Problem W6.1. Let $R$ be a commutative ring, let $S \subset R$ be a multiplicatively closed set containing 1, and let $S^{-1}R = R[S^{-1}]$ be the localization at $S$. Let $\phi : R \to S^{-1}R$ be the ring homomorphism $r \mapsto r/1$.

(a) Let $I \subseteq R$ be an ideal. Then $I$ is an $R$-module, so we have defined $S^{-1}I \subseteq S^{-1}R$, and

$$S^{-1}I = \{a/s : a \in I, s \in S\}.$$ 

Show that $S^{-1}I$ is an ideal in $S^{-1}R$. Show that $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.

(b) Show that every ideal $I' \subseteq S^{-1}R$ is of the form $I' = S^{-1}I$ for an ideal $I \subseteq R$.

(c) Show that there is a bijection between the prime ideals of $S^{-1}R$ and the prime ideals of $R$ disjoint from $S$.

Solution. For (a), it is straightforward to show that $S^{-1}I$ is an ideal. For the second statement, to prove $(\Leftarrow)$, if $a \in I \cap S$ then $a/a = 1/1 = 1 \in S^{-1}I$ so $S^{-1}I = S^{-1}R$; to prove $(\Rightarrow)$, if $S^{-1}I = S^{-1}R$ then $1 \in S^{-1}I$ so $1/1 = a/s$ for some $a \in I$ and $s \in S$ so $t(a-s) = 0$ with $t \in S$, and then $at = st \in I \cap S$ (because $I$ is an ideal and $S$ is multiplicatively closed).

For (b), let $I = \{a' \in R : a'/1 \in I'\}$. We claim that $I' = S^{-1}I$. To show $(\subseteq)$, let $a'/s \in I'$, then $s(a'/s) = a'/1 \in I'$, thus $a'/s \in S^{-1}I$ by definition. To show $(\supseteq)$, if $a'/s \in S^{-1}I$ with $a' \in I$ and $s \in S$, then $a'/1 \in I'$ so $a'/s = (a'(1)/1)/s \in I'$ as well.

Finally, part (c). First we write down a map. Let $P'$ be a prime ideal of $S^{-1}R$. Then by (a), $P' = S^{-1}P$ for some ideal $P \subseteq R$. We claim that $P$ is prime: indeed, if $a, b \in R$ have $ab \in P$, then $ab/1 = (a/1)(b/1) \in P'$, so $a/1 \in P'$ or $b/1 \in P'$ and by the construction in (b) we conclude $a \in P$ or $b \in P$. And by (a), since $P' \neq S^{-1}R$, we have $P \cap S = \emptyset$. To show this map is bijective, we write down an inverse. Let $P$ be a prime ideal of $R$ disjoint from $S$. Then $S^{-1}P$ is an ideal of $S^{-1}R$: by (a), we have $S^{-1}P \neq S^{-1}R$. We claim $S^{-1}P$ is prime: if $(a/s)(b/t) = ab/st \in S^{-1}P$ with $a, b \in R$ and $s, t \in S$, then $ab/1 = (ab/st)st \in P$ so since $P$ is prime we have $a \in P$ or $b \in P$ and therefore $a/s \in S^{-1}P$ or $b/t \in S^{-1}P$. The composition of these two maps in either direction is the identity map: if $P' = S^{-1}P$ then we attach $P$ then $S^{-1}P$ again, and starting with $P$ we attach $S^{-1}P$ and recover $P$! So the maps are bijections.

Problem W6.2.

(a) Let $R$ be a Euclidean domain with norm $N$. Let

$$m = \min(\{N(a) : a \in R, a \neq 0\}).$$

Show that every nonzero $a \in R$ with $N(a) = m$ is a unit in $R$. Deduce that a nonzero element of norm zero in $R$ is a unit; show by an example that the converse of this statement is false.

(b) Let $F$ be a field and let $R = F[[x]]$. Show that $R$ is Euclidean. What does part (a) tell you about $R^x$? What are the irreducibles in $R$, up to associates?

Solution. Of (a), let $a$ be a nonzero element of norm $m$. Then we can write $1 = qa + r$ with $r = 0$ or $N(r) < N(a) = m$. We cannot have the latter, since $m$ is the smallest such, hence $r = 0$ so $1 = qa$ and hence $a \in R^x$. For the second statement, if there is an element of norm zero then $m = 0$ so by what we just proved every nonzero element of norm zero is a unit. The converse of this statement is false, namely, that every unit has norm zero: the ring $\mathbb{Z}[i]$ is a Euclidean domain and $a \in \mathbb{Z}[i]$ is a unit with respect to the complex norm if and only it has norm 1.

