(worked w/ Joseph Sullivan)

1 Exercise 1.1 Prove that the following conditions of a module M over a commutative ring R are equivalent.

1. M is Noetherian (that is, every submodule of M is finitely generated).
2. Every ascending chain of submodules of M terminates.
3. Every set of submodules of M contains elements maximal under inclusion.
4. Given any sequence of elements $f_1, f_2, \ldots \in M$, there is a number m such that for each $n > m$ there is an expression $f_n = \sum_{i=1}^{m} a_i f_i$ with $a_i \in R$.

Proof. We will prove the following implications between the conditions:

$$1 \implies 2 \implies 3 \implies 4 \implies 1.$$

Assume condition 1 holds and let $N_1 \leq N_2 \leq \cdots \leq M$ be an ascending chain of submodules. We check that $N = \bigcup_{i\in\mathbb{N}} N_i \subseteq M$ is a submodule (i.e., subgroup) of M. If $x, y \in N$, then $x, y \in N_n$ for some $n \in \mathbb{N}$ large enough. Since $N_n \leq M$, then in fact $xy, x^{-1} \in N_n \subseteq N$. Applying condition 1, we have $N = R\{x_1, \ldots, x_m\}$, where each $x_i \in N$, implying $x_i \in N_{n_i}$ for some $n_i \in \mathbb{N}$. Defining $n = \max n_i$, we obtain $x_1, \ldots, x_m \in N_n$. Since $N_n \leq N$ and N is generated by the x_i's, which are contained in N_n, then $N_n = N$. Moreover, for all $k \geq n$, we have $N_n \leq N_k \leq N$, so $N_k = N$. In other words, the chain of submodules terminates (after at most n items), i.e., condition 2 holds.

(Condition 3 is immediately obtained from condition 2 by an application of Zorn's lemma, but can also be shown without the full axiom of choice. In particular, we can assume dependent choice.)

Assume condition 2 holds and let S be a set of submodules of M. Suppose, for contradiction, that S contains no elements maximal under inclusion. Then, by the axiom of dependent choice, there is a strictly increasing chain $N_1 < N_2 < \cdots$ of submodules in S. This contradiction condition 2, so we conclude that S must contain elements maximal under inclusion, i.e., condition 3 holds.

Assume condition 3 holds and let $f_1, f_2, \ldots \in M$ be a sequence of elements. For each $n \in \mathbb{N}$, define the submodule $N_n = R\{f_1, \ldots, f_n\} \leq M$. By condition 3, the set $\{N_n \mid n \in \mathbb{N}\}$ contains some N_m which is maximal under inclusion. Given $n \geq m$, we know $N_m \leq N_n$, but N_m is maximal, so $N_n = N_m$. By construction of the submodules, we now have

$$f_n \in N_n = N_m = R\{f_1, \ldots, f_m\},$$

so there exist $a_1, \ldots, a_m \in R$ such that $f_n = \sum_{i=1}^{m} a_i f_i$, i.e., condition 4 holds.

Assume condition 4 holds and let N be a submodule of M. We construct a sequence of elements of M inductively as follows (implicitly using dependent choice). Take f_1 to be any element of N. For $n \geq 2$, there are two cases: if $N \neq R\{f_1, \ldots, f_{n-1}\}$, choose $f_n \in N \setminus R\{f_1, \ldots, f_{n-1}\}$; otherwise, choose $f_n \in N$ arbitrarily. Applying condition 4, there is some m such that $f_n \in R\{f_1, \ldots, f_m\}$ for all $n \geq m$. In particular, $f_{m+1} \in R\{f_1, \ldots, f_m\}$, which means that we must have $N = R\{f_1, \ldots, f_m\}$. Hence, N is finitely generated, i.e., condition 1 holds.

