Exersise 9.1

(a) For any ideal $I \subset R \times S$, we have the projection maps $\pi_R : R \times S \to R, \pi_S : \mathbb{R} \times S \to S$ where $\pi_R(r,s) = r$ and $\pi_S(r,s) = s$. We have that I is the intersection of the ideals $P = \pi_R(I) \times S$ and $Q = R \times \pi_S(I)$. It is clear that $R \times S = P + Q$ since $R \times \{0\} \subset Q$ and $\{0\} \times S \subset P$. Thus we can use the chinese remainder theorem.

$$(R \times S)/I \cong (R \times S)/P \oplus (R \times S)/Q$$

We have that $(R \times S)/P = (R \times S)/(\pi_R(I) \times S) \cong R/\pi_R(I)$ and similarly $(R \times S)/Q \cong S/(\pi_S(I)$. Thus

$$(R \times S)/I \cong R/\pi_R(I) \oplus S/\pi_S(I)$$

Since R, S are semi-simple, we know that the short exact sequences

$$0 \to \pi_R(I) \to R \to R/(\pi_R(I)) \to 0$$

$$0 \to \pi_S(I) \to S \to S/(\pi_S(I)) \to 0$$

split, and we get

$$R \cong R/(\pi_R(I)) \oplus \pi_R(I), S \cong S/(\pi_S(I)) \oplus \pi_S(I)$$

So

$$R \times S \cong R/(\pi_R(I)) \oplus \pi_R(I) \times S/(\pi_S(I)) \oplus \pi_S(I)$$

from our chinese remainder theorem identity:

$$R \times S \cong (R \times S)/I \oplus \pi_R(I) \oplus \pi_S(I)$$

And $I = \pi_R(I) \oplus \pi_S(I)$ thus $R \times S$ is semi-simple.

(b) If a is square free, since a PID is a UFD we can factor a as a product of prime elements $a = p_1 p_2 \dots p_n$. Thus from the chinese remainder theorem.

$$R/(a) \cong R/(p_1) \oplus R/(p_2) \oplus \cdots \oplus R/(p_n)$$

each $R/(p_i)$ is a field (since the p_is are irriducible elements) and thus simple. Thus $R/(a)$ is a direct sum of simple modules over R and thus semi-simple.
Conversly if $p^2|a$ for some prime p then the chinese remainder theorem results in

$$R/(a) \cong R/(p^n) \oplus R/(b)$$

where $p \nmid b$ and $n \geq 2$. We have that the submodule generated by $(p,0)$ cannot split $R/(a)$. The reason for this is that our quotent becomes $(R/(a))/(p,0) \cong (R/(p^n) \oplus R/(b)/)(p,0) \cong R/(p) \oplus R/(b)$

$$R/(a) \cong (R/(p) \oplus R/(b)) \oplus (p,0)R/(a)$$

There would be no element in this new ring, which multiplied by p^{n-1} would be nonzero, but would be 0 multiplied by p^n as is the case for $(1,0) \in \mathbb{R}/(p^n) \oplus R/(b)$. Thus this split is not possible

Exersise 9.2

(a) We have the following isomorphism

$$\mathbb{C}[\mathbb{Z}/n] \cong \mathbb{C}[x]/(x^n - 1]$$

Where $e_0 \to 1, e_1 \to x, \dots e_{n-1} \to x^{n-1}$. This mapping we will call φ is an homorphism as follows

$$\varphi(e_i e_k) = \varphi(e_{i+k \pmod n}) = x^{i+k \pmod n} = x^i x^k = \varphi(e_i)\varphi(e_k)$$

And φ is bijective since there is a one to one and onto correspondence between generators as a $\mathbb{C}$ vectorspace.

