Exersise 8.1

Notice that the set of left proper ideals of R form a partialy ordered set P with inclusion as the ordering relation ($K \leq J \Leftrightarrow K \subseteq J$). We know that P is not empty since $I \in P$.
If we show that every chain in P has an upper bound in P then by Zorn's Lemma P has a maximal element (which is a maximal ideal). Considering any chain of proper ideals.

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

we have

$$U = \bigcup_{i=1}^{\infty} I_i \in P$$

U is an ideal since for any $x, y \in U, r \in R$, there exists I_n such that $x, y \in I_n$ then $x + y \in I_n \subseteq U, rx \in I_n \subseteq U$. U is proper since $1 \notin I_i \forall i$ so $1 \notin U$. We have that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq U$$

So every chain is bounded. Thus we are done.

Exersise 8.2

(a) For any $a \in D$, if we consider the set $1, a, a^2, a^3, \dots a^n$ where n is the dimension of D over k. We have $n + 1$ elements and thus they are linearly dependent. So there exists a nonzero polinomial

$$f(a) = k_n a^n + k_{n-1}a^{n-1} + \dots k_1 a + k_0 = 0$$

(b) $D = k$ since for any $a \in D$ and $f \in k[x]$, $f(a) = 0$ we can factor f completely since k is completely

$$f(a) = (a - a_n)(a - a_{n-1}) \dots (a - a_0)$$

Where $a_n, a_{n-1}, \dots a_0 \in k$. Since D is a domain we know $a = a_i$ for one of the a_i and thus $a \in k$. Thus $D \subseteq k$. We already know $k \subseteq D$ since there is an embedding from k to D.

Exersise 8.3

If M is some $k[G]$ module with submodule $N \subset M$, we have the surjective homomorphism $\pi : M \to M/N$. Since k is a subring of $k[G]$ M and M/N are k vectorspaces. We have a k linear section $s : M/N \to M$ such that $\pi \circ s = \text{id}$. The reason for this is because M/N has a basis B as a vectorspace so for each $b \in B$ there is some $m \in M$ with $\pi(m) = b$ then we define $s(b) = m$. s is a fully defined k linear map from where it sends its basis. We have that

$$s'(x) = \frac{1}{|G|} \sum_{g \in G} e_g s(e_{g^{-1}} x)$$

is a $k[G]$ module homomorphism. Checking the properties:
$s'(0) = \frac{1}{|G|}\sum_{g\in G} e_g s(0) = 0$
$s'(x+y) = s'(x) + s'(y)$, we can use the fact that $s(x+y) = s(x) + s(y)$

$$s'(x+y) = \frac{1}{|G|}\sum_{g\in G} e_g s(e_{g^{-1}}(x+y)) = \frac{1}{|G|}\sum_{g\in G} e_g s(e_{g^{-1}}x) + e_g s(e_{g^{-1}}y)) = s'(x) + s'(y)$$

For $s'(rx) = rs'(x)$ for $r \in k[G]$ we have that $r = e_{g_1}k_1 + e_{g_2}k_2 + \dots e_{g_n}k_n$ so

$$s'(rx) = s'(e_{g_1}k_1x + e_{g_2}k_2x + \dots e_{g_n}k_nx) = k_1s'(e_{g_1}x) + k_2s'(e_{g_2}x) + \dots k_ns'(e_{g_n}x)$$

We know s' is k linear since

$$s'(kx) = \frac{1}{|G|}\sum_{g\in G} e_g s(e_{g^{-1}}kx) = \frac{1}{|G|}\sum_{g\in G} e_g k s(e_{g^{-1}}x) = ks'(x)$$

Thus we must only check that $s'(e_hx) = e_hs'(x)$.

$$s'(e_hx) = \frac{1}{|G|}\sum_{g\in G} e_g s(e_{g^{-1}h}x)$$

We can relabel $z = h^{-1}g$ and $z^{-1} = g^{-1}h$. Since $h^{-1}G = G$ we have the same sum

$$= \frac{1}{|G|}\sum_{z\in G} e_{hz} s(e_{z^{-1}}x) = \frac{e_h}{|G|}\sum_{z\in G} e_z s(e_{z^{-1}}x) = e_hs'(x)$$

Thus s' is a $k[G]$ module homomorphism.
We have that $\pi \circ s'$ =id since

$$\pi \circ s'(x) = \frac{1}{|G|}\sum_{g\in G} e_g \pi(s(e_{g^{-1}}x)) = \frac{1}{|G|}\sum_{g\in G} x = x$$