Finally, part (b). For $\alpha = a_n x^n + \cdots \in F[[x]]$ with $a_n \neq 0$, we define the norm $N(\alpha) = n \geq 0$. Then $R$ is Euclidean under this norm as follows. Let $\alpha, \beta \in R$ with $\beta \neq 0$. If $N(\alpha) < N(\beta)$, then we can write $\alpha = 0\beta + \alpha$. Otherwise $N(\alpha) \geq N(\beta)$, and we claim $\beta | \alpha$, i.e., $\alpha = (\alpha/\beta)\alpha + 0$ with $\alpha/\beta \in F[[x]]$. Indeed,
write \( \alpha = x^{N(a)}a_0(x) \) and \( \beta = x^{N(b)}b_0(x) \) with \( b_0(x) = b_0 + \ldots + b_0 \neq 0 \). We claim that \( b_0(x) \in F[[x]]^\times \), indeed we can formally expand the geometric series

\[
\frac{1}{b_0 + (b_0 x + \cdots)} = b_0^{-1} \sum_{n=0}^{\infty} (-b_0^{-1} b_0 x + \cdots)^n
\]
as there are only finitely many terms in this expansion of any degree. Thus \( \alpha/\beta = x^{n-m}a_0(x)b_0(x)^{-1} \in F[[x]] \). Therefore \( F[[x]] \) is Euclidean under this norm. Then part (a) reminds us of the thing we just saw that \( R^x = F[[x]]^\times \) consists of the elements with nonzero constant term, reading off the definition of the norm. The only irreducible, up to associates, is \( x \). Indeed, we know that \( F[[x]] \) is a UFD so irreducibles are the same as primes, and \( F[[x]]/(x) \simeq F \) so \( x \) is irreducible; and any \( \alpha(x) = x^{N(a)}a_0(x) \neq 0 \) with \( a_0(x) \in F[[x]]^\times \) is then a factorization of \( \alpha(x) \) as a power of the irreducible \( x \) (times a unit).

**Problem W6.3.** Let \( R \) be a domain and let \( M \) be an \( R \)-module. Elements \( x_1, \ldots, x_n \in M \) are \( R \)-linearly independent if whenever \( a_1 x_1 + \cdots + a_n x_n = 0 \) with \( a_i \in R \), then \( a_1 = \cdots = a_n = 0 \).

The rank of \( M \) is the maximal number of \( R \)-linearly independent elements of \( M \).

(a) Suppose that \( M \) has rank \( n \) and that \( x_1, \ldots, x_n \) is any maximal set of \( R \)-linearly independent elements of \( M \). Let \( N = Rx_1 + \cdots + Rx_n \) be the \( R \)-submodule generated by \( x_1, \ldots, x_n \). Prove that \( N \) is isomorphic to \( R^n \) and that the quotient \( M/N \) is a torsion \( R \)-module. [Hint: Show that the map \( R^n \to N \) which sends the \( i \)-th standard basis vector to \( x_i \) is an isomorphism of \( R \)-modules.]

(b) Prove conversely that if \( M \) contains a submodule \( N \) that is free of rank \( n \) (i.e., \( N \cong R^n \)) such that the quotient \( M/N \) is a torsion \( R \)-module then \( M \) has rank \( n \). [Hint: Let \( y_1, \ldots, y_{n+1} \) be any \( n+1 \) elements of \( M \). Use the fact that \( M/N \) is torsion to write \( r_i y_i \) as a linear combination of a basis for \( N \) for some nonzero elements \( r_i \) of \( R \). Use an argument like Proposition 12.1.3 to show that the \( r_i y_i \), and hence also the \( y_i \), are linearly dependent.]

(c) Let \( R = \mathbb{Z}[x] \) and let \( M = (2, x) \) be the ideal generated by \( 2 \) and \( x \), considered as a submodule of \( R \). Show that \( \{2, x\} \) is not a basis of \( M \). Show that the rank of \( M \) is 1 but that \( M \) is not free of rank 1.

**Solution.** For (a), we define a map

\[
\pi : R^n \to N
\]
\[
e_i \mapsto x_i
\]
where \( e_i \) is the \( i \)-th standard basis vector (1 in the \( i \)-th position, 0 elsewhere). By construction this map is an \( R \)-module homomorphism. Moreover, \( \pi \) is surjective since the \( x_i \) generate \( N \). To show the map is injective, suppose that \( x \in \ker \phi \); then we can write \( x = \sum_i c_i e_i \) with \( c_i \in R \) so

\[
\phi(x) = \phi(\sum_i c_i e_i) = \sum_i c_i \phi(e_i) = \sum_i c_i x_i = 0.
\]

But the \( x_i \) are \( R \)-linearly independent, so \( c_i = 0 \) for all \( i \), hence \( x = 0 \).