We have from the chinese remainder theorem

$$\mathbb{C}[x]/(x^n - 1) = \mathbb{C}[x]/\left(\prod_{m=0}^{n-1}(x - e^{\frac{2\pi i m}{n}})\right) \cong \bigoplus_{m=0}^{n-1} \mathbb{C}[x]/(x - e^{\frac{2\pi i m}{n}})$$

Each $\mathbb{C}[x]/(x - e^{\frac{2\pi i m}{n}})$ is a free $\mathbb{C}$ module of rank 1 and thus $\mathbb{C}[x]/(x - e^{\frac{2\pi i m}{n}}) \cong \mathbb{C}$. So we have

$$\mathbb{C}[\mathbb{Z}/n] \cong \bigoplus_{m=0}^{n-1} \mathbb{C}$$

With the explicit isomorphism as the composition of the described isomorphisms: $e_0 \to 1 \to 1$, and

$$e_k \to x^k \to \bigoplus_{m=0}^{n-1} e^{\frac{2\pi i k m}{n}}$$

(b) We know that any division ring over $\mathbb{C}$ is $\mathbb{C}$ as shown in problem 8.2. Thus we know $\mathbb{C}[S_3]$ is isomorphic to a direct sum of matricies over $\mathbb{C}$. Since $\mathbb{C}[S_3]$ is dimension 6 over $\mathbb{C}$ the only possible dimension 6 forms are $\mathbb{C} \oplus \mathbb{C} \cdots \oplus \mathbb{C}$ and $M_2[\mathbb{C}] \oplus \mathbb{C} \oplus \mathbb{C}$. It cannot be $\mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C}$ however since the only elements of order 3 are of the form

$$\bigoplus_{i \in I \subset [6]} e^{\frac{\pm 2\pi}{3}} \bigoplus_{i \in I^c} 1$$

So we would have e_{123} maps to something of this form. but the only elements of order two are of the form

$$\bigoplus_{i \in I \subset [6]} -1 \bigoplus_{i \in I^c} 1$$

So e_{12}, e_{23} would map to something of this form. But then $e_{12}e_{23} = e_{123}$ would not be compatable since multiplying elements of the order 2 form would not yield elements of the order 3 form. Thus

$$\mathbb{C}[S_3] \cong M_2[\mathbb{C}] \oplus \mathbb{C} \oplus \mathbb{C}$$

For an explicit isomorphism we know

$$e_i \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \oplus 1 \oplus 1$$

We can consider the rational canonical form of matricies to figure out all matricies of order 2. The minimal polynomial must divide $x^2 - 1$ which yields the possible matricies

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

For matricies of order 3, the minimal polynomial must divide $x^3 - 1 = (x-1)(x-\zeta_3)(x+\zeta_3)$ (where ζ_3 is the 3rd root of unity) and thus must be either $x^2 + x + 1$ or $x^2 - (1 \pm \zeta_3)x \pm \zeta_3$ or $(x-1)$, $x \pm \zeta_3$. Which yields the possible matricies

$$\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & \pm\zeta_3 \\ 1 & 1 \pm \zeta_3 \end{bmatrix} \begin{bmatrix} \pm\zeta_3 & 0 \\ 0 & \pm\zeta_3 \end{bmatrix} \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm\zeta_3 \end{bmatrix}$$

After trying various conjugacy classes of the order two matricies, I found the following mapping to be compatable with multiplication:

$$e_{12} \to \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} e_{23} \to \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix} e_{13} \to \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} e_{123} \to \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} e_{13} \to \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

Exersise 9.3

$(iii) \Rightarrow (ii) \Rightarrow (i)$:

From the identities we established leading up to the Artin Wedernburn theorem, we know that $R \cong \mathrm{End}_{R^{op}}(R^{op}) \cong M_n(D)$, where $M_n(D) \cong \mathrm{End}(M_1 \oplus M_2 \oplus \dots M_n)$. This comes from the identity $R^{op} \cong \oplus_{i=1}^{n} M_n$ where M_n are simple modules. Since each M_i is isomorphic to each other we have R is the direct sum of only one matrix ring over a division ring. Thus $(iii) \Rightarrow (ii)$. In problem 7.6(1) we have shown $M_n(D)$ is simple. For Artinian condition, $M_n(D)$ as an R module is isomorphic to $D^n \oplus D^n \oplus \cdots \oplus D^n$ which are simple $M_n(D)$ modules. Thus, as we have established in lecture, $M_n(D)$ is Artinian since every every submodule is of the form $D^n \oplus D^n \oplus D^n \cdots \oplus D^n$ and so a decsending chain must terminate on some number of D^n as a direct sum. Thus $(ii) \Rightarrow (i)$.