Letting $Q = s'(M/N)$ we have the exact sequence

$$0 \to N \to^{id} M \to^{\pi} Q \to 0$$

Since π splits we know that $M = N \oplus Q$ and thus M is semisimple.
Important result used in other problems
We can write the middle module of a short exact sequence as a direct sum if the sequence splits as follows:
If we have

$$0 \to N \to^{id} M \to^{\pi} Q \to 0$$

where there exists $s' : Q \to M$ such that $\pi \circ s' = \text{id}$ then we can show $M = N \oplus Q$ by showing every $m \in M$ can be written uniquely as a sum $m = n + q$ where $n \in N, q \in Q'$. Here we define $Q' = \text{im } s'$ so $Q' \cong Q$. We have that $s'(\pi(m)) = q$ and $n = m - q$. We know $m - q \in N$ since in M/N the coset of q and m are the same since $\pi(q) = \pi(s'(\pi(m))) = \pi(m)$

so $m - q = 0 \Rightarrow m - q \in N$. If we show $N \cap Q' = 0$ then we have uniqueness since if $q + n = q' + n' \Rightarrow q - q' + n - n' = 0 \Rightarrow q - q' \in N, n - n' \in Q' \Rightarrow q - q', n - n' \in N \cap Q' \Rightarrow q - q' = 0, n - n' = 0 \Rightarrow q = q', n = n'$.
For any $p \in N \cap Q'$ we have that s' is surjective to Q' so there exists $q \in Q$ where $s'(q) = p$. We have $\pi(s'(q)) = q$. Since $p \in N$, $\pi(p) = 0$, thus $q = 0$. Since s' is a homomorphism we know s' maps 0 to 0, thus $p = 0$.

Exersise 8.4

Consider $R = \mathbb{Z}$ for some prime p we have the sequence of R modules

$$0 \to \mathbb{Z}/(p) \to \mathbb{Z}/(p^2) \to (\mathbb{Z}/(p^2))/(\mathbb{Z}/(p)) \cong \mathbb{Z}/(p) \to 0$$

We know $\mathbb{Z}/(p)$ is simple, yet $\mathbb{Z}/(p^2) \ncong \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$ since the generator must map to an element of order p^2, so $\mathbb{Z}/(p^2)$ is not simple

Exersise 8.5

(a)
$(i \Rightarrow ii)$
This follows directly from the definition. Letting $N = P$, $\pi = p$, $f =$id. By the definition of a projective there exists $s : P \to M$ with $p \circ s =$id.
$(ii \Rightarrow iii)$
Leting $M = R^P$, the free module with generating set P, we have the surjection $p : M \to P$ which is the identity mapping on the generators. Letting $Q = \ker \pi$ we have the exact sequence

$$0 \to Q \to^{id} R^P \to^{p} P \to 0$$

Since p splits, we know that $R^P = P \oplus Q$. (I showed this result in problem 8.3)
$(iii \Rightarrow i)$
For any R modules M, N, surjective homomorphism $\pi : M \to N$ and homomorphism $f : P \to N$ we can extend f as $f' : (P \oplus Q) \to N$ by setting $f' = (f, 0)$. We have that $P \oplus Q$ is free so has some generators $g_1, g_2, \ldots$ Since π is surjective, there exists $m_1, m_2, \dots \in M$ where $\pi(m_1) = f'(g_1), \pi(m_2) = f'(g_2) \ldots$ Thus we can define a homomorphism using the universal propertiy of free modules

$$g' : P \oplus Q \to M \text{ where } g_1 \to m_1, g_2 \to m_2 \ldots$$

We have that $\pi(g'(g_i)) = f'(g_i)$ and since homomorphisms from free modules are entirely determined by the image of the generators, $\pi \circ g' = f'$. Thus if we restrict g' to $g : P \to Q$ with $g(p) = g'(p)$ we get the mapping showing P is projective since $f = f'$ on P.

(b)
$(i \Rightarrow ii)$
This follows directly from the definition. To use the same notation in the assignments description of injective, letting $M = I$, $N = M$, $\pi = s$, $f =$ id it follows from the definition of injective there exists $p : M \to I$ with $p \circ s =$ id.

$(ii \Rightarrow i)$
For any M and homomorphism $f : M \to I$ and injective homomorphism $\pi : M \to N$, we create a module $(N \times I)/Q$ where Q is the image of the homomorphism $\phi : M \to M \times N$, $\phi(m) = (\pi(m), -f(m))$.
We have the natural projective map $s : N \times I \to (N \times I)/Q$. We also have the injective map $(0, \mathrm{id}) : I \to N \times I$. It is the case that $s \circ (0, \mathrm{id})$ is injective (I will show this later) and thus from (ii) there exists $p : (N \times I)/Q \to I$ where $p \circ s \circ (0, \mathrm{id}) = \mathrm{id}$. The $g : N \to I$ to show (i) is $g = p \circ s \circ (\mathrm{id}, 0)$. We have that

$$g \circ \pi = p \circ s \circ (\mathrm{id}, 0) \circ \pi$$

In the module $(N \times I)/Q$ we have the equivalent cosets $(\pi(m), 0) = (\pi(m), 0) - (\pi(m), -f(m)) = (0, f(m))$ so $s \circ (\mathrm{id}, 0) \circ \pi = s \circ (0, \mathrm{id}) \circ f$:

$$= p \circ s \circ (0, \mathrm{id}) \circ f = f$$

Since from how p was defined $p \circ s \circ (0, \mathrm{id}) = \mathrm{id}$. All that is left to show is that $s \circ (0, \mathrm{id})$ is injective:
We have that $S = \ker(s \circ (0, \mathrm{id})) = 0$ since for any $i \in S$, $s(0, i) = 0 \Rightarrow (0, i) \in Q$, ϕ is surjective to Q so there exists $m \in M$ where $(\pi(m), -f(m)) = (0, i)$. However since π is injective, the only possibility for m is 0 and since $-f(0) = 0$ we know that $i = 0$.

