Homework 4

Aleck Zhao

February 25, 2017

1. Let R be a ring, assumed commutative for simplicity, and let $f \in R[x]$ be a polynomial of degree $n \geq 1$ whose leading coefficient is a unit in R. show that $R[x]/\langle f\rangle$, regarded as an R-module via the composite ring homomorphism $R \to R[x] \twoheadrightarrow R[x]/\langle f\rangle$, is a free R-module containing a basis with n elements.

   Proof. The elements in $R[x]/\langle f\rangle$ are the cosets $g + \langle f\rangle$ where $g \in R[x]$. I claim that

$$\left\{1 + \langle f\rangle, x + \langle f\rangle, x^2 + \langle f\rangle, \cdots, x^{n-1} + \langle f\rangle\right\}$$

   is a basis for $R[x]/\langle f\rangle$. Consider any $g \in R[x]$. Since the leading coefficient of f is a unit, we may write $g = qf + r$, where $q, r \in R[x]$ and $\deg r < \deg f = n$. Then in $R[x]/\langle f\rangle$, we have

$$\overline{g} = \overline{qf + r} = \overline{r}$$

   since f gets sent to 0. Since $\deg r < n$, we may write

$$\begin{aligned}\overline{g} &= a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \\ \overline{g} + \langle f\rangle &= (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + \langle f\rangle \\ &= a_0(1 + \langle f\rangle) + a_1(x + \langle f\rangle) + \cdots + a_{n-1}(x^{n-1} + \langle f\rangle)\end{aligned}$$

   so

$$R[x]/\langle f\rangle = R(1 + \langle f\rangle) + R(x + \langle f\rangle) + \cdots + R(x^{n-1} + \langle f\rangle)$$

   Clearly, all of these submodules are disjoint because if $h + \langle f\rangle \in R(x^k + \langle f\rangle)$ then $\deg h = k$, and the degrees of all the x^k are different. Thus,

$$R[x]/\langle f\rangle = R(1 + \langle f\rangle) \oplus R(x + \langle f\rangle) \oplus \cdots \oplus R(x^{n-1} + \langle f\rangle)$$

   so these cosets are a basis with n elements, as desired. □

Section 7.1: Modules

8. Let R be an integral domain. Given ${}_R M$ let $T(M) = \{\, t \in M \mid t \text{ is torsion}\,\}$.

   (a) Show that $T(M)$ is a submodule of M - called the torsion submodule.

   Proof. Clearly, 0 is torsion since it annihilates with every ring element, so $0 \in T(M)$. Now, if $s, t \in T(M)$, then they are both torsion, so suppose $sx = ty = 0$ for $x, y \in R$ nonzero. Now, we have

$$(s + t)(xy) = sxy + txy = (sx)y + (ty)x = 0$$

   and since R is an integral domain, $xy \neq 0$, so $s + t$ is also torsion. Then $-s$ is also torsion because $(-s)x = -(sx) = 0$. Thus, $T(M)$ is a subgroup of M. Now, for any $r \in R$, we have $(rs)x = r(sx) = 0$, so $rs \in T(M)$, and thus $T(M)$ is a submodule of M, as desired. □

(b) Show that $T[M/T(M)] = 0$. We say $M/T(M)$ is torsion-free.

Proof. Consider a coset $m + T(M)$ in $M/T(M)$, where $m \in M$. Suppose $m + T(M)$ is torsion, so that

$$r(m + T(M)) = rm + T(M) = 0 + T(M) \implies rm \in T(M)$$

For some $r \in R$. Then rm is torsion in M, so suppose $p(rm) = 0$ for some $p \in R$ which means $(pr)m = 0$ so m is torsion. Thus, $m \in T(M) \implies m + T(M) = T(M)$, so the only coset that is torsion in $M/T/(M)$ is 0, as desired. □

11. Let $M = \mathbb{Z} \oplus \mathbb{Z}$, and $K = \{ (k, k) \mid k \in \mathbb{Z} \}$. Determine if $M = K \oplus X$ in case:

(a) $X = \{ (k, 0) \mid k \in \mathbb{Z} \}$

Solution. If $y \in K \cap X$, then $y = (k, k) = (i, 0)$ for some k, i so $k = 0 \implies y = (0, 0)$. Now consider $(m, n) \in M$, which has a unique decomposition $(m, n) = (n, n) + (m - n, 0)$, where $(n, n) \in K$ and $(m - n, 0) \in X$. Thus, $M = K \oplus X$. □

(b) $X = \{ (0, k) \mid k \in \mathbb{Z} \}$

Solution. If $y \in K \cap X$, then $y = (k, k) = (0, i)$ for some k, i so $k = 0 \implies y = (0, 0)$. Now consider $(m, n) \in M$, which has a unique decomposition $(m, n) = (m, m) + (0, n - m)$, where $(m, m) \in K$ and $(0, n - m) \in X$. Thus, $M = K \oplus X$. □

(c) $X = \{ (2k, 3k) \mid k \in \mathbb{Z} \}$

Solution. If $y \in K \cap X$, then $y = (k, k) = (2i, 3i)$ for some k, i, so $2i = 3i \implies i = 0 \implies y = (0, 0)$. Now consider $(m, n) \in M$, which has a unique decomposition

$$(m, n) = (3m - 2n, 3m - 2n) + (2(n - m), 3(n - m))$$

where $(3m - 2n, 3m - 2n) \in K$ and $(2(n - m), 3(n - m)) \in X$. Thus, $M = K \oplus X$. □

(d) $X = \{ (k, -k) \mid k \in \mathbb{Z} \}$

Solution. Suppose $(m, n) \in M$ had a decomposition $(m, n) = (k, k) + (i, -i) = (k + i, k - i)$ for some k, i. Now, $m + n = (k + i) + (k - i) = 2k$, so the only elements that have this decomposition are the ones where $m + n$ is even. Thus, $M \neq K \oplus X$. □

16. Given ${}_RM$, an R-linear map $\pi : M \to M$ is called a projection if $\pi^2 = \pi$.

(a) If π is a projection, show that $M = \pi(M) \oplus \ker \pi$.

Proof. Suppose $x \in \pi(M) \cap \ker \pi$. Then $\pi(x) = 0$ and $x = \pi(y)$ for some $y \in M$. Then $\pi^2(y) = 0 = \pi(y)$ since π is a projection, so $x = 0$, and the intersection is trivial. Now, for the term $x - \pi(x)$,

$$\pi(x - \pi(x)) = \pi(x) - \pi^2(x) = 0 \implies (x - \pi(x)) \in \ker \pi$$

Then since $\pi(x) \in \pi(M)$, we have

$$x = (x - \pi(x)) + \pi(x)$$

and thus $M = \pi(M) \oplus \ker \pi$ as desired. □

(b) If $M = N \oplus K$, find a projection π such that $N = \pi(M)$ and $K = \ker \pi$.

Solution. Let $\pi(x) = x$ for all $x \in M$. Then $N = \pi(M) \cong M$ and $K = \ker \pi = \{0\}$, so this is indeed a direct sum. □

23. If ${}_RM$ and ${}_RN$ are simple, prove Schur's Lemma: If $\alpha : M \to N$ is R-linear, then either $\alpha \equiv 0$ or α is an isomorphism.

Proof. Since $\ker\alpha$ is a submodule of M, it is either 0 or M since M is simple. By the Module Isomorphism Theorem, we have $M/\ker\alpha \cong \alpha(M)$. If $\ker\alpha = 0$, then $M/0 \cong M \cong \alpha(M)$, which means α is an isomorphism. If $\ker\alpha = M$, then $M/M \cong 0 \cong \alpha(M)$, so $\alpha \equiv 0$, as desired. □

24. Show that the following conditions on a finitely generated module P are equivalent:

(1) P is projective

(2) P is isomorphic to a direct summand of a free module.

(3) If α, β are R-linear and α is onto in the diagram, then γ exists such that $\alpha\gamma = \beta$.

(4) If $\alpha : M \to P$ is onto and R-linear, there exists $\gamma : P \to M$ such that $\alpha\gamma = 1_P$.

Proof. (1) $\implies$ (2) Since P is finitely generated, suppose by $p_1, \cdots, p_n$, then there exists a surjective, R-linear map $\varphi : R^n \twoheadrightarrow P$ where $\varphi(e_i) = p_i, \forall i$. Then since P is projective, we have $R^n = \ker\varphi \oplus P_1$. Since R^n is a free module, and $P_1 \cong P$, it follows that P is isomorphic to a direct summand of a free module.

