Math 361 lecture for Monday, Week 5

Noetherian rings

Definition 1. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Example 2. As a special case, one may consider R itself as an R-module. Its submodules are its ideals. Thus, for example, if R is a PID, it is Noetherian since each of its submodules is generated by a single element. For instance, $\mathbb{Z}$ is Noetherian, and the polynomial ring $K[x]$ is Noetherian for any field K.

Proposition 3. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the *ascending chain condition* on submodules: every ascending chain of submodules of M,
$$N_1 \subseteq N_2 \subseteq \cdots ,$$
eventually *stabilizes*. In other words, there exists k such that $N_k = N_{k+1} = \cdots$.
3. Every nonempty collection of submodules of M has a maximal element under inclusion.

Proof. ($1 \Rightarrow 2$) Suppose M is Noetherian and let $N_1 \subseteq N_2 \subseteq \cdots$ be a chain of submodules. Let $N := \cup_{i\geq 1} N_i$. Then N is a submodule of M (exercise). Hence, by assumption, N is finitely generated by, say $n_1, \dots, n_s \in N$. Since $N = \cup_{i\geq 1} N_i$, for each $i = 1, \dots, s$, we have $n_i \in N_{k_i}$ for some k_i. Let $k = \max\{k_i\}$. Then $n_i \in N_k$ for all i. It follows that
$$N = \mathrm{Span}_R\{n_1, \dots, n_s\} = N_k = N_{k+1} = \cdots .$$

($2 \Rightarrow 3$) Suppose every ascending chain of submodules of M stabilizes. Let $\mathcal{A}$ be a nonempty of submodules of M. Pick $N_1 \in \mathcal{A}$. If N_1 is not a maximal element of $\mathcal{A}$, there exists $N_2 \in \mathcal{A}$ with $N_1 \subsetneq N_2$. If N_2 is not a maximal element of $\mathcal{A}$, then there exists $N_3 \in \mathcal{A}$ such that $N_1 \subsetneq N_2 \subsetneq N_3$. Repeat. Since every ascending chain eventually stabilizes, we must eventually reach a maximal element of $\mathcal{A}$.

($3 \Rightarrow 1$) Suppose that every nonempty collection of submodules of M has a maximal element, and let N be a submodule of M. Let $\mathcal{A}$ be the collection of all finitely generated submodules of N. Then $\mathcal{A}$ is nonempty since it contains the zero module. Take a maximal element $N' \in \mathcal{A}$. So $N' \subseteq N$. For sake of contradiction, suppose that $N' \neq N$, and take $n \in N \setminus N'$. Consider the module $N'' := N' + Rn$, the smallest R-module containing both N' and n. Since $n \notin N'$, we have $N' \subsetneq N''$. However, $N'' \in \mathcal{A}$, too, contradicting the maximality of N'. □

Mappings of modules. A sequence of R-module mappings

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

is *exact at* M if $\operatorname{im}\phi = \ker\psi$.

Example 4. Consider the sequence of R-module mappings

$$0 \to M' \xrightarrow{\phi} M.$$

There is only one choice for the mapping $0 \to M'$. It sends 0 to $0 \in M'$. The sequence of mappings is exact at M' if and only if ϕ is injective. Similarly, a sequence of R-module mappings

$$M \xrightarrow{\psi} M'' \to 0$$

is exact at M'' if and only if ψ is surjective.

Short exact sequences. A *short exact sequence* of R-modules is a sequence of R-module mappings

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

if it is exact at M', M, and M''. In that case, M' is isomorphic to its image in M, so we can identify M' with its image and write $M' \subseteq M$. We then have an isomorphism of R-modules

$$M/M' \xrightarrow{\sim} M''.$$

where $\phi(\overline{m}) := \phi(m)$.

Proposition 5. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Proof. ($\Rightarrow$) Suppose that M is Noetherian. We may assume $M' \subseteq M$. Every submodule of M' is a submodule of M, and hence is finitely generated. Therefore, M' is Noetherian. Next, suppose that N is a submodule of M''. Then $\psi^{-1}(N)$ is a submodule of M (exercise). Since M is Noetherian, $\psi^{-1}(N)$ is finitely generated, say by $n_1, \dots, n_k$. It is straightforward to check that $\psi(n_1), \dots, \psi(n_k)$ generate N. Hence, M'' is Noetherian.

($\Leftarrow$) Suppose that M' and M'' are Noetherian, and let N be a submodule of M. Now $\psi(N)$ is a submodule of M'', hence finitely generated. Let $\overline{n_1}, \dots, \overline{n_k}$ be generators with corresponding $n_1, \dots. n_k \in M$ such that $\psi(n_i) = \overline{n_i}$ for all i. Next, identifying M' with its image $\phi(M')$, we have the submodule $N \cap M'$ of M'. Since M' is Noetherian, $N \cap M'$ is finitely generated by, say, $v_1, \dots, v_\ell$.

