Solutions to Homework 3

1. Cox, Appendix A.4, Exercise 5:
Let G be a group acting on a nonempty set X. Prove that the following are equivalent:

(i) G acts transitively on X. (I.e., for all $x, y \in X$, there exists $g \in G$ such that $gx = y$.)
(ii) For all $x \in X$, we have $G \cdot x = X$.
(iii) There exists $x \in X$ such that $G \cdot x = X$.

Proof. (i)⇒(ii): Given $x \in X$, the forward inclusion $G \cdot x \subseteq X$ is immediate from the definition of group action.
For the reverse inclusion, given $y \in X$, assumption (i) says that there exists $g \in G$ such that $gx = y$. Hence $y \in G \cdot x$. QED (i)⇒(ii)

(ii)⇒(iii): Since X is nonempty, there exists $x \in X$. By assumption (ii), then, we have $G \cdot x = X$. QED (ii)⇒(iii)

(iii)⇒(i): By assumption, there exists $w \in X$ such that $G \cdot w = X$.
Given $x, y \in X$, our assumption says that $x, y \in G \cdot w$, and hence there exist $g, h \in G$ such that $x = gw$ and $y = hw$. Thus, $hg^{-1} \in G$, and

$$(hg^{-1})x = (hg^{-1})gw = \big((hg^{-1})g\big)w = \big(h(g^{-1}g)\big)w = (he)w = hw = y,$$

as desired. QED

---

2. Cox, Section 2.4, Exercise 6(a,b): Let F be a field of characteristic 2.

(a) Let $b \in F$, and let $L \supseteq F$ be a (larger) field such that $b = \beta^2$ for some $\beta \in L$. Prove that β is unique. [In particular, β is the unique (double) root of $x^2 + b$, and we may write $\beta = \sqrt{b}$ with no ambiguity.]

(b) Let $f = x^2 + ax + b \in F[x]$ with $a \neq 0$, and suppose that f is irreducible over F. (So in particular, f has no roots in F.) Let α be a root of f in some larger field $L \supseteq F$. Prove that α **cannot** be written as $\alpha = u + v\sqrt{w}$ for any $u, v, w \in F$.

Proof. (a): In the ring $L[x]$, we have

$$(x - \beta)(x - \beta) = x^2 - 2\beta x + \beta^2 = x^2 + b,$$

since $2 = 0$ in $F \subseteq L$. Thus, the only root of $x^2 + b$ is β. QED

(b): Suppose α *can* be written as $\alpha = u + v\sqrt{w}$ for some $u, v, w \in F$. Then

$$0 = f(\alpha) = \alpha^2 + a\alpha + b = (u + v\sqrt{w})^2 + a(u + v\sqrt{w}) + b = u^2 + v^2 w + au + av\sqrt{w} + b.$$

Therefore, $av\sqrt{w} = u^2 + v^2 w + au + b$. [Side note: remember that $c = -c$ for any $c \in L$, since $2c = 0$ because we are in characteristic 2.] Since $a \neq 0$, a has a multiplicative inverse $a^{-1} \in F$. Thus,

$$\alpha = u + v\sqrt{w} = u + a^{-1}(u^2 + v^2 w + au + b) \in F.$$

Hence, f has a root α in F, contradicting the assumption that f is irreducible over F. This contradiction shows that α *cannot* be written as $\alpha = u + v\sqrt{w}$ with $u, v, w \in F$. QED

---

3. Cox, Section 2.4, Exercise 6(c,d): Let F be a field of characteristic 2.

(c) For $b \in F$, define $R(b)$ to be a root of the polynomial $x^2 + x + b$ (possibly in some larger field). Let's call $R(b)$ and $R(b) + 1$ the **2-roots** of b. Prove that $R(b)$ and $R(b) + 1$ are the two roots of $x^2 + x + b$, and (briefly) explain why adding 1 to $R(b) + 1$ yields $R(b)$.

(d) For $a, b \in F$ with $a \neq 0$, prove that the two roots of $f = x^2 + ax + b$ are $aR(b/a^2)$ and $a(R(b/a^2) + 1)$.

Proof. (c): We compute

$$\big(x - R(b)\big)\big(x - (R(b)+1)\big) = x^2 - \big(2R(b)+1\big)x + \big(R(b)^2 + R(b)\big) = x^2 - x - b = x^2 + x + b,$$

where in the second equality we use the fact that $R(b)$ is a root of x^2+x+b (so that $R(b)^2+R(b) = -b$), and in the third equality we used the facts that $1 = -1$ and $2 = 0$, since $\mathrm{char}(F) = 2$. Thus, the two roots of $x^2 + x + b$ are $R(b)$ and $R(b) + 1$.

