Test 3 – Solutions

1. (a) **State the Factor Theorem**
   If $F$ is a field and $f \in F[x]$, then $x-a \mid f$ if and only if $f(a) = 0$.

   (b) **State the Rational Root Test**
   If $f = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$, then any root $r \in \mathbb{Q}$ is of the form $\frac{r}{s}$ where $r \mid a_0$ and $s \mid a_n$.

   (c) **Define irreducible polynomial**.
   If $F$ is a field, a polynomial $f \in F[x]$ is irreducible if $\deg(f) > 0$ and its only divisors are associates and units.

   (d) **Define ideal of a ring**.
   A subset $I$ of a ring $R$ is an ideal of $R$ if $I$ is a subring such that for all $a \in I$ and all $r \in R$, $ra \in I$ and $ar \in I$.

2. **Let $R$ be a commutative ring with 1 and $a \in R$.**

   (a) **Define $(a)$, the principal ideal generated by $a$.**
   
   $$(a) = \{ra \mid r \in R\}$$

   (b) **Prove that $(a)$ is an ideal of $R$.**
   
   Since $0_R = 0_R \cdot a \in (a)$, $(a) \neq \emptyset$.
   
   For all $ra, sa \in I$, $ra - sa = (r-s)a \in I$.
   
   Finally, for all $ra \in I$ and $s \in R$, $s(ra) = (ra)s$ since $R$ is commutative and $s(ra) = (sr)a \in I$.

3. **Let $F$ be a field, $f \in F[x]$, and $a \in F$. Prove that the remainder when $f$ is divided by $x-a$ is $f(a)$.**

   We apply the Division Algorithm for $f$ divided by $x-a$ to get $f = (x-a) \cdot q + r$ where $q, r \in F[x]$ and $\deg(r) < \deg(x-a) = 1$. So, $r$ is a constant polynomial, i.e., $r \in F$. Now, evaluate at $a$ to get $f(a) = (a-a)q(a)+r = 0_F \cdot q(a)+r = 0_F + r = r$.

   (b) **Compute the remainder when $x^{500} - 5$ is divided by $x+1$ in $\mathbb{Q}[x]$, showing your work to justify your answer.**

   We apply the result from part (a) since $x+1 = x - (-1)$. So, the remainder is $(-1)^{500} - 5 = 1 - 5 = -4$.

4. **In each case, prove that the polynomial is irreducible in the given ring.**

   (a) **$x^8 + 6x + 12$ in $\mathbb{Q}[x]$**

   We can apply Eisenstein’s criterion with $p = 3$. Note, $p = 2$ does not work since $2^2 \mid 12$. 
(b) \( x^3 + 5x + 5 \) in \( \mathbb{Z}_7[x] \)

Note, the field is \( \mathbb{Z}_7 \), so theorems for polynomials over \( \mathbb{Z} \) and \( \mathbb{Q} \) do not apply (like Eisenstein’s criterion and the rational root test). Since the degree of the polynomial is 3, it suffices to show that it has no roots in \( \mathbb{Z}_7 \), which we do by exhaustive checking. Let \( f = x^3 + 5x + 5 \).

\[
\begin{align*}
    f(0) &= 0^3 + 5 \cdot 0 + 5 = 5 \\
    f(1) &= 1^3 + 5 \cdot 1 + 5 = 11 = 4 \\
    f(2) &= 2^3 + 5 \cdot 2 + 5 = 19 = 5 \\
    f(3) &= 3^3 + 5 \cdot 3 + 5 = 49 = 0 \\
    f(4) &= 4^3 + 5 \cdot 4 + 5 = 109 = 2 \\
    f(5) &= 5^3 + 5 \cdot 5 + 5 = 165 = 1 \\
    f(6) &= 6^3 + 5 \cdot 6 + 5 = 119 = 6
\end{align*}
\]

So, \( f \) is irreducible in \( \mathbb{Z}_7[x] \).

(c) \( x^4 + x + 1 \) in \( \mathbb{Q}[x] \) (hint: shifting will not help).

We give two approaches. First, is suffices to show that the polynomial is irreducible modulo \( p \) for some prime \( p \), and we use \( p = 2 \). So, we just have to show that \( x^4 + x + 1 \) is irreducible in \( \mathbb{Z}_2[x] \). It has no roots in \( \mathbb{Z}_2 \) by exhaustive checking, \( 0^4 + 0 + 1 = 1 \neq 0 \) and \( 1^4 + 1 + 1 = 3 = 1 \neq 0 \), so there are no degree 1 factors. If it were reducible, then the only possibility is two degree 2 factors.

But, in \( \mathbb{Z}_2[x] \), there are only four degree 2 polynomials: \( x^2 = x \cdot x, x^2 + x = x(x+1), x^2 + 1 = (x+1)^2, \) and \( x^2 + x + 1 \). The first three are not irreducible (as shown), so if \( x^4 + x + 1 \) is reducible, it must equal \( (x^2 + x + 1)^2 = x^4 + x^2 + 1 \), which it does not. So, \( x^4 + x + 1 \) is irreducible in \( \mathbb{Z}_2[x] \), so it is irreducible in \( \mathbb{Q}[x] \).

