_2(x), \ldots, \sigma_n(x)$. Since x is a root of $f(t)$, we cannot have all $s_i \in F$ otherwise x would be algebraic over F. Thus, some $s_i \in F_0 \backslash F$, which shows that K is not Galois over F.

Now suppose K is not Galois over F. Let $F_0 \neq F$ be the fixed field of $\mathrm{Gal}(K/F)$. Then $\mathrm{Gal}(K/F) = \mathrm{Galois}(K/F_0)$. However, by problem 10, from Homework 1, $[K : F_0] < \infty$. But this implies $|\mathrm{Gal}(K/F)| < \infty$, which, by part (i) implies that F is a finite field. □