24.20.1 Let $\varphi\colon R \to S$ be a ring epimorphism (of rings). Do an analogous anaylsis before The First Isomorphism Theorem for Groups for $\varphi\colon R \to S$ to see how ideals and factor rings arise naturally.

Solution Take the equivalence relation $\sim$ on R given by $a \sim b \iff \varphi(a) = \varphi(b) \iff a - b \in \ker\varphi$, and define $\overline{\varphi}\colon R/\ker\varphi \to S$ via $[a] \mapsto \varphi(a)$.

We would like to check if $R/\ker\varphi$ is still a ring. Since the results from group theory still hold, it suffices to check that $R/\ker\varphi$ is a monoid, with $[a]\cdot[b] = [ab]$. This is a well-defined product, since if $a \sim a'$ and $b \sim b'$, then

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a') \in \ker\varphi.$$

Let $[a], [b] \in R/\ker\varphi$.

$\overline{\varphi}$ is well-defined: if $b - a \in \ker\varphi$, then $\overline{\varphi}([b-a]) = \varphi(b - a) = 0 \implies \varphi(b) = \varphi(a)$.

It's also easy to see that $\overline{\varphi}$ is a homomorphism.

We now what $R/\ker\varphi$ to be a ring. Addition is fine, since $\ker\varphi$ is a normal subgroup, so we just need to check that the multiplication axioms hold:

$(a + \ker\varphi)(b + \ker\varphi) = ab + a\ker\varphi + b\ker\varphi + \ker\varphi$. We want $a\ker\varphi = b\ker\varphi = \ker\varphi$ for any a, b, which is the same as having closure under multiplication in an ideal.

Associativity is easy to check also. We lastly want distributivity:

$$a(x + y) + \ker\varphi = (a + \ker\varphi)(x + y + \ker\varphi) = ax + ay + \ker\varphi + (x + y)\ker\varphi + \ker\varphi.$$

To get equality, we want $x + y \in \ker\varphi$, which is the same as having closure under additivity.

24.20.2 Let $R = (\mathbb{Z}/2\mathbb{Z})[t]$, $f = f(t) = t^2 + t + 1$, and $g = t^2 + 1$. Show all of the following:

a. $R/(f)$ is a field with four elements.

b. $R/(g)$ is not a domain and has four elements.

c. Neither $R/(f)$ nor $R/(g)$ is isomorphic to the ring $\mathbb{Z}/4\mathbb{Z}$.

Solution a. Let $h \in R/(f)$. h must be of the form $\left[at^2 + bt + c\right]$, since any higher order terms t^n can be killed off by a scalar multiple of $t^{n-2}f(t)$. We have the following options:

$$\begin{aligned}
[t^2 + t + 1] &= [t^2 + t + 1 + t^2 + t + 1] = [0] \\
[t^2 + t] &= [t^2 + t + t^2 + t + 1] = [1] \\
[t^2 + 1] &= [t^2 + 1 + t^2 + t + 1] = [t] \\
[t + 1] &= [t + 1 + t^2 + t + 1] = [t^2] \\
&[t^2] \\
&[t] \\
&[1],
\end{aligned}$$

so our equivalence classes are $[0], [1], [t]$, and $[t^2]$. $R/(f)$ is a commutative ring, so we just need to show that it's a group under multiplication.

Multiplication clearly commutes, and every non-zero element has an inverse:

$$[t]\cdot[t^2] = [t^2]\cdot[t] = [t^3 + t(t^2 + t + 1) + t^2 + t + 1] = [1],$$

so $R/(f)$ is a field.

b. We have the following equivalence classes:

$$\begin{aligned}
[t^2+t+1] &= [t^2+t+1+t^2+1] = [t] \\
[t^2+t] &= [t^2+t+t^2+1] = [t+1] \\
[t^2+1] &= [0] \\
[t+1]& \\
[t^2] &= [t^2+t^2+1] = [1] \\
[t]& \\
[1]&,
\end{aligned}$$

so our equivalence classes are $[0], [1], [t]$, and $[t+1]$. Moreover,

$$[t+1]^2 = [t^2+1+2t] = [0],$$

but $[t+1] \neq 0$, so $R/(g)$ is not a domain.

c. Neither elements are isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +)$. Each element has order 2 under $+$.

