We know there are $a!$ permutations of a elements, we may rethink it in another way. We think $a!$ is the possibilities of the way that you pick a elements from a elements. Now, we can generailize the first a, that is, pick k elements from n elements. It's easy to see that it is exactly $n!$ but only first k terms, that is, $\frac{n!}{(n-k)!}$.

If we don't care about the order, we may divide $\frac{n!}{(n-k)!}$ by the amount of the permutations of k elements, that is $k!$.

We may denote pick k elements in n elements (without order) by C_k^n, which is exactly $\frac{n!}{(n-k)!k!}$.

Definition 0.1 (Ideal)**.** *A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$, and every $a \in A$, both ra and ar are in A.*

Theorem 0.1 (Ideal Test)**.** *A non-empty subset A of a ring R is an ideal of R, if:*

- *$a - b \in A$ for all a $b \in A$.*
- *$ar \in A$ and $ra \in A$ for all $a \in A$ and $r \in R$.*

Proof. Since $A \subseteq R$, we know $ab \in A$ for all a $b \in A$ from the second property. Therefore, A is a subring of R, and then it is an ideal of R by the second property. □

Example (Trivial Ideal)**.** *For any ring R, $\{0\}$ is an ideal of R, which is called the trivial ideal.*

Theorem 0.2 (Factor Ring)**.** *Let R a ring and A a subring of R. The set of coset $\{\ r + A \mid r \in R\ \}$ is a ring under:*

- *addition:* $(s + A) + (t + A) = (s + t) + A$
- *multiplication:* $(s + A)(t + A) = (st) + A$

iff A is an ideal of R.

Proof. Newline please!!

- ($\Rightarrow$) For any $r \in R$ and $a \in A$,

$$\begin{aligned} & 0 + A \\ =&(r + A)(0 + A) \\ =&(r + A)(a + A) \quad (\text{since } a \in A) \\ =&ra + A \end{aligned}$$

Then $0 + A = ra + A$, and then $ra \in A$ (Recall that $a + A$ means a coset of A). Similarly, $ar \in A$.

- ($\Leftarrow$) For any $s\ t \in R$,
  - Addition: $(s + A) + (t + A) = s + t + A + A = (s + t) + A$ by $(R, +)$ is Abelian group.
  - Multiplication:

$$\begin{aligned}
&(s + A)(t + A) \\
=&(s + A)t + (s + A)A \\
=&st + At + sA + AA \\
=&st + A + A + A' \quad \text{(since } A \text{ is an ideal)} \quad \text{where } A' \subseteq A \\
=&st + A \quad \text{(since } A \text{ is a group under addition)}
\end{aligned}$$

  - Assosiative and Distributive: Trivial by R is a ring.

□

Theorem 0.3. *Let R a commutative ring with unity and A an ideal of R. Prove that R/A is an integral domain iff A is a prime ideal.*

Proof.

- ($\Rightarrow$) For any $a\ b \in R$ and $ab \in A$, we have $ab + A = 0 + A$ and $(a + A)(b + A) = ab + A$, since R/A is integral domain, we know either $a + A$ or $b + A$ is zero, in the other word, $a \in A$ or $b \in A$.
- ($\Leftarrow$) For any $a\ b \in A$, if $(a + A)(b + A) = 0 + A$, then $ab + A = 0 + A$ which means $ab \in A$. We know $a = 0$ or $b = 0$ by A is a prime ideal, therefore $a + A = 0 + A$ or $b + A = 0 + A$, and R/A is an integral domain.

□

Theorem 0.4. *Let R a commutative ring with unity and A an ideal of R. Prove that R/A is a field iff A is a maximum ideal.*

Proof.

- ($\Rightarrow$) Let B an ideal of R and $A \subseteq B \subseteq R$. Let $b \in B$ but $b \notin A$, if we can't found such element, then $B = A$. Note that $b \neq 0$, so that $(b+A)^{-1}$ exists. For any $r \in R$, we have:

$$\begin{aligned} & r + A \\ =&(r + A)(b + A)(b + A)^{-1} \\ =&(rb + A)(b' + A) \quad (b' \text{ is not necessary in B}) \\ =&(rbb' + A) \end{aligned}$$

  where $rbb' \in B$, since B is an ideal. Therefore $(-rbb') + r \in B$ since $A \subseteq B$ and $r \in B$ since addition is closed. Now, $B \subseteq R$ and $R \subseteq B$, then $B = R$.

- ($\Leftarrow$) The following proof come from textbook.

  Let $b \in R$ but $b \notin A$, consider the set $B = \{\ br + a \mid r \in R, a \in A\ \}$. It is eazy to show that B is an ideal of R. Since B properly contains A, B must be R, so $1 \in B$. Then $1 = br + a$ and $1 + A = (br + a) + A = br + A = (b + A)(r + A)$, so $r + A$ is the inverse of $b + A$, now every non-zero element in R/A has an inverse. We must show that R/A is integral domain. For any $a + A$ and $b + A$, if $ab \in A$, and $a \notin A$, then $0 + A = (a + A)^{-1}(ab + A) = (a + A)^{-1}(a + A)(b + A) = b + A$, we know $b \in A$, and R/A is an integral domain.

□

Corollary 0.1. *Let R a commutative ring with unity and A a maximal ideal of R, then A is also a prime ideal.*

Exercise 0.7. *Let n an integer and p a divides n and $p \neq n$. Prove that $\langle p \rangle$ is a maximal ideal in Z_n if and only if p is prime.*

Proof.

- ($\Rightarrow$) Suppose $\langle p \rangle$ is a maximal ideal in Z_n, if p is not prime, then q divides p and $q \neq 1$ and $q \neq p$. We have $\langle q \rangle$ is a ideal that properly contains p but is not Z_n since $1 \notin \langle q \rangle$.

- ($\Leftarrow$) Suppose p is a prime, and let R a ideal of Z_n. If R properly contains $\langle p \rangle$, let $q \in R$ but $q \notin \langle p \rangle$, then $\gcd(p, q) = 1$ since p is prime, then $1 \in Z_n \rightarrow R = Z_n$.

□

Exercise 0.9. *Suppose that R is a commutative ring and $a \in R$. If $\{0\}$ is a maximal ideal of R, then $aR = \{\ ar \mid r \in R\ \} = \{0\}$ or $a \in aR$.*

Proof. We need to show that aR is an ideal, it is trivial that aR is a subring. For any $ar \in aR$ and $b \in R$, $(ar)b = a(rb) \in aR$, therefore aR is an ideal. If aR property contains $\{0\}$, then $aR = R$ since $\{0\}$ is maximal. □

Exercise 0.14. *If A and B are ideals of a ring R, show that the sum of A and B, $A + B = \{\ a + b \mid a \in A, b \in B\ \}$ is also an ideal.*

Proof. By ideal-test:

0. $A + B$ is non-empty, since A and B are non-empty.
1. For any $x\ y \in A+B$, $x-y = a_0+b_0-a_1-b_1 = (a_0-a_1)+(b_0-b_1) \in A+B$.
2. For any $x \in A + B$, $r \in R$, $xr = (a + b)r = ar + br \in A + B$

□

Exercise 0.16. *If A and B are ideals of a ring R, show that the product of A and B, $AB = \{\ a_0b_0+a_1b_1+\cdots+a_nb_n \mid a_i \in A, b_i \in B, n$ is positive integer $\}$, is an ideal. (Note that $a_i = a_j$ where $i \neq j$ is possible, same for b_i)*

Proof. Trivial, similar to Exercise 14.14. □

Exercise 0.18. *Let A and B be ideals of a ring, show that $AB \subseteq A \cap B$.*

Proof. It is trivial, every element in AB is also in A, since A ideal, similarly, is also in B, since B ideal. □

Exercise 0.22. *If R is a finite commutative ring with unity, prove that every prime ideal of R is also a maximal ideal.*

Proof. For any prime ideal I of R, we know R/I is an integral ideal, since R is finite, so is R/I, then we know R/I is a field. Therefore I is a maximal ideal. □

Exercise 0.39. *Prove that the only ideals of a field F are $\{0\}$ and F.*

Proof. Suppose I is an ideal of F that contains non-zero elements, otherwise, $I = \{0\}$. Let $a \in I$ where a is non-zero, then $aa^{-1} = 1 \in I$ since I is an ideal, then $I = F$ since $1 \in I$. □

Exercise 0.40. *Let R a commutative ring with unity, if the only ideals of R are $\{0\}$ and R, show that R is a field.*

Proof. Since the only ideals of R are $\{0\}$ and R, we know $\{0\}$ is the maximal ideal of R, then $R/\{0\}$ is a field, so is R.

