Fifth Homework Assignment

Turn-in problems due 10/6: Chapter 16 18,22,32,38,40,44; Chapter 17 12,16,28,30,32,34,36

18: The evaluation homomorphism from \( \mathbb{Q}[x] \) to \( \mathbb{Q} \) defined by 
\[ \phi_0(f(x)) = f(0) \]
is onto (for any \( r \in \mathbb{Q} \) the polynomial \( x + r \) satisfies \( \phi_0(x+r) = r \)) and the kernel is \( \langle x \rangle \). By the fundamental homomorphism theorem, \( \mathbb{Q}[x]/\langle x \rangle \cong \mathbb{Q} \), and hence the factor ring is a field. By the maximal ideal theorem, any factor ring that is a field must come from an ideal that is maximal and hence \( \langle x \rangle \) is maximal. (You could also prove directly that \( \langle x \rangle \) is maximal)

22: The ideal \( \langle x, 2 \rangle \) is not principal in \( \mathbb{Z}[x] \). To see this, suppose there is an \( f(x) \) so that \( \langle f(x) \rangle = \langle x, 2 \rangle \). This implies that \( x \in \langle f(x) \rangle \), which implies that there is a \( g(x) \) so that \( x = f(x)g(x) \). Similarly, \( 2 \in \langle f(x) \rangle \) implies that there is an \( h(x) \) so that \( 2 = f(x)h(x) \). The latter condition implies that \( f(x) \) must be a constant polynomial (otherwise the degrees wouldn’t match up) and hence \( f(x) \) must be either \( \pm 1 \) or \( \pm 2 \). If \( f(x) = \pm 1 \), then \( \langle f(x) \rangle = \mathbb{Z}[x] \), but \( \langle x, 2 \rangle \neq \mathbb{Z}[x] \), so that doesn’t work. If \( f(x) = \pm 2 \), then every polynomial in \( \langle f(x) \rangle \) would have even coefficients, but \( x \) doesn’t satisfy that property. Thus, the ideal \( \langle x, 2 \rangle \) must not be principal and hence \( \mathbb{Z}[x] \) is not a principal ideal domain.

32: Suppose \( n \) is prime. Problem 31, which we did in class (and was a star problem in Math 306 for those who took me for that!), demonstrates that the constant term is \( -1 = n - 1 \mod n \), and the constant term is \( (n - 1)! \). This proves one direction. For the other direction, suppose that \( n \) is composite, say \( n = mk \) for \( m, k \) not a unit in \( \mathbb{Z} \). Then \( (n - 1)! \) includes the product \( mk = 0 \mod n \) and hence \( (n - 1)! = 0 \mod n \) if \( n \) is composite.

38: Suppose \( I \) is a prime ideal in \( R \). We first need to show that \( I[x] = \{ f(x) = a_n x^n + \cdots + a_1 x + a_0 | a_i \in I \} \) is an ideal. The set \( I[x] \) is closed under subtraction since \( f(x) = a_n x^n + \cdots + a_1 x + a_0, g(x) = b_m x^m + \cdots + b_1 x + b_0 \in I[x] \) implies \( f(x) - g(x) = a_n x^n + \cdots + (a_m - b_m) x^m + \cdots + (a_1 - b_1) x + (a_0 - b_0) \) (I have assumed that \( n > m \), and all other cases are similar). Each of the \( a_i - b_i \in I \), so \( f(x) - g(x) \in I[x] \). If we multiply \( f(x) \) by any polynomial \( h(x) = c_k x^k + \cdots + c_0 \in R[x] \), the formula for
Use the evaluation homomorphism \( \phi \). Then the polynomial is irreducible. If we call the polynomial \( x \), our assumption that the fraction is in reduced form, and hence all of the \( a_i \) are in \( I \) and the sum of terms from \( I \) will still be in \( I \). Hence \( I[x] \) is an ideal in \( R[x] \). To see that \( I[x] \) is a prime ideal, Let \( f(x) \) and \( g(x) \) be arbitrary elements for \( R[x] \) and suppose that \( f(x)g(x) \in I[x] \). We must show that either \( f(x) \in I[x] \) or \( g(x) \in I[x] \). Suppose that \( g(x) \not\in I[x] \), and let \( b_k \) be the least value of \( k \) so that \( b_k \not\in I \). The coefficient of \( x^k \) in \( f(x)g(x) \) is \( b_k a_0 + b_{k-1} a_1 + \cdots + b_0 a_k \). This coefficient must be in \( I \), and all of the \( b_k a_{k-i} \) are in \( I \) except possibly \( b_k a_0 \). Thus, \( b_k a_0 \) must be in \( I \), but I is prime and hence \( a_0 \) must be in \( I \) (since \( b_k \) isn’t). Next do the coefficient of \( x^{k+1} \), which is \( b_{k+1} a_0 + b_{k+1} a_1 + \cdots + b_0 a_{k+1} \), and all of these terms are in \( I \) with the possible exception of \( b_k a_1 \). This forces \( a_1 \) to be in \( I \), and we can continue like this for all of the coefficients of \( f(x) \). Hence, \( f(x) \in I[x] \) and \( I[x] \) is a prime ideal.