$(i) \Rightarrow (iii)$:

R contains a simple submodule M as illustrated by the following process. If R is simple, we are done, otherwise R must contain some proper module M_1, either M_1 is simple or M_1 contains proper M_2. Continuing this logic yields a decsending chain of proper modules $R \supset M_1 \supset M_2 \dots$ since R is Artinian there exists M_n which terminates the chain, and thus must be simple.

We know that $\mathrm{Ann}_R(M)$ is a two sided ideal of R. Thus since R is simple, we know $\mathrm{Ann}_R(M) = 0$. We can now construct an isomorphism $\phi : R \to M^n$ for some n and thus proving R is semi-simple with every simple submodule of R isomorphic to M. Since in

lecture we established every simple R module is a submodule of R, this implies (iii). We construct this isomorphism as follows:
Let $\phi_0 : R \to M$ where $1 \to m_0$ for some $m_0 \in M$. Either $\ker \phi_0 = 0$ or $\exists r_0 \in \ker \phi_0$. Since $\mathrm{Ann}_R(M) = 0$ there exists $m_1 \in M$ such that $r_1 m_1 \neq 0$. We define the new homorphism $\phi_1 : R \to M^2$ where $1 \to (m_0, m_1)$ thus $r_1 \notin \ker \phi_1$ since $\phi_1(r_1) = (r_1 m_0, r_1 m_1) \neq (0, 0)$, either $\ker \phi_2 = 0$ or there exists $r_2 \in \ker \phi_1$ and $m_2 \in M$ with $r_2 m_2 \neq 0$. Thus we can define $\phi_2 : R \to M^3$ where $1 \to (m_0, m_1, m_2)$ and thus $r_2 \notin \ker \phi_2$. Continuing this process we get a decsending chain of submodules of R

$$\ker \phi_0 \supset \ker \phi_1 \supset \ker \phi_2 \supset \dots$$

Thus since R is Artinian this chain terminates, which means there exists $\phi_k = \phi : R \to M^n$ with $\ker \phi = 0$. So ϕ is an imbedding into M^n. Thus R is a submodule of M^n and thus $R \cong M^k$ for some $k \leq n$.

Exersise 9.4

(a) We have the bilinear map

$$f : \mathbb{Z}/m \times \mathbb{Z}/n \to \mathbb{Z}/d$$

$$(a, b) \to ab$$

This map is bilinear since if $(a, b) = 0 \in \mathbb{Z}/m \times \mathbb{Z}/n$ then $ab = 0 \in \mathbb{Z}/d$ so $0 \to 0$, and $f(a, b) + f(c, b) = ab + cb = (a + c)b = f(a + c, b)$
This induces the map

$$\varphi : \mathbb{Z}/m \otimes \mathbb{Z}/n \to \mathbb{Z}/d$$

$$a \otimes b \to ab$$

This map is bijective and thus an isomorphism as follows:
We know that evey $z \in \mathbb{Z}/d$ can be written as ab since we let $a = 1$ and since $m \geq d$ we can let $b = z$. Thus this mapping is surjective.
We have that there is only one generator. $\mathbb{Z}/m \otimes \mathbb{Z}/n$ is generated by $1_m \otimes 1_n = 1$ since both $\mathbb{Z}/m$ and $\mathbb{Z}/n$ have only the one generators. Since we are working with $\mathbb{Z}$ modules, this is equivalent to saying the group is cyclic. For any $a \otimes b$, from bilinearity

$$a \otimes b = ab(1 + n\mathbb{Z} \otimes 1 + m\mathbb{Z}) = (ab + n\mathbb{Z} + m\mathbb{Z})(1 \otimes 1) = (ab + d\mathbb{Z})(1 \otimes 1)$$