$\square$

2 Exercise 1.3 Let M' be a submodule of M. Show that M is Noetherian iff both M' and M/M' are Noetherian.

Proof. Suppose M is Noetherian. Any submodule of M' is also a submodule of M and, therefore, finitely generated. For any submodule $N \leq M/M'$, its preimage under the natural projection $\pi : M \to M/M'$ is a submodule of M and, therefore, finitely generated. Supposing $\pi^{-1}(N) = R\{x_1, \dots x_m\}$, we obtain $N = R\{\pi(x_1), \dots, \pi(x_m)\}$. Hence, both M' and M/M' are Noetherian.

Suppose M' and M/M' are Noetherian. Let N be a submodule of M, then we have the submodules $N \cap M' \leq M'$ and $(N + M')/M' \leq M/M'$. Since M' and M/M' are Noetherian, we have $N \cap M' = R\{x_1, \dots, x_n\}$ with $x_i \in N \cap M'$ and $(N + M')/M' = R\{\overline{y_1}, \dots, \overline{y_m}\}$ with $y_j \in N + M'$. Without loss of generality, we may assume all $y_j \in N$, since adding any element of M' does not change the equivalence class modulo M'. We claim that

$$N = R\{x_1, \dots, x_n, y_1, \dots, y_m\}.$$

As $x_i, y_j \in N$, the left inclusion is immediate, so it remains to prove the right inclusion. For any $f \in N$, we have $\overline{f} \in (N + M')/M'$, so $\overline{f} = \sum_{j=1}^m b_j \overline{y_j}$ for some $b_j \in R$. That is, $f = g + \sum_{j=1}^m a_j y_j$, for some $g \in M'$. Since $f, y_j \in N$, then we must also have $g \in N$, implying that $g \in N \cap M'$. So $g = \sum_{i=1}^n a_i x_i$ for some $a_i \in R$, giving us

$$f = \sum_{i=1}^n a_i x_i + \sum_{j=1}^m b_j y_j \in R\{x_1, \dots, x_n, y_1, \dots, y_m\}.$$

$\square$

3 Exercise 1.7

(a) Suppose that k is a field of characteristic $\neq 2$. Let the generator g of the group $G := \mathbb{Z}/2$ act on the polynomial ring $k[x, y]$ in two variables by sending x to $-x$ and y to $-y$. Show that the ring of invariants is $k[x^2, xy, y^2]$.

Proof. Denote $k[x^2, xy, y^2]$. Since G is the identity on k and invariant on the generators x^2, xy, and y^2, we can immediately see that $k[x^2, xy, y^2] \subseteq k[x, y]^G$.

Degrees are preserved under the action of G, so any polynomial in $k[x, y]^G$ must be a k-linear combination of G-invariant monomials. Therefore, to show the opposite inclusion, it suffices to prove that all G-invariant monomials in $k[x, y]$ are contained in $k[x^2, xy, y^2]$.

Suppose $x^a y^b \in k[x, y]^G$, where $a, b \in \mathbb{Z}_{\geq 0}$. Then

$$x^a y^b = g \cdot x^a y^b = (-x)^a (-y)^b = (-1)^{a+b} x^a y^b,$$

which implies $a + b \equiv 0 \pmod 2$. This means that a and b are either both even or both odd. In the first case, write $a = 2n$, $b = 2m$, then

$$x^a y^b = x^{2n} y^{2m} = (x^2)^n (y^2)^m \in k[x^2, xy, y^2].$$

In the second case, write $a = 2n + 1$, $b = 2m + 1$, then

$$x^a y^b = x^{2n+1} y^{2m+1} = (x^2)^n xy (y^2)^m \in k[x^2, xy, y^2].$$

Hence, $x^a y^b \in k[x^2, xy, y^2]$ for all monomials $x^a y^b \in k[x, y]^G$.

$\square$

Prove that $k[x^2, xy, y^2] \cong k[u, v, w]/(uw - v^2)$.

Proof. Consider the map

$$\begin{aligned} \varphi : k[u, v, w] &\to k[x^2, xy, y^2], \\ p(u, v, w) &\mapsto p(x^2, xy, y^2), \end{aligned}$$

on which we will use the first isomorphism theorem to obtain the result.