**40:** Use the evaluation homomorphism \( \phi_{\sqrt{2}}(f(x)) = f(\sqrt{2}) \). This homomorphism is clearly onto (if \( a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \), then choose \( f(x) = a + bx \in \mathbb{Q}[x] \)). The kernel of the homomorphism is \( \langle x^2 - 2 \rangle \), so by the fundamental homomorphism theorem we get \( \mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}] \).

**44:** This proof is identical to the proof that \( \sqrt{2} \) is irrational. Suppose that \( x \) has a square root in the field of quotients. Then \( x = (\frac{f(x)}{g(x)})^2 \) where we can assume that the greatest common divisor of \( f(x) \) and \( g(x) \) is 1 (otherwise divide by the gcd and get the fraction into “reduced form”). Multiply \( g(x)^2 \) to the other side to get \( f(x)^2 = x g(x)^2 \). This implies that \( f(x)^2 \) has a constant term of 0 (since it is a multiple of \( x \) and hence \( f(x) \) must have a constant term of 0 (if not the constant term of \( f(x)^2 \) would be the square of the constant term of \( f(x) \) which would be nonzero). If \( f(x) \) has a 0 constant term, then \( f(x) = x h(x) \) for some \( h(x) \), and \( f(x)^2 = x^2 h(x)^2 \). Thus, \( f(x)^2 = x^2 h(x)^2 = x g(x)^2 \) which implies that \( g(x)^2 = x h(x)^2 \). The same reasoning implies that \( g(x) \) must have a 0 constant term and hence \( g(x) \) is divisible by \( x \). However, this contradicts our assumption that the fraction is in reduced form, and hence there can’t be a square root of \( x \) in \( F(x) \).

**12:** Simply plug in all possible values: if there are no roots, then the polynomial is irreducible. If we call the polynomial \( f(x) = x^2 + x + 4 \), then \( f(0) = 4, f(1) = 6, f(2) = 10, f(3) = 5, f(4) = 2, f(5) = 1, f(6) = 2, f(7) = 5, f(8) = 10, f(9) = 6, \) and \( f(10) = 4 \) (all being done mod11).
16: Let $p$ be a prime. The easiest way to count this is to use exercise 15, which counts the number of reducible monic quadratics. Every reducible monic quadratic will have the form $(x-i)(x-j)$, where $i$ and $j$ range over the possible elements of $\mathbb{Z}_p$. To count these, if $i = 0$, then there are $p$ choices for $j$; if $i = 1$, then there are $p-1$ choices for $j$ since we don’t want to double count $(0, 1)$. Continuing in this way, if we only count those cases where $j > i$ we get that there are $p + (p-1) + \cdots + 1 = \frac{p(p+1)}{2}$ reducible polynomials. There are $p^2$ polynomials of the form $x^2 + ax + b$, so there are $p^2 - \frac{p(p+1)}{2}$ irreducible polynomials over $\mathbb{Z}_p$. For part b, there are $(p-1)p(p+1)$ reducible quadratic polynomials (not necessarily monic) out of a total of $(p-1)p^2$ quadratic polynomials (we are not allowing the initial coefficient to be 0), so there are $(p-1)(p^2 - \frac{p(p+1)}{2})$ irreducible quadratics over $\mathbb{Z}_p$.

28: If $f(x)$ is a polynomial in $\mathbb{Q}[x]$, then we can clear the denominators and consider the polynomial $cf(x) \in \mathbb{Z}[x]$ for $c$ an integer. We can apply the mod$p$ test to $cf(x)$. If $cf(x)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$ (if not, then $f(x) = g(x)h(x)$ implies that $cf(x) = (cg(x))h(x)$, and hence $cf(x)$ is reducible over $\mathbb{Q}$ and also over $\mathbb{Z}$).

30: This is clearly true if $p = 2$, so let $p$ be an odd prime. First observe that $x^{p-1} - x^{p-2} - \cdots - x + 1 = \frac{x^p+1}{x+1}$. If we substitute $1 - x$ in for $x$ and follow the argument for Corollary after Eisenstein’s criteria, we get that this polynomial is irreducible. (We could also argue that if $f(x)$ is irreducible, then $f(-x)$ is also irreducible and apply this to the corollary).

