Solutions to Homework 10

Problem 1. Cox, Section 7.2, Exercise 8:
Let G be a group, let $H \subseteq G$ be a subgroup, and define $N_G(H) = \{g \in G \,|\, gHg^{-1} = H\}$.

(a) Prove that $N_G(H)$ is a subgroup of G containing H.

(b) Prove that H is normal in $N_G(H)$.

(c) Let $N \subseteq G$ be a subgroup of G containing H.
Prove that H is normal in N if and only if $N \subseteq N_G(H)$.

(d) Prove that H is normal in G if and only if $N_G(H) = G$.

Proof. **(a)** First, for any $h \in H$, we have $hHh^{-1} = H$, and hence $H \subseteq N_G(H)$. Since $H \neq \varnothing$, this also shows that $N_G(H)$ is nonempty.
Second, for any $x, y \in N_G(H)$, we have

$$(xy)H(xy)^{-1} = xyHy^{-1}x^{-1} = x\big(yHy^{-1}\big)x^{-1} = xHx^{-1} = H,$$

where the last two equalities are because $y \in N_G(H)$ and $x \in N_G(H)$, respectively. Thus, $xy \in N_G(H)$. In addition,

$$x^{-1}H(x^{-1})^{-1} = x^{-1}Hx = x^{-1}\big(xHx^{-1}\big)x = (x^{-1}x)H(x^{-1}x) = eHe = H,$$

where the second equality is again because $x \in N_G(H)$. Thus, $x^{-1} \in H$. Hence, $N_G(H)$ is indeed a subgroup of G containing H. QED (a)

(b) We know that H is a group and a subset of the group $N_G(H)$; thus, H is a subgroup of $N_G(H)$. Given $x \in N_G(H)$, we have $xHx^{-1} = H$ by definition. Thus, H is normal in $N_G(H)$.

(c) Consider a normal subgroup $N \triangleleft G$ with $H \subseteq N$.

($\Rightarrow$): Assuming $H \triangleleft N$, then for any $x \in N$, we have $xHx^{-1} = H$ by definition of $H \triangleleft N$, whence $x \in N_G(H)$, as desired.

($\Leftarrow$): Conversely, assuming $N \subseteq N_G(H)$, then for any $x \in N$, we have $x \in N_G(H)$, and hence $xHx^{-1} = H$. Thus, $H \triangleleft N$. QED (c)

(d) ($\Rightarrow$): Assuming $H \triangleleft G$, then with $N = G$, the ($\Leftarrow$) direction of part (c) gives us $G \subseteq N_G(H)$, and hence $N_G(H) = G$.
($\Leftarrow$): Assuming $N_G(H) = G$, then again with $N = G$, the ($\Rightarrow$) direction of part (c) gives us $H \triangleleft G$. QED (d)

Problem 2. Cox, Section 7.3, Exercise 3, variant:
Let $L = \mathbb{Q}(i, \sqrt[4]{2})$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. We already know (cf. Homework 8, Problem 6b) that $L/\mathbb{Q}$ is Galois, with $|G| = [L : \mathbb{Q}] = 8$, and in fact $G \cong D_4$, with elements $\sigma, \tau \in G$ such that

$$\sigma(i) = i,\ \sigma(\sqrt[4]{2}) = i\sqrt[4]{2},\ \tau(i) = -i,\ \tau(\sqrt[4]{2}) = \sqrt[4]{2}$$

which satisfy $o(\sigma) = 4$, $o(\tau) = 2$, and $\tau\sigma = \sigma^{-1}\tau$. So $G = \{\sigma^j\tau^k \,|\, j \in \{0,1,2,3\} \text{ and } k \in \{0,1\}\}$.

(a) Let $K_1 = \mathbb{Q}(\sqrt[4]{2})$. Let $H_1 = \mathrm{Gal}(L/K_1)$. Determine H_1 as an explicit set of elements of the form $\sigma^j\tau^k$ with $j \in \{0,1,2,3\}$ and $k \in \{0,1\}$. Then verify that $H_1 \not\triangleleft G$ by finding $g \in G$ and $h \in H_1$ such that $ghg^{-1} \notin H_1$.

