1. \(3200 = 2^7 \cdot 5^2\). The number of isomorphism classes of abelian groups of order \(5^2\) is the number of partitions of 2. The partitions of 2 are 2 and (1,1), hence the number of isomorphism classes of abelian groups of order \(5^2\) is 2. The number of isomorphism classes of abelian groups of order \(2^7\) is the number of partitions of 7. The partitions of 7 are 7, (6,1), (5,2), (4,3), (5,1,1), (4,2,1), (3,3,1), (3,2,2), (4,1,1,1), (3,2,1,1), (2,2,2,1), (3,1,1,1,1), (2,2,1,1,1), (2,1,1,1,1,1), (1,1,1,1,1,1,1), which gives a total of 15 partitions. Therefore the number of isomorphism classes of abelian groups of order 3200 is \(2 \cdot 15 = 30\). Since exactly one of these groups is cyclic, we conclude that the number of noncyclic abelian groups is 29.

2. (a) This is not an ideal. For example 2 is in the described subset, but 2x is not.

(b) This is an ideal. Let \(I\) be described set. Then \(I\) is certainly an abelian group under addition. Finally consider \(4a_0 + 2a_1x + a_2x^2 + \cdots + a_nx^n\), where \(a_i \in \mathbb{Z}\) for all \(i\); this is the general element of \(I\). The general element of \(\mathbb{Z}[x]\) is \(b_0 + b_1x + \cdots + b_mx^m\), where \(b_i \in \mathbb{Z}\). When we multiply these two elements together, we get

\[
4a_0b_0 + 2(a_1b_0 + 2a_0b_1)x + (4a_0b_2 + 2a_1b_1 + a_2b_0)x^2 + \cdots + x^{n+m}.
\]

The above element is in \(I\) and it follows that \(I\) is an ideal of \(\mathbb{Z}[x]\). Finally let \(4c_0 + 2c_1x + c_2x^2 + \cdots + c_kx^k\) be another element of \(I\). Then \(I^2\) consists of sums of elements of the form

\[
16a_0c_0 + 8(a_1c_0 + a_0c_1)x + 4(a_2c_0 + a_1c_1 + a_0c_2)x^2 + 2(2a_3c_0 + a_2c_1 + a_1c_2 + 2a_0c_3)x^3 + \cdots + a_nc_kx^{n+k}.
\]

It follows that \(I^2\) consists of all elements whose constant coefficient is a multiple of 16, whose coefficient of \(x\) is a multiple of 8, whose coefficient of \(x^2\) is a multiple of 4, and whose coefficient of \(x^3\) is a multiple of 2. The coefficients of \(x^4\) and higher degree terms are arbitrary.

3. First we show that \(I < R\). Obviously \(0 \in I\), because \(0^1 = 0\). Next suppose \(x, y \in I\) and \(r \in R\). Then \(x^m, y^n = 0\) for some positive integers \(m, n\). We now have \((-x)^m = 0\) and \((xr)^m = x^mr^m = 0\), because \(R\) is commutative, so it remains to prove that \(x + y\) is nilpotent. We show that \((x + y)^{m+n} = 0\). If we expand this by the binomial theorem, we get

\[
(x + y)^{m+n} = x^{m+n} + (m+n)x^{m+n-1}y + \cdots + y^{m+n} = 0,
\]

since each of the terms is a multiple of either \(x^m\) or \(y^n\). Thus we have shown that \(I < R\).

Finally we show that \(R/I\) has no nonzero nilpotent elements, so suppose \(I + x\) is a nilpotent element of \(R/I\), where \(x \in R\). Then \((I + x)^n = I + x^n = I\) for some positive
integer $n$, hence $x^n \in I$. Since $I$ consists of nilpotent elements, we see that $(x^n)^m = 0$ for some positive integer $m$ and we deduce that $x^{mn} = 0$. Therefore $x$ is nilpotent, hence $x \in I$ and consequently $I + x = 0$, as required.