The second approach is to first apply the rational root test. If there is a rational root, it must be of the form \( r/s \) where \( r \mid 1 \) and \( s \mid 1 \), to the root would be \( \pm 1 \). But, \( 1^4 + 1 + 1 = 3 \neq 0 \) and \( (-1)^4 + (-1) + 1 = 1 \neq 0 \). So, the polynomial has no roots, so no degree one factors by the Factor Theorem. The only remaining possibility is that it is the product of two quadratic polynomials. Since \( x^4 + x + 1 \in \mathbb{Z}[x] \), it would have such a factorization in \( \mathbb{Z}[x] \):

\[
x^4 + x + 1 = (ax^2 + bx + c)(dx^2 + ex + f) \quad \text{with} \quad a, b, c, d, e, f \in \mathbb{Z}
\]

Looking at leading coefficients, \( ad = 1 \) so \( a = d = \pm 1 \). If they are both \( -1 \), multiply both factors by \( -1 \) to reduce to the case where \( a = d = 1 \). Then

\[
x^4 + x + 1 = x^4 + (b + e)x^3 + (c + f + 2bf + ce)x^2 + (bf + 2ce)x + cf
\]

Equating coefficients gives us \( b + e = 0 \) from the \( x^3 \) term. From the constant terms, \( cf = 1 \), so \( c = f = \pm 1 \). Then on the coefficient of \( x \), we get \( 1 = bf + ce = c(b + e) = c \cdot 0 = 0 \), a contradiction. Thus, the polynomial is irreducible.

5. **Prove that every ideal of** \( \mathbb{Z} \) **is principal**

Let \( I \) be an ideal of \( \mathbb{Z} \). If \( I = \{0\} \), then \( I = (0) \) so it is principal. Otherwise, there exists \( c \in I \) with \( c \neq 0 \). Since \( c \in I \) and \( -c = (-1) \cdot c \in I \) (by the absorption
property), $I$ must contain a positive integer (one of $c, -c$ is positive). Let $n$ be the smallest positive integer in $I$. Then for all $m \in \mathbb{Z}$, $mn \in I$, so $(n) \subseteq I$.

Now let $a \in I$. By the Division Algorithm for $a$ divided by $n$, there exists $q, r \in \mathbb{Z}$ with $a = nq + r$ and $0 \leq r < n$. Since $r = a - nq$ and $a \in I$ and $nq \in I$, we have $r \in I$. Since $r < n$, we must have $r = 0$ or we would contradict the minimality of $n$. Thus, $a = nq \in (n)$. So, $I \subseteq (n)$, and combining with the inclusion above, $I = (a)$.

6. Let $R$ be a commutative ring, $c \in R$ and $I$ an ideal of $R$. Let

$$J = \{a \in R \mid ca \in I\}$$

Prove that $J$ is an ideal of $R$ and that $I \subseteq J$.

First we note that $c \cdot 0 = 0 \in I$ (because $I$ is an ideal), so $0 \in J$. If $a_1, a_2 \in J$, $ca_1, ca_2 \in I$, so $c(a_1 - a_2) = ca_1 - ca_2 \in I$ because $I$ is closed under subtraction. Thus, $a_1 - a_2 \in J$. Finally, if $a \in J$ and $r \in R$, $ar = ra$ because $R$ is commutative and $ar \in J$ because $c(ar) = (ca)r$, and $ca \in I$ so $(ca)r \in I$ by the absorption property. Thus, $ra = ar \in J$, so $J$ is an ideal.

If $a \in I$, then $ca \in I$ by the absorption property, which implies $a \in J$. Thus, $I \subseteq J$.

7. Prove Eisenstein’s Criterion.

Suppose $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $p$ is a prime such that $p \nmid a_n$, $p \mid a_i$ for $0 \leq i < n$, and $p^2 \nmid a_0$. Suppose further that $f$ is reducible in $\mathbb{Q}[x]$. Then $f$ can be factored $f = gh$ where $g, h \in \mathbb{Z}[x]$ and both $g$ and $h$ have degrees which are positive.

Applying $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, the reduction modulo $p$ homomorphism, we get

$$\phi_p(f) = \phi_p(gh) = \phi_p(g)\phi_p(h)$$

But, the hypotheses on the coefficients of $f$ implies that $\phi_p(f) = \phi_p(a_n)x^n$ and $\phi_p(a_n) \neq 0$ since $p \nmid a_n$. By unique factorization for polynomials over a field, here $\mathbb{Z}_p$, we have $\phi_p(g) = bx^j$ and $\phi_p(h) = cx^{n-j}$ for some $b, c \in \mathbb{Z}_p^*$ where $1 \leq j < n$. But this implies that $p$ divides the constant terms of $g$ and of $h$, so $p^2$ divides the constant term of $f = gh$, a contradiction.