24.20.3 Let R be a commutative ring. Suppose for every element x in R there exists an integer $n = n(x) > 1$ such that $x^n = x$. Show that every prime ideal in R is maximal.

Solution Let $\mathfrak{p}$ be a prime ideal in R, $\mathfrak{A} \supsetneq \mathfrak{p}$, and let $x \in \mathfrak{A} \setminus \mathfrak{p}$. Now let $y \in \mathfrak{p}$. Then there exists $n > 1$ such that

$$\begin{aligned}
x + y = (x+y)^n &= x^n + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + y^n \\
x(1 - x^{n-1}) = x - x^n &= y\left[\binom{n}{1} x^{n-1} + \cdots + \binom{n}{n-1} x^1 y^{n-2} + y^{n-1} - 1\right] \in \mathfrak{p}.
\end{aligned}$$

Since $\mathfrak{p}$ is prime and $x \notin \mathfrak{p}$, this means that $1 - x^{n-1} \in \mathfrak{p} \subseteq \mathfrak{A}$.

But $x^{n-1} \in \mathfrak{A}$, so $1 = (1 - x^{n-1}) + x^{n-1} \in \mathfrak{A} \implies \mathfrak{A} = R$. Hence, $\mathfrak{p}$ is maximal.

24.20.5 Show that if the inclusion map $i\colon \mathbb{Z} \subseteq \mathbb{Q}$ satisfies $\psi_1 \circ i = \psi_2 \circ i$ whenever $\psi_1, \psi_2 \colon \mathbb{Q} \to R$ are ring homomorphisms, then $\psi_1 = \psi_2$. This shows that a surjective ring homomorphism is not equivalent to this property.

Solution Let $n \in \mathbb{Z}$. Then we have

$$\psi_1(n) = \psi_1(i(n)) = \psi_2(i(n)) = \psi_2(n),$$

so ψ_1 and ψ_2 agree on $\mathbb{Z}$.

Let $a/b \in \mathbb{Q}$, where $a, b \in \mathbb{Z}$, $b \neq 0$. Then because ψ_1 is a ring homomorphism,

$$\psi_1(a) = \psi_1\left(b \cdot \frac{a}{b}\right) = \sum_{i=1}^{b} \psi_1\left(\frac{a}{b}\right) = b\psi_1\left(\frac{a}{b}\right).$$

By the same argument,

$$\psi_2(a) = b\psi_2\left(\frac{a}{b}\right),$$

so since ψ_1 and ψ_2 agree on $\mathbb{Z}$,

$$\psi_1(a) = \psi_2(a) \implies b\psi_1\left(\frac{a}{b}\right) = b\psi_2\left(\frac{a}{b}\right) \implies \psi_1\left(\frac{a}{b}\right) = \psi_2\left(\frac{a}{b}\right),$$

so $\psi_1 = \psi_2$.

24.20.6 Let R be a commutative ring of characteristic $p > 0$, p a prime. Prove that the map $R \to R$ by $x \mapsto x^p$ is a ring homomorphism. It is called the *Frobenius homomorphism.* In particular, the *Children's Binomial Theorem* holds, i.e., $(x + y)^p = x^p + y^p$ in R for all x and y in R.

Solution Let $x, y \in R$, and call the map in the problem φ.

$\varphi(0) = 0^p = 0$.

$\varphi(1) = 1^p = 1$.

$\varphi(xy) = x^p y^p = \varphi(x)\varphi(y)$, by commutativity.

To show that φ preserves addition, first notice that if $1 \leq n \leq p - 1$,

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}.$$

Every factor in the denominator is strictly smaller than p, and p is prime, so $p \mid \binom{p}{n}$. Thus, because commutativity holds, we can use the binomial expansion formula to see

$$\varphi(x + y) = (x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} = x^p + y^p = \varphi(x) + \varphi(y),$$

so φ is a ring homomorphism.

24.20.8 Show that if R is a domain, so is the polynomial ring $R[t]$. In particular, show that there exist fields properly containing the complex numbers. Does the field that you constructed have the property that every non-constant polynomial over it has a root? Prove or disprove this.

