Some answers to midterm #2.

3. Show that \( \mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C} \).

PROOF 1. Since \([X^2] = [-1]\) in \( \mathbb{R}[X]/(X^2 + 1) \), every element of \( \mathbb{R}[X]/(X^2 + 1) \) has the form \([a + bX]\) for some \( a, b \in \mathbb{R} \). Also if \([a + bX] = [c + dX]\) for some \( a, b, c, d \in \mathbb{R} \), then \((a - c) + (b - d)X \in (X^2 + 1)\); then \((a - c) + (b - d)X = 0\) since nonzero multiples of \(X^2 + 1\) have degree at least 2; so \( a = c \) and \( b = d \). Therefore

\[
\text{every element of } \mathbb{R}[X]/(X^2 + 1) \text{ equals } [a + bX] \text{ for unique } a, b \in \mathbb{R}. \tag{*}
\]

Define \( f : \mathbb{R}[X]/(X^2 + 1) \to \mathbb{C} \) by \( f([a + bX]) = a + bi \). This is well-defined by (*). To check that it is a ring homomorphism: clearly \( f([1]) = 1 \),

\[
f([a + bX] + [c + dX]) = f([(a + c) + (b + d)X]) = (a + c) + (b + d)i = (a + bi) + (c + di) = f([a + bX]) + f([c + dX])
\]

\[
f([a + bX][c + dX]) = f([(a + bX)(c + dX)]) = f([(ac + (ad + bc)X + bdX^2)])
\]

\[
= f([(ac - bd) + (ad + bc)X]) = (ac - bd) + (ad + bc)i
\]

\[
= (a + bi)(c + di) = f([a + bX])f([c + dX]).
\]

(In checking that \( f \) preserves multiplication it is a key fact that \([X^2] = [-1]\).)

The kernel of \( f \) is \( (0) \) because if \( f([a + bX]) = 0 \) for some \( a, b \in \mathbb{R} \), then \( a + bi = 0 \) so \( a = b = 0 \) and \([a + bX] = 0\). Therefore \( f \) is injective.

For any \( z \in \mathbb{C} \), \( z = a + bi \) for some \( a, b \in \mathbb{R} \), so \( f([a + bX]) = z \). Therefore \( f \) is surjective.

Therefore \( f \) is an isomorphism, so \( \mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C} \).

PROOF 2. Define \( f : \mathbb{R}[X] \to \mathbb{C} \) by \( f(p(X)) = p(i) \) for every \( p \in \mathbb{R}[X] \), that is,

\[
f \left( \sum_{n=0}^{N} a_n X^n \right) = \sum_{n=0}^{N} a_n i^n.
\]

(This is clearly well-defined since a polynomial in \( \mathbb{R}[X] \) has uniquely determined coefficients.) To check that \( f \) is a ring homomorphism, clearly \( f(1) = 1 \). Let \( p(X) = \sum_{n=0}^{N} (a_n X^n) \) and \( q(X) = \sum_{n=0}^{N} (b_n X^n) \) be in \( \mathbb{R}[X] \) (by adding terms with 0 coefficients if necessary we may assume that both sums are from \( n = 0 \) to the same \( N \)). Then

\[
f(p + q) = (p + q)(i) = \sum_{n=0}^{N} (a_n + b_n)i^n = \sum_{n=0}^{N} a_n i^n + \sum_{n=0}^{N} b_n i^n = f(p) + f(q),
\]

\[
f(pq) = (pq)(i) = \sum_{n=0}^{2N} \sum_{j+k=n} (a_j b_k) i^n = \sum_{j=0}^{N} a_j i^j \sum_{k=0}^{N} b_k i^k = f(p)f(q).
\]
So $f$ is a ring homomorphism. Every $z \in \mathbb{C}$ has the form $z = a + bi$ for some $a, b \in \mathbb{R}$, so $z = f(a + bX)$. Therefore $f$ is surjective.