(b) Let $K_2 = \mathbb{Q}(i)$. Let $H_2 = \mathrm{Gal}(L/K_2)$. Determine H_2 as an explicit set of elements of the form $\sigma^j\tau^k$ with $j \in \{0,1,2,3\}$ and $k \in \{0,1\}$. Then verify that $H_2 \triangleleft G$ by proving $ghg^{-1} \in H_2$ for all $g \in G$ and $h \in H_2$.

(c) Let $H_3 = \{e, \sigma^2\} = \langle\sigma^2\rangle$, which is a normal subgroup of G. Determine the fixed field $K_3 = L_{H_3}$, and find a polynomial $f \in \mathbb{Q}[x]$ such that K_3 is the splitting field of f over $\mathbb{Q}$.

Solution/Proof. Observe that $\sigma^j(i) = i$ for every $j \in \{0,1,2,3\}$, and so $\sigma^j(\sqrt[4]{2}) = i^j\sqrt[4]{2}$. Also, $\tau^k(i) = (-1)^k i$ for each $k \in \{0,1\}$, and $\tau^k(\sqrt[4]{2}) = \sqrt[4]{2}$.
Thus, $\sigma^j\tau^k(i) = (-1)^k i$, and $\sigma^j\tau^k(\sqrt[4]{2}) = \sigma^j(\sqrt[4]{2}) = i^j\sqrt[4]{2}$.

(a) Since every $g \in G$ fixes all of $\mathbb{Q}$ already, we have $H_1 = \{g \in G \,|\, g(\sqrt[4]{2}) = \sqrt[4]{2}\}$. Therefore $\sigma^j\tau^k \in H_1 \Leftrightarrow i^j = 1$, and hence $H_1 = \{e, \tau\} = \boxed{\{\sigma^0\tau^0, \sigma^0\tau^1\}}$
Let $g = \sigma \in G$ and $h = \tau \in H_1$. Then $ghg^{-1} = \sigma\tau\sigma^{-1} = \sigma(\sigma\tau) = \sigma^2\tau \notin H_1$. QED (a)

(b) Since every $g \in G$ fixes all of $\mathbb{Q}$ already, we have $H_2 = \{g \in G \,|\, g(i) = i\}$. Therefore $\sigma^j\tau^k \in H_2 \Leftrightarrow (-1)^k = 1$, and hence $H_2 = \{e, \sigma, \sigma^2, \sigma^3\} = \boxed{\{\sigma^j\tau^0 \,|\, j \in \{0,1,2,3\}\}}$
Given $g \in G$ and $h \in H_2$, then there exist $j, m \in \{0,1,2,3\}$ and $k \in \{0,1\}$ such that $g = \sigma^j\tau^k$ and $h = \sigma^m$.
If $k = 1$, then noting that $\tau^{-1} = \tau$, we have $ghg^{-1} = \sigma^j\tau\sigma^m\tau\sigma^{-j} = \sigma^j\tau\tau\sigma^{-m}\sigma^{-j} = \sigma^{-m} \in H_2$.
And if $k = 0$, then $ghg^{-1} = \sigma^j\sigma^m\sigma^{-j} = \sigma^m \in H_2$. QED (b)

(c) By the Fundamental Theorem, we have $[L : K_3] = |H_3| = 2$, so by the Tower Theorem, $[K_3 : \mathbb{Q}] = [L : \mathbb{Q}]/[L : K_3] = 8/2 = 4$.
Since $e \in G$ fixes every element of L, we have $K_3 = \{\alpha \in L \,|\, \sigma^2(\alpha) = \alpha\}$. Then $i \in K_3$ since $\sigma^2(i) = i$.
In addition, we have $\sqrt{2} \in K_3$ since $\sigma^2(\sqrt{2}) = \sigma^2\big((\sqrt[4]{2})^2\big) = \big(\sigma^2(\sqrt[4]{2})\big)^2 = \big(i^2\sqrt[4]{2}\big)^2 = i^4\sqrt{2} = \sqrt{2}$.
[**Note**: We can discover i and $\sqrt{2}$ in this context by computing $\sigma^2(i^\ell(\sqrt[4]{2})^m)$ for $\ell = 0, 1$ and $m = 0, 1, 2, 3$, which are reasonable elements to look at since they form a basis of L over $\mathbb{Q}$.]
Thus, $K_3 \supseteq \mathbb{Q}(i, \sqrt{2})$. By Homework 8, Problem 2, we have $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$, so $K_3 = \mathbb{Q}(i, \sqrt{2})$.
Let $f = (x^2 + 1)(x^2 - 2)$, which has roots $\pm i$ and $\pm\sqrt{2}$. Thus, K_3 is the splitting field of f over $\mathbb{Q}$.
QED (c)

