1. (a) We begin by noting that:

$$0 + 0 = 0 \in S + I$$

$$1 + 0 = 1 \in S + I$$

Let $s_x + a_x, s_y + a_y \in S + I$. We note that $-s_x \in S$ and $-1 \cdot a_x \in I$. Thus:

$$-s_x + (-a_x) = -(s_x + a_x) \in S + I$$

For addition, we get that:

$$s_x + a_x + s_y + a_y = (s_x + s_y) + (a_x + a_y) \in S + I$$

For multiplication, we get that:

$$(s_x + a_x) \cdot (s_y + a_y) = (s_x s_y) + (s_y a_x + s_x a_y + a_x a_y) \in S + I$$

Thus, we conclude that $S + I$ is a subring.

(b) We begin by noting that $0 \in I$ and $0 \in S$, so $0 \in S \cap I$. Let $a, b \in S \cap I$. We note that $a + b \in S$ and $a + b \in I$. Thus, $a + b \in S \cap I$. Lastly, let $s \in S$. We note that $as \in S$ and $as \in I$, so $as \in S \cap I$. This proves $S \cap I$ is an ideal of S.

(c) We first note that $S \subseteq S + I$. Thus, the natural projection map $\pi : S \to (S + I)/I$ where $s \mapsto [s]$ is a ring homomorphism.

We then note that for all $x \in (S + I)/I$, there exists a $s + a$ such that $s \in S$ and $a \in I$ where $x = [s + a] = [s] + [a] = [s]$ because $I \mid a$, which implies $[a] = [0]$. Thus, $x = \pi(s)$. Hence, π is surjective, so it implies $\text{im}(\pi) = (S + I)/(I)$.

For $x \in S \cap I$, $\pi(x) = [x] = [0]$ as $I \mid x$, so $x \in \ker(\pi)$. Meanwhile, for $x \in \ker(\pi)$, we note that $[x] = [0]$, which implies $I \mid x$ or $x \in I$. Thus, we get $x \in S \cap I$ and that $\ker(\pi) = S \cap I$.

By the First Isomorphism Theorem, we get that $S/(S \cap I) \cong (S + I)/I$.

2. (a) We note that $[0] \in J'$, so $0 \in J$. For $a, b \in J$, we get that $[a], [b] \in J'$, so $[a+b] \in J'$ and $a + b \in J$. For $r \in R$, note that $[r] \in R/I$, so $[ra] \in J'$ thus $ra \in J$. This proves J is an ideal of R.

(b) We note that $0 \in J$, so $[0] \in J/I$. For $[a], [b] \in J/I$, we note that $a + b \in J$, so $[a+b] = [a] + [b] \in J/I$. For $[r] \in R/I$, we note that $ra \in J$, so $[ra] = [r] \cdot [a] \in J/I$. This proves J/I is an ideal of R/I.

(c) We note that the natural projection map of $\pi : R \mapsto R/I$ where $r \mapsto [r]_I$ is a ring homomorphism. Meanwhile, the natural projection map of $\hat{\pi} : R/I \to (R/I)/(J/I)$ where $[r]_I \mapsto [[r]_I]_{J/I}$ is a ring homomorphism. Hence, if we denote $\varphi = \hat{\pi} \circ \pi$, we get that $\varphi : R \mapsto (R/I)/(J/I)$ where $r \mapsto [[r]]$ is a ring homomorphism.

For all $x \in (R/I)/(J/I)$, there exists an $[r] \in R/I$ where $x = [[r]]$ and consequently, an $r \in R$ where $[[r]] = \varphi(r)$. This proves *varphi* is surjective, so $\mathrm{im}(\varphi) = (R/I)/(J/I)$.

For $x \in J$, $\varphi(x) = [[x]]$. We also note that $[x] \in J/I$, so $[[x]] = [[0]]$ thus $x \in \ker(\varphi)$. Meanwhile, for $x \in \ker(\varphi)$, $\varphi(x) = [[0]]$, so $[x] \in J/I$, which further implies $x \in J$. Thus, $\ker(\varphi) = J$.

By the First Isomorphism Theorem, $R/J \cong (R/I)/(J/I)$.

