Solutions to Homework 9

Problem 1. Cox, Section 6.4, Exercise 1, variant:
Let F be a field. For any $a, b \in F$, define $\gamma_{a,b} : F \to F$ by $\gamma_{a,b}(u) = au + b$.

(a) For any $a, b, c, d \in F$, prove that $\gamma_{a,b} \circ \gamma_{c,d} = \gamma_{s,t}$, where $s = ac$ and $t = ad + b$.

(b) For any $a, b \in F$, prove that $\gamma_{a,b}$ is bijective if and only if $a \neq 0$, and in that case, $\gamma_{a,b}^{-1} = \gamma_{c,d}$, where $c = a^{-1}$ and $d = -a^{-1}b$.

(c) Define $\mathrm{AGL}(1, F) = \{\gamma_{a,b} \,|\, (a, b) \in F^\times \times F\}$.
Prove that $\mathrm{AGL}(1, F)$ is a group under composition.

Proof. **(a)** Given $a, b, c, d \in F$, then for any $u \in F$, we have
$\gamma_{a,b} \circ \gamma_{c,d}(u) = \gamma_{a,b}\big(cu + d\big) = a\big(cu + d\big) + b = (ac)u + (ad + b) = \gamma_{s,t}(u)$, where $s = ac \in F^\times$ and $t = ad + b \in F$. QED (a)

(b) Given $a, b \in F$:
($\Rightarrow$): Assuming $\gamma_{a,b}$ is bijective, then since $0 \neq 1$ in F, we have $b = \gamma_{a,b}(0) \neq \gamma_{a,b}(1) = a + b$. Therefore $a = b$.
($\Leftarrow$): Assuming $a \neq 0$, define $c = a^{-1} \in F$ and $d = -a^{-1}b \in F$. Then by part (a), we have
$\gamma_{a,b} \circ \gamma_{c,d} = \gamma_{ac,ad+b} = \gamma_{1,0}$, since $ac = aa^{-1} = 1$ and $ad + c = -b + b = 0$,
and
$\gamma_{c,d} \circ \gamma_{a,b} = \gamma_{ca,cb+d} = \gamma_{1,0}$, since $ca = a^{-1}a = 1$ and $cb + d = a^{-1}b - a^{-1}b = 0$.
We have $\gamma_{1,0} = \mathrm{id}_F$ since $\gamma_{1,0}(u) = 1u + 0 = u$ for all $u \in F$. Thus, the two formulas above show that $\gamma_{a,b} \circ \gamma_{c,d} = \mathrm{id}_F$ and $\gamma_{c,d} \circ \gamma_{a,b} = \mathrm{id}_F$, so that $\gamma_{a,b}$ is bijective with inverse $\gamma_{c,d}$. QED (b)

(c) Consider the group S_F of all bijective functions $\phi : F \to F$ under composition. We will prove that $\mathrm{AGL}(1, F)$ is a subgroup of S_F.

First, $\mathrm{AGL}(1, F)$ is a subset of S_F by part (b), since every $\gamma \in \mathrm{AGL}(1, F)$ is bijective.

We have $(1, 0) \in F^\times \times F$, so $\gamma_{1,0} \in \mathrm{AGL}(1, F)$. [Note: As noted in (b) above, in fact, $\gamma_{1,0} = \mathrm{id}_F$ is the identity function.] Thus, $\mathrm{AGL}(1, F)$ is nonempty.

Given $\gamma_{a,b}, \gamma_{c,d} \in \mathrm{AGL}(1, F)$, we have $\gamma_{a,b} \circ \gamma_{c,d} = \gamma_{ac,ad+b}$ by part (a). Since $a, c \neq 0$, we have $ac \neq 0$, so that $\gamma_{a,b} \circ \gamma_{c,d} \in \mathrm{AGL}(1, F)$. Thus, $\mathrm{AGL}(1, F)$ is closed under $\circ$.

Finally, by part (b), the inverse of any $\gamma_{a,b} \in \mathrm{AGL}(1, F)$ is $\gamma_{c,d}$, where $c = a^{-1} \in F^\times$ and $d = -a^{-1}b \in F$, so that $\gamma_{c,d} \in \mathrm{AGL}(1, F)$. QED (c)

Problem 2. Cox, Section 6.4, Exercise 2, variant:
With notation as in the previous problem, define $\varphi : \mathrm{AGL}(1, F) \to F^\times$ by $\varphi(\gamma_{a,b}) = a$.