Problem 3. Cox, Section 7.3, Exercise 5, variant:
Let $F = \mathbb{C}(t^4)$, let $L = \mathbb{C}(t)$, and let $f(x) = x^4 - t^4 \in F[x]$.

(a) Prove that L is the splitting field of f over F, and hence L/F is Galois.

(b) Prove that f is irreducible over F, and that $[L : F] = 4$.

(c) Prove that there exists $\sigma \in \mathrm{Gal}(L/F)$ such that $\sigma(t) = it$.

(d) Prove that $\mathrm{Gal}(L/F)$ is cyclic of order 4, generated by σ.

(e) Determine all the subgroups H of $\mathrm{Gal}(L/F)$, and for each one, determine the corresponding intermediate field L_H.

Proof. **(a)** We have $f(x) = (x-t)(x+t)(x-it)(x+it)$ in $L[x]$, so f splits over L, with roots $\pm t, \pm it \in L$. The splitting field K is therefore $K = F(t, -t, it, -it) \subseteq L$. We also have $K = \mathbb{C}(t, -t, it, -it) \supseteq \mathbb{C}(t) = L$, so $K = L$, as desired. Thus, L/F is normal. The roots of f are distinct, so L/F is separable. [Alternatively, separability is automatic in characteristic zero.] Therefore, L/F is Galois. QED (a)

(b) Any proper factor of f has constant term ct^j where $1 \le j \le 3$ and $c \in \{\pm 1, \pm i\}$. It suffices to show that $t^j \notin F$, which we now prove by contradiction.
If not, then $t^j = g(t^4)/h(t^4)$ for some $g, h \in \mathbb{C}[t]$ with $h \neq 0$ and $\gcd(g, h) = 1$. Thus, $t^j h(t^4) = g(t^4)$ in $\mathbb{C}[t]$. The degree of the left side is $j + 4\deg(h)$, and the degree of the left side is $4\deg(g)$. Thus, $j = 4[\deg(g) - \deg(h)] \notin \{1, 2, 3\}$, a contradiction. QED (b)

(c) Since f is irreducible over F and L/F is normal, such $\sigma \in \mathrm{Gal}(L/F)$ exists (by Proposition 5.1.8). QED (c)

(d) Let $G = \mathrm{Gal}(L/F)$. We have $|G| = [L : F] = \deg(f) = 4$ by Proposition 6.2.1.
We have $\sigma(t) = it \neq t$, and $\sigma^2(t) = \sigma(it) = i\sigma(t) = i^2 t = -t \neq t$. Thus, $o(\sigma) \ge 3$. On the other hand, by Lagrange's Theorem, $o(\sigma)$ divides $|G| = 4$, so $o(\sigma) = 4$.

Thus, $\langle\sigma\rangle \subseteq G$ with $|\langle\sigma\rangle| = 4 = |G|$, so $\langle\sigma\rangle = G$. QED (d)