3. (a) A proper ideal I is prime ideal if and only if $ab \in I$ then $a \in I$ or $b \in I$

   (b) Assume (r) is a prime ideal. By contradiction, we assume r is not prime. Then there exists $a, b \in R$ where $r \mid ab$ but $r \nmid a$ and $r \nmid b$. We note that $ab \in (r)$. This implies either $a \in (r)$ or $b \in (r)$. If we assume $a \in (r)$, then there exists a $q \in R$ where $rq = a$, but that would mean $r \mid a$, a contradiction. Thus, if (r) is a prime ideal, then r is prime.

   Assume r is prime. By contradiction, we assume (r) is not a prime ideal, so there exists an $ab \in (r)$ where $a, b \notin (r)$. Since $ab \in (r)$, there exists a $q \in R$ where $ab = rq$, so $r \mid ab$. This implies either $r \mid a$ or $r \mid b$. We assume $r \mid a$, so there exists a $q' \in R$ where $q'r = a$. However, this implies $a \in (r)$, a contradiction. Thus, if r is prime, then (r) is a prime ideal.

   (c) Assume I is a prime ideal of R. By contradiction, we assume R/I is not an integral domain, so there exists $[a], [b] \neq [0]$ and $[ab] = [0]$. Since $[ab] = [0]$, $I \mid ab$. This implies either $I \mid a$ or $I \mid b$, so either $[a] = [0]$ or $[b] = [0]$, a contradiction. Thus, if I is a prime ideal, R/I is an integral domain.

   Assume R/I is an integral domain. By contradiction, I is not a prime ideal of R. Thus, there exists $a, b \notin I$ but $I \mid ab$. This implies $[ab] = [0]$. However, R/I is an integral domain, so either $[a] = [0]$ or $[b] = [0]$. But that implies either $I \mid a$ or $I \mid b$, a contradiction. Thus, if R/I is an integral domain, then I is a prime ideal of R.

   (d) We note that $\mathbb{Z}$ is a PID. Thus, for all prime ideals I of $\mathbb{Z}$, there exists an $x \in \mathbb{Z}$ where I = (x). From b), x must be prime. By Euclid's Lemma, all prime numbers are prime, so their principal ideals are also prime ideals. However, 0 satisfies the definition of prime because $\mathbb{Z}$ is an integral domain, so if $0 \mid ab$ then either a or b must be zero, so (0) is also a prime ideal. Thus, all prime ideals of $\mathbb{Z}$ are principal ideals of prime numbers and 0.

   (e) From 1b), we note that $S \cap I$ is an ideal. For $a, b \in S$, if $ab \in S \cap I$, then $ab \in I$, which implies either $a \in I$ or $b \in I$. In other words, we get that either $a \in S \cap I$ or $b \in S \cap I$. Thus, $S \cap I$ is a prime ideal.

4. (a) If $[x]^2 = [x]$ for $0 \leq x \leq 2024$, then it implies $[x^2 - x] = [0]$ or $2025 \mid x(x-1)$. We then note that $2025 = 81 \cdot 25$ and that $\gcd(81, 25) = 1$. Thus, we can apply Theorem 7.11, where $m = 81$ and $n = 25$ and note that:

$$\begin{aligned} [x(x-1)]_{2025} &\mapsto [x(x-1)]_{81} \times [x(x-1)]_{25} \\ [0] &\mapsto [0]_{81} \times [0]_{25} \end{aligned}$$

We also note that this map is a ring homomorphism, so since $[x^2 - x] = [0]$, it implies that $[x(x-1)] = [0]_{81}$ and $[x(x-1)] = [0]_{25}$. In other words, we get that $81 \mid x(x-1)$ and $25 \mid x(x-1)$. We then note that 25 is a prime power of 5^2. By Euclid's Lemma, either $5 \mid x$ or $5 \mid x - 1$. Since $\gcd(x-1, x) = 1$, only one of the factors could be divisible by 5 and will be the one also divisible by 25. A similar argument can be applied that only one of the factors is divisible by 81. Thus, we get that either and $25 \mid x$ or $25 \mid x - 1$ and $81 \mid x$ or $81 \mid x - 1$. This gives us 4 possible combinations.

Case 1 If $25 \mid x$ and $81 \mid x$, since 81 and 25 are co-prime, we get that $2025 \mid x$. The only x that satisfies this is if $x = 0$.

Case 2 If $25 \mid x-1$ and $81 \mid x-1$, since 81 and 25 are co-prime, we get that $2025 \mid x-1$. The only x that satisfies this is if $x - 1 = 0$ or $x = 1$.