(a) Prove that φ is a surjective group homomorphism.

(b) Let $T = \ker(\varphi) = \{\gamma_{1,b} \,|\, b \in F\}$. Prove that T is isomorphic to the group $(F, +)$

[**Note**: It follows that $\mathrm{AGL}(1, F)/T \cong F^\times$, and hence $\mathrm{AGL}(1, F) \cong F \rtimes F^\times$.]

Proof. **(a)** Given $\gamma_{a,b}, \gamma_{c,d} \in \mathrm{AGL}(1, F)$, we have $\gamma_{a,b} \circ \gamma_{c,d} = \gamma_{s,t}$ where $s = ac$ and $t = ad + c$, by Problem 1(a) above.
Thus, $\varphi(\gamma_{a,b} \circ \gamma_{c,d}) = \varphi(\gamma_{s,t}) = s = ac = \varphi(\gamma_{a,b})(\varphi(\gamma_{c,d})$, proving that φ is a homomorphism.
Given $a \in F^\times$, then $\gamma_{a,0} \in \mathrm{AGL}(1, F)$, and $\varphi(\gamma_{a,0}) = a$. So φ is surjective. QED (a)

(b) Define $\psi : F \to T$ by $\psi(b) = \gamma_{1,b}$. It suffices to prove that ψ is an isomorphism of groups.

Given $b, c \in F$, then $\psi(b + c) = \gamma_{1,b+c} = \gamma_{1,b} \circ \gamma_{1,c} = \psi(b) \circ \psi(c)$, where the second equality is by Problem 1(a), since $1 \cdot 1 = 1$ and $1 \cdot c + b = b + c$. Thus, ψ is a homomorphism.

Given $b \in F$ such that $\psi(b) = \mathrm{id}_F = \gamma_{1,0}$, we have $\gamma_{1,b} = \gamma_{1,0}$, and hence $b = \gamma_{1,b}(0) = \gamma_{1,0}(0) = 0$. Thus, $\ker \psi = \{0\}$, and hence ψ is injective.
Finally, given $\gamma_{1,b} \in T$, we have $b \in F$, and hence $\psi(b) = \gamma_{1,b}$. Thus, ψ is surjective. QED (b)

Problem 3. (not from Cox):
Let $p \geq 2$ be prime, and let $H \subseteq S_p$ be a subgroup. Suppose that $p \,\big|\, |H|$ and that H contains a transposition. Prove that $H = S_p$.

Proof. By Cauchy's Theorem (from group theory), H must contain an element of order p. The only elements of order p in S_p are p-cycles, so H contains a p-cycle. Reindexing the symbols $\{1, \ldots, p\}$ if necessary, we may assume that $\sigma = (1\,2\,\ldots\,p) \in H$. Reindexing again, we may further assume that the 2-cycle is $\tau = (1\,j) \in H$, for some $2 \leq j \leq p$.
Define $\tilde{\sigma} = \sigma^{j-1}$, which has order p since $1 \leq j - 1 \leq p$ and hence $\gcd(j-1, p) = 1$. Therefore, $\tilde{\sigma}$ is still a p-cycle, and because $\tilde{\sigma}(1) = j$, it is a p-cycle of the form $\tilde{\sigma} = (1\,j\,\ldots)$.
Therefore, we may reindex *again* to relabel j as 2, $\tilde{\sigma}(j)$ as 3, and so on (while preserving the label 1), so that H contains the p-cycle $(1\,2\,\ldots\,p)$ and the transposition $(1\,2)$.
Thus, by HW 8 Problem 8 (Cox Exercise 6.4.7), we have $H = S_p$. QED

Problem 4. Cox, Section 6.4, Exercise 13:
Let L be the splitting field of $f(x) = 2x^5 - 10x + 5$ over $\mathbb{Q}$. Prove that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$.