For the second statement, observe that $(R(b) + 1) + 1 = R(b) + 2 = R(b)$ since $2 = 0$. QED

(d): We compute

$$\begin{aligned}\big(x - aR(b/a^2)\big)\big(x - a(R(b/a^2)+1)\big) &= x^2 - \big(2aR(b/a^2) + a\big)x + a^2\big(R(b/a^2)^2 + R(b/a^2)\big)\\ &= x^2 - ax + a^2(-b/a^2) = x^2 + ax + b,\end{aligned}$$

again using the facts that $R(b/a^2)^2 + R(b/a^2) = -b/a^2$, that $2 = 0$, and that $-1 = 1$. QED

---

4. Cox, Section 3.1, Exercise 1:
Let F be a field, let $f, g, h \in F[x]$ with $f = gh \neq 0$. Let $I = \langle g\rangle$.
(a) Prove that g is constant if and only if $I = F[x]$.
(b) Prove that h is constant if and only if $I = \langle f\rangle$.

Proof. (a) ($\Rightarrow$): The forward inclusion $I \subseteq F[x]$ is clear.
For the reverse inclusion: By assumption we may write $g = c$ with $c \in F$. If $c = 0$, then $I = \{0\} \neq F[x]$, so we have $c \neq 0$. Thus $c^{-1} \in F$. Given $k \in F[x]$, we have $k = g \cdot (c^{-1}k) \in I$. QED ($\Rightarrow$)

($\Leftarrow$): We have $1 \in F[x]$, so by assumption there exists $k \in F[x]$ such that $kg = 1$.
Thus, $\deg(k)+\deg(g) = \deg(1) = 0$. Clearly $k, g \neq 0$ (or else $kg = 0$), so we must have $\deg(k), \deg(g) \geq 0$, and hence $\deg(g) = \deg(k) = 0$. In particular, since $\deg(g) = 0$, we have that g is constant. QED

(b) ($\Rightarrow$): Write $h = c \in F$. By hypothesis, $c = h \neq 0$, so $c^{-1} \in F$.

($\subseteq$): Given $k \in I$, there exists $P \in F[x]$ such that $k = gP$. Therefore, $k = gc(c^{-1}P) = f \cdot (c^{-1}P) \in \langle f\rangle$.

($\supseteq$): Given $k \in \langle f\rangle$, there exists $P \in F[x]$ such that $k = fP$. Then $k = (gh)P = g(hP) \in \langle g\rangle = I$. QED ($\Rightarrow$)

($\Leftarrow$): We have $g \in I = \langle f\rangle$. Thus, there exists $k \in F[x]$ such that $g = fk = ghk$. That is, $g\cdot(hk-1) = 0$. Since $F[x]$ is an integral domain and $g \neq 0$, we have $hk - 1 = 0$, and hence $hk = 1$.
Thus, $\deg(h)+\deg(k) = \deg(1) = 0$. Clearly $h, k \neq 0$ (or else $hk = 0$), so we must have $\deg(h), \deg(k) \geq 0$, and hence $\deg(h) = \deg(k) = 0$. In particular, since $\deg(h) = 0$, we have that h is constant. QED

---

5. Cox, Section 3.1, Exercise 5:
Let F be a field, let $f \in F[x]$ be irreducible, and let $g + \langle f\rangle$ a a nonzero coset in $L = F[x]/\langle f\rangle$.

(a) Prove that f and g are relatively prime.

(b) By the note on the problem list, part (a) says that there exist $A, B \in F[x]$ such that $Af + Bg = 1$. Prove that $B + \langle f\rangle$ is the multiplicative inverse of $g + \langle f\rangle$ in L.

Proof. (a): Let $h \in F[x]$ be a polynomial that divides both f and g. Since $h|f$, the fact that f is irreducible means that there is some nonzero constant $c \in F^\times$ (i.e., a unit in the ring $F[x]$) such that either $h = c$ or $h = cf$.
Suppose towards contradiction that $h = cf$. Then since $h|g$, there exists $k \in F[x]$ such that $g = hk$, and hence $g = (ck)f \in \langle f\rangle$. Thus, $g + \langle f\rangle = 0 + \langle f\rangle$ is the zero coset, contradicting our hypothesis.
Hence, we have $h = c$ is constant, as desired. QED

(b): By the note and by part (a), there exist $A, B \in F[x]$ such that $Af + Bg = 1$.
That is, $Bg - 1 = Af \in \langle f\rangle$. Therefore [by the coset condition], we have

$$(B + \langle f\rangle)(g + \langle f\rangle) = Bg + \langle f\rangle = 1|\langle f\rangle$$

and by commutativity, then $(g + \langle f\rangle)(B + \langle f\rangle) = 1|\langle f\rangle$ as well. QED

6. Cox, Section 3.1, Exercise 6:
Apply the method of the previous problem to find the multiplicative inverse of the coset $1+x+\langle x^2+x+1\rangle$ in the field $\mathbb{Q}[x]/\langle x^2+x+1\rangle$.

Solution. Let $f = x^2+x+1$ and $g = x+1$. We will find $A, B \in \mathbb{Q}[x]$ such that $Af + Bg = 1$. I could do this via the Euclidean algorithm, but I can just see that choosing $A = 1$ and $B = -x$, we have

$$Af + Bg = 1(x^2+x+1) - x(x+1) = x^2+x+1-x^2-x = 1.$$

By the previous problem, the desired inverse is $B + \langle f\rangle = \boxed{-x + \langle f\rangle}$

---

7. Cox, Section 3.2, Exercise 1:
For $f = \sum_{j\geq 0} a_j x^j \in \mathbb{C}[x]$, define $\bar{f} = \sum_{j\geq 0} \bar{a}_j x^j \in \mathbb{C}[x]$.