(e) By basic group theory, the subgroups of a cyclic group $\langle\sigma\rangle$ of order 4 are $\langle\sigma^m\rangle$ for each $m|4$. For $m = 1$, we have $\langle\sigma\rangle = G$, for $m = 2$, we have $\langle\sigma^2\rangle = \{e, \sigma^2\}$, and for $m = 4$, we have $\langle\sigma^4\rangle = \{e\}$. We now consider each of these three subgroups.
For $H = G$, we have $\boxed{L_G = F}$ in the Galois correspondence, because $\mathrm{Gal}(L/F) = G$.
For $H = \{e, \sigma^2\}$, we claim that $\boxed{L_H = \mathbb{C}(t^2)}$. Indeed, setting $K = \mathbb{C}(t^2) = F(t^2) = F(\sqrt{t^4})$, we have $[K : F] \leq 2$, and we also have $L = K(\sqrt{t^2})$, so that $[L : K] \leq 2$. Since $4 = [L : F] = [L : K][K : F]$ by the Tower Theorem, it follows that $[L : K] = 2 = |H|$, and hence $L_H = K$ by the Galois correspondence.
Finally, for $H = \{e\}$, we have $\boxed{L_{\{e\}} = L}$ in the Galois correspondence, because $\mathrm{Gal}(L/L)$ is trivial.
QED (e)

Problem 4. Cox, Section 7.3, Exercise 7, variant:
Let $p \geq 3$ be an odd prime. Recall that the cyclotomic polynomial $\Phi_p = x^{p-1} + \cdots + 1$, which we already know is irreducible over $\mathbb{Q}$, has root ζ_p. Let $L = \mathbb{Q}(\zeta_p)$, which we already know is the splitting field of Φ_p over $\mathbb{Q}$. We also already know that $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, with $j \in (\mathbb{Z}/p\mathbb{Z})^\times$ corresponding to $\sigma_j \in \mathrm{Gal}(L/\mathbb{Q})$ satisfying $\sigma_j(\zeta_p) = \zeta_p^j$.
Let $\tau = \sigma_{-1}$, and let $H = \langle\tau\rangle \subseteq \mathrm{Gal}(L/\mathbb{Q})$.

(a) Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Prove that K is the fixed field L_H corresponding to H.

(b) Prove that $K \subseteq \mathbb{R}$.
[**Suggestion**: Recall that $\zeta_p = e^{2\pi i/p} = \cos(2\pi/p) + i\sin(2\pi/p)$.]

(c) Prove that is $K/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(K/\mathbb{Q})$ cyclic of order $(p-1)/2$.

(d) Prove that the minimal polynomial of $\zeta_p + \zeta_p^{-1}$ over $\mathbb{Q}$ has degree $(p-1)/2$.

Proof. **(a)** Let $G = \mathrm{Gal}(L/\mathbb{Q})$. According to the isomorphism $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$, $\tau \in G$ corresponds to $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$, so that $\tau(\zeta_p) = \zeta_p^{-1}$. Thus, $\tau^2(\zeta_p) = (\zeta_p^{-1})^{-1} = \zeta_p$, and hence $\tau^2 = e$. Therefore, $H = \{e, \tau\}$, and

$$\tau\Big(\zeta_p + \zeta_p^{-1}\Big) = \zeta_p^{-1} + \zeta_p = \zeta_p + \zeta_p^{-1}.$$

Thus, defining $\xi_p = \zeta_p + \zeta_p^{-1}$, we have $\tau(\xi_p) = \xi_p$, and of course $e(\xi_p) = \xi_p$. Therefore, ξ_p lies in the fixed field L_H, and hence $K \subseteq L_H$, where $K = \mathbb{Q}(\xi_p)$.
On the other hand, ζ_p is a root of the polynomial $x^2 - \xi_p x + 1 \in K[x]$. (The other root is ζ_p^{-1}.) It follows that $[L : K] \leq 2$. Hence, we have the tower of fields $L/L_H/K$ with $[L : K] \leq 2$ but, by the Fundamental Theorem, with $[L : L_H] = |H| = 2$. Thus, by the Tower Theorem, we must have $[L_H : K] = 1$, so that $L_H = K$, as desired. QED (a)

(b) We have $\xi_p = \zeta_p + \zeta_p^{-1} = \big(\cos(2\pi/p) + i\sin(2\pi/p)\big) + \big(\cos(2\pi/p) - i\sin(2\pi/p)\big) = 2\cos(2\pi/p) \in \mathbb{R}$
Therefore, $K = \mathbb{Q}(\xi_p) \subseteq \mathbb{R}$. QED (b)

(c) Since $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is an abelian group, we have $H \triangleleft G$. Therefore, by the Fundamental Theorem, $K = L_H$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to G/H.
The group G/H has order $|G|/|H| = (p-1)/2$. Since we know from Math 350 that G is cyclic, it follows that any quotient of G is also cyclic. QED (c)

(d) Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of ξ_p over $\mathbb{Q}$. Then

$$\deg f = [K : \mathbb{Q}] = |\,\mathrm{Gal}(K/\mathbb{Q})| = (p-1)/2,$$

where the first equality is because $K = \mathbb{Q}(\xi_p)$, the second is because $K/\mathbb{Q}$ is Galois, and the third is by part (c). QED (d)

Problem 5. (Not from Cox.)

