Section 9.4

1. Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles.

   a. $x^2 + x + 1$ in $\mathbb{F}_2[x]$.

   b. $x^3 + x + 1$ in $\mathbb{F}_3[x]$.

   c. $x^4 + 1$ in $\mathbb{F}_5[x]$.

   d. $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

   (Schamel)

   a. Since $x^2 + x + 1$ is degree two, it suffices to show that $x^2 + x + 1$ has no roots in $\mathbb{F}_2$. Since $(1)^2 + 1 + 1 = 1$ in $\mathbb{F}_2$ and $(0)^2 + 0 + 1 = 1$ in $\mathbb{F}_2$, no roots exist and $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

   b. Note that $(1)^3 + 1 + 1 = 0$ in $\mathbb{F}_3$, so $x + 2$ is an irreducible factor of $x^3 + x + 1$ in $\mathbb{F}_3$. But then $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$ in $\mathbb{F}_3$. Note that $1^2 + 1 + 2 = 1$ in $\mathbb{F}_3$ and $2^2 + 2 + 2 = 2$ in $\mathbb{F}_3$, so $x^2 + x + 2$ is irreducible in $\mathbb{F}_3$ and we have found our factorization.

   c. Note that $x^4+1 = (x^2+2)(x^2+3)$ in $\mathbb{F}_5[x]$ and so is reducible in $\mathbb{F}_5[x]$. Since $1^4+1 = 1$,$2^4+1 = 2$, $3^4 + 1 = 3$, and $4^4 + 1 = 2$ in $\mathbb{F}_5$, $x^4 + 1$ has no roots in $\mathbb{F}_5$, and we have completely factored the polynomial.

   d. Note $x^4 + 10x^2 + 1 \geq 1$ for all $x \in \mathbb{Z}$, so has no roots in $\mathbb{Z}$. Thus if $x^4 + 10x^2 + 1$ were reducible, it must reduce into the product of two degree two polynomials:

   $$x^4 + 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.$$

   But then $bd = 1$ so b and d are units in $\mathbb{Z}$. Hence $b = d = \pm 1$. But we also require $a + c = 0$ so $a = -c$. We also need $d + b + ac = 10$ so either $ac = 12$ or $ac = 8$, but since $a = -c$ we have $ac = -a^2 \leq 0$, a contradiction. Hence no such factorization exists and $x^4 + 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$.

2. Prove that the following polynomials are irreducible in $\mathbb{Z}[x]$:

   a. $x^4 - 4x^3 + 6$

   b. $x^6 + 30x^5 - 15x^3 + 6x - 120$

   c. $x^4 + 4x^3 + 6x^2 + 2x + 1$

   d. $\frac{(x+2)^p - 2^p}{x}$, where p is an odd prime.

   (Schamel)

   a. Note that 2 divides all coefficients of $x^4 - 4x^3 + 6$ except the first, but 2^2 does not divide the constant term. Hence $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$ by the Eisenstein Criterion for $\mathbb{Z}[x]$.

   b. We see 3 divides all coefficients of $x^6 + 30x^5 - 15x^3 + 6x - 120$ except for the first, but 3^2 does not divide the constant term. By the Eisenstein Criterion for $\mathbb{Z}[x]$, $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible in $\mathbb{Z}[x]$.

   c. Substituting $x - 1$ for x, we see that $(x - 1)^4 + 4(x - 1)^3 + 6(x - 1)^2 + 2(x - 1) + 1 = x^4 - 2x + 2$. Then 2 divides all terms of $x^4 - 2x + 2$ except the first while 2^2 does not divide the constant term, so $x^4 - 2x + 2$ is irreducible in $\mathbb{Z}[x]$ by the Eisenstein Criterion. Since the map from $\mathbb{Z}[x]$ to $Z[x]$ taking $f(x)$ to $f(x - 1)$ is a ring automorphism, $x^6 + 30x^5 - 15x^3 + 6x - 120$ is also irreducible in $\mathbb{Z}[x]$.

d. By the binomial theorem

$$\frac{(x+2)^p - 2^p}{x} = x^{p-1} + 2px^{p-2} + \cdots + \frac{2^{p-2}p(p-1)}{2}x + 2^{p-1}p.$$

But then p divides every coefficient of the polynomial except the first, and since p is not even, p^2 does not divide the constant term. Hence $\frac{(x+2)^p-2^p}{x}$ is irreducible in $\mathbb{Z}[x]$ by the Eisenstein Criterion for $\mathbb{Z}[x]$.

