1. Recall: Modules

Let R be a ring, always associative and with 1. Recall that a left R-module M over R is an abelian group M, together with a function,

$$R \times M \to M, \qquad (r, m) \mapsto rm,$$

such that:

(1) $r(m_1 + m_2) = rm_1 + rm_2$.
(2) $(r + s)m = rm + sm$.
(3) $(rs)m = r(sm)$.
(4) $1m = m$.

One defines right R-modules similarly where the action now is $M \times R \to R$. We have the notion of a submodule and quotient module: a submodule is a subgroup which is closed under multiplication by R. If $N < M$ is a submodule then the quotient group M/N is naturally an R-module under $r\overline{m} := \overline{rm}$.

An R-module homomorphism $f\colon M_1 \to M_2$ between R-modules M_1, M_2, is a function,

$$f\colon M_1 \to M_2,$$

which is a group homomorphism and satisfies $f(rm) = rf(m)$. The kernel and image of f are then R-modules. We have the isomorphism theorems for R-modules, the most basic of which is that given $f\colon M_1 \to M_2$ and a submodule $N < \mathrm{Ker}(f)$ there is a canonical R-module homomorphism $F\colon M/N \to M_2$, given by $F(\overline{m}) = f(m)$, such that the following diagram is commutative:

$$\begin{tikzcd}
M_1 \arrow[rr, "f"] \arrow[dr, "\text{can.}"'] & & M_2 \\
& M/N \arrow[ur, "F"'] &
\end{tikzcd}$$

Furthermore, the kernel of F is $\mathrm{Ker}(f)/N$.

A short exact sequence of modules is a diagram of modules and homomorphisms

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

such that the image of every map is the kernel of the following one. Namely, $M_1 \to M_2$ is injective, $M_2 \to M_3$ is surjective and the image of M_1 is the kernel of $M_2 \to M_3$. Thus, $M_3 \cong M_2/\mathrm{Im}(M_1)$.

1.1. Free modules.

Recall that a module M is a called free on a set $X \subset M$, $X = \{x_\alpha : \alpha \in I\}$, if every function $f\colon X \to N$ (of sets), where N is an R-module, extends uniquely to an R-module homomorphism $F\colon M \to N$ such that $F(x) = f(x)$, for $x \in X$. Equivalently, every element of M has a unique expression as $m = \sum_{\alpha \in I} r_\alpha x_\alpha$, with $r_\alpha \in R$ and $r_\alpha = 0$ except for finitely many α's (so there is no issue of convergence). Still equivalently,

$$M \cong \oplus_{\alpha \in I} R = \{(r_\alpha)_{\alpha \in I} : r_\alpha \in R, r_\alpha = 0 \text{ for almost all } \alpha\}.$$

1.2. Modules over a field.

If R is a field, then a module over R is just a vector space. Every module is free.

Exercise 1. *Let R be a division ring. Prove that every module over R is free.* You will need to use Zorn's lemma:

Recall that a partially order set (=poset) S is a set with a relation $x \leq y$ defined between some pairs of elements $x, y \in S$, such that: (i) $x \leq x$; (ii) $x \leq y$ and $y \leq x$ implies $x = y$; (iii)

$x \leq y, y \leq z \Rightarrow x \leq z$. A chain in S is a subset $T \subset S$ such that for all t, t' in T, either $t \leq t'$ or $t' \leq t$. We say that a chain has an upper bound if there's an element $s \in S$ (we don't require $s \in T$) such that $s \geq t$ for all $t \in T$. Zorn's lemma states for a non-empty poset S that if every chain in S has an upper bound than S has a maximal element, namely an element $s_0 \in S$ such that if $s \in S$ and $s \geq s_0$ then $s = s_0$ (note that we do not require that $s_0 \geq s$ for all $s \in S$). If you have never seen Zorn's lemma in action, try to use it to prove that any ring R has a maximal left ideal. Take S to be the set of ideals $I \neq R$ of R with the partial order $I \leq J$ if $I \subseteq J$.