32: The factor ring is the Gaussian integers. The element 2 does not have a multiplicative inverse in the Gaussian integers, so the ideal can’t be maximal. The Gaussian integers are a domain (no zero divisors) so the ideal must be prime. You could also show directly that the ideal is not maximal (find an ideal between it and that whole ring).

34: The polynomial for the standard tetrahedral dice is $P(x) = x + x^2 + x^3 + x^4 = x(x+1)(x^2+1)$. If a general die has the form $P(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4}$, then $P(x) = x^{q}(x+1)^{r}(x^2+1)^{t}$ for some $q, r, t$. Evaluating $P(1)$ in both ways yields $4 = 2^22^t$, so $r + t = 2$. Similarly, we get that $q$ cannot be 0. The standard dice use $r = t = 1$, and the weird dice have the form $P(x) = x(1+x)^2 = x + 2x^2 + x^3$ and $P(x) = x + 2x^3 + x^5$. It is easy to verify that these dice work!

36: Do the same analysis.
\* problem, 20 pts.: Let \( F[x_1, x_2, \ldots, x_r] \) be the ring of polynomials in \( r \) variables over a field \( F \).

\textbf{a}: If \( F \) is finite and \( r = 1 \), show that there is a nonzero polynomial \( f(x_1) \) so that \( f(a) = 0 \) for every \( a \in F \). Show that if \( r > 1 \) and \( F \) is finite that there is a nonzero polynomial \( f(x_1, x_2, \ldots, x_r) \) so that \( f(a_1, a_2, \ldots, a_r) = 0 \) for every \( (a_1, a_2, \ldots, a_r) \in F^r \).

If \( F \) is finite, then the field is \( F = \{0, 1, a_1, a_2, \ldots, a_k\} \). In the \( r = 1 \) case, the polynomial \( f(x) = x(x - 1)(x - a_1)(x - a_2) \cdots (x - a_k) \) satisfies \( f(a) = 0 \) for every \( a \in F \). In the general case, the polynomial \( f(x_1, x_2, \ldots, x_r) = x_1(x_1 - 1)(x_1 - a_1)(x_1 - a_2) \cdots (x_1 - a_k) \) will satisfy \( f(a_1, a_2, \ldots, a_r) = 0 \) for every \( (a_1, a_2, \ldots, a_r) \in F^r \) (there are many possible answers to both of these questions).

\textbf{b}: If \( F \) is infinite and \( r = 1 \), show that any nonzero polynomial \( f(x_1) \) will have an \( a \in F \) so that \( f(a) \neq 0 \). Use induction on the number of variables to argue that any nonzero polynomial \( f(x_1, x_2, \ldots, x_r) \) must have elements \( a_1, a_2, \ldots, a_r \in F \) satisfying \( f(a_1, a_2, \ldots, a_r) \neq 0 \).

Suppose that \( F \) is infinite, and let \( f(x_1) \) be any nonzero polynomial in \( F[x] \). If the degree of \( f \) is \( n \), then \( f \) can have at most \( n \) roots, but there are an infinite number of elements of \( F \) to plug in to \( f \), so there must be at least one of those elements \( a \) satisfying \( f(a) \neq 0 \). Now suppose this claim is true for any polynomials in \( r - 1 \) variables, and let \( f(x_1, x_2, \ldots, x_r) \) be a polynomial in \( r \) variables. We can write \( f(x_1, x_2, \ldots, x_r) = f_0(x_1, x_2, \ldots, x_{r-1}) + f_1(x_1, x_2, \ldots, x_{r-1})x_r + f_2(x_1, x_2, \ldots, x_{r-1})x_r^2 + \cdots + f_k(x_1, x_2, \ldots, x_{r-1})x_r^k \). By the inductive hypothesis, there will be \( (a_1, a_2, \ldots, a_{r-1}) \in F^{r-1} \) so that \( f_0(a_1, a_2, \ldots, a_{r-1}) \neq 0 \). Thus, the polynomial \( f(a_1, a_2, \ldots, a_{r-1}, x_r) = f_0(a_1, a_2, \ldots, a_{r-1}) + f_1(a_1, a_2, \ldots, a_{r-1})x_r + f_2(a_1, a_2, \ldots, a_{r-1})x_r^2 + \cdots + f_k(a_1, a_2, \ldots, a_{r-1})x_r^k \) is a nonzero polynomial in the variable \( x_r \). By the first part, any nonzero polynomial in one variable must have an \( a_r \) so that \( f(a_1, a_2, \ldots, a_{r-1}, a_r) \neq 0 \), proving the result.