Solutions to Homework 1

Problem 1. (6 points) Cox, Section 1.1, Problem 3: Prove that when $p = 0$, Cardano's formulas still correctly give the roots of the cubic equation $y^3 + py + q = 0$.

Proof. When $p = 0$, the cubic equation is $y^3 + q = 0$, i.e., $y^3 = -q$. So the three roots are $\omega^j \sqrt[3]{-q}$, for $j = 0, 1, 2$.
Also when $p = 0$, the quantities z_1, z_2 in equation (1.7) on page 7 are

$$z_1 = \sqrt[3]{\frac{1}{2}\big(-q + \sqrt{q^2 + 0}\big)} = \sqrt[3]{\frac{1}{2}(-q + q)} = 0$$

and

$$z_2 = \sqrt[3]{\frac{1}{2}\big(-q - \sqrt{q^2 + 0}\big)} = \sqrt[3]{\frac{1}{2}(-q - q)} = \sqrt[3]{-q}$$

Thus, Cardano's formulas give

$$y_1 = z_1 + z_2 = \sqrt[3]{-q}, \quad y_2 = \omega z_1 + \omega^2 z_2 = \omega^2 \sqrt[3]{-q}, \quad y_3 = \omega^2 z_1 + \omega z_2 = \omega \sqrt[3]{-q},$$

which, as noted above, are the three roots of $y^3 + q = 0$. QED

Problem 2. (10 points) Cox, Section 1.1, Problem 6:
Consider the equation $x^3 + x - 2 = 0$. Note that $x = 1$ is a root.

(a): Use Cardano's formula to prove that $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}} = 1$.

(b): Verify that $\left(\frac{1}{2} \pm \frac{1}{2}\sqrt{\frac{7}{3}}\right)^3 = 1 \pm \frac{2}{3}\sqrt{\frac{7}{3}}$, where the two $\pm$'s are either both $+$ or both $-$, and then use this fact to prove the formula in part (a) again.

Proof. (a): In Cardano's formula for $x^3 + x - 2$, i.e., with $p = 1$ and $q = -2$,
note that $q^2 + \frac{4p^3}{27} = 4 + \frac{4}{27} = \frac{4 \cdot 28}{27} = \frac{4^2 \cdot 7}{3^2 \cdot 3}$, and hence
$\frac{1}{2}\left(-q \pm \sqrt{q^2 + \frac{4p^3}{27}}\right) = \frac{1}{2}\left(2 \pm \frac{4}{3}\sqrt{\frac{7}{3}}\right) = 1 \pm \frac{2}{3}\sqrt{\frac{7}{3}}$.
Thus, by Cardano's formula, $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}$ is one of the three roots of $x^3 + x - 2$.
Observe that $7/3 > 0$, we have $\sqrt{7/3} \in \mathbb{R}$, and hence the quantity on the left side of the desired equation is also real.
We have $x^3 + x - 2 = (x - 1)(x^2 + x + 2)$, so the three roots of the cubic are 1 and the two roots of $x^2 + x + 2$. By the quadratic formula, the roots of $x^2 + x + 2$ are $\frac{-1 \pm \sqrt{1-8}}{2}$, which are not real since the discriminant -7 is negative. Thus, the only real root of the cubic is 1.

Therefore, being a real root of the cubic, we must have $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}} = 1$. QED

(b): We compute $\left(\frac{1}{2} \pm \frac{1}{2}\sqrt{\frac{7}{3}}\right)^3 = \frac{1}{8}\left(1 \pm 3\sqrt{\frac{7}{3}} + 3 \cdot \frac{7}{3} \pm \frac{7}{3}\sqrt{\frac{7}{3}}\right) = \frac{1}{8}\left(8 \pm \frac{16}{3}\sqrt{\frac{7}{3}}\right) = 1 \pm \frac{2}{3}\sqrt{\frac{7}{3}}$.
Thus, $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}} = \left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{7}{3}}\right) + \left(\frac{1}{2} - \frac{1}{2}\sqrt{\frac{7}{3}}\right) = 1$ QED

Problem 3. (6 points) Cox, Section 1.2, Problem 4:
We say that a cubic $x^3 + bx^2 + cx + d$ has a *multiple root* if it can be factored as $(x - r_1)^2(x - r_2)$. Prove that $x^3 + bx^2 + cx + d$ has a multiple root if and only if its discriminant is zero.