But unfortunately, we can't use ring isomorphism for now. □

Exercise 0.41. *Prove that every idempontent ($a^2 = a$) in a commutative ring with unity other than 0 and 1 is a zero divisor.*

Proof. For any idempontent a, $a + (1 - a) = 1 \to a^2 + (1 - a)a = a \to a + (1-a)a = a \to (1-a)a = 0$. Therefore, a is a zero divisor with $(1-a)$. □

Exercise 0.42. *Show that $\boldsymbol{R}[x]/\langle x^2 + 1\rangle$ is a field.*

Proof. We need to show $\langle x^2+1\rangle$ is maximal in $\mathbf{R}[x]$. We denote $\langle x^2+1\rangle$ by I, observe that in $\mathbf{R}[x]/I$, x^2 is treated as -1 since $x^2 + 1 + I = 0 + I$, therefore any element in $\mathbf{R}[x]/I$ has form $ax+b+I$. Let J an ideal that properly contains I and $ax + b$ a non-zero element in J, then

$$\begin{aligned}
&0 + J \\
=&(ax + b)(ax - b) + J \\
=&(a^2x^2 - b^2) + J \\
=&- a^2 - b^2 + J \quad (\text{since } I \subset J) \\
=&(-a^2 - b^2)\Big(\frac{1}{-a^2 - b^2}\Big) + J \\
=&1 + J
\end{aligned}$$

Therefore $1 \in J$ and $J = \mathbf{R}[x]$, which proves that $I = \langle x^2+1\rangle$ is maximal. □

Exercise 0.45. *Let R be the ring of continuous functions from $\boldsymbol{R}$ to $\boldsymbol{R}$. Show that $I = \{\ f \in R \mid f(0) = 0\ \}$ is maximal ideal of R.*

Proof. It is trivial that I is an ideal. Let J an ideal that properly contains I, then there is $f \in J$ where $f(0) \neq 0$. Let $g(x) = f(0) - f(x)$, then $g(0) = f(0)-f(0) = 0$ and $g \in J$. Let $h(x) = f(x)+g(x) = f(x)+f(0)-f(x) = f(0)$, then $h(x)$ is a constant function. It is easy to find $h^{-1}(x) = \dfrac{1}{f(0)}$ and show that $h^{-1}(x)h(x) = 1 \in J$. The continuity of g is trivial. □

Exercise 0.50. *Let R be a ring and I an ideal of R. Prove that R/I is commutative iff $rs - sr \in I$ for all $r\ s \in R$.*

Proof.

- ($\Rightarrow$) For any $r\ s \in R$, $rs + I = (r + I)(s + I) = (s + I)(r + I) = sr + I$, therefore $rs - sr \in I$.
- ($\Leftarrow$) For any $r\ s \in R$, $(r + I)(s + I) = rs + I = sr + I = (s + I)(r + I)$, since $rs - sr \in I$ implies $rs + I = sr + I$.

□

Exercise 0.57. *An integral domain D is called a principal ideal domain, if every ideal of D has form $\langle a \rangle = \{\ ar \mid r \in D\ \}$ for some $a \in D$. Show that Z is a principal ideal domain.*

Proof. Admit. □

Exercise 0.60. *Let R a principal ideal domain, show that every non-trivial prime ideal is maximal.*

Proof. Let $\langle p \rangle$ a non-trivial prime ideal, note that $p \neq 0$ since $\langle p \rangle$ is non-trivial. Then for any ideal $\langle r \rangle$ that properly contains $\langle p \rangle$, we can show $r \notin \langle p \rangle$, if so, then $\langle r \rangle$ is the smallest ideal that contains r, but $\langle p \rangle$ is smaller and $r \in \langle p \rangle$.

Since $p \in \langle r \rangle$, we know there is k such that $rk = p$, note that $k \neq 0$, since $p \neq 0$. Now by $\langle p \rangle$ is prime and $r \notin \langle p \rangle$, we know $k \in \langle p \rangle$ and there is $q \in R$ such that $pq = k$, similarly, $q \neq 0$. Then $rkq = pq = k$, by cancellation we know $rq = 1$ and $1 \in \langle r \rangle$, therefore $\langle r \rangle = R$ and $\langle p \rangle$ is maximal. □

Exercise 0.61. *Let R a commutative ring and $A \subseteq R$. Show that the annihilator of A, $\mathrm{Ann}(A) = \{\ r \in R \mid ra = 0\ \forall a \in A\ \}$ is an ideal.*

Proof.

0. $\mathrm{Ann}(A)$ is non-empty, since $0a = 0$.
1. For any $s\ t \in \mathrm{Ann}(A)$ and $a \in A$, $(s - t)a = sa - ta = 0 - 0 = 0$.
2. For any $s \in \mathrm{Ann}(A)$, $t \in R$ and $a \in A$, $sta = tsa = t0 = 0$.

□

Exercise 0.81. *Let R a commutative ring with unity and for any $a \in R$, $a^2 = a$. Let I be a prime ideal of R, show that $|R/I| = 2$.*

Proof. We know R/I is an integral ideal since I is prime, then for any $a \in R$ but $a \notin I$, $a + I$ is non-zero element of R/I, then by $a^2 + I = a + I$, we know $a + I = 1 + I$, therefore $|R/I| = |\{0 + I, 1 + I\}| = 2$. □

Definition 0.2 (Ring Homo/Isomorphism)**.** *A mapping ϕ from ring R to S is a ring homomorphism, if it preserve the operations, that is:*

$$\phi(a + b) = \phi(a) + \phi(b) \quad \phi(ab) = \phi(a)\phi(b0)$$

If the mapping is one-to-one and onto, then it is also a ring isomorphism.

Theorem 0.5 (Properties of Ring Homomorphism)**.** *Let ϕ a homomorphism from ring R to ring S.*

1. *For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$*
2. *Let A a subring of R, then $\phi(A) = \{\ \phi(a) \mid a \in A\ \}$ is a subring of S.*
3. *If A is an ideal and ϕ is onto, then $\phi(A)$ is an ideal of S.*
4. *Let B a ideal of S, then $\phi^{-1}(B) = \{\ a \in R \mid \phi(a) \in B\ \}$ is an ideal of R.*
5. *If R is commutative, then $\phi(R)$ is commutative.*
6. *If R has a unity, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S, and for any $r \in R$ where r is a unit, then $\phi(r)$ is also a unit.*
7. *ϕ is a isomorphism iff ϕ is onto and* $\operatorname{Ker}\phi = \{\ a \in R \mid \phi(a) = 0\ \} = \{0\}$.
8. *If ϕ is a isomorphism, then ϕ^{-1} is a isomorphism.*

Proof.

- Trivial, since homomorphism preserve operations.
- Trivial.
- For any $s \in S$, there is $r \in R$ such that $\phi(r) = s$ since ϕ onto, then for any $\phi(a) \in \phi(A)$, $\phi(a)s = \phi(a)\phi(r) = \phi(ar) \in \phi(A)$, same for $s\phi(a)$.

- For any $r \in R$, $\phi(r\phi^{-1}(B)) = \phi(r)B \subseteq B$, therefore $r\phi^{-1}(B) \subseteq \phi^{-1}(B)$.
- Trivial.
- For any $s \in S$, $s = \phi(1\phi^{-1}(s)) = \phi(1)s$, therefore $\phi(1)$ is the unity.
- For any $ab \in R$, $\phi(a) = \phi(b) \to \phi(a) - \phi(b) = 0 \to \phi(a - b) = 0$, therefore $a - b = 0$ since $\operatorname{Ker}\phi = \{0\}$, and $a = b$. Then ϕ is one-to-one.
- ...

□

Theorem 0.6 (Kernals are Ideals)**.** *Let ϕ a ring homomorphism from R to S, then* $\operatorname{Ker}\phi$ *is an ideal of R.*

Proof. By ideal-test:

0. $\operatorname{Ker}\phi$ is non-empty, since $0 \in \operatorname{Ker}\phi$.
1. For any $a\ b \in \operatorname{Ker}\phi$, $\phi(a - b) = \phi(a) - \phi(b) = 0 - 0 = 0$.
2. For any $a \in \operatorname{Ker}\phi$ and $b \in R$, $\phi(ab) = \phi(a)\phi(b) = 0\phi(b) = 0$.