Solution Let R be a domain, and let $f, g \in R[t]$ non-zero with $fg \equiv 0$. Write

$$f(t) = \sum_{i=0}^{N} a_i t^i \quad \text{and} \quad g(t) = \sum_{j=0}^{M} b_j t^j.$$

Assume that a_k, b_ℓ are the first non-zero coefficients of f and g, respectively. Then

$$(fg)(t) = a_k b_\ell t^{k+\ell} + \cdots \equiv 0 \implies a_k b_\ell = 0.$$

Since R is a domain, this implies that $a_k = 0$ or $b_\ell = 0$, a contradiction. Hence, one of these functions must be identically 0, so $R[t]$ is a domain.

24.20.10 Prove the isomorphism statement about the multiplicative groups in the Chinese Remainder Theorem 24.19.

Solution It suffices to prove that if $A \simeq B \times C$, then $A^\times \simeq B^\times \times C^\times$. Then by induction and the Chinese Remainder Theorem for the additive group in the theorem statement, we're done.

Let $\varphi \colon A \to B \times C$ be a ring isomorphism. We wish to show that its restriction to $A^\times$ gives a bijection to $B^\times \times C^\times$.

If $x \in A^\times$, there exists $y \in A^\times$ so that $xy = 1$. Since φ is a homomorphism,

$$1 = \varphi(1) = \varphi(xy) = \varphi(x)\varphi(y),$$

so $\varphi(x)$ is a unit, which means its components are units are also. Since φ was a bijection, it follows that its restriction is a bijection to $B^\times \times C^\times$ also, so $A^\times \simeq B^\times \times C^\times$.

25.18.1 Let V be a finite dimensional vector space over R with ordered basis $\{v_1, \ldots, v_n\}$. Define a lexicographic order of V relative to this ordered basis.

Solution Define the lexicographic order $\alpha = a_1 v_1 + \cdots + a_n v_n \leq_L b_1 v_1 + \cdots + b_n v_n = \beta$ by:

$\alpha \leq_L \beta$ if $a_i = b_i$ for all i. If not, then $\alpha \leq_L \beta$ if $a_k \leq b_k$ for some $1 < k \leq n$, and $a_i = b_i$ for $1 \leq i < k$.

25.18.2 Prove the following proposition:

Proposition. *Let V be a nonzero vector space over a field F and S a spanning set for V. Then a subset of S is a basis of V.*

Solution Consider the poset P of linearly independent sets $\mathfrak{B} \subseteq S$. Consider a chain $\mathcal{C} \subseteq P$. Then $\cup\mathcal{C}$ is an upper bound. Indeed, any finite subset of $\cup C$ is contained in some $B \in \mathcal{C}$, since it's totally ordered, so any finite subset is linear independent. Hence, the entire set is linearly independent, so $\cup\mathcal{C} \in P$ and is a valid upper bound.

P is also non-empty; take any non-zero singleton in S. Hence, Zorn's lemma gives us a maximal linearly independent set $\mathfrak{B}$. By the same argument to show that any vector space has a basis, $\mathfrak{B}$ is a basis, and it is a subset of S, so we are done.

25.18.4i Let R be a commutative ring. Let $\mathcal{S}$ be the set of non-finitely generated ideals in R. Suppose $\mathfrak{A}$ is a maximal element in $\mathcal{S}$. Then $\mathfrak{A}$ is a prime ideal.

Solution Let $ab \in \mathfrak{A}$. Assume $a, b \notin \mathfrak{A}$. Then $\mathfrak{A} \subsetneq \mathfrak{A} + (a)$ and $\mathfrak{A} \subsetneq \mathfrak{A} + (b)$. Since $\mathfrak{A}$ was the maximal element in $\mathcal{S}$, it follows that $\mathfrak{A} + (a)$ and $\mathfrak{A} + (b)$ are finitely generated. But this means that

$$(\mathfrak{A} + (a))(\mathfrak{A} + (b)) = \mathfrak{A} + (ab) = \mathfrak{A}$$

is finitely generated, a contradiction. Hence, a or b must lie in $\mathfrak{A}$.

25.18.5 Let R be a commutative ring. Prove

a. If x is nilpotent in R, then $1 + x$ is a unit in R.

b. The nilradical of R is an ideal.

c. Compute the nilradical of the rings: $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $n > 1$, and $\mathbb{Z}$.

