Homework 3 Key

14.1.1) Let R be a ring and let V be the R-module R. Assume $\varphi : V \to V$ is a homomorphism. Let $\alpha = \varphi(1)$. Then for any $v \in V$, we must have $\varphi(v) = \varphi(v \cdot 1) = v\varphi(1) = v\alpha$, so any homomorphism must be of the form $\varphi(v) = v\alpha$ for some $\alpha \in R$. It is straightforward to verify that for any $\alpha \in R$, this map is a valid homomorphism, so we conclude that these are all the homomorphisms $\varphi : V \to V$.

14.1.2) Let V be an abelian group. Assume V has the structure of a $\mathbb{Q}$-module with its given law of composition as addition. By definition $0v = 0$ must hold. Then if $v = \frac{1}{n}x$, for $n \geq 1$, we must have $nv = x$, and if there were two such elements v, v', we would have $n(v' - v) = nv - nv' = x - x = 0$. Multiplying by $\frac{1}{n}$, since $1y = y$ for all $y \in V$, we get $v' - v = 0$, so $v' = v$.

Now we show that $\frac{m}{n}x$ is uniquely defined for $m, n \geq 1$ and any $x \in V$. For any $m \geq 1$ and any $y \in V$, we must have $my = \sum_{i=1}^{m} y$ by distributivity. Then $\frac{m}{n}x = m(\frac{1}{n}x) = \sum_{i=1}^{m} \frac{1}{n}x$. Since addition is uniquely defined and we have shown that $\frac{1}{n}x$ is uniquely defined, we get that $\frac{m}{n}x$ is uniquely defined.

Finally, we show that $\frac{m}{n}x$ is uniquely defined for $m < 0, n \geq 1$. We must have $\frac{m}{n}x = -(\frac{-m}{n}x)$, where $-m, n \geq 0$, so $\frac{-m}{n}x$ is uniquely defined, so $-(\frac{-m}{n}x)$ is uniquely defined since the additive inverse is uniquely defined by the group structure.

We conclude that the structure is uniquely determined.

14.1.4) (a) Let S be a simple R-module and let $s \in S$ be nonzero. The map $\varphi : R \to S$ given by $\varphi(r) = rs$ is surjective because the image is a nonempty submodule of S (it contains $s = \varphi(1)$) and by simplicity, $\operatorname{Im} \varphi = S$. By the first isomorphism theorem, $R/\ker\varphi \cong S$, so $R/\ker\varphi$ is simple as well. Let $r + \ker\varphi \in R/\ker\varphi$ be nonzero. Then $0 \neq (r + \ker\varphi) \subseteq R/\ker\varphi$, so $(r + \ker\varphi) = R/\ker\varphi$ by simplicity, so $1 + \ker\varphi \in (r + \ker\varphi)$, so $r + \ker\varphi$ is invertible as an element of the ring $R/\ker\varphi$. Thus $R/\ker\varphi$ is a field, which is true if and only if $\ker\varphi$ is a maximal ideal.

(b) Notice that $\operatorname{Im}\varphi$ is a submodule of S', so by simplicity we must have either $\operatorname{Im}\varphi = 0$ or $\operatorname{Im}\varphi = S'$. In the former case, φ is the zero map, so in that case we are done.

Assume $\operatorname{Im}\varphi = S'$, i.e. φ is surjective. Since $\ker\varphi$ is a submodule of S', by simplicity we must have $\ker\varphi = 0$ or $\ker\varphi = S$. The latter cannot happen since that would force $\operatorname{Im}\varphi = 0$, which we have assumed is not the case. Thus $\ker\varphi = 0$, so φ is injective, and we conclude that φ is an isomorphism.

14.2.1) First notice that M cannot be principle, because if we had $M = (f)$ for some $f \in$, then since $x \in M$, we must have $fg = x$ for some $g \in \mathbb{C}[x, y]$. Then we must have $\deg f = 1$ and $\deg g = 0$ or $\deg f = 0$ and $\deg g = 1$. In the latter case, we have f constant, but M does not contain any nonzero constants. In the latter case, we have $f(x, y) = ax + by + c$ for some $a, b, c \in \mathbb{C}$. If $a \neq 0$. then any nonzero element in M must have x-degree at least 1, but $y \in M$ has x-degree 0, and likewise if $b \neq 0$. But then f is constant, and we arrive at the same problem as above.

Thus if M is free, then it must have at least two basis elements $\alpha, \beta \in R$. But then since we are working in an R module, we may use elements of R as scalars. Then since R is commutative, $\beta\alpha + (-\alpha)\beta = 0$, contradicting linear independence. Thus M is not free.

14.2.4) Let I be an ideal of a ring R.

(a) I is a free module if and only if I is 0 or I is a principal ideal generated by some $r \in R$ that is not a zero-divisor:

$\Longrightarrow$ Assume I is free. If $I = 0$, we are done, so assume $I \neq 0$. Assume for a contradiction that I is not principal, and let $\mathcal{B} \subseteq R$ be a minimal generating set with at least two distinct elements x, y. Then since $x, y \in R$, we have $yx + (-xy) = 0$, contradicting linear independence, so I is principal.

Now assume for a contradiction that $I = (r)$ for a zero-divisor, so $mr = 0$ for some nonzero m. Then for a basis $\{x\}$ of I, since $x \in I$, we must have $x = ra$ for some $a \in R$. Then $mx = m(ra) = (mr)a = 0$, contradicting linear independence of $\{x\}$, so I must be generated by an element that is not a zero divisor.

$\Longleftarrow$ If $I = 0$, then I is a zero-dimensional free module with basis $\emptyset$. If $I = (r)$ where r is not a zero divisor, then $\{r\}$ is linearly independent and spanning, and thus I is free.