□

Theorem 0.7 (First Isomorphism Theorem for Rings)**.** *Let ϕ a ring homomorphism from R to S, then the mapping from $R/\operatorname{Ker}\phi$ to $\phi(R)$, given by $\psi(r + \operatorname{Ker}\phi) = \phi(r)$ is a isomorphism, that is, $R/\operatorname{Ker}\phi \approx \phi(R)$.*

Proof. We know First Isomorphism Theorem works on (additive) groups, so we need to check that ϕ preserve multiplication. For any $s + \operatorname{Ker}\phi$ and $t + \operatorname{Ker}\phi$:

$$\begin{aligned}
&\psi((s + \operatorname{Ker}\phi)(t + \operatorname{Ker}\phi)) \\
=&\psi(st + \operatorname{Ker}\phi) \\
=&\phi(st) \\
=&\phi(s)\phi(t) \\
=&\psi(s + \operatorname{Ker}\phi)\psi(t + \operatorname{Ker}\phi)
\end{aligned}$$

□

Theorem 0.8 (Ideals are Kernals)**.** *For any ideal I of some ring R, I is the kernal of homomorphism: $\phi(r \in R) = r + I$.*

Theorem 0.9 (Homomorphism from Z to a Ring with Unity)**.** *Let R be a ring wuth unity, the mapping $\phi(n) = n \cdot 1$ is a homomorphism from Z to R.*

Proof. Obviously, ϕ is a function, then we need to check whether ϕ is a homomorphism, for all $a\ b \in Z$:

- $\phi(a+b) = (a+b)\cdot 1 = a\cdot 1 + b\cdot 1 = \phi(a) + \phi(b)$
- $\phi(ab) = (ab)\cdot 1 = (a\cdot 1)(b\cdot 1) = \phi(a)\phi(b)$

□

Corollary 0.2. *Let R a ring with unity, then R contains Z_n where $n > 0$ is the characteristic of R or $\mathbb{Z}$ if the characteristic of R is 0.*

Proof. By Theorem 15.5, we know $\phi(n) = n\cdot 1$ is a homomorphism from $\mathbb{Z}$ to R, if $\operatorname{char} R = m$ where $m > 0$, then we know $\operatorname{Ker}\phi =$ the set of multiple of m $= m\mathbb{Z} = \langle m\rangle$, therefore $\phi(\mathbb{Z}) \approx \mathbb{Z}/m\mathbb{Z} \approx Z_m$ is a subring of R. If $\operatorname{char} R = 0$, then $\operatorname{Ker}\phi = \{0\}$, therefore $\phi(\mathbb{Z}) \approx \mathbb{Z}$ is a subring of R. □

Corollary 0.3. *For any positive integer m, the mapping $\phi(x) = x \bmod m$ is a homomorphism from Z to Z_m.*

Corollary 0.4. *Let F a field, then F contains Z_p if F has a non-zero characteristic p or Q if F has a zero characteristic.*

Proof. By Corollary 15.1, we know F contains Z_p if $\operatorname{char} F$ is non-zero. We claim the mapping $\phi(\frac{a}{b}) = (a\cdot 1)(b\cdot 1)^{-1}$ is a homomorphism from Q to F. We need to show that ϕ **is** a function. For any $\dfrac{a}{b} = \dfrac{c}{d}$, we know $ad = bc$,

$$\begin{aligned} ad\cdot 1 &= bc\cdot 1 \\ (a\cdot 1)(d\cdot 1) &= (b\cdot 1)(c\cdot 1) \\ (a\cdot 1)(b\cdot 1)^{-1} &= (c\cdot 1)(d\cdot 1)^{-1} \end{aligned}$$

therefore $\phi(\frac{a}{b}) = \phi(\frac{c}{d})$.

Then we need to check that ϕ preserves operations, for any $\dfrac{a}{b}\ \dfrac{c}{d}\ in\mathbb{Q}$:

- $$\begin{aligned}&\phi(\frac{a}{b}+\frac{c}{d})\\=&\phi(\frac{ad+bc}{bd})\\=&((ad+bc)\cdot 1)(bd\cdot 1)^{-1}\\=&(ad\cdot 1+bc\cdot 1)(bd\cdot 1)^{-1}\\=&(ad\cdot 1)(bd\cdot 1)^{-1}+(bc\cdot 1)(bd\cdot 1)^{-1}\\=&\phi(\frac{ad}{bd})+\phi(\frac{bc}{bd})\\=&\phi(\frac{a}{b})+\phi(\frac{c}{d})\end{aligned}$$

- $$\begin{aligned}&\phi(\frac{a}{b}\times\frac{c}{d})\\=&\phi(\frac{ac}{bd})\\=&(ac\cdot 1)(bd\cdot 1)^{-1}\\=&(a\cdot 1)(c\cdot 1)(d\cdot 1)^{-1}(b\cdot 1)^{-1}\\=&(a\cdot 1)(b\cdot 1)^{-1}(c\cdot 1)(d\cdot 1)^{-1}\\=&\phi(\frac{a}{b})\phi(\frac{c}{d})\end{aligned}$$

Therefore ϕ is a homomorphism from $\mathbb{Q}$ to F, then $\phi(\mathbb{Q})\approx\mathbb{Q}/\operatorname{Ker}\phi$ is a subring of F. We claim $\operatorname{Ker}\phi=\langle 0\rangle$. For any $\frac{a}{b}\in\operatorname{Ker}\phi$, we know $\phi(\frac{a}{b})=\phi(0)=0$, therefore $(a\cdot 1)(b\cdot 1)^{-1}=0$, we know F is an integral domain, so one of $(a\cdot 1)$ and $(b\cdot 1)^{-1}$ is zero. But we know no one have 0 as invert element, so $(a\cdot 1)$ must be 0. By $\operatorname{char}F=0$, we know no positive a such that $a\cdot 1=0$, so $a=0$ and $\frac{a}{b}=0$. □

Exercise 0.23. *Show that the homomorphism preserve idempotent.*

Proof. $\phi(a)=\phi(a^2)=\phi(a)^2$. □

Exercise 0.36. *The sum of the squares of three consecutive integers can not be a square.*

Proof. This proof comes from math stackexchange.

For any integer x, we found $(x-1)^2 + x^2 + (x+1)^2 = 3x^2 + 2$, if such square exists, then it must not a multiple of 3, and the remainder should be 2, therefore, the number we want has form $3n + r$ where n is integer and $0 < r < 3$ (Note that $0 \neq r$ since the number we want is not a multiple of 3). Then $(3n+r)^2 = 9n^2 + 6nr + r^2$, and $1^2 = 1$, $2^2 = 1$. Therefore no r such that $r^2 = 2$, so $3x^2 + 2$ can not be a square. □

Exercise 0.46. *Prove that any automorphism of a field F is the identity from the prime subfield to itself.*

Proof. We know prime subfield is a subfield that does not contain any proper non-trivial subfield, therefore it is the minimal subfield that contains 1. It is finite if $\operatorname{char} R \neq 0$ and it is Q if $\operatorname{char} R = 0$.

Let ϕ a automorphism of F, then $\phi(1) = 1$, any element in such prime subfield has form $n \cdot (b \cdot 1)^{-1}$ where n and b are integers. Note that $\phi(n \cdot (b \cdot 1)^{-1})$ is determined by $\phi(1)$, and $\phi(1) = 1$, so ϕ is the identity. □

Exercise 0.49. *Let R and S be commutative rings with unity, ϕ a homomorphism from R onto S and* $\operatorname{char} R \neq 0$. *Prove that* $\operatorname{char} S$ *divides* $\operatorname{char} R$.

Proof. Since ϕ is onto and R has unity, we know $\phi(1) = 1$. Let $\operatorname{char} R = n$, then $\phi(n \cdot 1) = n \cdot \phi(1) = 0$, therefore the order of unity of S under additive divides n. □

Exercise 0.52. *Show that a homomorphism from a field onto a non-zero ring must be an isomorphism.*

Proof. We need to show that such homomorphism ϕ is one-to-one. Since F a field, we know $\operatorname{Ker} \phi$ is either a zero ideal or F itself. We may suppose $\operatorname{Ker} \phi = F$, since another case is trivial. Then $\phi(F) = \{0\}$, however, ϕ is onto and the codomain is not a zero-ring, so $\phi(F)$ cannot be $\{0\}$. □

Exercise 0.53. *Suppose that R and S are commutative ring with unities. Let ϕ a homomorphism from R to S and let A be an ideal of S:*

- *If A is prime, show that $\phi^{-1}(A)$ is also prime.*
- *If A is maximal, show that $\phi^{-1}(A)$ is also maximal.*

Proof. If A is prime, for any element $ab \in \phi^{-1}(A)$, we have $\phi(ab) \in A$, therefore $\phi(a)$ or $\phi(b)$ in A, which implies a or $b \in \phi^{-1}(A)$.