Solution a. Since x is nilpotent, there exists $n > 1$ so that $x^n = 0$. Then if n is odd,

$$1 = 1 + x^n = (1 + x)(1 + x + \cdots + x^{n-1}).$$

Otherwise, if n is even,

$$1 = 1 + x^{n+1} = (1 + x)(1 + x + \cdots + x^n) = (1 + x)(1 + x + \cdots + x^{n-1}).$$

In either case, $1 + x$ is a unit.

b. Let $x, y \in \operatorname{nil} R$, and let $r \in R$.

By definition, there exist $n, m > 1$ so that $x^n = y^m = 0$. Then by direct calculation via the binomial expansion theorem, one finds that $(x + y)^{n+m} = 0$. Indeed, each term $x^a y^b$ must satisfy $a + b = n + m$, which means that $a \geq n$ or $b \geq m$ for every term, so each term is 0.

Since R is commutative, $(rx)^n = r^n x^n = 0$.

Thus, $\operatorname{nil} R$ is an ideal.

c. For $\mathbb{Z}/12\mathbb{Z}$, we must have $12 \mid x^n$ for some $n > 1$. In particular, $3 \mid x$ and $2 \mid x$, so our possibilities are $0, 6$. By calculation, we see that $\operatorname{nil} R = \{0, 6\}$.

For $\mathbb{Z}/n\mathbb{Z}$, again, we need $n \mid x^m$ for some m. If $p_1, \ldots, p_k$ are the prime factors of n, then we have $p_i \mid x$ for every i. If x contains all the prime factors, then eventually, $x^m = 0$ since x^m will be n times some powers of n's prime factors.

So, if we write $n = p_1^{\ell_1} \cdots p_k^{\ell_k}$, then a nilpotent element of R is of the form $p_1^{j_1} \cdots p_k^{j_k}$, where $j_i \leq \ell_k$ for each k, where equality does not happen for every k.

For $\mathbb{Z}$, the nilradical is just $\{0\}$.

25.18.6 Let R be a commutative ring. The *Jacobson radical* of R is defined to be $\operatorname{rad}(R) := \bigcap_{\operatorname{Max}(R)} \mathfrak{m}$, the intersection of all maximal ideals in R. Show that x lies in $\operatorname{rad}(R)$ if and only if $1 - yx$ is a unit in R for all y in R.

Solution "$\implies$"

Let $x \in \operatorname{rad}(R)$. Suppose there exists $y \in R$ so that $1 - yx$ is not a unit in R. This means $(1 - yx)$ is an ideal, so it is contained in some maximal ideal $\mathfrak{m}$ in R. But $yx \in \mathfrak{m} \implies 1 = 1 - yx + yx \in \mathfrak{m} \implies \mathfrak{m} = R$, a contradiction.

"$\impliedby$"

Let x be so that $1 - yx$ is a unit for any $y \in R$, and suppose there exists a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$.

Then $\mathfrak{m} + (x) = R$, since $\mathfrak{m}$ was maximal. In particular, there exists $m \in \mathfrak{m}$ and $r \in R$ so that $m + rx = 1 \implies m = 1 - rx$. But this implies that m is a unit, which implies that $\mathfrak{m} = R$, a contradiction.

25.18.7 Let R be a commutative ring and $\mathfrak{A} < R$ an ideal. Define the *radical* of $\mathfrak{A}$ to be the set

$$\sqrt{\mathfrak{A}} := \{x \in R \mid x^n \in \mathfrak{A} \text{ for some } n \in \mathbb{Z}^+\}.$$

Show the following:

a. $\sqrt{\mathfrak{A}}$ is an ideal and

$$\sqrt{\mathfrak{A}} = \bigcap_{\substack{\mathfrak{A} \subseteq \mathfrak{p} < R \\ \mathfrak{p} \text{ a prime ideal}}} \mathfrak{p}.$$

b. Let $\overline{\cdot} \colon R \to R/\mathfrak{A}$ be the canonical ring epimorphism. Then $\operatorname{nil}(\overline{R}) = \sqrt{\mathfrak{A}}/\mathfrak{A}$.