5. Find all monic irreducible polynomials of degree ≤ 3 in $\mathbb{F}_3[x]$.
(Baggett) We have that the monic polynomial of degree 0 is a unit, and is hence not irreducible. All monic first degree polynomials are irreducible in $\mathbb{F}_3[x]$. For polynomials of degree 2 and 3, we need only check whether or not the polynomial has a root in $\mathbb{F}_3$. Thus, we obtain that the following monic polynomials are irreducible in $\mathbb{F}_3[x]$:
x
$x+1$
$x+2$
x^2+1
x^2+x+2
x^2+2x+2
x^3+2x+1
x^3+2x+2
x^3+x^2+2
x^3+x^2+x+2
x^3+x^2+2x+1
x^3+2x^2+1
x^3+2x^2+x+1
x^3+2x^2+2x+2

6. (Lawless) Construct fields of order 9, 49, 8, and 81.

$$|(\mathbb{Z}/3\mathbb{Z})[x]/(x^2+1)| = 9$$

$$|(\mathbb{Z}/7\mathbb{Z})[x]/(x^2+1)| = 49$$

$$|(\mathbb{Z}/2\mathbb{Z})[x]/(x^3+x+1)| = 8$$

$$|(\mathbb{Z}/3\mathbb{Z})[x]/(x^4+2x+2)| = 81$$

18. (Lawless) Show that $6x^5+14x^3-21x+35$ and $18x^5-30x^2+120x+360$ are irreducible in $\mathbb{Q}[x]$.

Proof. (a) Notice that 7 divides 14, 21, and 35, but that $7^2 = 49$ does not divide 35. Since the content of the polynomial is 1, then by Eisenstein's criterion, $6x^5+14x^3-21x+35$ is irreducible over $\mathbb{Q}[x]$.

(b) $18x^5-30x^2+120x+360$ is irreducible in $\mathbb{Q}[x]$, since the content is 1, and by Eisenstein's criterion ($p=5$.) Thus, the polynomial is irreducible in $\mathbb{Q}[x]$.

□

Section 9.5

1. Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Describe the nilradical of $F[x]/(f(x))$ in terms of the factorization of $f(x)$.

Proof. (Buchholz)

Let $f(x) = a_n f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$ be a nonconstant polynomial in $F[x]$ where each of the $f_i(x)$ are distinct irreducible polynomials. Note that $f(x)$ is either monic or, by multiplying $\frac{1}{a_n}$ then $g(x)$ is associate of $f(x)$ which is monic. Therefore, without loss of generality, we may assume that $f(x)$ is monic. Thus by proposition 16 we have the following isomorphism:

$$F[x]/(f(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

So the nilradical of $F[x]/(f(x))$ is

$$\mathrm{Nil}(F[x]/(f(x))) = \langle f_1(x) f_2(x) \cdots f_k(x) \rangle$$

□

3. Let p be an odd prime in $\mathbb{Z}$ and let n be a positive integer. Prove that $x^n - p$ is irreducible over $\mathbb{Z}[i]$.

   Proof. (Bastille) Recall that $\mathbb{Z}[i]$ is a Euclidean Domain (p. 272) and thus an integral domain and a UFD. By Proposition 18, p is either irreducible (if $p \equiv 3 \bmod 4$) or $p = a^2 + b^2$ (for $p \equiv 1 \bmod 4$) such that $p = (a + bi)(a - bi)$ where $a + bi, a - bi$ are distinct and irreducible in $\mathbb{Z}[i]$. We treat both cases separately but in a similar manner.

   - if $p \equiv 3 \bmod 4$, then p is irreducible and therefore prime (because $\mathbb{Z}[i]$ is a UFD) so (p) is a prime ideal of $\mathbb{Z}[i]$. Furthermore since $-p \in (p)$ but $-p \notin (p^2)$, by Eisenstein's Criterion (Proposition 13), $x^n - p$ is irreducible in $\mathbb{Z}[i]$.
   - if $p \equiv 1 \bmod 4$, then $a + bi$ is irreducible in $\mathbb{Z}[i]$, and therefore prime so $(a + bi)$ is a prime ideal of $\mathbb{Z}[i]$. Furthermore, $-p = -(a - bi)(a + bi) \in (a + bi)$ but $-p \notin ((a + bi)^2)$ since that factorization is unique (up to units) and $a - bi \notin (a + bi)$ (by Proposition 18). So by Eisenstein's Criterion, $x^n - p$ is irreducible in $\mathbb{Z}[i]$.

   □

Section 10.1

8. An element m of the R-module M is called a TORSION ELEMENT if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted:

$$\mathrm{Tor}\,(M) = \{\, m \in M \mid \exists r \in R \backslash \{0\} : rm = 0 \,\}$$

   (a) Prove that if R is an integral domain then $\mathrm{Tor}\,(M)$ is a submodule of M (called the TORSION SUBMODULE of M).

   Proof (Granade). Suppose that R is an integral domain, and that $x, y \in \mathrm{Tor}\,(M)$. Let $r \in R \backslash \{0\}$ be an arbitrary element. Since $0 \in \mathrm{Tor}\,(M)$ trivially, we must show that there exist elements $a, b \in R \backslash \{0\}$ such that $a\,(x + y) \in \mathrm{Tor}\,(M)$ and such that $bry \in \mathrm{Tor}\,(M)$. Note, however, that there exists $s \in R$ such that $sx = 0$, since $x \in \mathrm{Tor}\,(M)$. Similarly, there exists $t \in R$ such that $ty = 0$.

   Thus, $(rt)\,y = r\,(ty) = r0 = 0$. Since R is an integral domain, we have that $rty = try$. Moreover, since $r, t \neq 0$ we have that $rt \neq 0$, and so $ry \in \mathrm{Tor}\,(M)$.