If A is maximal, for any ideal I that properly contains $\phi(A)^{-1}$ in R, then $\phi(I)$ properly contains A and $\phi(I) = S$, therefore $I = \phi(S)^{-1} = R$. □

Exercise 0.54. *Show that the homomorphic image of a principal ideal ring is also a principal ideal ring.*

Proof. Let ϕ a homomorphism from a principal ideal ring R onto some ring S, then S is commutative and has a unity. For any ideal I of S, $\phi^{-1}(I)$ is a principal ideal, say, $\langle r \rangle = rR$, then $I = \phi(rR) = \phi(r)\phi(R) = \phi(r)S$, therefore I is a principal ideal ring which generated by $\phi(r)$. □

Exercise 0.57. *Show that Z_{mn} is ring-isomorphic to $Z_m \oplus Z_n$ when m is coprime to n.*

Proof. By Group Theory, we know Z_{mn} is group-isomoprhic to $Z_m \oplus Z_n$, then there is an isomorphism ϕ that maps $\phi(1)$ to any generator of $Z_m \oplus Z_n$, we choose $\phi(1) = (1, 1)$. Then, for any $a\ b \in Z_{mn}$

$$\begin{aligned}
&\phi(a\ b)\\
=&\phi((a \cdot 1)b)\\
=&\phi(a \cdot (1b))\\
=&a \cdot \phi(b)\\
=&a \cdot (\phi(1)\phi(b))\\
=&(a \cdot \phi(1))\phi(b)\\
=&\phi(a \cdot 1)\phi(b)\\
=&\phi(a)\phi(b)
\end{aligned}$$

□

Exercise 0.58. *Let m and n are distinct positive integer, Show that $mZ \approx nZ$ implies False.*

Proof. Note that a ring isomorphism $\phi : mZ \to nZ$ is also a (additive) group isomorphism, therefore $\phi(m) = n$ or $-n$. Consider $\phi(m^2)$, we know $n^2 = \phi(m^2) = \phi(m \cdot m)$ since we are in Z, then $m \cdot \phi(m) = m \cdot (\pm n) = \pm mn$, we get $\pm m = n$ by cancellation (since Z is an integral domain). We know both m and n are positive, so $-m = n$ is impossible, therefore $m = n$, but we also know m and n are distinct. □

Exercise 0.59. *Let D an integral domain and let F be the field of quotient of D. For any field E that contains D, show that F is ring-isomorphic to some subfield of E.*

Proof. Consider the mapping $\phi(a/b) = ab^{-1}$, but we have to show that it **is** a mapping. For any a/b and c/d in F such that $a/b = c/d$, that is, $ad = bc$. Then $\phi(a/b) = ab^{-1} = ab^{-1}dd^{-1} = bcb^{-1}d^{-1} = cd^{-1} = \phi(c/d)$ (recall that E is commutative).

We claim ϕ is a homomorphism from F to E, for any a/b $c/d \in F$ (We denote $+_F$ as the addition of F and $+$ as the addition of E):

- $$\begin{aligned}&\phi(a/b +_F c/d)\\ =&\phi((ad+bc)/bd)\\ =&(ad+bc)(bd)^{-1}\\ =&add^{-1}b^{-1} + bcd^{-1}b^{-1}\\ =&ab^{-1} + cd^{-1}\\ =&\phi(a/b) + \phi(c/d)\end{aligned}$$

- $$\begin{aligned}&\phi(a/b \cdot c/d)\\ =&\phi(ac/bd)\\ =&ac(bd)^{-1}\\ =&ab^{-1}cd^{-1}\\ =&\phi(a/b)\phi(c/d)\end{aligned}$$

Further more, we hope that ϕ is also one-to-one, suppose $\phi(a/b) = \phi(c/d)$, we know $ab^{-1} = cd^{-1}$ and then $ad = bc$, which implies $a/b = c/d$.

Therefore, $F \approx \phi(F)$ where $\phi(F)$ is a subfield of E (it is a field since F is a field). □

Theorem 0.2 (Division Algorithm for $F[x]$)**.** *Let F be a field and $f(x)$ $g(x) \in F[x]$ where $g(x) \neq 0$. Then there are unique $q(x)$ $r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.*

Proof. If $\deg f(x) < \deg g(x)$, then $q(x) = 0$ and $r(x) = f(x)$, otherwise, we induction/recursion on the degree of $f(x)$: Let $m = \deg f(x)$ and $n = \deg g(x)$,

- Base: For any $g(x)$, if $0 \geq n$ which implies $n = 0$, then there is q such that $f(x) = g(x) \times q + 0$ and $0 = 0$.

- Induction: For any $f(x)$ with degree belows m, and any $g(x)$, there are $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, then there are q such that $f_m = g_n \times q$, also, by induction hypothesis, we know there are $q'(x)$ and $r(x)$ such that $f(x) - g(x)qx^{m-n} = g(x)q'(x) + r(x)$, which is in fact $f(x) = g(x)q'(x) + r(x) + g(x)qx^{m-n} = g(x)(q'(x) + qx^{m-n}) + r(x)$.

The result is unique by comparing the degree. □

Corollary 0.5 (Remainder Theorem)**.** *Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.*

Proof. Induction on the degree of $f(x)$ with hypothesis: Let $n = \deg F[x]$, $m \in F$, then $f(a) + ma^{n+1}$ is the remainder in the division of $f(x) + max^n$ by $x - a$.

- Base: Let $n = 0$, $m \in F$, then the remainder in the divison of $f(x) + max^0 = f_0 + ma$ by $x - a$ is obviously $f_0 + ma = f(a) + ma^{0+1} = f(a) + ma$.

- Induction: Let $n = \deg f(a)$, $m \in F$, the remainder in the division of $f(x) + max^n$ by $x - a$ is the divison of $f(x) + max^n - (f_n + ma)x^{n-1}(x - a) = f'(x) + (f_n + ma)x^{n-1}a$ by $x - a$ where $f'(x) = f(x) - f_n x^n$. By induction hypothesis, we know the remainder in the divison of $f'(x) + (f_n + ma)x^{n-1}$ by $x - a$ is $f'(a) + (f_n + ma)a^{n-1+1} = f'(a) + (f_n + ma)a^n = f(a) + ma^{n+1}$.

Then, choose $m = 0$, we get $f(a)$ is the remainder is the divison of $f(a)$ by $x - a$.

The Path: It doesn't work that we induction on the origin proposition, we need to prove that $f(x) - f_n x^{n-1}(x - a) = f'(x) + f_n x^{n-1}a$ divided by $x - a$ produces the remainder we want. Therefore, we need a weaker induction hypothesis. By comparing with the origin proposition, we find that we can prove the origin proposition by replacing f_n with 0 if the new induction hypothesis is true. □

Corollary 0.6 (Factor Theorem)**.** *Let F be a field, $a \in F$ and $f(x) \in F[x]$, then a is a zero of $f(x)$ (i.e. $f(a) = 0$) iff $x - a$ is a factor of $f(x)$.*

Proof.

- ($\Rightarrow$) If $f(a) = 0$, then by Corollary 16.1.
- ($\Leftarrow$) If $x - a$ is a factor of $f(x)$, then the remainder is 0. By Corollary 16.1, we know $f(a)$ is the remainder in the division of $f(x)$ by $x-a$, then $f(a) = 0$, which implies a is a zero of $f(x)$.

□

Theorem 0.3 (Polynomials of Degree n Have at Most n Zeros)**.** *A polynomials of degree n over a field has at most n zeros.*

Proof. We induction on n.

- Base: A polynomials with degree 0 has 0 zero (recall that $f(x) = 0$ has no degree).
- Induction: For any $f(x) \in F[x]$, if $f(x)$ has no zero, then trivial. Suppose $f(a) = 0$ for some $a \in F$, then $f(x) = (x - a)q(x)$. By induction hypothesis, we know $q(x)$ has at most $n - 1$ (1 comes from $\deg(x - a)$) zeros (note that a can be the zero of $q(x)$), then $f(x)$ has at most $n-1+1$ zeros: $q(x)$ has at most $n - 1$ zeros, $(x - a)$ has only one zero (a).

We may count duplicate zeros at once, by replacing $(x - a)$ with $(x - a)^k$, so that $q(a)$ won't be 0. □

Theorem 0.4 ($F[x]$ is a principal integral domain)**.** *Let F be a field, then $F[x]$ is a principal integral domain.*

Proof. F is an integral domain, so is $F[x]$. For any ideal I, let $f(x) \in I$ where $\deg f(x)$ is smallest in I beside the element 0, we claim $\langle f(x)\rangle = I$. For any element $g(x)$ in I, we know $f(x) = g(x)q(x) + r(x)$, then $r(x) = f(x) - g(x)q(x) \in I$. We know $r(x) = 0$ or $\deg r(x) < \deg f(x)$, if $r(x) = 0$, then $g(x) \in \langle f(x)\rangle$, otherwise, $\deg r(x) < \deg f(x)$ contradicts the selection of $f(x)$. Therefore, $I \subseteq \langle f(X)\rangle$.