Thus the characteristic is d so the domain and codomain of φ have the same size. Since φ is surjective, it is thus injective

(b) We have that $\mathbb{Z}$ is a subring of $\mathbb{Q}$. Thus as established in Corollary 18 of 10.4 of Dummit and Foote, the tensor extends the scalers:

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}_{\mathbb{Q}}$$

Where $\mathbb{Q}_{\mathbb{Q}}$ is a $\mathbb{Q}$ module. We know that $\mathbb{Q}_{\mathbb{Q}} \cong \mathbb{Q}$ as a group, thus we are done

(c) For any $m \otimes r + I \in M \otimes R/I$ we have $m \otimes r + I = rm \otimes 1 + I$ thus every element can be written in the form $rm \otimes 1 = m' \otimes 1$.

$$\varphi : M \otimes R/I \to M/IM$$

$$m \otimes 1 \to m + IM$$

This map is well defined since if $\varphi(m \otimes 1) = m + IM = m' + IM$, then $m = m' + in$ for some $i \in I$, $n \in M$. By bilinearity we have

$$m \otimes 1 = m' + in \otimes 1 = m' \otimes 1 + i(n \otimes 1) = m' \otimes 1 + n \otimes 0 = m' \otimes 1$$

We have that $n \otimes 0 = n \otimes (0 + 0) = n \otimes 0 + n \otimes 0 \Rightarrow n \otimes 0 = 0$ for that last equality. Thus φ is well defined. φ is surjective since for any $m + IM$ we have $\varphi(m \otimes 1) = m + IM$. φ is injective since if $\varphi(m' \otimes 1) = \varphi(m \otimes 1)$ then as we have shown in proving φ is well defined, $m + IM = m' + IM \Rightarrow m \otimes 1 = m' \otimes 1$. Thus φ is an isomorphism

(d) We have the mapping

$$\varphi : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \times \mathbb{C}$$

$$1 \otimes 1 \to (1, 1), 1 \otimes i \to (1, i), i \otimes 1 \to (i, 1), i \otimes i \to (i, i)$$

This mapping is a ring isomorphism as follows.
Since $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is an $\mathbb{R}$ vectorspace and thus a free module, we know the mapping is $\mathbb{R}$ linear and bijective since the map bijects basis. Thus all that needs to be checked is multiplication of the basis elements. From how the ring structure is defined over the tensor product (as established in prop 21 page 374 of Dummit and Foote), it is clear the multiplicative structure is preserved, since

$$\varphi((a \otimes b)(c \otimes d)) = \varphi(ab \otimes cd) = (ab, cd) = \varphi(a \otimes b)\varphi(c \otimes d)$$

Where a, b, c, d represents either 1 or i

(e) Using the hint we have that $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(f)$, thus $\mathbb{F}_{p^n}$ is a $\mathbb{F}_p$ free module. From Corollary 18 of Dummit and Foote we know as $\mathbb{F}_{p^n}$ modules

$$\mathbb{F}_{p^n} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^n} \cong \mathbb{F}_{p^n} \otimes_{\mathbb{F}_p} \mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}^n$$

This applies as ring homorphisms since the multiplicative structure of $\mathbb{F}_{p^n}$ is preserved. ie for

$$(a \otimes (b_0 + b_1 x + b_2 x^2 \dots b_{n-1} x^{n-1}) \in \mathbb{F}_{p^n} \otimes_{\mathbb{F}_p} \mathbb{F}_p[x]/(f)$$

We have

$$(a \otimes (b_1 + b_2 x + b_3 x^2 \dots b_{n-1} x^{n-1}) = a(b_1(1 \otimes 1) + b_2(1 \otimes x) + \dots b_n(1 \otimes x^{n-1})) \to a(b_0, b_1 \dots b_n)$$