1.3. **Group rings.** Let G be a finite group and k a field. The group ring $k[G]$ has elements $\sum_{g \in G} a_g g$, where $a_g \in k$. The operations are

$$\sum_{g \in G} a_g \cdot g + \sum_{g \in G} b_g \cdot g = \sum_{g \in G} (a_g + b_g) \cdot g,$$

and

$$\left(\sum_{g \in G} a_g \cdot g\right)\left(\sum_{g \in G} b_g \cdot g\right) = \sum_{g \in G}\left(\sum_{h \in G} a_h b_{h^{-1}g}\right) \cdot g.$$

We view k as contained in $k[G]$ via $a \mapsto a \cdot 1_G$.

A k-linear representation of G, or a representation of G over k, is a homomorphism

$$\rho : G \to Aut(V),$$

from G to the automorphism group – invertible k-linear transformations – of a vector space V over k. Every such representation ρ makes V into a $k[G]$-module, where we let

$$\left(\sum_{g \in G} a_g \cdot g\right) \cdot v = \sum_{g \in G} a_g \cdot \rho(g)(v), \qquad v \in V,$$

and, conversely, if V is a $k[G]$-module, then the action of k makes V into a k-vector space, and we get a representation of G by

$$g \mapsto \rho(g), \qquad \rho(g)(v) := gv.$$

Exercise 2. *Analyze the structure of the rings $\mathbb{Q}[G]$, $\mathbb{C}[G]$, where G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$.*

1.4. **Modules over a PID.** Let R be a PID and let M be a finitely generated module over R, which, recall, means that there is a surjective map of R-modules $R^n \to M$, for some positive integer n; equivalently, there are elements $x_1, \dots, x_n$ of M such that every element in M is of the form $r_1 x_1 + \cdots + r_n x_n$ for some $r_i \in R$ (but such an expression is usually not unique). The main theorem is that M is isomorphic to $R^a \oplus \oplus_{i=1}^b R/\mathfrak{a}_i$, where $R \neq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_b \neq \{0\}$ are ideals of R and r is a non-negative integer. Moreover, such an expression is unique.

Important cases are $R = \mathbb{Z}$, the ring of integers, and $R = \mathbb{F}[x]$, the ring of polynomials in the variable x over a field $\mathbb{F}$. Since an abelian group is the same thing as a $\mathbb{Z}$-module, the first case gives the classification of finitely generated abelian groups. The second case gives the theory of Jordan canonical form, when $\mathbb{F} = \mathbb{C}$. This requires some more explanation, but the main point is that given a linear transformation $T : V \to V$, we can make V into a $\mathbb{C}[x]$ module by letting $xv = T(v)$.

1.5. **Localization.** In this section we assume that R is a commutative ring. Let $S \subset R$ be a multiplicative set, i.e., $1 \in S$ and $s, t \in S \Rightarrow st \in S$. For example, R can be the ring of complex analytic functions on $\mathbb{C}$ and S can be the functions that do not vanish at zero. Or R can be the integers $\mathbb{Z}$ and S can be all integers not divisible by p. Both these examples are a special case of the following.

Exercise 3. *Let I be a prime ideal in R and $S = R - I$ then S is a multiplicative set. Find the relevant ideals in the examples just mentioned.*

We now define a ring $R[S^{-1}]$ as follows: consider symbols $\frac{r}{s}$ where $r \in R$ and $s \in S$ and define a relation:

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \iff \exists t \in S \quad t(r_1 s_2 - r_2 s_1) = 0.$$

Exercise 4. *Prove that this is an equivalence relation. Prove that the operations*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2},$$

make $R[S^{-1}]$ into a commutative ring and that the natural map

$$R \to R[S^{-1}], \qquad r \mapsto \frac{r}{1}$$

is a ring homomorphism. Find its kernel. Give examples when the kernel is trivial and when the kernel is not trivial.

Example 1.5.1. Let R be an integral domain and $S = R - \{0\}$. The set S is multiplicative and $R[S^{-1}]$ is actually a field containing R, called its field of fractions. It is the "minimal" field containing R.