4. (a) If two rings are isomorphic, then their underlying abelian groups are certainly isomorphic; this is not the case for $\mathbb{Z}/4\mathbb{Z}$. An alternative argument is to note that $\mathbb{Z}/4\mathbb{Z}$ has an element of additive order 4, namely $\bar{1}$, whereas $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ does not.

(b) Suppose $\theta : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$ is an isomorphism. Since $1^2 - 1 = 0$, we see that $(\theta(1))^2 - \theta(1) = 0$, consequently $\theta(1) = 1$ or 0. But $\theta(1) \neq 0$ because $\theta$ is an isomorphism and we deduce that $\theta(1) = 1$. Set $x = \theta(\sqrt{2})$. Since $(\sqrt{2})^2 - 1 - 1 = 0$, we see that $x^2 - 2 = 0$. Therefore $x = \pm \sqrt{2}$ and we deduce that we may write $\sqrt{2} = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$. Since $\sqrt{2}$ and $\sqrt{3}/2$ are irrational, we see that $a, b \neq 0$. Squaring, we obtain $2 = a^2 + 3b^2 + 2ab\sqrt{3}$. Since $ab \neq 0$, we deduce that $\sqrt{3} \in \mathbb{Q}$, which is not the case. The result follows.

5. Define a ring homomorphism $\theta : \mathbb{Q}[x] \to \mathbb{Q}$ by $\theta q = q$ for $q \in \mathbb{Q}$ and $\theta x = 1/2$. Another way to describe $\theta$ is $\theta(f) = f(1/2)$ for $f \in \mathbb{Q}[x]$. Then $\theta$ is clearly onto and $x - 1/2 \in \ker \theta$, consequently $(2x - 1) \subseteq \ker \theta$. Finally if $f \in \ker \theta$, then $f(1/2) = 0$, hence $x - 1/2$ is a factor of $f$ and we deduce that $f \in (2x - 1)$. Thus $\ker \theta = (2x - 1)$ and the result now follows from the fundamental isomorphism theorem.

6. Since $xR \subseteq yR$, we may write $x = yr$ for some $r \in R$. Suppose $yR \neq xR$. Then clearly $y \notin xR$ and since $xR$ is prime, we see that $r \in xR$. Therefore we may write $r = xs$ for some $s \in R$ and then we have $x = yxs$. Since $R$ is an integral domain and $x \neq 0$, it follows that $1 = yx$, so $y$ is a unit and we deduce that $yR = R$.

7. First we show that $S^{-1} I \triangleleft S^{-1} R$. Obviously $0 \in I$, because $0 = 0/1$. Next let $x, y \in I$. Then we may write $x = a/s$ and $y = b/t$ where $a, b \in I$ and $s, t \in S$. Then $-x = (-a)/s \in I$ and $x + y = a/s + b/t = (at + bs)/(st) \in S^{-1} I$, because $at, bs \in I$. Finally let $z \in S^{-1} R$. Then we may write $z = c/u$ where $c \in R$ and $u \in S$ and we have $xz = (ac)/(su) \in S^{-1} I$, because $ac \in I$.

We haven’t yet used $S \cap I = 0$, but we need it to prove $S^{-1} I \neq R$. If $S^{-1} I = R$, then $1 \in S^{-1} I$ and hence $s/s \in S^{-1} I$, where $s \in S$ and $s \in I$. This contradicts $S \cap I = 0$.

8. Define $\theta : \mathbb{C}[x] \to \mathbb{C} \times \mathbb{C}$ by $\theta(a) = (a, a)$ for $a \in \mathbb{C}$ and $\theta(x) = (i, -i)$ (where $i$ is the square root of $-1$). Thus for, example, $\theta(a_0 + a_1 x + a_2 x^2) = (a_0 + a_1 i - a_2, a_0 - a_1 i - a_2)$, and in general $\theta(f(x)) = (f(i), f(-i))$. This will be a homomorphism. We want to apply the fundamental homomorphism theorem, so we determine ker $\theta$ and prove that $\theta$ is onto.