Solution a. Let $x, y \in \sqrt{\mathfrak{A}}$ and $r \in R$.

By assumption, there exist $n, m \geq 1$ so that $x^n, y^m \in \mathfrak{A}$. Then $(x + y)^{n+m} \in \mathfrak{A}$. Indeed, each term $x^a y^b$ must satisfying $a + b = n + m$, which implies that $a \geq n$ or $b \geq m$ for every term. So, each term is in $\mathfrak{A}$, which means that any linear combination (i.e., $(x + y)^{n+m}$) lies in $\mathfrak{A}$, so $x + y \in \mathfrak{A}$.

$(rx)^n = r^n x^n \in \mathfrak{A}$, since $\mathfrak{A}$ is an ideal. Hence, $\sqrt{\mathfrak{A}}$ is an ideal.

Call the right-hand side P. It's clear that $\sqrt{\mathfrak{A}} \subseteq P$.

Now suppose $x \notin \sqrt{\mathfrak{A}}$. Then if $S = \{x, x^2, x^3, \ldots\}$, then $S \cap P = \emptyset$.

Let Z be all the ideals $\mathfrak{a}$ such that $\mathfrak{a} \cap S = \emptyset$. If $\mathcal{C} \subseteq Z$ is a chain, then clearly $\bigcup \mathcal{C}$ excludes S. Moreover, it is an upper bound for Z. Z is also non-empty, since $\{0\} \in Z$, so by Zorn's lemma, there exists a maximal element $\mathfrak{I}$.

We claim that $\mathfrak{I}$ is prime. Let $ab \in \mathfrak{I}$, and suppose $a, b \notin \mathfrak{I}$. Then $\mathfrak{I} + (a)$ and $\mathfrak{I} + (b)$ are strictly larger than $\mathfrak{I}$, which is the maximal element of Z, so there exist $m, n \geq 1$ so that $x^n \in \mathfrak{I} + (a)$ and $x^m \in \mathfrak{I} + (b)$. But this implies that $x^{n+m} \in \mathfrak{I} + (ab) = \mathfrak{I}$. But this is a contradiction, since we assumed that $\mathfrak{I}$ excluded S, so $\mathfrak{I}$ is prime.

Thus, $\mathfrak{I}$ is a prime ideal which doesn't include x, so $x \notin P$, which implies that

$$(\sqrt{\mathfrak{A}})^{\mathrm{c}} \subseteq P^{\mathrm{c}} \implies P \subseteq \sqrt{\mathfrak{A}},$$

as desired.

b. Let $x + \mathfrak{A} \in \operatorname{nil}(\overline{R})$. By definition, there exists $n \geq 1$ so that $(x + \mathfrak{A})^n = \mathfrak{A}$. But this implies that $x^n \in \mathfrak{A}$, so $x \in \sqrt{\mathfrak{A}}$, which means that $x + \mathfrak{A} \in \sqrt{\mathfrak{A}}/\mathfrak{A}$.

Now let $x + \mathfrak{A} \in \sqrt{\mathfrak{A}}/\mathfrak{A}$. By definition, there exists $n \geq 1$ so that $x^n \in \mathfrak{A}$. Then

$$(x + \mathfrak{A})^n = x^n + \sum_{i=1}^{n} \binom{n}{i} x^i \mathfrak{A}^{n-i} = x^n + \mathfrak{A} = \mathfrak{A},$$

so $x + \mathfrak{A}$ is nilpotent.

Hence, the two sets are equal.

25.18.8 Let R be a commutative ring, $\mathfrak{A} < R$ an ideal, and $\bar{\cdot}: R \to R/\mathfrak{A}$ be the canonical epimorphism. We say that $\mathfrak{A}$ is a *primary ideal* if $ab \in \mathfrak{A}$ implies that $a \in \mathfrak{A}$ or $b^n \in \mathfrak{A}$ for some positive integer n.

Let $\mathfrak{A} < R$ be an ideal. Show both of the following:

a. $\mathfrak{A}$ is a primary ideal if and only if every zero divisor of $R/\mathfrak{A}$ is nilpotent.

b. If $\mathfrak{A}$ is primary, then its radical, $\sqrt{\mathfrak{A}}$ is a prime ideal.