Let F be a field with $\operatorname{char} F \neq 2$, and let K/F be an extension with $[K : F] = 2$.
Prove that there exists $a \in F$ such that $K = F(\sqrt{a})$.

[**Suggestion**: Use the quadratic formula.]

Proof. Pick $\gamma \in K \smallsetminus F$. [Such γ exists since $K \supsetneq F$] Then $F(\gamma)/F$ is a field extension of degree at least 2; since $[K : F] = 2$, we must have $K = F(\gamma)$. Thus, γ must be a root of some irreducible quadratic polynomial $f(x) = x^2 + Bx + C \in F[x]$. Since $\operatorname{char} F \neq 2$, we may apply the quadratic formula, yielding that the two roots of f are $(-B \pm \sqrt{B^2 - 4C})/2$. Let $a = B^2 - 4C$, so that $\gamma \in F(\sqrt{a})$. Note that this implies $\sqrt{a} \notin F$, or else $\gamma \in F$, a contradiction. Thus, $[F(\sqrt{a}) : F] = 2$, whence $K = F(\sqrt{a})$. QED

Problem 6. Cox, Section 7.3, Exercise 9:
Let F be a field with $\operatorname{char} F \neq 2$, and let L/F be a finite extension. Prove that the following are equivalent:

(i) L/F is Galois with $\operatorname{Gal}(L/F) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

(ii) There exist $a, b \in F$ for which none of a, b, or ab is a square in F, such that L is the splitting field of $(x^2 - a)(x^2 - b)$ over F.

Proof. Let $G = \operatorname{Gal}(L/F)$.

(i)$\Longrightarrow$(ii): Since $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we may write $G = \{e, \sigma, \tau, \sigma\tau\}$, where $\sigma^2 = \tau^2 = e$. Let $K_1 = L_{\langle\sigma\rangle}$ and $K_2 = L_{\langle\tau\rangle}$. By the Fundamental Theorem, each K_i is an extension of F of degree $|G|/|\langle\sigma\rangle| = 4/2 = 2$. Therefore, by Problem 5, there exist $a, b \in F$ with $\sqrt{a}, \sqrt{b} \notin F$ such that $K_1 = F(\sqrt{a})$ and $K_2 = F(\sqrt{b})$.
Moreover, since $\langle\sigma\rangle \neq \langle\tau\rangle$, we have $K_1 \neq K_2$, and hence $\sqrt{b} \notin K_1$. Thus, $[K_1(\sqrt{b}) : K_1] = 2$, and therefore the Tower Theorem yields $[K_1(\sqrt{b}) : F] = 4$. It follows that $L = K_1(\sqrt{b}) = F(\sqrt{a}, \sqrt{b})$, which is the desired splitting field of $(x^2 - a)(x^2 - b)$.
We have already seen that $\sqrt{a}, \sqrt{b} \notin F$. If $\sqrt{ab} \in F$, then $a\sqrt{b} = \sqrt{ab} \cdot \sqrt{a} \in K_1$. Since $a \neq 0$ (which we know because $\sqrt{a} \notin F$), dividing by a would yield $\sqrt{b} \in K_1$, a contradiction. Thus, $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin F$.
QED ($\Longrightarrow$)

(ii)$\Longrightarrow$(i): The four roots of $f(x) = (x^2 - a)(x^2 - b)$ are $\pm\sqrt{a}$ and $\pm\sqrt{b}$, which are all distinct. Indeed, $\sqrt{a} \neq -\sqrt{a}$ because $2\sqrt{a} \neq 0$, which in turn is because $\sqrt{a} \notin F$ and $\operatorname{char} F \neq 2$. Similarly, $\sqrt{b} \neq -\sqrt{b}$. Finally, $\pm\sqrt{a} \neq \pm\sqrt{b}$, because otherwise, multiplying by $\pm\sqrt{b}$, we would have $\sqrt{ab} = \pm b \in F$, contradicting our assumptions.
Thus, f is separable, so its splitting field $L = F(\sqrt{a}, \sqrt{b})$ is a Galois extension of F. Let $K_1 = F(\sqrt{a})$. We claim that $\sqrt{b} \notin K_1$.