Note that $\theta(x^2 + 1) = i^2 + 1 = 0$, so $x^2 + 1 \in \ker \theta$ and we deduce that $(x^2 + 1) \subseteq \ker \theta$. Now suppose $f \in \ker \theta$. Then $f(i) = f(-i) = 0$ which shows that $x - i$ and $x + i$ divide $f$. Therefore $x^2 + 1$ divides $f$, hence $f \in (x^2 + 1)$ and it follows that $\ker \theta = (x^2 + 1)$. 
Finally we show that \( \theta \) is onto. Let \( a, b \in \mathbb{C} \). Since \( \theta(x+i) = (2i,0) \) and \( \theta(x-i) = (0,-2i) \), we see that \( \theta(a(x+i)/(2i) + b(x-i)/(-2i)) = (a,b) \), i.e. \( \theta((-ai/2 + bi/2)x + (a/2 + b/2)) = (a,b) \). Thus \( \theta \) is onto and the result now follows from the fundamental homomorphism theorem.

**An alternative proof**  First note that \( \mathbb{C}[X]/(x-i) \cong \mathbb{C} \). This is because we can define a homomorphism \( \theta: \mathbb{C}[X] \to \mathbb{C} \) by \( \theta z = z \) for \( z \in \mathbb{C} \) and \( \theta X = i \). Clearly \( \theta \) is onto and \( (x-i) \subseteq \ker \theta \). If \( f \in \ker \theta \), then \( f(i) = 0 \) and we see that \( (x-i) \) divides \( f \) and so \( f \in (x-i) \). Therefore \( \ker \theta = (x-i) \). It now follows from the fundamental homomorphism theorem that \( \mathbb{C}[X]/(x-i) \cong \mathbb{C} \). Similarly \( \mathbb{C}/(X+i) \cong \mathbb{C} \). Now \( (X-i) \) and \( (X+i) \) are distinct maximal ideals of \( \mathbb{C}[X] \), so by the Chinese remainder theorem \( \mathbb{C}[X]/(X-i)(X+i) \cong \mathbb{C} \times \mathbb{C} \). It is easy to check that \( (X-i)(X+i) = (X^2+1) \) (more generally if \( R \) is a commutative ring with a 1 and \( p, q \in R \), then \( pRqR = pqR \)). We conclude that \( \mathbb{C}[X]/(X^2+1) \cong \mathbb{C} \times \mathbb{C} \).

9. If \( \ker \theta = 0 \), then \( \theta \) is an isomorphism, so we may assume that \( \ker \theta \neq 0 \). By the fundamental homomorphism theorem, \( R/\ker \theta \cong S \), so \( R/\ker \theta \) is an integral domain. Therefore \( \ker \theta \) is a nonzero prime ideal of \( R \), and since \( R \) is a PID, we see that \( \ker \theta \) is a maximal ideal of \( R \). We deduce that \( R/\ker \theta \) is a field and it follows that \( S \) is a field.

10. (a) Since \( x^2 + x + 1 \) has no root in \( k \) (if we plug in 0 or 1 for \( x \), we get 1), this polynomial is certainly irreducible. The other degree 2 polynomials are \( x^2 + 1 \) and \( x^2 + x \), neither of which are irreducible (note that \( x^2 + 1 = (x+1)^2 \)).

(b) We need to prove that \( x^4 + x + 1 \) is irreducible. Since it has no root in \( k \) (if we plug in 0 or 1 for \( x \), we get 1), it has no linear factor. Therefore the only way it is not irreducible is if it is a product of two irreducible degree two factors. By (a), this means that \( x^4 + x + 1 = (x^2 + x + 1)^2 \), which is certainly not the case.

It now follows that \( k[x]/(x^4 + x + 1) \) is a field with \( 2^4 = 16 \) elements.

The exam is on Wednesday May 11, 10:05 a.m. to 12:05 p.m. in Smyth 331. It is comprehensive (includes material from the first two tests). The material since the second test is Sections 5.1,5.2, 7.1–6, and parts of sections 8.2,9.1,9.2. One of the problems will be identical to one of the ungraded homework problems since the second test.