Algebra Assignment 8 Solutions

1. Let $p$ be a prime of the form $p = 3k + 1$. Let $g$ be a generator, so that the elements of $\mathbb{Z}_p^*$ can be written $1, g, g^2, \ldots, g^{3k-1}$ with $g^{3k} = 1$.

(a) Show that there is an element $\omega \in \mathbb{Z}_p^*$ with $\omega \neq 1$ and $\omega^3 = 1$.

Solution: Easy! Take $\omega = g^k$. Then $\omega^3 = g^{3k} = 1$. Another one that works is $g^{2k}$.

(b) (*) Show that there exists $\eta \in \mathbb{Z}_p^*$ with $\eta^2 = -3$. [Hint: The formula for $\omega$ in the complex numbers will be helpful!]

Solution: The formula in $C$ is that $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ so that $2\omega + 1 = \sqrt{-3}$. So lets try $\eta = 2\omega + 1$. So $\eta^2 = 4\omega^2 + 4\omega + 1$. As $\omega$ satisfies $x^3 - 1 = 0$ and $\omega \neq 1$, it satisfies $\omega^2 + \omega + 1 = 0$. Thus $\eta^2 = 4(\omega^2 + \omega + 1) - 3 = -3$. [Caution: We don’t know a priori that this will work. After all, $C$ is not $\mathbb{Z}_p$. But we see an analogy and try something. Then – hooray! – it leads to a solution.]

2. Now suppose $p$ be a prime of the form $p = 3k + 2$.

(a) Again using a generator $g$ show that there is no element $\omega \in \mathbb{Z}_p^*$ with $\omega \neq 1$ and $\omega^3 = 1$.

Solution: Write $\omega = g^i$. Then $g^{3i} = 1$. As $g$ has order $p - 1 = 3k + 1$ we must have $(3k + 1)|3i$ so that $(3k + 1)|i$ which would give $\omega = 1$. Alternatively, $\mathbb{Z}_p^*$ has $p - 1 = 3k + 1$ elements so that it can’t have an element of order 3.

(b) (*) Show that there does not exist $\eta \in \mathbb{Z}_p^*$ with $\eta^2 = -3$.

Solution: Reverse the above argument, setting $\omega = \frac{1}{2}(-1 + \eta)$. Then

$$\omega^2 = \frac{\eta^2 - 2\eta + 1}{4} = \frac{-2\eta - 2}{4} = -\frac{\eta - 1}{2} = -\omega - 1$$

so $\omega^3 = 1$ and $\omega \neq 1$ which doesn’t exist.

Note: Together we get a necessary and sufficient condition for when $-3$ is a square in $\mathbb{Z}_p$. There is a result in Number Theory called The Law of Quadratic Reciprocity, which we do not cover in this course, which tells you when $a$ is a square in $\mathbb{Z}_p$.

3. Let $F$ be a finite field with $q = p^n$ elements. Define $\sigma : F \rightarrow F$ by $\sigma(\alpha) = \alpha^p$. 
(a) Show that \(\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)\) for all \(\alpha, \beta \in F\).
(b) Show that \(\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)\) for all \(\alpha, \beta \in F\).
(c) Show that \(\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}\) for all nonzero \(\alpha \in F\).
(d) (*) Show that \(\sigma\) is injective. That is, show that if \(\sigma(\alpha) = \sigma(\beta)\) then \(\alpha = \beta\).
(e) Deduce that \(\sigma\) is surjective. (Use that \(|F^*| = p^n - 1\).

Note: Together this gives that \(\sigma\) is an automorphism, an isomorphism from \(F\) to itself. \(\sigma\) is often called the Frobenius automorphism.