This map is surjective as u, v, w map to x^2, xy, y^2, respectively. We claim that its kernel is precisely the ideal $(uw - v^2)$. Since $\varphi(uw - v^2) = x^2y^2 - (xy)^2 = 0$, the ideal is contained in the kernel.

Let $p(u, v, w) \in \ker \varphi$, so $p(x^2, xy, y^2) = 0$. We perform polynomial long division on p by $v^2 - uw$ in $(k[u, w])[v]$, giving us

$$p = (v^2 - uw)q + r,$$

for some $q, r \in k[u, v, w]$, where the v-degree of r is at most one. We claim that $r = 0$. We have

$$r(u, v, w) = r_1(u, w) + v r_2(u, w),$$

for some $r_1, r_2 \in k[u,w]$, then

$$0 = p(x^2, xy, y^2) = r(x^2, y^2) = r_1(x^2, y^2) + xyr_2(x^2, y^2).$$

Note that $r_1(x^2, y^2)$ has only even powers of x and y, while $xyr_2(x^2, y^2)$ has only odd powers, i.e., the two share no terms. So

$$0 = r_1(x^2, y^2) \quad \text{and} \quad 0 = xyr_2(x^2, y^2) \implies 0 = r_2(x^2, y^2).$$

Note that $\varphi|_{k[u,w]}$ defines an isomorphism $k[u,w] \cong k[x^2, y^2]$. So in fact $r_1 = r_2 = 0 \in k[u,w]$. Hence, $r = 0$, so $p \in (uw - v^2)$.

□

Show that this is not isomorphic to any polynomial ring over a field.

Proof. A polynomial ring over a field is a UFD, so any ring which is not a UFD cannot be isomorphic to a polynomial ring over a field. We claim that $R = k[x^2, xy, y^2]$ is not a UFD. In particular, the element x^2y^2 has the decompositions

$$(xy)(xy) = x^2y^2 = (x^2)(y^2).$$

It can be seen that x^2, xy, y^2 are irreducible in R, as a decomposition in R would also be a decomposition in $k[x,y]$. The only decompositions in $k[x,y]$ are $x^2 = xx, xy, y^2 = yy$. Since $x, y \notin R$, then these decompositions are not possible in R. Hence the elements in question are irreducible. Thus, we have two distinct irreducible decompositions of x^2y^2 in R, so R is not a UFD. □

(b) More generally, let G be any finite abelian group, acting linearly on the space of linear forms of the ring $S = k[x_1, \ldots, x_r]$. Assume that G acts by characters; that is, assume that there are homomorphisms $\alpha_i : G \to k^\times$, and $g(x_i) = \alpha_i(g)x_i$ for all $g \in G$, where $k^\times$ is the multiplicative group of the field k. Show that the invariants of G are generated by those monomials $\prod x_i^{a_i}$ whose exponent vectors $(a_1, \ldots, a_r)$ are in the kernel of a map from $\mathbb{Z}^r$ to a certain finite abelian group.

Proof. Since $\alpha_i(g) \in k^\times$, the action of G on S preserves degrees, so any polynomial in S^G must be a k-linear combination of G-invariant monomials. For $x = (x_1, \ldots, x_r)$ and $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r_{\geq 0}$, denote by x^a the product $\prod x_i^{a_i}$. Define the map

$$\begin{aligned} \alpha : G &\to (k^\times)^r, \\ g &\mapsto (\alpha_1(g), \ldots, \alpha_r(g)), \end{aligned}$$

which is a group homomorphism since each component α_i is a group homomorphism. Then the action of g on a monomial $x^a \in S$ is given by

$$g \cdot x^a = (\alpha(g)x)^a = \alpha(g)^a x^a.$$

This means that x^a is G-invariant if and only if $\alpha(g)^a = 1$ for all $g \in G$. In other words, x^a is G-invariant if and only if a is in the kernel of the group homomorphism

$$\begin{aligned} \Phi : \mathbb{Z}^r &\to \mathrm{Hom}(G, k^\times), \\ a &\mapsto \alpha(-)^a. \end{aligned}$$

(One can check that the map $g \mapsto \alpha(g)^a = \prod \alpha_i(g)^{a_i}$ is a group homomorphism $G \to k^\times$.) Since $\mathrm{Hom}(G, k^\times)$ is a group under multiplication (i.e., for $\varphi, \psi \in \mathrm{Hom}(G, k^\times)$, $\varphi\psi$ is the homomorphism $g \mapsto \varphi(g)\psi(g)$), then $k^\times$ being abelian implies $\mathrm{Hom}(G, k^\times)$ is abelian.