Exersise 8.6

(a) For any division ring R and R modules M, P, N. We know that division ring modules have a basis so let B be the basis of P. If there exists surjective homomorphism $\pi : M \to N$ and homomorphism $f : P \to N$ we have that f is fully determined by the image of B. Since π is surjective for every $b \in B$ there is an $m_b \in M$ such that $\pi(m_b) = f(b)$. Thus we can use the universal property of free modules to define $g : P \to M$ where $g(b) = m_b$ for all $b \in B$. We have that for every $b \in B$, $\pi \circ g(b) = f(b)$ so $\pi \circ g = f$. So P is projective.
For any injective homomorphism $\pi : M \to N$ and homomorphism $f : M \to P$ there exists a basis B for M where π and f are fully defined by the images of B. Since π is injective, we know that $\pi(B)$ is a basis for $\pi(M)$. We have that $N/\pi(M)$ has a basis E', and so N has the basis $\pi(B) \cup E$ where E is a set in N whose cosets are E'. We can define $g : N \to P$ where $g(e) = 0$ for all $e \in E$ and $g(\pi(b)) = f(b)$. Thus we have $g \circ \pi = f$ so P is injective.

(b) If P is a free R module it is clear that P is projective from condition (iii).
Conversely P is finitely generated and thus we know

$$P \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_n)$$

with $a_1 | a_2 | \dots a_n$.
With P projective there exists Q such that $P \oplus Q \cong R^B$ is a free R module. This can only be the case if $a_1 = a_2 = \dots a_n = 0$ which would mean P is free. This is because any basis element of $P \oplus Q$ which generates an element in $R/(a_i)$ cannot be linearly independent since it is not torsion free.

(c) We can use Baer's Criterion to show that $\mathbb{Q}$ is injective. Baer's criterion states that a module over a unit ring R is injective if every module homomorphism from an ideal $I \subset R$ to M can be extended to a homomorphism. We have that every module homomorphism $f : n\mathbb{Z} \to \mathbb{Q}$ extends to a homomorphism $f' : \mathbb{Z} \to \mathbb{Q}$ by taking $y \in \mathbb{Q}$ such that $ny = f(n)$ and we define $f'(x) = xy$.
$\mathbb{Q}$ is not projective since if it were, then $\mathbb{Q}$ would be a submodule of some free $\mathbb{Z}$ module F. We would then have the projection map $\pi : F \to \mathbb{Q}$ and the inclusion map $i : \mathbb{Q} \to F$ where $\pi \circ i = \text{id}$.
We have that $i(1) = a_1b_1 + a_2b_2 + \dots a_nb_n$ where b_is are basis elements of F and $a_i \in \mathbb{Z}$. Choose $N \in \mathbb{Z}$ so that $N > |a_i|$ for all a_i. We have that

$$i(1) = N \cdot i(1/N) = a_1b_1 + \dots a_nb_n$$

Which means $N|a_i$ for all i (since $i(1/N)$ is written as a unique sum of basis elements). This is a contradiction however since $N > |a_i|$ so $a_i = 0$ which contradicts $1 = \pi(i(1)) \neq \pi(0) = 0$

Exersise 8.7

$(i \Rightarrow ii)$
For R modules M, P and surjective homomorphism $\pi : P \to M$, since P, M are semisimple we can write them as a sum of simple modules

$$P = \bigoplus P_i, M = \bigoplus M_j$$

We can write π as a direct sum of its components from each P_i. Since the set of homomorphisms from each simple module is a division ring, we know that either $\pi_i : P_i \to M$ is zero, or there exists $s_i : \pi_i(P_i) \to P$ such that $\pi_i \circ s_i = \text{id}$. Thus since π is surjective we can define over all M $s : M \to P$ where $s(m) = \bigoplus s_i(m)$. We then have that $\pi \circ s = \text{id}$ and thus (ii) is satisfied so P is projective.

$(ii \Rightarrow iii)$
We have that for any R module I and M we wish to show any injective $\pi : I \to M$ splits. We have the short exact sequence

$$I \to^{\pi} M \to^{p} M/I$$

Since M/I is projective we know that p splits. As I have shown in 8.3 this means that $M = M/I \oplus I$. Thus since $\pi(I) = 0 \oplus I$ we can extend the inverse on the image $\pi^{-1} : \pi(I) \to I$ to $(0, \pi^{-1}) : M//I \oplus I \to I$ with $\pi \circ (0, \pi^{-1}) = \text{id}$.

$(iii \Rightarrow i)$
For any submodule I of R we have the inclusion mapping $i : I \to R$. Since R is injective there exists $g : R \to I$ with $g \circ i = \text{id}$. Thus we have that the short exact sequence

$$0 \to \ker g \to^{i} R \to^{g} I$$

and g splits ($g \circ i = \mathrm{id}$). Thus $R = (\ker g) \oplus I$ as we have shown in problem 8.3. Therefore R is semisimple.