To show that \( M/N \) is torsion, let \( y + N \in M/N \) by any element with \( y \in M \). Then \( x_1, \ldots, x_n, y \) are \( R \)-linearly dependent, since \( x_i \) are a maximal such set. This implies that there exist \( c_i, c \in R \) such that \( \sum_i c_i x_i + cy = 0 \); but this exactly means that \( c(y + N) = cy + N = N \), i.e., \( y + N \in M/N \) is torsion.

For (b), we follow the hint: suppose that \( N \cong R^n \) and let \( x_1, \ldots, x_n \) be a maximal \( R \)-linearly independent set. Let \( y_1, \ldots, y_{n+1} \) be any \( n+1 \) elements of \( M \). Since \( M/N \) is torsion, for each \( i \) there exists \( r_i \) such that \( r_i(y_i + N) = r_i y_i + N = N \), i.e., \( r_i y_i \in N \), so that \( r_i y_i = \sum_j c_{ij} x_j \). This gives us \( n+1 \) equations with \( n \) variables \( x_j \); by elementary operations which yield an elimination of variables, as in Proposition 12.1.3, we obtain an equation \( \sum_i s_i y_i = 0 \), i.e., the \( y_i \) are \( R \)-linearly dependent.

For (c), we have \( x(2) + (-2)(x) = 0 \), so \( 2, x \) are not \( R = \mathbb{Z}[x] \)-linearly independent. Indeed, \( M \) is of rank 1 since \( x \in M \) is linearly independent, but if one chooses any two elements \( f(x), g(x) \in M \subset R \) then \( q(x)f(x) + (-f(x))q(x) = 0 \) so \( f(x), g(x) \) are \( R \)-linearly dependent. If \( M \) were free of rank 1, then \( M = f(x)R \) for some \( f(x) \in R \), i.e., \( M = (f(x)) \)—but we already noted in class that \( M \) is not a principal ideal, so this is impossible.

**Problem W6.4.**
(a) Let $N \leq \mathbb{Z}^2$ be the submodule generated by $(2, 4)$ and $(8, 10)$. Write $\mathbb{Z}^2/N$ as a product of cyclic groups.

(b) Let $R$ be a PID. Let $M \subseteq R^n$ be an $R$-submodule such that

$$\#(R^n/M) = [R^n : M] = p$$

where $p \in \mathbb{Z}$ is prime and $p$ is a nonzerodivisor in $R$. Show that $M$ is free of rank $n$ and there is a basis $x_1, \ldots, x_n$ of $R^n$ and $q \in R$ such that $M = Rx_1 \oplus \cdots \oplus Rqx_n$ and $[R : (q)] = p$.

Solution. For part (a), the module $\mathbb{Z}^2/N$ is the module generated by $e_1, e_2$ subject to $2e_1 + 4e_2 = 0$ and $8e_1 + 10e_2 = 0$, so we have the relations matrix $A = \begin{pmatrix} 2 & 4 \\ 8 & 10 \end{pmatrix}$; the Smith normal form of this matrix is $\begin{pmatrix} 0 & 0 \\ 2 & 6 \end{pmatrix}$, so $\mathbb{Z}^2/N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

For part (b), we will work explicitly with the exact sequence

$$0 \to M \to R^n \to R^n/M \to 0$$

with generators and bases. First, recall from class that a submodule of $R^n$ is free, (finitely) generated by $n$ elements, say $y_1, \ldots, y_n$. Write these generators in the standard basis for $R^n$ as $y_j = \sum_{i=1}^{n} a_{ij} e_i$. Consider the matrix $A = (a_{ij})_{i,j}$, whose columns are these generators. Then $A$ has a Smith normal form, and we can write $PAQ = D$ where $P, Q \in \text{GL}_n(R)$ are invertible and $D = \text{diag}(d_1, \ldots, d_n)$ is diagonal. The matrix $Q$ acts by column operations corresponding to elementary operations on the generators of $M$, so the columns of $AQ$ are again generators $z_1, \ldots, z_n$ for $M$. The matrix $P$ acts by row operations corresponding to elementary operations on the basis for $R^n$, so by invertibility the matrix $P$ acts by a change of basis with new basis $x_1, \ldots, x_n$. The expression $PAQ = D$ says that if we take the generators $z_1, \ldots, z_n$ are write them in the basis $x_1, \ldots, x_n$, then $z_i = d_i x_i$ for $i = 1, \ldots, n$.

From this, it follows that $R^n/M \cong R/(d_1) \oplus \cdots \oplus R/(d_n)$. We are given that $R^n/M$ is an abelian group with $p$ elements, so it is necessarily cyclic. But by the uniqueness of invariant factors, that means that all but the last factor must be trivial, which is to say (without loss of generality) $d_i = 1$ for $i = 1, \ldots, n - 1$, and $d_n = q$ is such that $R/(q) \cong \mathbb{Z}/p\mathbb{Z}$.