Solution: The easy ones are
\[
\sigma(\alpha\beta) = \alpha^p\beta^p = \sigma(\alpha)\sigma(\beta)
\]
and
\[
\sigma(\alpha^{-1}) = \alpha^{-p} = (\alpha^p)^{-1} = \sigma(\alpha)^{-1}
\]
and the amazing one is
\[
\sigma(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \sigma(\alpha) + \sigma(\beta)
\]
The critical middle equality is because by the Binomial theorem
\[
(\alpha + \beta)^p = \alpha^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^{p-i}\beta^i + \beta^p
\]
The binomial coefficients have a \(p\) in the numerator and not in the denominator and so are divisible by \(p\) and hence are zero (!!) in a field of characteristic \(p\). Clearly \(\sigma(\alpha) = \alpha^p = 0\) has only the solution \(\alpha = 0\). If \(\alpha^p = \sigma(\alpha) = \sigma(\beta) = \beta^p \neq 0\) then, setting \(\gamma = \alpha/\beta\), \(\gamma^p = 1\). The order of \(\gamma\) must divide \(p^n - 1\) so it can’t be \(p\), but it must divide \(p\) so it must be 1. That is, \(\gamma = 1\) and \(\alpha = \beta\), proving injectivity. As \(F\) is a finite set an injective map from it to itself must be surjective by pigeonhole.

4. Let \(F = \mathbb{Z}_3[x]/(x^2 + 1)\).

(a) List the elements of \(F\).
   Solution: 0, 1, 2, \(x\), \(x + 1\), \(2x\), \(2x + 2\).
(b) Find a generator \(g\) of \(F^*\).
   Solution: \(x\) doesn’t work as \(x^2 = 2\) so \(x^4 = 1\). But \(g = x + 1\) works. The powers are \(g^2 = x^2 + 2x + 1 = 2x\), \(g^3 = 2x^2 + 2x = 2x + 1\), \(g^4 = (g^2)^2 = 4x^2 = 8 = 2 = -1\) and once we get halfway we know we are done as the order must divide 8 and is now bigger than 4.
(c) For each $\alpha \in F$ find the minimal polynomial $p_\alpha(y)$ of $\alpha$ in $Z_3[y]$.
Solution: For $\alpha = 0, 1, 2$ the minimal polynomial is simply $y - \alpha$. The others have been ordered to indicate the pairs with the same minimal polynomial.
For $\alpha = x$, $\alpha^2 = x^2 = 2$, $p_\alpha(y) = 1 + y^2$.
For $\alpha = 2x$, $\alpha^2 = 4x^2 = 2$, $p_\alpha(y) = 1 + y^2$.
For $\alpha = x + 1$, $\alpha^2 = x^2 + 2x + 1 = 2x$, $p_\alpha(y) = y^2 + y + 2$.
For $\alpha = 2x + 2$, $\alpha^2 = x^2 + 2x + 1 = 2x$, $p_\alpha(y) = y^2 + 2y + 2$.
For $\alpha = x + 2$, $\alpha^2 = x^2 + x + 1 = x$, $p_\alpha(y) = y^2 + 2y + 2$.
For $\alpha = 2x + 1$, $\alpha^2 = x^2 + x + 1 = x$, $p_\alpha(y) = y^2 + y + 2$.

(d) Factor $y^6 - y$ in $F[y]$.
Solution: As all $\alpha \in F$ are roots this factors into nine linear terms

$$y^6 - y = y(y - 1)(y - 2)(y - x)(y - (x + 1))(y - (x + 2))(y - 2x)(y - (2x + 1))(y - (2x + 2))$$

(e) Factor $y^6 - y$ in $Z_3[y]$. Show how the factors in $F[y]$ join to form factors in $Z_3[y]$.
Solution: We still get $y(y - 1)(y - 2)$ are before. For other $\alpha \in F$ the minimal polynomial of $\alpha$ over $Z_3[y]$ gives the factor. So we get

$$y^6 - y = y(y - 1)(y - 2)(y^2 + 1)(y^2 + y + 2)(y^2 - y + 2)$$

Each of the three quadratics has two roots $\alpha, \beta \in F$ from above and so further factors into $(y - \alpha)(y - \beta)$ in $F[y]$.

5. When a monic $f(x) \in Z[x]$ is reducible it is reducible in $Z_p[x]$. The converse doesn’t hold – for example, $x^2 + 1$ is irreducible in $Z[x]$ but is $(x + 2)(x + 3)$ in $Z_5[x]$. Here we give a surprising example of an irreducible monic $f(x) \in Z[x]$ which reduces in all $Z_p[x]$. We set $f(x) = (x^2 - 5)^2 - 24 = x^4 - 10x^2 + 1$. Let $p$ be any prime.