Lastly, we check that $\mathrm{Hom}(G, k^\times)$ is finite. Since G is finite, then each $g \in G$ has some finite order $n \in \mathbb{Z}$, with $g^n = 1$. Then for any $\varphi \in \mathrm{Hom}(G, k^\times)$, we have $\varphi(g)^n = 1$, which means that $\varphi(g)$ is some nth root of unity in k. Since there are only finitely many nth roots of unity, then each $g \in G$ has only finitely many possible destinations in $k^\times$ under a group homomorphism. And since there are only finitely many elements in G, we have an upper bound $\prod_{g \in G} |g|$ on the order of $\mathrm{Hom}(G, k^\times)$.

□

Conclude that the quotient field of S^G is isomorphic to a field of rational functions in r variables.

Proof. The monomials in S^G are a semigroup under multiplication, and generate a multiplicative group M isomorphic to the additive group $\ker \Phi \leq \mathbb{Z}^r$, under the map $x^a \leftrightarrow a$. This M is precisely the set of monomials in the fraction (quotient) field $\mathrm{Frac}\, S^G$, which means that we have $\mathrm{Frac}\, S^G = \mathrm{Frac}\, k[M]$.

Equivalently, we may consider these as modules over the PID $\mathbb{Z}$. Then $\ker \Phi$ is a free $\mathbb{Z}$-module, and we can choose a basis $x_1, \ldots, x_r$ for $\mathbb{Z}^r$ such that $a_1x_1, \ldots, a_sx_s$ is a basis for $\ker \Phi$, for some $0 \leq s \leq r$ and $a_i \in \mathbb{Z}$.

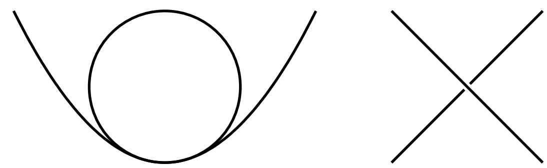
Now, $M \cong \ker \Phi \cong \mathbb{Z}^s$ and we claim that $s = r$. We have

$$\mathbb{Z}^{r-s} \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z} \cong \mathbb{Z}^r / \ker \Phi \cong \mathrm{im}\, \Phi \leq \mathrm{Hom}(G, k^\times).$$

Since $\mathrm{Hom}(G, k^\times)$ is finite, then we must have $r - s = 0$.Then, there is a basis $y_1, \ldots, y_r$ for M as a free $\mathbb{Z}$-module, which gives us $k[M] = k[y_1, \ldots, y_r]$.

□

4 Exercise 1.10 Find rings to represent the following figures.



The first represents the union of a circle and a parabola in the plane, and the second shows the union of two skew lines in 3-space.

The circle is the zero locus of $f = x^2 + y^2 - 1$ and the parabola is the zero locus of $g = x^2 - 2y - 2$. Their union is $Z(fg)$, so the coordinate ring of this affine variety is $k[x, y]/\sqrt{\langle fg \rangle}$.

After an affine transformation of $\mathbb{A}^3$, we can assume one of the skew lines is the z-axis, which is $Z(x, y)$. The other line is a codimension 2 subvariety of $\mathbb{A}^3$, so it is the zero locus of two polynomials $f, g \in k[x, y, z]$. Their union is the zero locus of the ideal $I = \langle x, y \rangle \langle f, g \rangle$, so the coordinate ring is $k[x, y, z]/\sqrt{I}$