Proof. $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of S_5 [by Proposition 6.3.1].
By Eisenstein's Criterion with $p = 5$, we see that f is irreducible over $\mathbb{Q}$. Therefore [e.g., by HW 8 Problem 5, i.e. Cox Exercise 6.2.6], $|\,\mathrm{Gal}(L/\mathbb{Q})|$ is divisible by $\deg(f) = 5$.
We have $L \subseteq \mathbb{C}$. We claim that L contains exactly three real roots of f. To see this, observe that

$$f(-2) = -39 < 0, \qquad f(0) = 5 > 0, \qquad f(1) = -3 < 0, \qquad f(2) = 17 > 0.$$

Since polynomials are continuous, it follows (from the Intermediate Value Theorem) that f has (at least) one root $\alpha_1 \in (-2, 0)$, (at least) one root $\alpha_2 \in (0, 1)$, and (at least) one root $\alpha_3 \in (1, 2)$. These three roots are all distinct, since they lie in disjoint intervals.
On the other hand, we have $f'(x) = 10x^4 - 10 = 10(x^4 - 1)$, which has real roots only at $x = \pm 1$. More precisely, $|f'(x)| > 0$ for $x < -1$ and $x > 1$, and $|f'(x)| < 0$ for $-1 < x < 1$. Thus, on the real line, f is:

- strictly increasing on $(-\infty, -1]$, and hence has at most one root there,
- strictly decreasing on $[-1, 1]$, and hence has at most one root there,
- strictly increasing on $[1, \infty)$, and hence has at most one root there.

[More technically, this is by the Mean Value Theorem, or by Rolle's Theorem: Since f is differentiable on $\mathbb{R}$, if $f(a) = f(b)$ for real numbers $a < b$, then there exists $c \in (a, b)$ such that $f'(c) = 0$.] Thus, $\alpha_1, \alpha_2, \alpha_3$ are the only three real roots of f, proving our claim.

Let α_4, α_5 denote the other two (non-real) roots of f. Let $\tau : \mathbb{C} \to \mathbb{C}$ denote complex conjugation. Then τ must map roots of f to roots of f (since the coefficients of f are real and hence are fixed by τ), so τ must be an automorphism of $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$. Since τ fixes each of $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ but not α_4, α_5, it follows that τ must swap α_4 and α_5.

Thus, $\mathrm{Gal}(L/\mathbb{Q})$, viewed as a subgroup H of S_5, has order divisible by 5 and contains a transposition. Because 5 is prime, by the previous problem, we have $H = S_5$. QED

Problem 5. Cox, Section 7.1, Exercise 1:
Let L/F be a finite extension, and let $H \subseteq \mathrm{Gal}(L/F)$ be a subgroup. Define

$$L_H = \{\alpha \in L \,|\, \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Prove that L_H is a subfield of L that contains F.

Proof. First, observe that for any $a \in F$, and any $\sigma \in H$, we have $\sigma(a) = a$, so $a \in L_H$. Thus, $F \subseteq L_H$.

To prove L_H is a subfield of L, we already know $L_H \supseteq F$ is nonempty. Given $\alpha, \beta \in L_H$, then for any $\sigma \in H$, we have:

$$\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta) = \alpha+\beta, \quad \sigma(-\alpha) = -\sigma(\alpha) = -\alpha, \quad \text{and} \quad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha \pm \beta,$$

so that $\alpha+\beta, -\alpha, \alpha\beta \in L_H$. Furthermore, if $\beta \neq 0$, then $\sigma(\beta^{-1}) = \sigma(\beta)^{-1} = \beta^{-1}$, so $\beta^{-1} \in L_H$ as well. Thus, L_H is a nonempty subset of L that is closed under the arithmetic operations, and hence L_H is a subfield of L. QED

Problem 6. Cox, Section 7.1, Exercise 9:
For each of the following extensions, determine whether it is a Galois extension. Of course, justify your answers, usually using one of the criteria in Theorem 7.1.1 or Theorem 7.1.5.

(a) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$

(b) $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$, where α, β are distinct roots of $x^3 + x^2 + 2x + 1$.

(c) $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$, where $p \geq 2$ is prime and t is a (formal) variable.

(d) $\mathbb{C}(t)/\mathbb{C}(t + t^{-1})$, where t is a (formal) variable.

(e) $\mathbb{C}(t)/\mathbb{C}(t^n)$, where $n \geq 1$ is an integer and t is a (formal) variable.

Solutions/Proofs. **(a)** **Not** Galois Observe that $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ has $L \subseteq \mathbb{R}$. However, the irreducible polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ has one root in L (namely $\sqrt[3]{2}$). We know that $\beta = \zeta_3\sqrt[3]{2}$ is another root of f, and that $\beta \notin \mathbb{R}$, so $\beta \notin L$. Thus, f has a root in L but does not split completely in L, so $L/\mathbb{Q}$ is **not** a normal extension, and hence not Galois. (That's condition (c) of Theorem 7.1.1.)