Case 3 If $25 \mid x - 1$ and $81 \mid x$, it implies there exist $a, b \in \mathbb{Z}$ where $25a = x - 1$ and $81b = x$. Thus:

$$\begin{aligned} 25a &= 81b - 1 \\ 1 &= 81b + 25(-a) \end{aligned}$$

We apply the Division Algorithm strategy back in Claim 2.7 to compute that $b = 21$, so $x = 21 \cdot 81 = 1701$.

Case 4 If $25 \mid x$ and $81 \mid x - 1$, it implies there exist $a, b \in \mathbb{Z}$ where $25a = x$ and $81b = x - 1$. Thus:

$$\begin{aligned} 81b &= 25a - 1 \\ 1 &= 25a + 81(-b) \end{aligned}$$

We apply the same strategy to compute that $a = 13$ thus $x = 13 \cdot 25 = 325$

Hence, there are 4 idempotent elements in $\mathbb{Z}/2025\mathbb{Z}$.

(b) We note that $0^2 = 0$ and $1^2 = 1$, so $0, 1 \in S$. For $a, b \in S$, we note that:

$$\begin{aligned} (a+b)^2 &= a^2 + 2ab + b^2 \\ &= a^2 = 2 \cdot 1 \cdot ab + b^2 \\ &= a^2 + b^2 \\ &= a + b \end{aligned}$$

Thus, $a + b \in S$. Meanwhile::

$$\begin{aligned} (ab)^2 &= a^2 b^2 \\ &= ab \end{aligned}$$

Thus, $ab \in S$. Lastly, we note that:

$$\begin{aligned} a + a &= 2a \\ &= 2 \cdot 1 \cdot a \\ &= 0 \end{aligned}$$

Thus, we note that $-a = a$ and since $a \in S$, we get that $-a \in S$. We proved S is a subring of R.

(c) We first note that $(0) = \{r0 : r \in R\} = \{0\}$. Meanwhile, we note that the map $\varphi : R \to R$ where $r \mapsto r$ is a ring homomorphism. Meanwhile, the $\mathrm{im}(\varphi) = R$ and that $\ker(\varphi) = \{0\} = (0)$. By the First Isomorphism Theorem, we get that $R/(0) \cong R$.

For $(e) + (1 - e)$, we note that for all $r \in R$ that

$$er + (1 - e)r = 1r = r$$

Hence, $r \in (e) + (1 - e)$ and $(e) + (1 - e) = R$. This allows us to apply Theorem 8.24 to get that $R/((e)(1 - e)) \cong R/(e) \times R/(1 - e)$. We then note that for any $a, b \in R$, we get that

$$(1 - e)a \cdot (e)b = (e - e^2)ab = 0ab = 0$$

This implies that any finite sum in the form of $\sum (e)a_i(1 - e)b_i$ is a sum of finitely many zeros, which sums to zero. Hence, $(1 - e)(e) = \{0\} = (0)$ and we get that $R \cong R/(0) \cong R/(e) \times R/(1 - e)$ or $R \cong R/(e) \times R/(1 - e)$ as desired.

(d) Let $|R| = 2$ where $R = \{0, 1\}$. By Theorem 7.16, $|R| \cdot 1 = 0$. Thus, $\mathrm{char}(R) = 2$ (we note that $\mathrm{char}(R) = 1$ is impossible because it implies $0 = 1$). By Exercise 7.5 (I proved it in HW5 1c), since $\mathrm{char}(R) = |R|$, we get that $R \cong \mathbb{F}_2$. By induction, we assume all finite commutative ring R where every element is idempotent with $2 \leq |R| \leq k$ for $k \in \mathbb{N}$ is isomorphic to a product of $\mathbb{F}_2$. We now assume such ring R where $|R| = k+1$.

If there exists an $e \in R$ where it is non-zero and non-unit, by c), we get that $R \cong R/(e) \times R/(1 - e)$. For all $r \in R$, we note that:

$$\begin{gathered} [r]_e^2 = [r^2]_e = [r]_e \\ [r]_{1-e}^2 = [r^2]_{1-e} = [r]_{1-e} \end{gathered}$$

Since the natural projections $R \to R/(e)$ and $R \to R/(1 - e)$ are surjective, we note that all elements in both rings are idempotent. Since both (e) and $(1 - e)$ are the kernels of their respective natural projections, by the pigeonhole principle, a non-injective but surjective map implies $|R/(e)|, |R/(1 - e)| < |R|$. Hence, by the induction hypothesis, both are isomorphic to a product of $\mathbb{F}_2$. Hence, we get that:

$$\begin{gathered} R \cong (\mathbb{F}_2 \times \cdots \times \mathbb{F}_2) \times (\mathbb{F}_2 \times \cdots \times \mathbb{F}_2) \\ R \cong \mathbb{F}_2 \times \cdots \times \mathbb{F}_2 \end{gathered}$$