The Path: We may suppose the proposition is true, and find out what properties the generator should hold. Obviously, it has to have the smallest degree, unless it will unable to generate the element those have smaller degree. Also, it is easy to see that any element with the smallest degree is acceptable since F is a field, we can always get other elements by multiple a field element (degree 0). □

Exercise 0.13. *Let $\phi : R \to S$ a ring homomorphism, define $\overline{\phi} : R[x] \to S[x]$ by $\overline{\phi}(a_n x^n + a_{n-1}x^{n-1} + \dots) = \phi(a_n)x^n + \phi(a_{n-1})x^{n-1} + \dots$. Show that $\overline{\phi}$ is a ring homomorphism.*

Exercise 0.14. *If R and S are ring isomorphic, then $R[x]$ and $S[x]$ are ring isomorphic.*

Exercise 0.16. *Let $f(x)$ and $g(x)$ are cubic polynomials with integer coefficients such that $f(a) = g(a)$ for four (distinct) integer values a. Prove that $f(x) = g(x)$, Generalize.*

Proof. Consider $h(x) = f(x) - g(x)$, $\deg h(x) \leq 3$, therefore there are at most 3 zeros. However, we found that there are four values a such that $f(a) - g(a) = 0$, so $h(x) = 0 \to f(x) = g(x)$.

Moreover, we can show that any polynomials with degree n is determined by $n + 1$ points. □

Exercise 0.19 (Degree Rule)**.** *Let D be an integral domain and $f(x)$ $g(x) \in D[x]$. Prove that* $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Proof. Let $n = \deg f(x)$ and $m = \deg g(x)$. Degree is determined by the leading term, while the leading term of $f(x)g(x)$ is $f_n x^n g_m x^m = f_n g_m x^{n+m}$. $f_n g_m$ will never be 0, since D is an integral domain. □

Exercise 0.32. *Give an example of a polynomial of $Z_5[x]$ of positive degree that has the property that $f(a) = 1$ for all $a \in Z_5$.*

Proof. Try $(x-4)(x-3)(x-2)(x-1)x + 1$, normalized $x^5 + 4x + 1$.

The Path: I was trying to find it directly, but I failed, cause I assume that its degree is lower than 5, which is an unappropriate assumption, because $x^5 = x$ is the key of this problem.

Moreover, consider $f(x) = x^p + (p-1)x + 1$ for some prime p, we have $f(a) = 1$ for all $a \in Z_p$. □

Exercise 0.43. *Let F a field, $f(x)$ and $g(x)$ in $F[x]$ and not both zero. If there is no polynomial of positive degree in $F[x]$ that divides both $f(x)$ and $g(x)$, prove that there exist polynomials $h(x)$ and $k(x)$ in $F[x]$ such that $f(x)h(x) + g(x)k(x) = 1$.*

Proof. This problem can be solved by showing $1 \in \langle f(x), g(x) \rangle$. Consider the ideal $\langle f(x), g(x) \rangle$, we know it is principal ideal so that there is $h(x) \in F[x]$

such that $\langle h(x)\rangle = \langle f(x), g(x)\rangle$. We also know $h(x)$ has the minimum degree in $\langle f(x), g(x)\rangle$ and there are $s(x)$ $t(x) \in F[x]$ such that $h(x)s(x) = f(x)$ and $h(x)t(x) = g(x)$, therefore $h(x)$ has to have degree 0. So $h(x) = h_0$ and $h_0 h_0^{-1} \in \langle h(x)\rangle$ since $\langle h(x)\rangle$ is an ideal.

We know every element in $\langle f(x), g(x)\rangle$ has form $f(x)h(x) + g(x)k(x)$ for some $h(x)$ $k(x) \in F[x]$ and $1 \in \langle f(x), g(x)\rangle$. □

Exercise 0.44. *Let F a field, $f(x)$ and $g(x)$ in $F[x]$ and not both zero. A polynomial $d(x) \in F[x]$ is said to be a greatest common divisor of $f(x)$ and $g(x)$ if $d(x)$ divides both $f(x)$ and $g(x)$, and $d(x)$ has maximum degree among all such polynomials. Prove that $\langle f(x), g(x)\rangle = \langle d(x)\rangle$, and there is a unique monic gcd.*

Proof. Trivial. □

Exercise 0.57. *For every prime p, show that $x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-2))(x-(p-1))$ in $Z_p[x]$.*

Proof. It is easy to see that both side have degree $p-1$, and for any element $a \in Z_p$, a is a zero of both side, therefore they are equal to each other (See Exercise 16.16). □

Exercise 0.58 (Wilson's Theorem)**.** *For every integer $n > 1$, prove that $(n-1)! = n-1 \pmod{n}$ iff n is prime.*

Proof.

- ($\Rightarrow$) Suppose n is not prime and does **NOT** have form p^2 where p is prime, then there is a pair of zero-divisor that makes the left hand side zero. So we suppose $n = p^2$, then the product of all element in $U(p^2) \cup \{p\}$ is $n-1$, then $p = (n-1)(\text{product of } U(p^2))^{-1} \in U(p^2)$.

- ($\Leftarrow$) By let x in Exercise 16.57 be 0, we know $-1 = (-1)^{n-1}(n-1)!$, recall that $-1 = n-1$ in Z_n (even n is not prime) and $a^{n-1} = 1$ in $U(n)$, since $|U(n)| = n-1$. So $n-1 = 1(n-1)!$.

□

Exercise 0.66. *Let R a commutative ring with unity, I is a prime ideal of R. Prove that $I[x]$ is a prime ideal of $R[x]$.*

Proof. For any $f(x)$ $g(x) \in R[x]$ where $f(x)g(x) \in I[x]$, we induction on $(\deg f(x), \deg g(x))$.

- Base (Left): If $\deg f(x) = 0$, since each coefficients are in I, we know that either $f_0 \in I$ or $g(x) \in I[x]$. If $f(x) = 0$, then trivial.
- Base (Right): Ditto.
- Induction: Suppose $\deg f(x) = m$ and $\deg g(x) = n$ where m and n are positive. Consider the leading coefficient of $f(x)g(x)$, it is produced by $f_m g_n$, therefore, one of them is in I. We may suppose $f_m \in I$, otherwise we just swap them. Then $f(x)g(x) = f_m g(x) + f'(x)g(x)$ (where $f'(x)$ is $f(x)$ without leading coefficient), we know $f_m g(x) \in I[x]$ since $f_m \in I$, then by induction hypothesis, we know either $f'(x)$ or $g(x)$ in $I[x]$. If $f'(x) \in I[x]$, so is $f(x) = f_m x^m + f'(x)$, otherwise, $g(x) \in I[x]$.

Note that we don't claim which one is in $I[x]$ at the beginning, cause we don't have sufficient information. □

Exercise 0.70. *Let F a field and let $I = \{\ f(x) \in F[x] \mid \forall a \in F, f(a) = 0\ \}$. Prove that I is an ideal of $F[x]$. Prove that I is infinite when F is finite and $I = \{0\}$ when F is infinite. Find a monic polynomial $g(x)$ such that $I = \langle g(x) \rangle$ when F is finite.*

Proof. I is an ideal cause:

- Non-empty
- For any $f(x)\ g(x) \in I$, $a \in F$, $f(a) + g(a) = 0$.
- For any $f(x) \in I$, $g(x) \in F[x]$, $a \in F$, $f(a)g(a) = 0g(a) = 0$

Suppose F is finite, then the polynomial $f(x) = (x - a_0)(x - a_1) \cdots$ where $a_i \in F$ is in I, and for any positive integer n, $f(x)x^n \in I$ with degree $\deg f(x) + n$, therefore I is infinite. If F is infinite, then there is no polynomial has infinite zeros except $f(x) = 0$.

If F is finite, the $f(x)$ above is such monic polynomial. □

Exercise 0.75. *Suppose F is a field and there is a ring homomorphism from Z onto F. Show that F is isomorphic to Z_p for some prime p.*

Proof. Why this exercise here...?

$Z/\operatorname{Ker}\phi$ has to be a integral domain, therefore $\operatorname{Ker}\phi = \langle p \rangle$. □

Definition 0.3 (Irreducible Polynomials)**.** *Let D an integral domain and $f(x) \in D[x]$ where $f(x)$ is neither zero polynomial nor a unit. We say $f(x)$ is irreducible over D, if $f(x) = g(x)h(x)$ where $g(x)$ $h(x) \in D[x]$, then one of them is unit. A nonzero, nonunit element of $D[x]$ is not irreducible over D is called reducible over D.*

Definition 0.4 (Content)**.** *The content of a non-zero polynomial is the greatest common divisor of the coefficients. A primitive polynomial is an element of $Z[x]$ with content 1.*

Theorem 0.5 (Gauss's Lemma)**.** *The product of two primitive polynomials is primitive.*

Proof. This proof comes from textbook.

Suppose $f(x) = g(x)h(x)$ where $g(x)$ $h(x)$ are primitive. If $f(x)$ is not primitive, then we denote n as the content of $f(x)$, then p divides n where p is prime. Consider $\overline{f}(x)\,\overline{g}(x)\,\overline{h}(x)$, which are polynomials with coefficients mod p.

