Math 237  
First midterm exam  
October 20, 2010

Be sure to write your name on your bluebook. Use a separate page (or pages) for each problem. Show all of your work.

1. Give definitions of each of the following. (4 points each)

(a) Principal ideal domain

Solution: See 8.6.2 in the textbook.

(b) Splitting field of a polynomial \( f(x) \in F[x] \) for a field \( F \).

Solution: See 10.3.5 in the textbook.

(c) Maximal ideal

Solution: See 7.2.23 in the textbook.

(d) Minimal polynomial over \( F \) of an element \( \alpha \in E \) for fields \( E \) and \( F \) with \( F \subset E \)

Solution: See 10.2.13 in the textbook.

(e) Irreducible polynomial

Solution: See 8.4.1 in the textbook.

2. Find the minimal polynomial \( f(x) \) for \( \alpha = \sqrt{2} + \sqrt{3} \) over each of the following fields \( F \). (5 points each)

(a) \( F = \mathbb{Q} \)

Solution:

\[
\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \\
(\alpha^2 - 5)^2 = \alpha^4 - 10\alpha^2 + 25 = (2\sqrt{6})^2 = 24 \\
\text{so } f(x) = x^4 - 10x^2 + 1.
\]

(b) \( F = \mathbb{Q}(\sqrt{2}) \)
Solution:

\[ \alpha - \sqrt{2} = \sqrt{3} \]
\[ (\alpha - \sqrt{2})^2 = \alpha^2 - 2\sqrt{2} + 2 = 3 \]
so \[ f(x) = x^2 - 2\sqrt{2}x - 1 \]

(b) \( F = \mathbb{Q}(\sqrt{3}) \)

Solution:

\[ \alpha - \sqrt{3} = \sqrt{2} \]
\[ (\alpha - \sqrt{3})^2 = \alpha^2 - 2\sqrt{3} + 3 = 2 \]
so \[ f(x) = x^2 - 2\sqrt{3}x + 1 \]

(d) \( F = \mathbb{Q}(\sqrt{6}) \)

Solution:
Since \( \alpha^2 = 5 + 2\sqrt{6}, \alpha^2 - 2\sqrt{6} - 5 = 0 \) and \( f(x) = x^2 - 2\sqrt{6} - 5 \).

3. (20 POINTS) Let \( R \) be a commutative ring with 1 and let \( I \) be an ideal in \( R \). Show that \( I \) is a prime ideal of \( R \) if and only if \( R/I \) is an integral domain.

Solution: See Theorem 7.2.27 in the textbook.

4. (20 POINTS) Let \( F \subseteq E \) with \( [E : F] = m \). If \( p(x) \in F[x] \) is irreducible over \( F \) of degree \( n \) with \((n, m) = 1\), show that \( p(x) \) has no roots in \( E \).

Solution: Suppose \( p(\alpha) = 0 \) for some \( \alpha \in E \). Let \( K = F(\alpha) \) and \( L = F[x]/(P(x)) \).
Then \( K \) is a subfiled of both \( E \) and \( L \). This means that \([K : F]\), which is bigger than 1, must divide both \([E : F] = m\) and \([L : F] = n\). This is impossible since \((m, n) = 1\).

5. Without using the result of the previous problem, use direct calculation to show (10 POINTS EACH) that

(a) \( x^2 + x + 1 \) has no roots in \( E = \mathbb{Z}/2[y]/(y^3 + y + 1) \), the field with 8 elements.
**Solution:** Let $x = ay^2 + by + c \in E$ for $a, b, c \in \mathbb{Z}/2$. Then
\[
\begin{align*}
x^2 &= (ay^2 + by + c)^2 \\
    &= ay^4 + by^2 + c \\
    &= a(y^2 + y) + by^2 + c \\
    &= (a + b)y^2 + ay + c
\end{align*}
\]
so
\[
\begin{align*}
x^2 + x + 1 &= (a + b)y^2 + ay + c + ay^2 + by + c + 1 \\
    &= by^2 + (a + b)y + 1
\end{align*}
\]
and this is never zero.

(b) $x^3 - x + 1$ has no roots in $E = \mathbb{Z}/3[y]/(y^2 + 1)$, the field with 9 elements.

**Solution:** Let $x = ay + b$ for $a, b \in \mathbb{Z}/3$. Then
\[
\begin{align*}
x^3 &= (ay + b)^3 = ay^3 + b \\
    &= -ay + b
\end{align*}
\]
so
\[
\begin{align*}
x^3 - x + 1 &= -ay + b - ay - b + 1 \\
    &= -2ay + 2 = ay + 1
\end{align*}
\]
which is never zero.

**Hints:** When working mod $p$, $(x + y)^p = x^p + y^p$. Each element $a \in \mathbb{Z}/p$ satisfies $a^p = a$. 