(b) **Galois** Let $L = \mathbb{Q}(\alpha, \beta)$, and let γ be the third root of $f(x) = x^3 + x^2 + 2x + 1$ Since the x^2-coefficient of f is 1, we have $\alpha + \beta + \gamma = -1$, and hence $\gamma = -1 - \alpha - \beta \in L$. Thus, f splits completely over L.
We claim that f is separable. There are various ways to see this. One would be to run the Euclidean algorithm on f and $f' = 3x^2 + 2x + 2$ to verify that $\gcd(f, f') = 1$, and invoke Proposition 5.3.2. A less computational way is to observe that f is irreducible: if f is reducible over $\mathbb{Q}$, then being a cubic polynomial, it has a root $a \in \mathbb{Q}$. Writing $a = m/n$ in lowest terms, we have $n = 1$ (and hence $a = m$) because $f \in \mathbb{Z}[x]$ is monic, and hence looking at the constant term, we have $m|1$, so that $a = \pm 1$. But $f(1) = 5$ and $f(-1) = 1$, so f has no roots in $\mathbb{Q}$ and hence is irreducible and therefore (since $\operatorname{char}\mathbb{Q} = 0$) also separable, proving the claim. Thus, $L = \mathbb{Q}(\alpha, \beta, \gamma)$ is the splitting field of the separable polynomial f over $\mathbb{Q}$, so by Theorem 7.1.1(a), it is Galois over $\mathbb{Q}$.

[**Note**: Actually, even if f weren't irreducible or even separable, we could factor f as $g_1^{m_1} \cdots g_s^{m_s}$ with $g_1, \ldots, g_s \in \mathbb{Q}[x]$ irreducible. Then let $h = g_1 \cdots g_s$ has the same roots as f does, so L is the splitting field of the separable polynomial $h \in \mathbb{Q}[x]$.]

(c) **Not** Galois Let $F = \mathbb{F}_p(t^p)$ and $L = \mathbb{F}_p(t)$. Then $t \in L$ is a root of $f(x) = x^p - t^p$, which is an irreducible polynomial in $F[x]$, by Proposition 4.2.6. That is, $t \in L$ has minimal polynomial f over F, but $f(x) = (x-t)^p$ is not separable. Thus, by definition, t is not separable over F. Also by definition, then, L/F is **not** a separable extension, and hence not Galois. (That's condition (c) of Theorem 7.1.1.)

(d) **Galois** Let $F = \mathbb{C}(t + t^{-1})$ and $L = \mathbb{C}(t)$. Let $u = t + t^{-1}$. Motivated by the computation $tu = t^2 + 1$, we see that $t \in L$ is a root of $f(x) = x^2 - ux + 1 \in F[x]$. The two roots of f are $t, t^{-1} \in L$, which are distinct, so f is separable. Moreover, $L = F(t) = F(t, t^{-1})$ is the splitting field of f over F. Thus, L is the splitting field of the separable polynomial f over F, so by Theorem 7.1.1(a), it is Galois over F.

(e) **Galois** Let $F = \mathbb{C}(t^n)$, let $L = \mathbb{C}(t)$, and let $f(x) = x^n - t^n \in F[x]$. Then the n roots of f are $\{\zeta_n^j t : j = 0, 1, \ldots, n-1\} \subseteq L$, which are all distinct, so f is separable. In addition, because $\zeta_n \in \mathbb{C} \subseteq F$, we have $L = F(t) = F(t, \zeta_n t, \ldots, \zeta_n^{n-1} t)$, and hence L is the splitting field of f over F.

Thus, L is the splitting field of the separable polynomial f over F, so by Theorem 7.1.1(a), it is Galois over F.

Problem 7. Cox, Section 7.2, Exercise 1:
Consider the extension $L/\mathbb{Q}$, where $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, as in Example 7.3.2 and diagram (7.3).

(a) Prove that the conjugate fields of $\mathbb{Q}(\sqrt[3]{2})$ are itself, $\mathbb{Q}(\omega\sqrt[3]{2})$, and $\mathbb{Q}(\omega^2\sqrt[3]{2})$.

(b) Prove that the only conjugate field of $\mathbb{Q}(\omega)$ is itself.

Proof. Let $\alpha = \sqrt[3]{2}$, let $L = \mathbb{Q}(\omega, \alpha)$, and let $G = \mathrm{Gal}(L/\mathbb{Q})$.

