Algebra Assignment 6 Solutions

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

(a) Show that there is an element \( \omega \in Z_p^* \) 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 \( \eta \in Z_p^* \) 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 let's 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 \textit{a priori} that this will work. After all, \( C \) is not \( Z_p \). 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 \( \omega \in Z_p^* \) 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 \( (3k + 1)|i \) so that \( (3k + 1)|i \) which would give \( \omega = 1 \). Alternatively, \( Z_p^* \) has \( p - 1 = 3k + 1 \) elements so that it can't have an element of order 3.

(b) (*) Show that there does not exist \( \eta \in Z_p^* \) 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 \( Z_p \). 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 \( Z_p \).

3. Let \( F \) be a finite field with \( q = p^n \) elements. Define \( \sigma : F \to F \) 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: $0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$.
(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 \( \mathbb{Z}_3[y] \).

**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 \( y^9 - y \) in \( F[y] \).

**Solution:** As all \( \alpha \in F \) are roots this factors into nine linear terms

\[
y^9 - y = y(y-1)(y-2)(y-x)(y-(x+1))(y-(x+2))(y-2x)(y-(2x+1))(y-(2x+2))
\]

(e) Factor \( y^9 - y \) in \( \mathbb{Z}_3[y] \). Show how the factors in \( F[y] \) join to form factors in \( \mathbb{Z}_3[y] \).

**Solution:** We still get \( y(y-1)(y-2) \) are before. For other \( \alpha \in F \) the minimal polynomial of \( \alpha \) over \( \mathbb{Z}_3[y] \) gives the factor. So we get

\[
y^9 - y = y(y-1)(y-2)(y^2 + 1)(y^2 + y + 2)
\]

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. Assume the following theorem: Let \( q = p^n \) and set \( f(x) = x^q - x \). Then, in \( \mathbb{Z}_p[x] \), \( f(x) \) factors into the product of all monic irreducible (over \( \mathbb{Z}_p[x] \)) polynomials of all degrees \( d \), where \( d \) is a divisor (including 1 and \( q \)) of \( q \).

(a) How many irreducible quadratic polynomials are there over \( \mathbb{Z}_5[x] \)? (Count degrees in the factorization of \( x^{25} - x \).)

**Solution:** This degree 25 polynomial factors into 5 linear polynomials and \( A \) quadratics, where \( A \) is the number we are seeking. So 25 = 5 + 2A and \( A = 10 \).

(b) How many irreducible cubic polynomials are there over \( \mathbb{Z}_5[x] \)? (Count degrees in the factorization of \( x^{125} - x \).)

**Solution:** This degree 125 polynomial factors into 5 linear polynomials and \( B \) cubics, where \( B \) is the number we are seeking. So 125 = 5 + 3B and \( B = 40 \).
(c) (*) How many irreducible polynomials of degree six are there over 
\( \mathbb{Z}_5[x] \)? (Count degrees in the factorization of \( x^{15625} - x \).)

**Solution:** This degree 15625 polynomial factors into 5 linear polynomials and 10 quadratics, 40 cubics, and \( D \) degree six polynomials, where \( D \) is the number we are seeking. So 15625 = 
\[ 5 + 10(2) + 40(3) + 6D \]
and \( D = 2580 \).