Now let $I = \ker(f)$, an ideal of $\mathbb{R}[X]$. $\mathbb{R}$ is a field, so $\mathbb{R}[X]$ is a Euclidean domain, therefore a PID, so $I = (q)$ for some $q \in \mathbb{R}[X]$. But $f(X^2 + 1) = i^2 + 1 = 0$, so $X^2 + 1 \in I$, and so $q$ divides $X^2 + 1$. But in $\mathbb{R}[X]$, $X^2 + 1$ has no roots, so (being quadratic) is irreducible. Therefore $q$ is associated with $X^2 + 1$. ($q$ can’t be a unit since if it were, $q = a \in \mathbb{R} - \{0\}$ and $f(q) = a \neq 0$, contradiction.) Therefore $(q) = (X^2 + 1)$, so $\ker f = (X^2 + 1)$. By the Fundamental Theorem of Ring Theory, $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

4. True or false? Justify your answers.

(a) In $\mathbb{Z}_{17}[X]$, $X - 1$ divides $X^{16} + X^{15} + X^{14} + \ldots + X^2 + X + 1$.

Let $f(X) = X^{16} + \cdots + X + 1 \in \mathbb{Z}_{17}[X]$. Then $f(1) = 1 + \cdots + 1 + 1 = 0$ so the assertion is true by the Factor Theorem.

(b) $X^2 - 2$ is irreducible in $\mathbb{Z}_7[X]$.

$3^2 - 2 = 0$ in $\mathbb{Z}_7$, so $X - 3$ divides $X^2 - 2$ by the Factor Theorem. The assertion is false.

5. Let $I$ and $J$ be two ideals of a ring $R$. Suppose that $J \subseteq I$.

(a) Construct a well-defined surjective ring homomorphism $\phi : R/J \to R/I$ (and prove that it has these properties).

Define $\phi : R/J \to R/I$ by $\phi([a]_J) = [a]_I$, for all $a \in R$. Then $\phi$ is a well-defined function because every element of $R/J$ has the form $[a]_J$ for some $a \in R$, and if $a, b \in R$ satisfy $[a]_J = [b]_J$, then $a - b \in J \subseteq I$, so $a - b \in I$, so $[a]_I = [b]_I$.

$\phi$ is a homomorphism because $\phi([1]_J) = [1]_I$,

$$\phi([a]_J + [b]_J) = \phi([a + b]_J) = [a + b]_I = [a]_I + [b]_I = \phi([a]_J) + \phi([b]_J)$$

for all $a, b \in R$, and similarly, $\phi$ preserves multiplication.

Any element of $R/I$ has the form $[a]_I$ for some $a \in R$, so equals $\phi([a]_J)$. Therefore $\phi$ is surjective.

(b) Illustrate with the example $R = \mathbb{Z}$, $J = (n)$ and $I = (m)$, by answering the following questions. What does the condition $J \subseteq I$ mean in terms of divisibility? What is $\ker \phi$ in this case?

The condition $(n) \subseteq (m)$ (in $\mathbb{Z}$) means that $m \mid n$. Since $\phi([a]_n) = [a]_m$, the kernel of $\phi$ consists of those $[a]_n$ such that $m \mid a$. So $\ker \phi = ([m])$ (in $\mathbb{Z}_n$).
6. Factor $z = 2 + 11i$ into irreducibles in $\mathbb{Z}[i]$. (Hint. First factor $\delta(z)$ in $\mathbb{Z}$.) Use $\delta$ to explain why your irreducibles really are irreducible.

$$\delta(z) = 2^2 + 11^2 = 125 = 5 \cdot 5 \cdot 5.$$ Look for factors $y \in \mathbb{Z}[i]$ such that $\delta(y) = 5$, so that $y = 2 + i$ or an associate. A computation shows that $2 + 11i = (2 + i)^3$.

The explanation depends on the multiplicativity of $\delta$. If $2 + i = ab$, $a, b, \in \mathbb{Z}[i]$, then $5 = \delta(ab) = \delta(a)\delta(b)$. Hence either $\delta(a) = 1$ or $\delta(b) = 1$ and so $a$ or $b$ is a unit. Therefore $2 + i$ is irreducible.

7. Let $S = \mathbb{Z}_2[X]/(X^2 + X + 1)$.

(a) List the elements of $S$ and write out the multiplication table for $S$, thereby showing that $S$ is a field.

Since $[X^2] = [-X - 1] = [X + 1]$, every element $[p(X)] \in S$ with $\deg p \geq 2$ is equal to some $[q(X)] \in S$ with $\deg q < \deg p$. Therefore every element of $S$ has the form $[p(X)]$ for some $p$ of degree 0 or 1. So $S = \{[0], [1], [X], [X + 1]\}$. The multiplication table (brackets removed) has a 1 in every nonzero row so $S$ is a field – obviously being commutative:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>X</th>
<th>X + 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>X</td>
<td>X + 1</td>
</tr>
<tr>
<td>X</td>
<td>0</td>
<td>X</td>
<td>X + 1</td>
<td>1</td>
</tr>
<tr>
<td>X + 1</td>
<td>0</td>
<td>X + 1</td>
<td>1</td>
<td>X</td>
</tr>
</tbody>
</table>

(b) Independently, one of our theorems implies that $S$ must be a field. Which theorem is it, and why does it apply?