Then $\overline{f}(x)$ is a zero polynomial in $Z_p[x]$ since the content of $f(x)$ is dividible by p. We know $Z_p[x]$ is an integral domain since Z_p is an integral domain, then either $g(x)$ or $h(x)$ is a zero polynomial, which means the content of $g(x)$ or $h(x)$ is dividible by p, which contradicts to the assumption that $g(x)$ and $h(x)$ are primitive. □

Lemma 0.1. *If $f(x)$ is reducible, then $(n \cdot 1)f(x)$ is reducible where n is a positive integer.*

Proof. Suppose $f(x) = g(x)h(x)$ where both not unit, then $(n \cdot 1)f(x) = (n \cdot 1)g(x)h(x)$. We claim $(n \cdot 1)g(x)$ is not unit. If $(n \cdot 1)g(x)$ is an inverse $\overline{g}$, then $(n \cdot 1)g(x)\overline{g} = g(x)(n \cdot 1)\overline{g} = 1$, therefore $g(x)$ is a unit. (Recall that a polynomial ring is commutative). □

Theorem 0.6. *Let $f(x) \in Z[x]$, if $f(x)$ is reducible over Q, then it is reducible over Z.*

Proof. This proof comes from textbook.

Suppose $f(x) = g(x)h(x)$ where $g(x)$ $h(x) \in Q[x]$ and both not unit. We may suppose $f(x)$ is primitive, otherwise by Lemma 17.1, $nf(x)/n$ is reducible where n is the content of $f(x)$. Let a and b are the lcm of denominators of $g(x)$ and $h(x)$ respectively, then $abf(x) = ag(x)bh(x)$. Furthermore, we may divide $ag(x)$ and $bh(x)$ by their contents, now $abf(x) = cg'(x)dh'(x)$ where c d are the contents of $ag(x)$ $bh(x)$ respectively. We know $g'(x)$ and $h'(x)$ are

primitive, so is $g'(x)h'(x)$. Then the content of right hand side is cd and left hand side is ab. Then $f(x) = g'(x)h'(x)$, it is easy to show $g'(x)$ and $h'(x)$ is not unit.

Furthermore, those two polynomials have non-zero degrees, if $f(x)$ is primitive, and $\deg g'(x) = \deg cg'(x) = \deg ag(x) = \deg g(x)$, which implies $g(x)$ is a unit; if $f(x)$ is not primitive, then $f(x)/n$ can be expressed as two polynomials with non-zero degree, so is $nf(x)/n$. □

Theorem 0.7. *Let p a prime and $f(x) \in Z[x]$ with $\deg f(x) \geq 1$. Let $\overline{f}(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\overline{f}(x)$ is irreducible over Z_p and $\deg \overline{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over Q.*

Proof. This proof comes from textbook.

Suppose $f(x)$ is reducible over Q, then $f(x)$ is reducible over Z. Then $f(x) = g(x)h(x)$ where $g(x)$ $h(x) \in Z[x]$ and both not unit, and $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. We know $\deg f(x) = \deg \overline{f}(x)$, then $\deg g(x) = \deg \overline{g}(x)$ and $\deg h(x) = \deg \overline{h}(x)$ cause reducing coefficients of modulo p doesn't increase the degree. Then we know both $\overline{g}(x)$ and $\overline{h}(x)$ are not unit (cause they have non-zero degree), then $\overline{f}(x)$ is reducible over Z_p. □

Theorem 0.5. *Let F a field and $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ iff $p(x)$ is irreducible over F.*

Proof.

- ($\Rightarrow$) If $p(x) = g(x)h(x)$ for some $g(x)$ $h(x) \in F[x]$, we know $\langle p(x) \rangle$ is a prime ideal since it is maximal, then one of $g(x)$ and $h(x)$ is in $\langle p(x) \rangle$. We may suppose $g(x) \in \langle p(x) \rangle$, then $g(x)$ is either zero or $\deg g(x) \geq \deg p(x)$, but $g(x) \neq 0$ and $\deg g(x) \leq \deg p(x)$ (since $p(x) = g(x)h(x)$), therefore $\deg g(x) = \deg p(x)$ and then $\deg h(x) = 0$, which implies $h(x)$ is a unit.

- ($\Leftarrow$) Suppose I is an ideal that properly contains $\langle p(x) \rangle$, we know $F[x]$ is a principal ideal domain. Suppose $I = \langle q(x) \rangle$ for some $q(x)$, then we know $p(x)$ can be expressed by $q(x)r(x)$ for some $r(x)$ since $p(x) \in \langle q(x) \rangle$. Then one of $q(x)$ and $r(x)$ is unit, if $q(x)$ is unit, then $1 \in \langle q(x) \rangle$, if $r(x)$ is unit, then $q(x) = p(x)r^{-1}(x)$, which implies $q(x) \in \langle p(x) \rangle$, it contradict to the assumption that I properly contains $\langle p(x) \rangle$.

□

Corollary 0.7. *Let $p(x)$ a irreducible polynomial of $F[x]$ and $p(x) \mid a(x)b(x)$. Then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.*

Proof. By Theorem 17.5, we know $\langle p(x) \rangle$ is a maximal ideal, therefore it is a prime ideal. The rest of proof is trivial. □

Corollary 0.8. *Let $f(x)$ is irreducible polynomial of $F[x]$, then $F[x]/\langle f(x) \rangle$ is a field.*

Proof. By Theorem 0.5 and Theorem 14.4. □

Theorem 0.6 (Unique Factorization)**.** *Every polynomial in $Z[x]$ that is not a zero polynomial or a unit in $Z[x]$ can be expressed in the form*

$$\boxed{b_0 b_1 \dots b_{s-1} p_0(x) p_1(x) \dots p_{m-1}(x)}$$

where the b_i's are irreducible polynomials of degree 0 (In other words, they are primes), and $p_i(x)$'s are irreducible polynomials of positive degree.

Furthermore, if is can be expressed in two ways, then they have the same s and m, and they have the same b_i's and p_i's with $\pm$ if needed.

Proof. Let $f(x) \in Z[x]$ where $f(x)$ is not a zero polynomial and not a unit in $Z[x]$. Induction on the degree of $f(x)$.

- Base: we can written $f(x) = f_0$ in the product of primes, and we know that is a unique factorization.
- Ind: We can always express $f(x)$ in form $cg(x)$ where c is the content of $f(x)$ when $f(x)$ is not primitive, then c has unique factorization. We need to show that $g(x)$ has unique factorization. If $g(x)$ is irreducible, then we the only factorization of $g(x)$ is itself. If $g(x)$ is reducible, we know there is $p(x) \in Z[x]$ such that $p(x) \mid g(x)$ and $p(x)$ is irreducible and primitive. We know $p(x)$ must be contained in every factorization of $g(x)$ by Corollary 17.1, then by induction hypothesis, $g(x)/p(x)$ has unique factorization and $g(x) = p(x)g(x)/p(x)$.

□

Exercise 0.76. *Suppose that D is an integral domain and F is a field that containing D. If $f(x) \in D[x]$ and $f(x)$ is irreducible over F but reducible over D, what can we say about the factorization of $f(x)$ over D.*

Proof. There must be a polynomial of degree 0 that is not a unit in D but a unit in F and that polynomial divides $f(x)$. □

Exercise 0.3. *Show that a non-constant polynomial from $Z[x]$ that is irreducible over Z is primitive.*

Proof. Let $f(x) \in Z[x]$ that is irreducible over Z and non-constant. Let c be the content of $f(x)$. We know $\deg f(x) > 0$ since it is non-constant. If c is not 1, then by $f(x) = cf(x)/c$, we know $f(x)/c$ is a unit since $f(x)$ is irreducible and c is not a unit. However, $\deg f(x)/c = \deg f(x) > 0$, that means $f(x)$ is not a unit since Z is an integral domain. □

Exercise 0.4. *Let $f(x) \in Z[x]$ where the leading coefficient of $f(x)$ is 1. Let r a rational number and $(x - r)$ divides $f(x)$, show that r is an integer.*

Proof. We denote $x - r$ by $g(x)$ and $f(x)/g(x)$ by $h(x)$. Suppose $r = \frac{s}{t}$ where $\gcd(s, t) = 1$, and let q be the lcm of the denominators of the coefficients of $h(x)$. Then both $tg(x)$ and $qh(x)$ are in $Z[x]$, and now $tqf(x) = tg(x)qh(x)$. Let a be the content of $tg(x)$ and b be the content of $qh(x)$, we observe that a is 1 since $\gcd(t, s) = 1$, therefore $tqf(x) = 1(tg(x)/1)b(qh(x)/b)$. The content of lhs is tq (since the leading coefficient of $f(x)$ is 1), and the content of rhs is b (since both $(tg(x))/1$ and $(qh(x)/b)$ are primitive, so is their product), so $b = tq$. Since $(qh(x))/b = (qh(x))/(tq) = h(x)/t \in Z[x]$, so is $h(x)$, therefore q is 1. Since both $f(x)$ and $g(x)$ are monic, so is $h(x)$, therefore the content of $qh(x) = h(x)$ is 1, so $b = 1$, therefore $1 = t$, which implies r is an integer.