Solution a. "$\implies$"

Let $\mathfrak{A}$ be a primary ideal, and let $x + \mathfrak{A} \in R/\mathfrak{A}$ be a zero divisor. Then there exists a non-zero $y + \mathfrak{A}$ with $xy + \mathfrak{A} = \mathfrak{A} \implies xy \in \mathfrak{A}$. Then $x^n \in \mathfrak{A}$, since $y \notin \mathfrak{A}$, for some value of n, so $R/\mathfrak{A}$ is nilpotent.

"$\impliedby$"

Suppose every zero divisor of $R/\mathfrak{A}$ is nilpotent, and let $xy \in \mathfrak{A}$.

If $y \notin \mathfrak{A}$, then

$$(x + \mathfrak{A})(y + \mathfrak{A}) = xy + \mathfrak{A} = \mathfrak{A},$$

which means that x is a zero divisor, so $x + \mathfrak{A}$ is nilpotent. Thus, there exists $n \geq 1$ with $x^n + \mathfrak{A} = \mathfrak{A} \implies x^n \in \mathfrak{A}$, so $\mathfrak{A}$ is primary.

b. Let $\mathfrak{A}$ be primary, and let $xy \in \sqrt{\mathfrak{A}}$.

By assumption, there exists $n > 1$ so that $x^n y^n = (xy)^n \in \mathfrak{A}$. Since $\mathfrak{A}$ is primary, $x^n \in \mathfrak{A}$ or $y^{n+m} \in \mathfrak{A}$ for some $m > 1$. Thus, $x \in \sqrt{\mathfrak{A}}$ or $y \in \sqrt{\mathfrak{A}}$, so $\sqrt{\mathfrak{A}}$ is prime.

25.18.10 Let R be a commutative ring. An element e of R is called an *idempotent* if $e^2 = e$. For example, if S is another commutative ring, the element $(1_R, 0_S)$ is an idempotent in the ring $R \times S$. The objective of this exercise is to prove a converse. Let e be an idempotent of R. Then prove

a. $e' := 1 - e$ is an idempotent of R.

b. The principle ideal Re of R is a ring with identity $1_{Re} = e$.

c. R is ring isomorphic to $Re \times Re'$.

Solution a. $(e')^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e = e'$, so e' is an idempotent.

b. Re is an abelian group under addition: If $x \in Re$, then $-1 \cdot x = -x \in Re$. It's clearly abelian and associative since R was.

If $x = a_1 e + \cdots + a_n e$, then $xe = ex = a_1 e^2 + \cdots + a_n e^2 = a_1 e + \cdots + a_n e = x$, so e is indeed the identity.

If $x = \sum a_n e$ and $y = \sum b_n e$, then $xy = \sum \sum a_n b_m e^2 = \sum \sum a_n b_m e \in Re$. Multiplication also commutes since it commutes in R, and it distributes since it does in R as well. Thus, Re is a ring.

c. Let $r \in R$, and decompose it via $r = r(e + 1 - e) = re + re'$ so that we can define the homomorphism $\varphi \colon R \to Re \times Re'$ with $\varphi(r) = (re, re')$.
This is well-defined: If $(re, re') = (se, se')$, then

$$re + re' = se + se' \implies r = s.$$

We have $\varphi(1) = (e, e') = (1_{Re}, 1_{Re'}) = 1_{Re\times Re'}$, $\varphi(0) = (0, 0) = 0_{Re\times Re'}$.
If $x, y \in R$, then

$$\varphi(x + y) = (xe + ye, xe' + ye') = (xe, xe') + (ye, ye') = \varphi(x) + \varphi(y),$$

and

$$\varphi(xy) = (xye, xye') = (xeye, xe'ye') = (xe, xe')(ye, ye') = \varphi(x)\varphi(y),$$

so φ is a homomorphism.
Now let $(ae, be') \in Re \times Re'$. Then because $ee' = 0$,

$$\varphi(ae + be') = (ae^2 + bee', aee' + be'^2) = (ae, be'),$$

so φ is onto.
Lastly, if $\varphi(x) = \varphi(y)$, then $xe = ye$ and $xe' = ye'$, so

$$x = xe + xe' = ye + ye' = y,$$

so φ is one-to-one.
Thus, φ is an isomorphism.