Meanwhile, if there is no non-zero and non-unit element in R, then R must be a field because every non-zero element is a unit. For all $a \in R^\times$, there exists a $b \in R^\times$ where $ab = 1$. This implies $a(ab) = a$, but $a^2b = ab$, so $1 = ab = a$. Thus, $R^\times = \{1\}$. Since R is a field, we get that $R = \{0, 1\}$, which contradicts our assumption of $|R| = k + 1$, making it impossible.

We proved that all finite commutative rings R where every element is idempotent is isomorphic to a product of $\mathbb{F}_2$.

5. (a) We first prove that $\mathrm{im}(ev_a)$ is a subring of $\mathbb{C}$. We note that $1, 0 \in \mathbb{Z}[x]$, so $0, 1 \in \mathrm{im}(ev_a)$. For all $d, e \in \mathrm{im}(ev_a)$, there exists a $f, g \in \mathbb{Z}[x]$ where $f(a) = d$ and $g(a) = e$. We note that $-f \in Z[x]$, so $-f(a) = -d \in \mathrm{im}(ev_a)$. Meanwhile, $f + g, fg \in \mathbb{Z}[x]$, so $f(a) + g(a) = d + e, f(a)g(a) = de \in \mathrm{im}(ev_a)$. This proves $\mathrm{im}(ev_a)$ is a subring of $\mathbb{C}$. We also note $x \in \mathbb{Z}[x]$, so $a \in \mathrm{im}(ev_a)$.

We now prove it is the smallest subring containing a. For any subring S containing a, for all $x \in \mathrm{im}(ev_a)$, there also exists an $f \in \mathbb{Z}[x]$ where $f(a) = x$. f is a polynomial and S is closed under addition and multiplication for all of its elements. We also note $\mathbb{Z} \subseteq S$ because we can add $1, -1 \in S$ and we can add them indefinitely. This implies $f(a) = x \in S$, so $\mathrm{im}(ev_a) \subseteq S$. Since all subrings S containing a contains $\mathrm{im}(ev_a)$, it is the smallest subring containing a, which implies $\mathrm{im}(ev_a) = \mathbb{Z}[a]$.

(b) For each β_k, there exists a $f_k \in \mathbb{Z}[x]$ where $f_k(a) = \beta_k$ from our result in (a). We then denote $d = \max\{\deg(f_1), \cdots, \deg(f_k)\} + 1$. Since $-a^d \in \mathbb{Z}[a]$, there exists, $c_1, \cdots, c_n$ where $c_1 f_1(a) + \cdots + c_n f_n(a) = -a^d$. We construct the polynomial:

$$f(x) = x^d + c_1 f_1(x) + \cdots + c_n f_n(x)$$

We note that $f(a) = 0$. Since $\deg(x^d) \geq \deg(f_k)$ for all $1 \leq k \leq n$, the leading coefficient of f is 1. Thus, we constructed a monic polynomial where $f(a) = 0$.

(c) We denote $C = \{c_0 + c_1 a + \cdots + c_{d-1} a^{d-1} : c_0, c_1, \ldots, c_{d-1} \in \mathbb{Z}\}$.

For all $c \in \mathbb{Z}[a]$, there exists $f \in \mathbb{Z}[x]$ with $f(a) = c$ as proven in (a). By Proposition 9.4, $f(x) = q(x)g(x) + r(x)$ for $q, r \in \mathbb{Z}[x]$ since $g(x)$ is monic, so its leading coefficient is a unit and $\deg r < \deg g$. Since $g(a) = 0$, we get $f(a) = r(a)$. Since $\deg r \leq d - 1$, we get that $r(a)$ is a sum of integer coefficients up to a^{d-1}, so $r(a) = c \in C$.

For all $c \in C$, we have $c = c_0 + c_1 a + \cdots + c_{d-1} a^{d-1}$. The polynomial $f(x) = c_0 + c_1 x + \cdots + c_{d-1} x^{d-1} \in \mathbb{Z}[x]$, so $f(a) = c \in \mathbb{Z}[a]$. Hence, $\mathbb{Z}[a] = C$.

6. (a)