To prove the claim, suppose $\sqrt{b} \in K_1$. Then there exist $x, y \in F$ such that $\sqrt{b} = x + y\sqrt{a}$. If $y = 0$, then $\sqrt{b} = x \in F$, a contradiction. If $y \neq 0$ but $x = 0$, then multiplying by $\sqrt{b}$, we have $b = y\sqrt{ab}$, whence $\sqrt{ab} = b/y \in F$, another contradiction. Finally, if $x, y \neq 0$, then squaring both sides gives $b = x^2 + ay^2 + 2xy\sqrt{a}$. Since $\operatorname{char} F \neq 2$ and $xy \neq 0$, then, we have $\sqrt{a} = (2xy)^{-1}(-x^2 - ay^2) \in F$, yet another contradiction, proving our claim.

[**Note**: This claim above is similar to portions of Problems 1 and 2 of Homework 8. However, those results were stated over $\mathbb{Q}$ specifically, so we cannot just quote them here.]

By the claim, we have $[L : K_1] = 2$. Since $\sqrt{a} \notin F$, we also have $[K_1 : F] = 2$. Thus, by the Tower Theorem, $[L : F] = 4$. Since L/F is Galois, we also have $|G| = 4$.
On the other hand, since $L = F(\sqrt{a}, \sqrt{b})$, each $\sigma \in G$ is determined by the values $\sigma(\sqrt{a})$ and $\sigma(\sqrt{b})$. Furthermore, we must have $\sigma(\sqrt{a}) = \pm\sqrt{a}$ and $\sigma(\sqrt{b}) = \pm\sqrt{b}$, since these images must be roots of $x^2 - a$ and $x^2 - b$, respectively. Since there are $4 = |G|$ possibilities for $\sigma(\sqrt{a})$ and $\sigma(\sqrt{b})$, then, each of the four must occur. Each such $\sigma \in G$ has order 2, except for the identity e, with order 1. Thus, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. QED

Problem 7. Cox, Section 7.3, Exercise 12, variant:
Let G be a group, and let $H \subseteq G$ be a subgroup. Define $N = \bigcap_{g \in G} gHg^{-1}$.

(a) Prove that N is a normal subgroup of G. [**Note**: Don't forget the "subgroup" part!]

(b) Let K be a normal subgroup of G contained in H. Prove that $K \subseteq N$.

[**Note**: This problem shows that N is the largest normal subgroup of G contained in H.]

Proof. **(a) (Nonempty)** For any $g \in G$, we have $e = geg^{-1} \in gHg^{-1}$. Therefore $e \in N$.

(Closure) Given $x, y \in N$, then for any $g \in G$, we have $x, y \in gHg^{-1}$, and hence there exist $h_1, h_2 \in H$ such that $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$. Thus, $xy = (gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1}$, since $h_1h_2 \in H$. Therefore $xy \in N$.

(Inverses) Given $x \in N$, then for any $g \in G$, we have $x \in gHg^{-1}$, and hence there exists $h \in H$ such that $x = ghg^{-1}$. Thus, $x^{-1} = (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$, since $h^{-1} \in H$. Therefore $x^{-1} \in N$.