Exersise 9.5

(a) Letting $A(t) = \sum_{i\geq 0} h_i t$ and $B(t) = \sum_{i\geq 0} e_i t$, we can using combinatorial reasoning to write these series in a new form.
When we multiply out

$$\prod_{i=1}^{n}(1+x_i t) = (1+x_1 t)(1+x_2 t)\dots(1+x_n t)$$

We get $B(t)$. The reasoning for this is because for each k, a t^k only shows up in the product by choosing k $x_i t$ terms and multiplying by 1 for the other terms. Thus every t^k term is of the form $x_{j_1}x_{j_2}\dots x_{j_k}$ where $1 \leq j_1 < j_2 < \dots j_n \leq n$, and conversly all $x_{j_1}x_{j_2}\dots x_{j_k}$ show up uniquely as a coefficient of one of the t^k terms by choosing $x_{j_1}x_{j_2}\dots x_{j_k}$ and multiplying out by 1 for the other terms. Summing up all these terms we get the symmetric polynomials:

$$\sum_{1\leq j_1<j_2<\dots j_k\leq n} x_{j_1}\dots x_{j_k}t^k = e_k t^k$$

Thus $B(t) = \prod_{i=1}^{n}(1+x_i t)$ since each coefficient of t^k is the same in both polynomials.
For $A(t)$ we have the following product of the closed form of the geometric series

$$\prod_{i=1}^{n}\frac{1}{1-x_i t} = \prod_{i=1}^{n}\left(1 + x_i t + (x_i t)^2 + (x_i t)^3 \dots + (x_i t)^k \dots\right)$$

When we factor out this product we get $A(t)$. The reasoning for this is because for each k, a t^k only shows up in the product if we choose $(x_{j_1}t)^{n_1}, (x_{j_2}t)^{n_2}, \dots (x_{j_l}t)^{n_l}$ so that $n_1+n_2\dots n_l = k$ and multiply by the 1 term for every other term in the product. Thus every t^k term is one of the terms in h_k. We have that every term of h_k shows up uniquely as a coefficient of one of the t^k since any monomial $x_{j_1}^{n_1}x_{j_2}^{n_2}\dots x_{j_l}^{n_l}$ of total degree k shows up only by choosing the terms $(x_{j_1}t)^{n_1}(x_{j_2}t)^{n_2}\dots(x_{j_l}t)^{n_l}$ and 1s in the other terms. Thus when we sum up all the t^k terms we get $h_k t^k$.

(b) From our product identities we have the equality

$$A(t)B(-t) = \prod_{i=1}^{n}(1-x_i t)\prod_{i=1}^{n}\frac{1}{1-x_i t} = 1$$

By factoring out $A(t)B(-t)$ we get the constant term $e_0 h_0 = 1$, thus subtracting the constant term on both sides we get the sum of nonconstant terms is 0. Thus for each $k \geq 1$ the coefficient of t^k is zero. We have that every t^k coefficient term is of the form $h_n(-1)^m e_m$ where $m+n = k$. Thus the sum of the coefficients of the t^k terms is $h_k - h_{k-1}e_1 + h_{k-2}e_2 - \dots + (-1)^k e_k$. This coefficient must be zero, thus we have Newtons identity

$$h_k - h_{k-1}e_1 + h_{k-2}e_2 - \dots + (-1)^k e_k = 0$$

(c) From Newtons identity we can that $\Lambda_n = \mathbb{Z}[h_1, \dots h_n]$. We from lecture that $\Lambda_n = \mathbb{Z}[e_1, \dots e_n]$ thus if we show $\mathbb{Z}[h_1, \dots h_n] = \mathbb{Z}[e_1, \dots e_n]$ we are done. By showing that $h_1, \dots h_n$

linearly spans $e_1 \dots e_n$ we are done (we already know $e_1, e_2 \dots e_n$ spans $h_1 \dots h_n$ since $e_1, \dots e_n$ generate all symmetric polynomials). Using induction we have the base case $h_0 = e_0$. From Newtons identity:

$$(-1)^{k-1}(h_k - h_{k-1}e_1 + h_{k-2}e_2 - \dots e_{k-1}h_1) = e_k$$

We have that each e_k is a linear sum of e_i and h_j where $i < k$ thus from our inductive hypothesis each e_i is a linear sum of h_js and thus e_k is a linear sum of h_js.