(b) If $I = 0$, then $R/I \cong R$ is free generated by $1 \in R$. If $I = R$, then $R/I \cong 0$ is free with basis $\emptyset$. Now assume I is a nonzero proper ideal of R. Let $\mathcal{B}$ be a generating set for R/I. Let $x + I \in \mathcal{B}$ and let $r \in I$ be nonzero. Then $rx \in I$ since I is an ideal, so $r(x+I) = rx + I = I$, where I is the zero element of R/I, so $\mathcal{B}$ is not linearly independent. Thus R/I is not free.

3) Let R be a ring and let $f : M \to N$ be a homomorphism of R-modules with $\ker f, \operatorname{Im} f$ finitely generated R-modules. We will show that M is a finitely generated R-module. Let $\mathcal{K} = \{k_1, \ldots, k_n\}$ be a generating set for $\ker \varphi$. By the first isomorphism theorem, $M/\ker f \cong \operatorname{Im} f$, so $M/\ker f$ is finitely generated. Let $\mathcal{I} = \{i_1 + \ker f, \ldots, i_m + \ker f\}$ be a generating set for $M/\ker f$ for representatives $i_1, \ldots, i_m \in M$. Let $\mathcal{I}' = \{i_1, \ldots, i_m\}$.

I claim that $\mathcal{B} := \mathcal{K} \cup \mathcal{I}'$ is a generating set for M: Let $x \in M$. Then since $\mathcal{I}$ is a generating set for $M/\ker f$, there are $c_1, \ldots, c_m \in R$ such that

$x + \ker f = c_1(i_1 + \ker f) + \cdots + c_m(i_m + \ker f) = (c_1 i_i + \ldots + c_m i_m) + \ker f.$

This implies that

$$x - (c_1 i_i + \ldots + c_m i_m) \in \ker f,$$

and since $\ker f$ is generated by $\mathcal{K}$, there are $d_1, \ldots, d_n \in R$ such that

$$x - (c_1 i_i + \ldots + c_m i_m) = d_1 k_1 + \cdots + d_n k_n,$$

or equivalently,

$$x = c_1 i_i + \ldots + c_m i_m + d_1 k_1 + \cdots + d_n k_n.$$

This proves that $\mathcal{B}$ is a finite generating set for M.

4) (a) It suffices to show that for any $m, n \in \operatorname{Tor}(M)$ and any $r, s \in R$, we have $rm + sn \in \operatorname{Tor}(M)$: since $m, n \in \operatorname{Tor}(M)$, there are nonzero $r', s' \in R$ such that $r'm = s'n = 0$. Since R is an integral domain, we have $r's' \neq 0$, and moreover it is a commutative ring, so we have

$$r's'(rm + sn) = rs'(r'm) + r's(s'n) = rs'(0) + r's(0) = 0,$$

so $rm + sn \in \operatorname{Tor}(M)$,so $\operatorname{Tor}(M)$ is an R-submodule of M.

(b) Let $m + \operatorname{Tor}(M) \in \operatorname{Tor}(M/\operatorname{Tor}(M))$. Then there is some nonzero $r \in R$ such that $rm + \operatorname{Tor}(M) = r(m + \operatorname{Tor}(M)) = \operatorname{Tor}(M)$. This implies that $rm \in \operatorname{Tor}(M)$, so there is some nonzero $r' \in R$ with $(r'r)m = r'(rm) = 0$. Since R is an integral domain, $r'r \neq 0$, so $m \in \operatorname{Tor}(M)$, so $m + \operatorname{Tor}(M) = \operatorname{Tor}(M)$, the zero element of $M/\operatorname{Tor}(M)$. We conclude that $\operatorname{Tor}(M/\operatorname{Tor}(M)) = 0$.

(c) I claim that $\operatorname{Tor}(M) = \mathbb{Q}[i]/\mathbb{Z}[i]$. First, we see that any element $(p + qi) + \mathbb{Z}[i] \in \mathbb{Q}[i]/\mathbb{Z}[i]$ is a torsion element. Since $p, q \in \mathbb{Q}$, we have $p = \frac{m}{n}, q = \frac{r}{s}$ for integers m, n, r, s with $n, s \neq 0$. Notice that $n, s \in \mathbb{Z}[i]$ with $ns \neq 0$, and $ns((p + qi) + \mathbb{Z}[i]) = (sm + nri) + \mathbb{Z}[i] = \mathbb{Z}[i]$, the zero element of M, so any element in $\mathbb{Q}[i]/\mathbb{Z}[i]$ is indeed a torsion element.

Now, assume $(x + yi) + \mathbb{Z}[i] \in M$ is any torsion element, with $x, y \in \mathbb{R}$ Then there is some nonzero $a + bi \in \mathbb{Z}[i]$ with

$$(a + bi)\Big((x + yi) + \mathbb{Z}[i]\Big) = \mathbb{Z}[i],$$

so $(a + bi)(x + yi) = (ax - by) + (ay + bx)i \in \mathbb{Z}[i]$. Thus $M := ax - by$ and $N := ay + bx$ are both integers. By assumption at least one of a, b is nonzero. If either is zero, say $b = 0$ without loss of generality, then we get $M = ax, N = ay$ are both integers, so $x = \frac{M}{a}$ and $y = \frac{N}{a}$ are both rational, so assume a, b are both nonzero. Solving the above system of equations for x and y, we get

$$x = \frac{aM + bN}{a^2 + b^2},$$
$$y = \frac{aN - bM}{a^2 + b^2}.$$

Since a, b, M, N are all integers, we get that x, y are rational. We conclude that $\operatorname{Tor}(M) = \mathbb{Q}[i]/\mathbb{Z}[i]$.