The Big Theorem asserts that if $R$ is a Euclidean domain (or PID, even), and $a \in R - \{0\}$, then $R/(a)$ is a field if and only if $a$ is irreducible. Here $S$ is Euclidean, and $X^2 + X + 1$ has no roots in $\mathbb{Z}_2$ (check 0 and 1), so being quadratic, it is irreducible.

8. Which of the following groups are cyclic? How many elements of order 2 does each group have? Justify your answers.

(a) $G = U(\mathbb{Z}_8)$

$G = \{[\pm 1], [\pm 3]\}$ has order 4 and $g^2 = e$ for every $g \in G$. Therefore $G$ is not cyclic and has 3 elements of order 2.

(b) $G = U(\mathbb{Z}_{11})$

Since 11 is prime, $|G| = 11 - 1 = 10$. Also $G \cong \mathbb{Z}_{10}$, justified either by finding a generator (e.g. showing that $[2]$ has order 10) or by quoting the theorem in 7.3 that
any finite subgroup of the multiplicative group of a field is cyclic (class, 11/14). In \( \mathbb{Z}_{10} \) and hence in \( G \), there is exactly one element of order 2 (in \( G \) it is \([10] = [-1]\)).

(c) \( G \) = symmetry group of a regular hexagon.

\(|G| = 12\). In \( G \) there are six reflections (the hexagon has 6 axes of symmetry, three passing through vertices, three bisecting a pair of opposite sides). There are six rotations \( \rho^i \), \( 0 \leq i < 6 \), where \( \rho \) is a rotation through \( \pi/3 \) radians. The elements of \( \langle \rho \rangle \) have orders 1, 2, 3, or 6. So \( G \) has 7 elements of order 2: \( \rho^3 \) and the six reflections. As \( G \) has no element of order 12, \( G \) is not cyclic.

9. Suppose that \( R \) is an integral domain, \( a, b \in R - \{0\} \). For each of the following give a proof or counterexample.

(a) \( a = b \) if and only if \( a \) and \( b \) are associates.

PROOF. Suppose \( a = b \). Then \( a \in (b) \) so \( a = rb \) for some \( r \in R \). Similarly, \( b = sa \) for some \( s \in R \). Then \( a = rsa \). Since \( R \) is an integral domain, the cancellation law holds for multiplication, so \( rs = 1 \). Therefore \( r \in U(R) \). Since \( a = rb \), \( a \sim b \).

Conversely, suppose \( a = ub \) for some \( u \in U(R) \). Then \( a \in (b) \), so \( (a) \subseteq (b) \). Similarly \( b = u^{-1}a \), so \( b \in (a) \) and \( (b) \subseteq (a) \).

(b) If \( a \) and \( b \) are associates, and \( a \) is irreducible, then \( b \) is irreducible.

PROOF. Suppose that \( b = rs \) for some \( r, s \in R \).

Since \( a \sim b \), \( a = ub \) for some \( u \in U(R) \). Then \( a = u rs = (ur)s \). Since \( a \) is irreducible, either \( s \in U(R) \) or \( ur \in U(R) \). In the second case \( r = u^{-1}(ur) \in U(R) \), since the product of units is always a unit.

Therefore either \( r \) or \( s \) is a unit, so \( b \) is irreducible by definition of “irreducible”.

10. Suppose that \( G \) is a finite group and is abelian. Let \( g_1, g_2, \ldots, g_n \) be the distinct elements of \( G \). Define \( x := g_1 g_2 \cdots g_n \), the product of all the elements of \( G \). Show that \( x^2 = e \).

PROOF. The mapping \( g \mapsto g^{-1} \) is a bijection from \( G \) to \( G \) (this mapping is its own inverse since \((g^{-1})^{-1} = g \) for all \( g \in G \)). Therefore \( G = \{g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\} \). Since \( G \) is abelian, \( x = g_1^{-1} g_2^{-1} \cdots g_n^{-1} = (g_1 g_2 \cdots g_n)^{-1} = x^{-1} \). Therefore \( x^2 = e \).