Hints to solutions- Exercise sheet 8

1. (a) A direct calculation shows that the module $Hom(R,\mathbb{Q}/\mathbb{Z})$ is isomorphic with R itself. This implies that R is injective as an R-module. But then every finitely generated free R-module is also injective, and every projective module is also injective. In the other direction , every finitely generated injective R-module is a direct summand of R^m for some m (because R is now also co-free), and therefore every finitely generated injective module is also projective (we use here the fact that finite direct sums and finite direct products are isomorphic).

   (b) The module M is finitely generated. So we already know that it will be injective if and only if it will be projective. Consider now the short exact sequence

   $$0 \to \mathbb{Z}/n/m \xrightarrow{i} R \xrightarrow{p} \mathbb{Z}/m \to 0$$

   where $i(x) = xm$ and $p(x) = x$ (all formulas are modulo the relevant numbers). Then M is projective if and only if this sequence split. Assume that this sequence splits. Let $s : \mathbb{Z}/m \to R$ be a splitting, and write $s(1) = x$. Then $mx = 0 \bmod n$ and $x = 1 \bmod m$. From the second equation we get that $x = am+1$ for some $a \in \mathbb{Z}$, and from the second equation we get that $n|mx$ so that $n/m|x$. We write $x = cn/m$ and get that $cn/m - am = 1$. This implies that $gcd(m,n/m) = 1$. On the other hand, if $gcd(m,n/m) = 1$ we get a similar equation which enables us to construct a splitting of the above sequence.

2. For modules which are not finitely generated the statement is not true. Take for example $Z = \oplus_n R$, an infinite direct sum of copies of R, take $X = R$ and $Y = 0$. Then both $X \oplus Z$ and $Y \oplus Z$ are isomorphic to $\oplus_n R$, but X and Y are not isomorphic. For finitely generated modules the statement is true. Indeed, we can write $X = R^{n_X} \oplus_i R/p_i^{a_i}$, $Y = R^{n_Y} \oplus_j R/q_j^{b_j}$ and $Z = R^{n_Z} \oplus_k R/r_k^{c_k}$ for primes p_i, q_j, r_k. We then write $X \oplus Z = R^{n_X+n_Z} \oplus_i R/p_i^{a_i} \oplus_k R/r_k^{c_k} \cong Y \oplus Z = R^{n_Y+n_Z} \oplus_j R/q_j^{b_j} \oplus_k R/r_k^{c_k}$ Then since the decomposition into direct sum of a free module and cyclic modules of the form R/p^n is unique, we get that $n_X = n_Y$ and that $\{p_i^{a_i}\} = \{q_j^{b_j}\}$, which means that X and Y are also isomorphic.

3. (a) The module $\mathbb{Z}/60$ is already of the form $\mathbb{Z}/n$. On the other hand, the chinese remainder theorem enables us to write $\mathbb{Z}/60 \cong \mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5$.

(b) The group $\mathbb{Z}^2$ is a free abelian group of rank 2. Let us write $v = (2,3)$. Then $A = \mathbb{Z}^2/3v$. Consider the vector $w = (1,1)$. Then $\{v,w\}$ is a basis for $\mathbb{Z}^2$. By using this basis, it is clear that $A = \mathbb{Z} \oplus \mathbb{Z}/3$. The free module in A has rank 1 and we have an isomorphism $A/Tor(A) \cong \mathbb{Z}$. To find all possible free direct summands, we just need to find a lifting for $A \to A/Tor(A)$. Such a lifting will send $1 \in \mathbb{Z}$ to $(1,a)$ for some $a \in \mathbb{Z}/3$. It is easy to see that all $a \in \mathbb{Z}/3$ will give us valid liftings, and so we have exactly 3 options for the free direct summand.

4. (a) A finitely generated R-module will be a finitely generated $\mathbb{Z}$-module upon which p^r acts trivially. Let M be such a module. Since M is a finitely generated $\mathbb{Z}$-module we know that we can write M as the direct sum $M \cong \mathbb{Z}^n \oplus_i \mathbb{Z}/p_i^{a_i}$ for some natural n and some prime powers $p_i^{a_i}$. Since p^r acts trivially on this module, it follows that n must be zero, that all the p_i must be equal to p, and that all a_i must be less than or equal to r. Thus, every finitely generated R-module is of the form $\oplus_i \mathbb{Z}/p^{a_i}$ with all $a_i \leq r$. From the structure theorem of modules over a PID it follows that the numbers a_i are uniquely defined.

(b) The cardinality of the module $\oplus_i \mathbb{Z}/p_i^a$ is $\prod_i p^{a_i} = p^{\sum_i a_i}$. Thus, the number of modules of cardinality p^n will be exactly the number of elements in the set $X_{n,r} := \{(a_i) | \sum_i a_i = n, a_i \leq r\}$. We can view the elements of $X_{n,r}$ as the number of *partitions* of n (a_i) in which all the elements are less than or equal to r. If we simply consider the number of p-groups, then the restriction $a_i \leq r$ disappears, and we are left with the number of partitions of n, which is also the number of conjugacy classes in S_n.