The following proof comes from MathStackExchange. Suppose $r = \frac{s}{t}$. Since $x - r$ divides $f(x)$, we know $f(r) = s^n t^{-n} + a_{n-1}(s^{n-1}t^{-n+1}) + \cdots + a_0 = 0$. We may mutiply both side by t^{n-1} so that every term except the leading term is an integer, that is, $t^{n-1}f(r) = s^n t^{-1} + a_{n-1}(s^{n-1}) + a_{n-2}(s^{n-2}p) + \cdots + a_0 p^{n-1} = 0$. Therefore $s^n t^{-1}$ is an inverse under addition of another integer, then $s^n t^{-1}$ has to be an integer, then $t = 1$, which implies r is an integer. □

Mistake. *Suppose $f(x) = g(x)h(x)$, where $f(x)$ $g(x) \in Z[x]$, then $h(x)$ needs not in $Z[x]$*

Proof. It is impossible to show that $h(x)$ has to be an element of $Z[x]$ by Z is UFD (Theorem 17.6), cause the factorization of $g(x)$ may not be contained in the factorization of $f(x)$ when $h(x)$ is NOT in $Z[x]$. Also, dividing the factorization of $h(x)$ from $f(x)$ is actually performed under Q, not Z (when $h(x)$ is not in $Z[x]$).

Counterexample: $f(x) = 1 = 2(1/2)$. □

Exercise 0.5. *Let F a field and let a be a nonzero element of F.*

- *If $af(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.*
- *If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.*
- *If $f(a+x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.*
- *Use the third property to prove $8x^3 - 6x + 1$ is irreducible over Q.*

Proof.

- Suppose $f(x) = g(x)h(x)$, then $af(x) = ag(x)h(x)$ and we know $ag(x)$ is a unit or $h(x)$ is a unit by $af(x)$ is irreducible.
- Suppose $f(x) = g(x)h(x)$, then by $f(ax) = g(ax)h(ax)$ is irreducible, we may suppose $g(ax)$ is a unit. Then $\deg g(ax) = 0 = \deg g(x)$, therefore $g(ax) = g(x)$ and $g(x)$ is a unit.
- Ditto
- ???

□

Exercise 0.6. *Let F a field and $f(x) \in F[x]$, let a the leading coefficient of $f(x)$, then $a^{-1}f(x)$ is irreducible implies $f(x)$ is irreducible. Note that $a^{-1}f(x)$ is monic (the leading coefficient is 1).*

Proof. Suppose $f(x) = g(x)h(x)$, then $a^{-1}f(x) = a^{-1}g(x)h(x)$ and one of $a^{-1}g(x)$ and $h(x)$ is unit, if $h(x)$ is unit, then trivial. If $a^{-1}g(x)$ is unit, then $g(x)$ is unit with inverse $a^{-1}(a^{-1}g(x))^{-1}$. □

Exercise 0.10. *Suppose that $f(x) \in Z_p[x]$ and $f(x)$ is irreducible over Z_p, where p is a prime. If $\deg f(x) = n$, prove that $Z_p[x]/\langle f(x)\rangle$ is a field with p^n elements.*

Proof. $Z_p[x]/\langle f(x)\rangle$ is a field by Corollary 17.2. Every distinct element in $Z_p[x]$ with degree that below $\deg f(x)$ implies distinct element in $Z_p[x]/\langle f(x)\rangle$, cause they will never produce an element in $\langle f(x)\rangle$, unless they are equal to each other. Therefore $Z_p[x]/\langle f(x)\rangle$ has the same elements as $(Z_p)_0 \oplus (Z_p)_1 \oplus \cdots \oplus (Z_p)_{n-1}$ (the coefficients), which is exactly p^n. □

Exercise 0.18. *Let $f(x) \in Z_2[x]$ and $\deg f(x) = 5$. If neither 0 nor 1 is a zero of $f(x)$. Show that it is sufficient to prove that $f(x)$ is irreducible over Z_2 by showing $x^2 + x + 1$ is not a factor of $f(x)$.*

Proof. Since $f(x)$ has no zero, we know there is no factor with degree 1. Since $f(0) = 1$, we know $f_0 = 1$, therefore any factor $g(x)$ of $f(x)$ must has the property $g(0) = 1$. Now consider $x^2 + 1$, obviously 1 is a zero, but $f(x)$ does not have one. For any factor with degree $n > 2$, we know it must have a factor with degree $5 - n \leq 2$. Therefore the last cast is $x^2 + x + 1$, comes from the hypothesis. □

Exercise 0.19. *For the field $Z_7[x]/I$ where $I = \langle x^2 + 2 \rangle$. Find the multiplicative orders of $x + I$ and $x + 1 + I$. Find the multiplicative inverse of $x + I$.*

Proof. By Exercise 17.10, we know $|Z_7[x]/I| = 7^2 = 49$, therefore the order of the multiplicative group of $Z_7[x]$ is 48. It is easy to see that $x^2 = -2$, and $|-2| = |5| = 6$ since $-2 \in U(7)$, therefore $(x^2)^6 = 1$. Since $|x| \neq 1$, $|x|$ is even (otherwise $x^{|x|}$ would have degree 1) and $|x| \geq 12$ (otherwise $|-2|$ will no longer 6), we know that $|x| = 12$. By simply calculate $(x + 1)^4 = 3x$, we see $(x + 1)^{24} = 1$. We need to show that $3, 6, 12$ can not be the order of $x + 1$:

- By $(x + 1)^7 = x^7 + 1 = 6x + 1$ (since $\operatorname{char} Z_7[x]/I = 7$), we know $|x + 1| \neq 6$, otherwise $6x + 1 = x + 1$.
- $|x + 1| \neq 12$ by $|(x + 1)^4| = 6 \neq 3$.
- $|x + 1| \neq 3$ since $(x + 1)^4 = 3x$ and $3x \neq x + 1$.

It is easy to see that $3x$ is an inverse of x since $-6 = 1$. □

Exercise 0.20. *Let F be a field and $f(x) \in F[x]$ be reducible over F with $\deg f(x) > 1$. Prove that $F[x]/\langle f(x) \rangle$ is not an integral domain.*

Proof. By Theorem 14.3, we only need to show that $\langle f(x) \rangle$ is not a prime ideal. Since $f(x)$ is reducible, we know $f(x) = g(x)h(x)$ and both $g(x)$ and $h(x)$ are not unit. We also know that $\deg g(x)$ and $\deg h(x)$ are lower than $\deg f(x)$, therefore both $g(x)$ and $h(x)$ are not in $\langle f(x) \rangle$, which implies $\langle f(x) \rangle$ is not a prime ideal. □

Exercise 0.32. *Let $f(x) \in Z_p[x]$ (or any field). Prove that $f(x)$ has no quadratic factor over Z_p if $f(x)$ has no factor of the form $x^2 + ax + b$.*

Proof. For any quadratic factor of $f(x)$, it has the form $ax^2 + bx + c$, then $ax^2 + bx + c = a(x^2 + a^{-1}bx + a^{-1}c)$, which is impossible. □

Exercise 0.34. *Given that π is not the zero of a nonzero polynomial with rational coefficients, prove that π^2 cannot be written in the form $a\pi + b$, where a b are rational.*

Proof. Consider $f(x) = -x^2 + ax + b$, then π is not the zero of $f(x)$, therefore $\pi^2 \neq a\pi + b$. □

Exercise 0.35 (Rational Root Theorem)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in Z[x]$ with degree n. If r and s are relatively prime integers and $f(\frac{r}{s}) = 0$, show that $r \mid a_0$ and $s \mid a_n$.*

Proof. We know $(x - \frac{r}{s})$ divides $f(x)$ since $f(\frac{r}{s}) = 0$, so does $sx - r$. Therefore there must be $c \in Z$ such that $sxcx^{n-1} = a_n x^n$, which implies $sc = a_n$ and then $s \mid a_n$. Similarly, at the final step of division, there is $c \in Z$ such that $rc = a_0$. □

Exercise 0.38. *If p is a prime, prove that $f(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1$ is irreducible over Q.*

Proof. If $p = 2$, then $x + 1$ is irreducible over Q. If $p \neq 2$, then p is an odd integer, we need to show that $f(-x) = x^{p-1} - (-x^{p-2}) + x^{p-3} - \cdots - (-x) + 1$ is irreducible over Q. It follows that the pth Cyclotomic Polynomial is irreducible over Q when p is a prime. (Corollary of Theorem 17.4, I am sorry that it is not in my note) □

Exercise 0.39. *Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If E a field and $F \subseteq E$ and $a \in E$ such that $p(a) = 0$. Show that the mapping $\phi(f(x)) = f(a) : F[x] \to E$ is a ring homomorphism with kernel $\langle p(x) \rangle$.*

Proof. It is easy to see that $\phi(f(x) + g(x)) = f(a) + g(a) = \phi(f(x)) + \phi(g(x))$ and $\phi(f(x)g(x)) = f(a)g(a) = \phi(f(x))\phi(g(x))$.