(a) From past examples, we know that for all $\sigma \in G$, we have $\sigma(\alpha) = \omega^j\alpha$ for some $j = 0, 1, 2$; we also know that each of $j = 0, 1, 2$ is attained by some $\sigma \in G$.

For each $j = 0, 1, 2$, let $K_j = \mathbb{Q}(\omega^j\alpha)$; we must show that K_j is a conjugate of K_0. To do so, pick $\sigma \in G$ such that $\sigma(\alpha) = \omega^j\alpha$; we will prove that $K_j = \sigma K_0$.

To prove ($\supseteq$): Given $\gamma \in \sigma K_0$, we have $\gamma = \sigma(\beta)$ for some $\beta \in K_0$. Then by definition, $\beta = h(\alpha)$ for some rational function $h(x) \in \mathbb{Q}(x)$. Hence,

$$\gamma = \sigma\big(h(\alpha)\big) = h\big(\sigma(\alpha)\big) = h\big(\omega^j\alpha\big) \in K_j.$$

To prove ($\subseteq$): Given $\gamma \in K_j$, we may write $\gamma = h(\omega^j\alpha)$ for some rational function $h(x) \in \mathbb{Q}(x)$. Hence,

$$\gamma = h\big(\omega^j\alpha\big) = h\big(\sigma(\alpha)\big) = \sigma\big(h(\alpha)\big) \in \sigma K_0. \qquad \text{QED}$$

(b) Let $M = \mathbb{Q}(\omega)$. Given $\sigma \in G$, we know from past examples that $\sigma(\omega) = \omega^j$ for some $j = 1, 2$. For each choice of j, we must show that $\sigma M = M$.

To prove ($\subseteq$): Given $\gamma \in \sigma M$, we have $\gamma = \sigma(\beta)$ for some $\beta \in M$. Then by definition, $\beta = h(\omega)$ for some rational function $h(x) \in \mathbb{Q}(x)$. Hence,

$$\gamma = \sigma\big(h(\omega)\big) = h\big(\sigma(\omega)\big) = h\big(\omega^j\big) \in M.$$

To prove ($\supseteq$): Given $\gamma \in M$, we may write $\gamma = h(\omega)$ for some rational function $h(x) \in \mathbb{Q}(x)$. Observe that $\sigma(\omega^j) = (\omega^j)^j = \omega$ for both $j = 1$ and $j = 2$. Thus,

$$\gamma = h(\omega) = h\big(\sigma(\omega^j)\big) = \sigma\big(h(\omega^j)\big) \in \sigma M. \qquad \text{QED}$$

Problem 8. Cox, Section 7.2, Exercise 2:
Let $L/K/F$ be finite extensions, and let $\sigma \in \mathrm{Gal}(L/F)$. Finish the proof of Lemma 7.2.4 by proving that $\mathrm{Gal}(L/\sigma K) \subseteq \sigma\,\mathrm{Gal}(L/K)\sigma^{-1}$.

Proof. Given $\tau \in \mathrm{Gal}(L/\sigma K)$, define $\lambda = \sigma^{-1}\tau\sigma$. Clearly we have $\tau = \sigma\lambda\sigma^{-1}$, so it suffices to show that $\lambda \in \mathrm{Gal}(L/K)$.
Note that $\lambda : L \to L$ is a field automorphism, since it is a composition of field automorphisms. It remains only to show that λ is the identity on K.
Given $\alpha \in K$, we have $\sigma(\alpha) \in \sigma K$, and hence $\tau(\sigma(\alpha)) = \sigma(\alpha)$. Therefore,

$$\lambda(\alpha) = \sigma^{-1}\Big(\tau\big(\sigma(\alpha)\big)\Big) = \sigma^{-1}\big(\sigma(\alpha)\big) = \alpha, \qquad \text{QED}$$

Problem 9. Cox, Section 7.2, Exercise 3:
Let $L/K_2/K_1$ be extensions of fields. Prove that $\mathrm{Gal}(L/K_2) \subseteq \mathrm{Gal}(L/K_1)$.

Proof. Given $\sigma \in \mathrm{Gal}(L/K_2)$, we have that $\sigma : L \to L$ is a field automorphism. In addition, for any $a \in K_1$, we have $a \in K_2$, and hence $\sigma(a) = a$. Thus, $\sigma \in \mathrm{Gal}(L/K_1)$. QED