(2) $\implies$ (3) Suppose $F = P \oplus Q$ is free for some module Q. Then define $\pi : F \to P$ by $\pi(p + q) = p$ for all $p \in P$ and $q \in Q$. If $\{x_1, \cdots, x_n\}$ is a basis of F choose $m_i \in M$ such that $\alpha(m_i) = \beta\pi(x_i)$ for each i, and the m_i exists because α is surjective. Since x_i are a basis for F, there exists a map $\theta : F \to M$ such that $\theta(x_i) = m_i$ for each i. Thus,

$$\beta\pi(x_i) = \alpha(m_i) = \alpha\theta(x_i)$$

and since x_i form a basis for F, we must have $\beta\pi = \alpha\theta$. Now, let $\gamma : P \to M$ be the restriction of θ to P, so that $\gamma(p) = \theta(p)$ for $p \in P$. This is the existence we require, since

$$\beta\pi(p) = \beta(p) = \alpha\gamma(p)$$

for all $p \in P$, and the statement is proven.

(3) $\implies$ (4) Let $N = P$ and $\beta = 1_P$, which trivially proves the statement.

(4) $\implies$ (1) It suffices to show that $M = \ker\alpha \oplus P_1$ where $P_1 \cong P$. Let $x \in \ker\alpha \cap \gamma(P)$, so $\alpha(x) = 0$ and $x = \gamma(y)$ for some $y \in P$. Then $\alpha(\gamma(y)) = y = 0$, so $x = \gamma(y) = \gamma(0) = 0$, and the intersection is trivial. Now, for the term $x - \gamma\alpha(x)$, we have

$$\alpha(x - \gamma\alpha(x)) = \alpha(x) - \alpha\gamma\alpha(x) = \alpha(x) - \alpha(x) = 0 \implies (x - \gamma\alpha(x)) \in \ker\alpha$$

Then since $\gamma\alpha(x) \in \gamma(P)$, we have

$$x = (x - \gamma\alpha(x)) + \gamma\alpha(x)$$

and thus $M = \ker\alpha \oplus \gamma(P)$, so P is projective, as desired. □

25. Show that $\mathbb{Q}$ is a torsion-free $\mathbb{Z}$-module that is not free.

Proof. Call an additive group Q divisible if for all $0 < n \in \mathbb{Z}$ and all $q \in Q$, the equation $nx = q$ has a solution $x \in Q$.

Clearly $\mathbb{Q}$ is divisible because for any $n \in \mathbb{Z}$ and $q = a/b \in \mathbb{Q}$, we have

$$nx = q \implies x = q\frac{a}{bn} \in \mathbb{Q}$$

Now, suppose $Q = P \oplus R$ where Q is divisible. Let $nx = p$ where $p \in P \subset Q$ and since Q is divisible, $x \in Q$. Then write $x = y + z$ where $y \in P$ and $z \in R$, so $nx = ny + nz = p$. Since $ny \in P$ and $nz \in Q$, we must have $nz = 0 \implies nx = ny$. Thus, this $y \in P$ exists such that $ny = p$ so P is divisible.

$\mathbb{Z}$ is not divisible. Consider $2x = 3$, then there is no solution $x \in \mathbb{Z}$.

To show that $\mathbb{Q}$ is torsion free, let $q \in \mathbb{Q}$ and $n \in \mathbb{Z}$ such that $nq = 0$ where $n \neq 0$. Then we have $q = \frac{1}{n}(nq) = 0$, so the only torsion element in $\mathbb{Q}$ is 0. Now, suppose $\mathbb{Q}$ has a finite basis $\{x_1, \cdots, x_n\}$. Then $\mathbb{Q}$ decomposes as

$$\mathbb{Q} = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$$

We know $\mathbb{Q}$ is divisible, so each of the $\mathbb{Z}x_i$ is divisible, but this is a contradiction since $\mathbb{Z}$ is not divisible, and $\mathbb{Z} \cong \mathbb{Z}x_i$, so such a basis cannot exist, and $\mathbb{Q}$ is not free, as desired. $\square$