(a) Show that $\pm \sqrt{2} \pm \sqrt{3}$ are the complex roots of $f(x)$.
Solution: For $\kappa = \pm \sqrt{2} \pm \sqrt{3}$, $\kappa^2 = 5 \pm 2\sqrt{6}$ so $(\kappa^2 - 5)^2 = (2\sqrt{6})^2 = 24$.

(b) Show that $f(x)$ is irreducible in $Z[x]$.
Solution: There are a variety of approaches. One: Let $a, b, c, d$ be the above roots of $f(x)$. These are irrational so there is no factor $x - a \in Z[x]$. If $(x - a)(x - b) \in Z[x]$ we must have $a + b \in Z$ and $ab \in Z$ and that never happens. Two: There are no integer
roots (just try \(\pm 1\)) so we’d need \(f(x)\) to factor into quadratics so it would be \((x^2 + cx \pm 1)(x^2 + dx \pm 1)\), with the same choice of \(\pm 1\). The coefficient of \(x^3\) would be \(c + d = 0\) so we would have \(f(x) = (x^2 + cx \pm 1)(x^2 - cx \pm 1)\). Now the coefficient of \(x^2\) is \(-c^2 \pm 2\) which must be zero, so \(c \not\in \mathbb{Z}\). Three: Your own method!

**General Idea:** Let \(F\) be the (unique!) field with \(p^2\) elements. In \(F\) there exist \(\alpha, \beta\) with \(\alpha^2 = 2, \beta^2 = 3\). Set \(\kappa = \alpha + \beta\). Then \(\kappa \in F\). Let \(g(x)\) denote the minimal polynomial of \(\kappa\) over \(\mathbb{Z}_p\). Then \(g(x)\) is either linear or quadratic. But \(\kappa\) is a root of \(f(x)\). So \(g(x)\) is a factor of \(f(x)\).

(c) Assume there exists \(\alpha \in \mathbb{Z}_p\) with \(\alpha^2 = 2\). Show that \(f(x) \in \mathbb{Z}_p[x]\) is reducible. In the separate cases below we can give a specific factorization.

**Solution:** Now \(\kappa = \alpha + \sqrt{3} \in F\). Then \((\kappa - \alpha)^2 - 3 = 0\) and \(g(x) = (x - \alpha)^2 - 3\). The factorization is

\[
f(x) = [(x - \alpha)^2 - 3][(x + \alpha)^2 - 3]
\]

(d) Assume there exists \(\beta \in \mathbb{Z}_p\) with \(\beta^2 = 3\). Show that \(f(x) \in \mathbb{Z}_p[x]\) is reducible.

**Solution:** Similarly

\[
f(x) = [(x - \beta)^2 - 2][(x + \beta)^2 - 2]
\]

(e) Assume there exists \(\gamma \in \mathbb{Z}_p\) with \(\gamma^2 = 6\). Show that \(f(x) \in \mathbb{Z}_p[x]\) is reducible.

**Solution:** Now \((\alpha + \beta)^2 = 5 + 2\gamma\) so \(g(x) = x^2 - (5 + 2\gamma)\). The factorization is

\[
f(x) = (x^2 - (5 + 2\gamma))(x^2 - (5 - 2\gamma))
\]

(f) Show that at least one of the \(\alpha, \beta, \gamma\) above must exist.

**Solution:** The quadratic residues in \(\mathbb{Z}_p\) form a subgroup \(H \subset \mathbb{Z}_p^*\) of index two. There are two cosets, the residues and the nonresidues. Hence the product of two nonresidues is a residue. (Another approach: Set \(p = 2k + 1\) and let \(g\) be a generator. Then the residues are those \(g^i\) with \(i\) even; the nonresidue with \(i\) odd – and odd plus odd is even.) So if 2 and 3 are nonresidues, \(6 = 2 \cdot 3\) must be a residue.

Hence: \(f(x)\) reduces in all \(\mathbb{Z}_p[x]\).