   Next, consider $x + y$. Note that $st\,(x + y) = stx + sty = tsx + sty = t\,(sx) + s\,(ty) = t0 + s0 = 0$. Again, since R is an integral domain, and since $s, t \neq 0$, $st \neq 0$ and so we have that $x+y \in \mathrm{Tor}\,(M)$. We conclude that $\mathrm{Tor}\,(M)$ is a submodule of M. □

(b) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule. [Consider the torsion elements in the R-module R.]

Example: (Granade) Consider $\mathbb{Z}/6\mathbb{Z}$ as a $\mathbb{Z}/6\mathbb{Z}$-module. Since this is not an integral domain, the previous problem does not apply. We have that $\overline{3} \in \mathrm{Tor}(\mathbb{Z}/6\mathbb{Z})$ since $\overline{2} \cdot \overline{3} = \overline{0}$ in this module. By the same reasoning, $\overline{2} \in \mathrm{Tor}(\mathbb{Z}/6\mathbb{Z})$. We can now see that $\mathrm{Tor}(\mathbb{Z}/6\mathbb{Z})$ fails to be a group under addition, since $\overline{2} + \overline{3} = \overline{5} \notin \mathrm{Tor}(\mathbb{Z}/6\mathbb{Z})$.

(c) If R has zero divisors, prove that every nonzero R-module has nonzero torsion elements.

Proof (Granade). Let M be a nonzero R-module and recall that $0_R m = 0_M$ for all $m \in M$. Moreover, suppose that R has zero divisors a, b. Then, choose $m \in M \setminus \{0\}$. If $bm = 0$, then $m \in \mathrm{Tor}(M)$, and so we are done. Hence, suppose that $bm \neq 0$. Then, $a(bm) = (ab)m = 0m = 0$, and so $bm \in \mathrm{Tor}(M)$. In both cases, we have demonstrated a nonzero torsion element, and so we are done. □

10.1.9 If N is a submodule of M, the annihilator of N in R is defined to $A = \{r \in R \mid rn = 0 \text{ for all } n \in N\}$. Prove that the annihilator of N in R is a two-sided ideal of R.

Proof. (Gillispie)

By Problem 10.1.1 we know that $0_R n = 0$ for all $n \in N$, so $0_R \in A$.
Suppose $x, y \in A$ and let $m \in N$. Notice that $(x - y) \cdot m = x \cdot m + (-y) \cdot m = 0_M - (y \cdot m) = 0_M$, therefore by the subgroup test $(A, +)$ is a subgroup of $(R, +)$.
Now see that $(xy) \cdot m = x \cdot (y \cdot m) = x \cdot 0_M = 0_M$ by Problem 10.1.1 and the definition of modules.
We've thus established that A is a sub-ring of R.

Let $r \in R$, $a \in A$, and $n \in N$. We find that $(ra) \cdot n = r \cdot (a \cdot n) = r \cdot 0_M = 0_M$. Since our choice of n was arbitrary this holds for all $n \in N$, similarly $ra \in A$ for all $r \in R$ and $a \in A$. So $rA \subset A$ for all $r \in R$, and A is a left ideal of R.
Because N is an R-module, it's the case that $r \cdot n \in N$, and so $(ar) \cdot n = a \cdot (r \cdot n) = 0_M$ and so $ar \in A$.
Again since our choices were arbitrary, this holds for any $a \in A$, $r \in R$ and $n \in N$, telling us that $Ar \subset A$, and therefore A is a right ideal of R.
This concludes the proof.

□

10. If I is a right ideal of R, the *annihilator of I in M* is defined to be $\{m \in M \mid am = 0 \text{ for all } a \in I\}$. Prove that the annihilator of I in M is a submodule of M.

Proof. (Mobley) We have that $0 \in \mathrm{Ann}(I)$ and therefore $\mathrm{Ann}(I) \neq \varnothing$. Let $x, y \in M$ and so $ax = 0$ and $ay = 0$ for all $a \in I$. Then for $r \in R$ and for all $a \in I$, we have $a(x + ry) = ax + ary = 0 + ary = ary$. Since I is a right ideal $ar \in I$. Then $ary = 0$ and hence $(x + ry) \in \mathrm{Ann}(I)$ and Ann(I) is a submodule of M. □

11. Let M be the abelian group $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.

a. Find the annihilator of M in $\mathbb{Z}$.
The annihilator of M in $\mathbb{Z}$ is $600\mathbb{Z}$. We can see this by noting that the least common multiple of 24, 15, and 50 is 600. So the smallest positive integer that will annihilate (1,1,1) is 600. Anything that annihilates (1,1,1) will annihilate any $x \in \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$. Therefore $600\mathbb{Z}$, the ideal generated by 600, is the annihilator of M in $\mathbb{Z}$.

b. Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.
The annihilator of I in M is $< 12 > \times < 0 > \times < 25 >$. Note, anything that annihilates 2 will also annihilate any multiple of 2. The only things that annihilate 2 are elements of the subgroup $< 12 > \times < 0 > \times < 25 >$. Therefore the annihilator of I in M is $< 12 > \times < 0 > \times < 25 >$.