(Normal) Given $x \in N$ and $g_1 \in G$, we must show $g_1xg_1^{-1} \in N$. For any $g_2 \in G$, that is, we must show that $g_1xg_1^{-1} \in g_2Hg_2^{-1}$.
Let $g = g_1^{-1}g_2 \in G$. Then because $x \in N$, we have $x \in gHg^{-1}$, and hence there exists $h \in H$ such that $x = ghg^{-1} = g_1^{-1}g_2hg_2^{-1}g_1$. Thus, $g_1xg_1^{-1} = g_2hg_2^{-1} \in g_2Hg_2^{-1}$. QED (a)

(b) Let K be a normal subgroup of G contained in H. Given $x \in K$, we must show $x \in N$. That is, given any $g \in G$, we must show that $x \in gHg^{-1}$.
Since $K \lhd G$, we have $g^{-1}xg \in K \subseteq H$. Thus, $x \in gHg^{-1}$, as desired. QED (b)

Problem 8. Cox, Section 7.4, Exercise 2, variant:
Use Proposition 7.4.2 and the formula $\Delta(x^3+px+q) = -4p^3 - 27q^2$ from equation (1.22) to determine the Galois groups of the following cubic polynomials:

(a) $x^3 - 4x + 2$ over $\mathbb{Q}$ (b) $x^3 - 4x + 2$ over $\mathbb{Q}(\sqrt{37})$

(c) $x^3 - t$ over $\mathbb{C}(t)$ (d) $x^3 - t$ over $\mathbb{Q}(t)$

Solution/Proof. All the fields in this problem are of characteristic zero, and hence all irreducible polynomials over them are separable.

(a) The polynomial $f = x^3 - 4x + 2$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$.
We have $\Delta(f) = -4(-4)^3 - 27(2)^2 = 256 - 108 = 148 = 2^2 \cdot 37$, which is **not** a square in $\mathbb{Q}$. Thus, by Proposition 7.4.2, we have $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$.

(b) If the polynomial $f = x^3 - 4x + 2$ were reducible over $\mathbb{Q}(\sqrt{37})$, then it would have a root α in $\mathbb{Q}(\sqrt{37})$, since $\deg(f) = 3$. However, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$ by the irreducibility over $\mathbb{Q}$ from part (a), so $2 = [\mathbb{Q}(\sqrt{37}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{37}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 3$, a contradiction. Thus, f is irreducible over $\mathbb{Q}(\sqrt{37})$. [**Note**: This irreducibility can also be proven using the Fundamental Theorem and part (a).]
From part (a), we have $\Delta(f) = 2^2 \cdot 37 = (2\sqrt{37})^2$, which **is** a square in $\mathbb{Q}(\sqrt{37})$ Thus, by Proposition 7.4.2, we have $\mathrm{Gal}(f/\mathbb{Q}(\sqrt{37})) \cong \mathbb{Z}/3\mathbb{Z}$.

(c) We claim the polynomial $g = x^3 - t$ is irreducible over $\mathbb{C}(t)$. Indeed, if g were reducible, then it would have a root $a \in \mathbb{C}(t)$. Writing a in lowest terms as $a = h_1/h_2$ (i.e., with $h_i \in \mathbb{C}[t]$, and $h_2 \neq 0$, and $\gcd(h_1, h_2) = 1$), we have $a^3 = t$ and hence $h_1^3 = th_2^3$. The power of the irreducible $t \in \mathbb{C}[t]$ on the left is divisible by 3, but on the right it is 1 (mod 3), a contradiction to unique factorization. [**Note**: Comparing degrees is another way to get a contradiction.] This proves our claim, that g is irreducible over $\mathbb{C}(t)$.
We have $\Delta(g) = -4(0)^3 - 27(t)^2 = -27t^2 = (\sqrt{-27}\,t)^2$, which **is** a square in $\mathbb{C}(t)$. Thus, by Proposition 7.4.2, we have $\mathrm{Gal}(g/\mathbb{C}(t)) \cong \mathbb{Z}/3\mathbb{Z}$.

(d) We saw in part (c) that $g = x^3 - t$ is irreducible over $\mathbb{C}(t)$. Therefore, it is also irreducible over the smaller field $\mathbb{Q}(t)$.
We have $\Delta(g) = -4(0)^3 - 27(t)^2 = -27t^2$, which is **not** a square in $\mathbb{Q}(t)$, since $-27 < 0$ is not a square in $\mathbb{Q}$. Thus, by Proposition 7.4.2, we have $\mathrm{Gal}(g/\mathbb{Q}(t)) \cong S_3$.