Let M be an R-module and S a multiplicative set. We may then define $M[S^{-1}]$ as the equivalence classes of elements $\frac{m}{s}, m \in M, s \in S$ where $\frac{m_1}{s_1} \sim \frac{m_2}{s_2}$ if there exists a $t \in S$ such that $t(s_2 m_1 - s_1 m_2) = 0$. Then $M[S^{-1}]$ is an $R[S^{-1}]$ module, where

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}, \qquad \frac{r}{s} \cdot \frac{m_1}{s_1} = \frac{r m_1}{s s_1}.$$

It is easy to see that if $f \colon M_1 \to M_2$ is a homomorphism then the canonical map $f : M_1[S^{-1}] \to M_2[S^{-1}]$, given by $f(m/s) = f(m)/s$ is well-defined homomorphism.

A particular and important case of localization of modules is the following.

Exercise 5. *Let I be an ideal of R then $I[S^{-1}]$ is an ideal of $R[S^{-1}]$, which is the ideal generated by I in $R[S^{-1}]$. Conversely, if $\varphi : R \to R[S^{-1}]$ is the natural map and J is an ideal of $R[S^{-1}]$ then $\varphi^{-1}(J)$ is an ideal of R. Prove that $(\varphi^{-1}(J))[S^{-1}] = J$ and if $I \cap S = \emptyset$ then $\varphi^{-1}(I[S^{-1}]) = I$ (while if $I \cap S \neq \emptyset$ then $\varphi^{-1}(I[S^{-1}]) = R$).*

Conclude that if I is a prime ideal and $S = R - I$ then there is a bijection between the ideals of R contained in I and the ideals of $R[S^{-1}]$, which takes prime ideals to prime ideals. In particular, $R[S^{-1}]$ is a local ring whose maximal ideal is $I[S^{-1}]$.

Exercise 6. *Let S be a multiplicative set and $0 \to M_1 \to M_2 \to M_3 \to 0$ an exact sequence of R-modules. Prove that the sequence $0 \to M_1[S^{-1}] \to M_2[S^{-1}] \to M_3[S^{-1}] \to 0$ is also exact.*

1.6. **On the notion of rank.** Let R be an integral domain and M a module over R. A set $X = \{x_\alpha : \alpha \in I\} \subset M$ is independent if $\sum_{\alpha \in I} r_a x_\alpha = 0$ (where all $r_\alpha = 0$ except for finitely many) implies $r_\alpha = 0$ for all α. The rank of M is the supremum of the cardinalities of independent sets $X \subset M$.

Still assuming that R is an integral domain, recall that an element $m \in M$ is called a torsion element if $\exists r \in R, r \neq 0$ such that $rm = 0$. For example, if $R = \mathbb{Z}$, all the element of M that are of finite order (in the sense of the underlying abelian group) are torsion. One lets $\mathrm{tor}(M)$ denote the collection of all torsion elements of M. This is a submodule of M. This submodule has rank 0. Indeed, given an element $m \in \mathrm{tor}(M)$ and $r \in R, r \neq 0$, such that $rm = 0$ we find that the element m is linearly dependent: the non-trivial linear combination rm is equal to zero.

Exercise 7. *Let R be an integral domain. Prove that a free R-module M on a set X, has rank $|X|$. You may assume this result for vector spaces and reduce to this case. Prove further that a finitely generated module has finite rank.*

Exercise 8. *Let $R = \mathbb{Z}[\sqrt{-5}]$ and I the ideal $\langle 2, 1 + \sqrt{-5}\rangle$. Prove that I is not a free R-module and that it has rank 1.*

Exercise 9. *Show that* $\mathrm{rk}(M) = \mathrm{rk}(M/\mathrm{tor}(M))$.

Exercise 10. *Let R be an integral domain and M an R-module. (i) Show that the rank of M is equal to the cardinality of a maximal free submodule of M. (ii) Suppose that this rank is n. Prove that every $n+1$ elements of M are dependent. (iii) Let $N \subset M$ be a maximal free submodule. Prove that M/N is torsion.*

Exercise 11. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of finitely generated modules. Prove that* $\mathrm{rk}(M_2) = \mathrm{rk}(M_1) + \mathrm{rk}(M_3)$.