(a) Prove that for any $f, g \in \mathbb{C}[x]$, prove that $\overline{fg} = \bar{f}\bar{g}$.

(b) Let $\alpha \in \mathbb{C}$. Prove that if $\bar{f}(\alpha) = 0$, then $f(\bar{\alpha}) = 0$.

Proof. (a): Given $f, g \in \mathbb{C}[x]$, write $f = \sum_{j\geq 0} a_j x^j$ and $g = \sum_{j\geq 0} A_j x^j$ with $a_j, A_j \in \mathbb{C}$, so that $\bar{f} = \sum_{j\geq 0} \bar{a}_j x^j$ and $\bar{g} = \sum_{j\geq 0} \bar{A}_j x^j$. Thus, $fg = \sum_{j\geq 0}\left(\sum_{k=0}^{j} a_k A_{j-k}\right)x^k$, and hence

$$\overline{fg} = \sum_{j\geq 0}\overline{\left(\sum_{k=0}^{j} a_k A_{j-k}\right)}x^k = \sum_{j\geq 0}\left(\sum_{k=0}^{j}\overline{a_k A_{j-k}}\right)x^k = \sum_{j\geq 0}\left(\sum_{k=0}^{j}\bar{a}_k\bar{A}_{j-k}\right)x^k = \bar{f}\bar{g} \qquad \text{QED}$$

(b): Given such f and α, write $f = \sum_{j\geq 0} a_j x^j$. Then

$$f(\bar{\alpha}) = \sum_{j\geq 0} a_j(\bar{\alpha})^j = \sum_{j\geq 0}\overline{\bar{a}_j\alpha^j} = \overline{\sum_{j\geq 0}\bar{a}_j\alpha^j} = \overline{\bar{f}(\alpha)} = \bar{0} = 0 \qquad \text{QED}$$

---

8. Cox, Section 3.2, Exercise 7:
Let F be a field. Prove that F is algebraically closed if and only if every non-constant polynomial in $F[x]$ has a root in F.

Proof. ($\Rightarrow$): Given $f \in F[x]$ nonconstant, let $n = \deg(f) \geq 1$. Since F is algebraically closed, f splits completely over F, i.e., there exist $c, \alpha_1, \ldots, \alpha_n \in F$ such that $f(x) = c\prod_{i=1}^{n}(x-\alpha_i)$. Because $n \geq 1$, then, f has at least one root $\alpha_1 \in F$.

($\Leftarrow$): Given $f \in F[x]$ nonconstant, we must show that f splits completely over F. We proceed by induction on $n = \deg(f) \geq 1$.
Base Case. If $n = 1$, then $f = cx+b$ with $b, c \in F$ and $c \neq 0$. Let $\alpha_1 = -b/c \in F$. Then $f = c(x-\alpha_1)$ splits.
Inductive Step. Suppose $n \geq 2$ and the conclusion holds for all polynomials of degree $n-1$. By hypothesis, f has at least one root $\alpha_n \in F$. Let $h(x) = x - \alpha_n \in F[x]$.
Apply the division algorithm to f divided by h in $F[x]$; there exist $q, r \in F[x]$ so that $f = qh + r$ and $\deg(r) < 1 = \deg(h)$, so that r is a constant polynomial. Evaluating $r = f - qh$ at $x = \alpha_n$ yields

$$r(\alpha_n) = f(\alpha_n) - q(\alpha_n)\cdot(\alpha_n - \alpha_n) = 0 - 0 = 0.$$

Since r is constant, we have $r = 0$, and hence $f = qh$.
Therefore, $\deg(q) = n-1$. By our inductive hypothesis, there exist $c, \alpha_1, \ldots, \alpha_{n-1} \in F$ such that $q(x) = c\prod_{i=1}^{n-1}(x-\alpha_i)$. Thus,

$$f(x) = q(x)\cdot(x-\alpha_n) = c\prod_{i=1}^{n}(x-\alpha_i),$$

as desired. QED

---

9. Cox, Section 4.1, Exercise 2:
Let F be a field, and let $f, g \in F[x]$ be monic polynomials. Suppose that f and g both divide each other. Prove that $f = g$.

Proof. By hypothesis, there are polynomials $h, k \in F[x]$ such that $f = gh$ and $g = fk$. Thus, $f = fhk$. Since f is monic, we have $f \neq 0$; therefore, since $F[x]$ is an integral domain, we may cancel f from both sides to obtain $hk = 1$.
Taking degrees, we have $\deg h + \deg k = 0$. Since $h, k \neq 0$ (because $hk = 1$), we have $\deg h \geq 0$ and $\deg k \geq 0$; thus, $\deg h = \deg k = 0$. That is, both h and k are nonzero constants.
The leading term of g is 1 since g is monic, and hence the leading term of $f = gh$ is the constant h. But f is also monic, so its leading term is 1. That is, $h = 1$, and hence $f = g \cdot 1 = g$. QED