We first show that $\deg p(x)$ is minimal such that $p(a) = 0$. Let $f(x) \in F[x]$ a non-zero element with minimal degree such that $f(a) = 0$, then we know $p(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. Then $p(a) = f(a)q(a) + r(a)$ which is $0 = 0 + r(a)$, therefore $r(a) = 0$ and then $r(x) = 0$, otherwise it contradicts to the assumption that $\deg f(x)$ is minimal such that $f(a) = 0$. Then $p(x) = f(x)q(x)$, since $p(x)$ is irreducible over F, and $f(x)$ is

not a unit (since $f(x) \neq 0$ and $f(a) = 0$), therefore $q(x)$ is a unit, and then $\deg f(x) = \deg p(x)$.

For any $f(x) \in F[x]$ such that $f(a) = 0$, we have $f(x) = p(x)q(x) + r(x)$, since $\deg p(x)$ is minimal such that $p(a) = 0$, we know $r(x) = 0$, therefore $p(x)$ divides $f(x)$, which means $f(x) \in \langle p(x) \rangle$.

The Path: I was trying to show that $p(x)$ divides $f(x)$ where $f(a) = 0$, but there is an annoying remainder, so I trying to show that $\deg p(x)$ is minimal by supposing a $g(x) \in F[x]$ such that $\deg g(x) \leq \deg p(x)$ and $g(a) = 0$. However, it is not enough, there is still a remainder, but I found that supposing $\deg g(x)$ is minimal such that $g(a) = 0$ may solve this problem. That is why I don't like LEM. □

Exercise 0.41. *Let F be a field and let $p(x) \in F[x]$ such that $p(x)$ is irreducible over F. Show that $\{ a + \langle p(x) \rangle \mid a \in F \}$ is a subfield of $F[x]/\langle p(x) \rangle$ that is isomorphic to F. For any $a + \langle p(x) \rangle$ and $b + \langle p(x) \rangle$, if $a + \langle p(x) \rangle = b + \langle p(x) \rangle$, then $a - b \in \langle p(x) \rangle$, which means $\langle p(x) \rangle = F[x]$ since $a - b \in F$ is a unit unless $a = b$. Therefore $a = b$, and it is isomorphic to F (bijective), therefore it is a field, and a subfield of $F[x]/\langle p(x) \rangle$.*

Exercise 0.43. *The polynomial $2x^2 + 4$ is irreducible over Q but reducible over Z. State a condition on $f(x)$ that makes the converse of Theorem 17.2 true.*

Proof. $f(x)$ is primitive. Then whenever $f(x)$ is reducible, it must be the product of two non-constant polynomial (otherwise $f(x)$ is no longer primitive), therefore it is reducible over Q. □

Definition 0.5 (Associates, Irreducibles, Primes)**.** *Let $a\ b \in D$ where D is an integral domain, a and b are called associates if $a = ub$ where u is a unit of D. If a is non-zero and not a unit, and whenever $a = bc$ for some $b\ c \in D$ implies b or c is a unit, then a is called irreducible. If a is non-zero and not a unit, and $a \mid bc$ implies $a \mid b$ or $a \mid c$, then a is called a prime.*

Theorem 0.7. *In an integral domain, every prime is an irreducible.*

Proof. Let D an integral domain and $p \in D$ a prime. Suppose $p = ab$ for some $a\ b \in D$, then $p \mid ab$ since $p = 1ab$, which implies $p \mid a$ or $p \mid b$, we may suppose $p \mid a$. Then $a = pc$ for some $c \in D$, therefore $p = pcb$. By cancellation (since we are in an integral domain) we know $1 = cb$, therefore b is a unit and $b^{-1} = c$. □

Theorem 0.8. *In a principal ideal domain, an element is irreducible iff it is a prime.*

Proof. Since a principal ideal domain is an integral domain, ($\Leftarrow$) is trivial.

($\Rightarrow$) Let P a principal ideal domain and $p \in P$, and suppose $I = \langle q \rangle$ an ideal (we know it has form $\langle q \rangle$ since we are in a principal ideal domain) such that $\langle p \rangle \subseteq \langle q \rangle$. Since $p \in \langle q \rangle$, we know $p = qr$ for some $r \in P$, according to p is irreducible, we know either q or r is unit. If q is unit, then $\langle q \rangle = P$. If r is unit, then $q = pr^{-1}$, therefore $q \in \langle p \rangle$ and $\langle p \rangle = \langle q \rangle$. This shows that $\langle p \rangle$ is a maximal ideal, therefore it is a prime ideal, and $\langle p \rangle$ is prime ideal implies p is prime. □

Lemma 0.2. *In a principal ideal domain, any strictly increasing chain of ideals $I_0 \subset I_1 \subset \dots$ must be finite.*

Proof. This proof comes from textbook.

Let D be that principal ideal domain and $I = I_0 \cup I_1 \cup \dots$, for any element $i \in I$ and $a \in D$, i must be an element of an ideal in the chain, say I_i, then $ia \in I_i \subseteq I$. Therefore I is an ideal.

then $I = \langle a \rangle$, and a must belongs to an ideal in the chain, say I_n. For any ideal I_m in the chain, we have $I_m \subseteq I_n$ since a divides the "generator" of I_m. Therefore I_n is the last member of the chain. □

Definition 0.6 (Unique Factorization Domain)**.** *An integral domain D is a unique factorization domain if:*

1. *Every non-zero element of D that is not a unit can be written as a product of irreducibles of D.*

2. *The factorization into irreducibles is unique* ***up to associates****.*

Therefore, $4 = 2 \times 2 = (-2) \times (-2)$ is considered "the same", cause 2 is associated with -2 by $2 = (-1)2$.

Theorem 0.9 (PID implies UFD)**.** *Every pincipal ideal domain is a unique factorization domain.*

Proof. Let D a principal ideal domain and $a \in D$ a non-zero, non-unit element.

We first show that for any reducible, there is an irreducible divides it. Suppose $a \in D$ is reducible, then $a = bc$ where $b\ c \in D$ are non-zero and non-unit. If b or c is irreducible, then trivial. If both b and c are reducible, then $\langle a \rangle \subset \langle b \rangle$, it is trivial that $\langle a \rangle \subseteq \langle b \rangle$, if $b \in \langle a \rangle$, then $b = ad$, which means $a = bc \to a = adc$, which implies c is a unit but it isn't. Then we perform this algorithm on b, and we have a strictly increasing chain of ideals $\langle a \rangle \subset \langle b \rangle \subset \dots$.

According to the Lemma 0.2, we know the chain is finite, therefore the algorithm must stop at some point. We found that the algorithm only stops when it meets an irreducible, therefore there is a irreducible divides a.

We repeat applying this algorithm to the factor of a, the factor of the factor of a and so on, then we have a series $a = p_0p_1p_2\dots$ where p_i are irreducibles. If this series is infinite, then $b = p_1p_2\cdots$ and $\langle a\rangle \subset \langle b\rangle$ (properly containing by p_0 is not a unit). Therefore, we have a infinite strictly increasing chain $\langle p_0p_1p_2\dots\rangle \subset \langle p_1p_2p_3\dots\rangle \subset \dots$ which is impossible. Therefore $a = p_0p_1\cdots p_n$ where p_i are irreducibles.

If $a = p_0p_1\cdots p_n = q_0q_1\cdots q_m$, we induction on n:

- Base: If $a = p_0 = q_0q_1\cdots q_m$, then p_0 must divides some q_i. Since q_i is irreducible, we know p_0 and q_i are associates. Then the product of the remaining irreducibles are a unit by cancellation, which only makes sense when there is no remaining irreducibles. Therefore $0 = m$.

- Induction: If $a = p_0p_1\cdots p_{n+1} = q_0q_1\cdots q_m$, then p_0 must divides some q_i

□

Exercise 0.44. *Let $N(a + b\sqrt{d}) = |a^2 - db^2|$ be the norm of $a + b\sqrt{d}$ where $a+b\sqrt{d} \in Z[\sqrt{d}]$ where d is not 1 and is not divisible by the square of a prime. Verify the following properties:*

1. *$N(x) = 0$ iff $x = 0$*
2. *$N(xy) = N(x)N(y)$*
3. *$N(x) = 1$ iff x is a unit*
4. *$N(x)$ is prime implies x is irreducible over $Z[\sqrt{d}]$*

Proof.

1. If $N(x) = 0$, then $a^2 = db^2$, however, d is not divisible by the square of any prime and a^2 is a product of some squares of prime, therefore $a = b = 0$.

2.

□