We claim that $\{v_1, \ldots, v_\ell, n_1, \ldots, n_k\}$ generate N. To see this, let $n \in N$. We can then write $\psi(n) = \sum_{i=1}^k r_i \overline{n_i}$ for some $r_i \in R$. We have $\psi(n - \sum_{i=1}^k r_i n_i) = 0$. So $n - \sum_{i=1}^k r_i n_i \in \ker \psi = \operatorname{im} \phi$ (and recall that we are identifying $\operatorname{im} \phi$ with M' since ϕ is injective). Thus, $n - \sum_{i=1}^k r_i n_i \in N \cap M'$. So we can write

$$n - \sum_{i=1}^{k} r_i n_i = \sum_{j=1}^{\ell} s_j v_j.$$

So $n \in \operatorname{Span}_R\{v_1, \ldots, v_\ell, n_1, \ldots, n_k\}$, as claimed. □

Corollary 6. If R is Noetherian, so is R^n for each $n \in N$.

Proof. If $n = 0, 1$, the result is trivial. Let $n > 1$, and suppose the statement is true for R^k with $0 \geq k < n$. We have the short exact sequence

$$0 \to R \xrightarrow{\psi} R^n \xrightarrow{\phi} R^{n-1} \to 0.$$

where $\psi(r) = (r, 0, \ldots, 0)$ and $\phi(r_1, \ldots, r_n) = (r_2, \ldots, r_n)$. The result now follows by induction and Proposition 5. □

Corollary 7. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Suppose that M is Noetherian. Then *every* submodule of M is finitely generated, which includes M, itself.

($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \operatorname{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi \colon R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i.$$

Let $M' := \ker \psi$. We have a short exact sequence

$$0 \to M' \to R^n \xrightarrow{\psi} M \to 0$$

where $M' \to M$ is the inclusion mapping. Since R is Noetherian, so is R^n by Corollary 6. Proposition 5 then allows us to conclude that M is Noetherian. □

Corollary 8. Let K be a number field. Then its ring of integer $\mathfrak{O}_K$ is Noetherian.

Proof. This follows since $\mathbb{Z}$ is a PID, hence, Noetherian, and $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module. □

Theorem 9. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. We start by considering a set of principal ideals in R. Let

$$\mathcal{A} = \{(x) : x \in R, x \neq 0,\ x \text{ is a non-unit and cannot be factored into irreducibles}\}.$$

Our goal is to prove that $\mathcal{A} = \emptyset$. For sake of contradiction, suppose that it is not. Since R is Noetherian, $\mathcal{A}$ then has a maximal element (x) with respect to inclusion. By definition of $\mathcal{A}$, the element x is not irreducible. Therefore, there exist non-units $y, z \in R$ such that $x = yz$. It follows that $x \in (y) := \{ry : r \in R\}$, and hence, $(x) \subseteq (y)$. Further, it is not possible for $(x) = (y)$, for otherwise, we would have $y \in (x)$. This would mean there exists $w \in R$ such that $y = xw$. However, then

$$y = xw = yzw \quad \Rightarrow \quad y(1 - zw) = 0.$$

Since $0 \neq x = yz$, and R is a domain, we see $y \neq 0$. Then, since the cancellation law holds for domains, $y(1 - zw) = 0$ implies $1 - zw = 0$, i.e., $zw = 1$. So z is a unit, which is a contradiction.

We have shown that $(x) \subsetneq (y)$. Similarly, $(x) \subsetneq (z)$. My maximality of (x) in $\mathcal{A}$, we know (y) and (z) are not in $\mathcal{A}$. So y and z can be factored into irreducibles, say as $y = \prod_{i=1}^{m} y_i$ and $z = \prod_{i=1}^{n} z_n$. However, it then follows that x factors into irreducibles: $x = yz = \prod_{i=1}^{m} y_i \prod_{i=1}^{n} z_n$. That contradicts the fact that x cannot be factored into irreducibles. $\square$

Corollary 10. Let K be a number field. Then every element of its ring of integers, $\mathfrak{O}_K$, can be factored into irreducibles in $\mathfrak{O}_K$.

Example 11. Note that *Corollary 10 does not say that the ring of integers is a UFD.* In homework, we considered the quadratic field $\mathbb{Q}(\sqrt{-5})$, whose ring of integers is $\mathbb{Z}[\sqrt{-5}]$. In this ring,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and we showed $2, 3, 1 \pm \sqrt{-5}$ are non-units and irreducible. So 6 has at least two factorizations into irreducibles in $\mathbb{Z}[\sqrt{-5}]$. This result is consistent with Corollary 10.