Proof. ($\Rightarrow$): The three roots of the cubic are $x_1 = x_2 = r_1$ and $x_3 = r_2$. By definition, the discriminant is

$$\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = (r_1 - r_1)^2(r_1 - r_2)^2(r_1 - r_2)^2 = 0 \qquad \text{QED } (\Rightarrow)$$

($\Leftarrow$): Call the three roots of the cubic x_1, x_2, x_3. By assumption and by definition of the discriminant, we have

$$0 = \Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

and hence (at least one of) $x_1 - x_2$ or $x_1 - x_3$ or $x_2 - x_3$ is 0. Without loss of generality (i.e., by re-indexing if necessary), we have $x_1 - x_2 = 0$, so that $x_1 = x_2$.
Let $r_1 = x_1 = x_2$, and let $r_2 = x_3$. Then the cubic is

$$x^3 + bx^2 + cx + d = (x - x_1)(x - x_2)(x - x_3) = (x - r_1)^2(x - r_2) \qquad \text{QED}$$

Problem 4. (8 points) Cox, Section 1.2, Problem 5:
Define $\sqrt{\Delta} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. Prove that an even permutation of $\{x_1, x_2, x_3\}$ takes $\sqrt{\Delta}$ to $\sqrt{\Delta}$, while an odd permutation takes $\sqrt{\Delta}$ to $-\sqrt{\Delta}$.

Proof. We consider each $\sigma \in S_3$ individually.
If $\sigma = e$ is the identity, which is even, clearly $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$.
If $\sigma = (1, 2)$, which is a 2-cycle and hence odd, then
$\sigma(\sqrt{\Delta}) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = -\sqrt{\Delta}$.
If $\sigma = (1, 3)$, which is a 2-cycle and hence odd, then
$\sigma(\sqrt{\Delta}) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = (-1)^3(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = -\sqrt{\Delta}$.
If $\sigma = (2, 3)$, which is a 2-cycle and hence odd, then
$\sigma(\sqrt{\Delta}) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) = -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = -\sqrt{\Delta}$.
If $\sigma = (1, 2, 3)$, which is a 3-cycle and hence even, then
$\sigma(\sqrt{\Delta}) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = (-1)^2(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{\Delta}$.
Finally, if $\sigma = (1, 3, 2)$, which is a 3-cycle and hence even, then
$\sigma(\sqrt{\Delta}) = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = (-1)^2(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{\Delta}$. QED

Note: One could alternatively prove this by observing it holds for the three 2-cycles (as above) and then writing each element of S_3 as a product of 2-cycles. (Another proof would be to use an equivalent characterization of the parity of σ as the parity of the number of *inversions* of σ.) But all of these proofs are about the same amount of work to write down.

Problem 5. (10 points) Cox, Section 2.1, Problem 1:
Let F be a field. In the ring $F[x, y]$, prove that the ideal

$$\langle x, y \rangle = \{xg + yh \mid g, h \in F[x, y]\}$$

is *not* a principal ideal.

Proof. Let $I = \langle x, y \rangle$. Suppose there exists $f \in I$ such that $I = \langle f \rangle$.
Since $x \in I$, there exists $g \in F[x, y]$ such that $x = fg$.
However, $F[x, y]$ is a UFD, and x is irreducible (since it has total degree 1).
Therefore, by the uniqueness of the factorization, one of f and g must be a unit (that is, a nonzero constant $c \in F^\times$), and the other must be $c^{-1}x$.
However, if $f = c$ is a unit, then $1 = c^{-1}f \in \langle f \rangle = I$, and hence $I = F[x, y]$, a contradiction. Thus, g must be a unit, and we must have $f = ax$ where $a = c^{-1} \in F^\times$.
Since $y \in I$, there exists $h \in F[x, y]$ such that $y = fh$. Thus, $y = axh$. Evaluating both sides at $(x, y) = (0, 1)$, then, we have $1 = 0$ in F, a contradiction. QED

Note: There are a lot of ways to prove this, using the same basic contradiction proof structure, and using some combination of unique factorization, (total) degree comparisons, and evaluating.