To finish, we need to argue that $x_1, \ldots, x_{n-1}, qx_n$ is a basis for $M$. We know they generate, so we need to show that these elements are $R$-linearly independent. Suppose that $c_1 x_1 + \cdots + c_{n-1} x_{n-1} + c_n qx_n = 0$ with $c_i \in R$. Since the $x_i$ are linearly independent (they are a basis for $R^n$), we immediately conclude that $c_1 = \cdots = c_{n-1} = 0$ and $c_n q = 0$. Assume for purposes of contradiction that $c_n \neq 0$: then since $R$ is a domain, we have $q = 0$, which means that $R/(q) = R \cong \mathbb{Z}/p\mathbb{Z}$. But then $p = 0$ in $R$, contradicting our hypothesis. So $c_n = 0$, and we have a basis.

**Problem W6.5.**

(a) Prove that two $2 \times 2$ matrices over $F$ which are not scalar matrices are similar if and only if they have the same characteristic polynomial.

(b) Prove that two $3 \times 3$ matrices are similar if and only if they have the same characteristic and minimal polynomials. Give an explicit counterexample to this assertion for $4 \times 4$ matrices.

**Solution.** First, we show that if $A, B \in M_n(F)$ are similar then they have the same characteristic and minimal polynomials. One can prove each of these directly. For the characteristic polynomial, if $B = P^{-1}AP$, then

$$\text{det}(B - Ix) = \text{det}(P^{-1}AP - Ix) = \text{det}(P^{-1}(A - Ix)P) = \text{det}(A - Ix).$$

For the minimal polynomial, we note that if $m_A(x)$ is the minimal polynomial that $A$ then $P^{-1}m_A(A)P = m_A(P^{-1}AP) = m_A(B) = 0$, thus $m_B(x) \mid m_A(x)$; reversing the roles of $A$ and $B$ we see that $m_A(x) = m_B(x)$. Here is a second proof for each of these: two matrices are similar if and only if they have the same invariant factors, and the characteristic polynomials is the product of the invariant factors while the minimal polynomial is the invariant factor of largest degree.

Now, for the converse for (a), suppose $A, B \in M_2(F)$ are not scalar matrices and have the same characteristic polynomial $c(x)$ of degree 2. We show they have the same invariant factors. Note that a matrix is a scalar matrix if and only if its minimal polynomial has degree 1. Since $A, B$ are not scalar matrices, each
must have minimal polynomial $m_A(x), m_B(x)$ of degree 2; but then $m_A(x) = c(x) = m_B(x)$. Hence both $A$ and $B$ have the same single invariant factor of degree 2, and hence are similar.

For (b), suppose $A, B$ have the same characteristic and minimal polynomials, denoted $c(x), m(x) \in F[x]$, respectively. If $\deg m(x) = 3$, then $A, B$ have the same rational canonical form given by a single invariant factor $m(x) = c(x)$. If $\deg m(x) = 2$, then since $m(x) \mid c(x)$ we have $c(x) = m(x)g(x)$ for some $g(x) \mid m(x)$ of degree 1; thus both $A$ and $B$ have the invariant factors $g(x), m(x)$. If $\deg m(x) = 1$, then both $A$ and $B$ have the same invariant factors $m(x), m(x), m(x)$.

For the counterexample, we find matrices $A, B$ which have minimal polynomial $m(x) = x^2$ and characteristic polynomial $f(x) = x^4$ but are not similar. We have two possibilities for the invariant factors.

$$x, x, x^2$$

The corresponding matrices, which are therefore not similar, are:

$$\begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

**Problem W6.6.** Find all similarity classes of $6 \times 6$ matrices over $\mathbb{Q}$ with minimal polynomial $(x + 2)^2(x - 1)$. [It suffices to give all lists of invariant factors and write out some of their corresponding matrices.]

**Solution.** We consider the possible invariant factors. We have $a_1(x) \mid \cdots \mid a_m(x) = (x + 2)^2(x - 1)$. This gives the following possibilities:

$$(x + 2)^2(x - 1), (x + 2)^2(x - 1)$$

$$(x + 2), (x + 2)^2, (x + 2)^2(x - 1)$$

$$(x + 2), (x + 2)^2(x - 1), (x + 2)^2(x - 1)$$

$$(x - 1), (x + 2)(x - 1), (x + 2)^2(x - 1)$$

$$(x + 2), (x + 2), (x + 2), (x + 2)^2(x - 1)$$

$$(x - 1), (x - 1), (x - 1), (x + 2)^2(x - 1)$$

The matrix corresponding to the fourth one, for example, is the matrix

$$\begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{pmatrix}$$

since $(x + 2)(x - 1) = x^2 + x - 2$ and $(x + 2)^2(x - 1) = x^3 + 3x^2 - 4$. 
