Math 361

January 25, 2023

Quiz

Let R be a ring.

1. What does it mean to say that $p \in R$ is prime?
2. What does it mean to say R is a integral domain?
3. Let R be a integral domain, and let $a, b, c \in R$. Suppose that $ab = ac$ and $a \neq 0$. Prove that $b = c$.

Rings

Definition. A *ring* is a set R with two operations, addition $+ \colon R \times R \to R$ and multiplication $\cdot \colon R \times R \to R$ satisfying the following axioms:

Rings

Definition. A *ring* is a set R with two operations, addition $+ \colon R \times R \to R$ and multiplication $\cdot \colon R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

Rings

Definition. A *ring* is a set R with two operations, addition $+ \colon R \times R \to R$ and multiplication $\cdot \colon R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

Rings

Definition. A *ring* is a set R with two operations, addition $+ \colon R \times R \to R$ and multiplication $\cdot \colon R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

Rings

Definition. A *ring* is a set R with two operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

Rings

Definition. A *ring* is a set R with two operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

(In the following, we follow the usual convention of writing ab for $a \cdot b$.)

Rings

Definition. A *ring* is a set R with two operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

(In the following, we follow the usual convention of writing ab for $a \cdot b$.)

M1. $ab = ba$ for all $a, b \in R$ (commutativity of multiplication).

Rings

Definition. A *ring* is a set R with two operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

(In the following, we follow the usual convention of writing ab for $a \cdot b$.)

M1. $ab = ba$ for all $a, b \in R$ (commutativity of multiplication).

M2. $a(bc) = (ab)c$ for all $a, b, c \in R$ (associativity of multiplication).

Rings

Definition. A *ring* is a set R with two operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

(In the following, we follow the usual convention of writing ab for $a \cdot b$.)

M1. $ab = ba$ for all $a, b \in R$ (commutativity of multiplication).

M2. $a(bc) = (ab)c$ for all $a, b, c \in R$ (associativity of multiplication).

M3. There exists an element $1 \in R$ such that $a1 = a$ for all $a \in R$ (multiplicative identity).

Rings

Definition. A *ring* is a set R with two operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

(In the following, we follow the usual convention of writing ab for $a \cdot b$.)

M1. $ab = ba$ for all $a, b \in R$ (commutativity of multiplication).

M2. $a(bc) = (ab)c$ for all $a, b, c \in R$ (associativity of multiplication).

M3. There exists an element $1 \in R$ such that $a1 = a$ for all $a \in R$ (multiplicative identity).

D. For all $a, b, c \in R$, we have $(a + b)c = ac + bc$.

Rings

Name all the rings you know.

Primes versus irreducibles

Let R be an integral domain. Then if p is prime, it follows that p is irreducible.

Ideals

Definition. A nonempty subset I of a ring R is an *ideal* if

1. I is closed under addition, and
2. if $r \in R$ and $a \in I$, then $ra \in I$.

Ideals

Definition. A nonempty subset I of a ring R is an *ideal* if

1. I is closed under addition, and
2. if $r \in R$ and $a \in I$, then $ra \in I$.

Definition. An ideal I in a ring R is *generated by* $a_1, \ldots, a_n \in R$ if every element of I is an R-linear combination of elements of $a_1, \ldots, a_n$, i.e., for all $a \in I$, we can write

$$a = \sum_{i=1}^{n} r_i a_i$$

for some elements $r_i \in R$. We then write

$$I = (a_1, \ldots, a_n).$$

Principal ideals

Definition. We say I is a *principal ideal* if it can be generated by a single element, i.e., if there exists $a \in R$ such that $I = (a) = \{ra : r \in R\}$, all multiples of a single element a of R.

Principal ideals

Definition. We say I is a *principal ideal* if it can be generated by a single element, i.e., if there exists $a \in R$ such that $I = (a) = \{ra : r \in R\}$, all multiples of a single element a of R.

Definition. An integral domain R in which every ideal is principal is called a *principal ideal domain*, abbreviated PID.

Primes versus irreducibles

Let R be a ring. We have seen that if $p \in R$ is prime, then it is irreducible. If R is a PID, the converse is true.

Primes versus irreducibles

Let R be a ring. We have seen that if $p \in R$ is prime, then it is irreducible. If R is a PID, the converse is true.

Proof. Math 332.

PID $\Rightarrow$ UFD

Proposition. Let R be a principal ideal domain. Then R is a *unique factorization domain* (UFD):

PID $\Rightarrow$ UFD

Proposition. Let R be a principal ideal domain. Then R is a *unique factorization domain* (UFD): Let $r \in R$. Then r has a factorization

$$r = u \prod_{n=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are prime, each e_i is a positive integer, and $k \in \mathbb{N}$.

PID $\Rightarrow$ UFD

Proposition. Let R be a principal ideal domain. Then R is a *unique factorization domain* (UFD): Let $r \in R$. Then r has a factorization

$$r = u \prod_{n=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are prime, each e_i is a positive integer, and $k \in \mathbb{N}$. The factorization is unique in the following sense; if $r = v \prod_{i=1}^{\ell} q_i^{f_i}$ for some unit v, primes q_i, positive integers f_i, and $\ell \in \mathbb{N}$,

PID $\Rightarrow$ UFD

Proposition. Let R be a principal ideal domain. Then R is a *unique factorization domain* (UFD): Let $r \in R$. Then r has a factorization

$$r = u \prod_{n=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are prime, each e_i is a positive integer, and $k \in \mathbb{N}$. The factorization is unique in the following sense; if $r = v \prod_{i=1}^{\ell} q_i^{f_i}$ for some unit v, primes q_i, positive integers f_i, and $\ell \in \mathbb{N}$, then $k = \ell$ and up to re-indexing, $p_i = u_i q_i$ with u_i a unit and $e_i = f_i$ for all i.

PID $\Rightarrow$ UFD

Proposition. Let R be a principal ideal domain. Then R is a *unique factorization domain* (UFD): Let $r \in R$. Then r has a factorization

$$r = u \prod_{n=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are prime, each e_i is a positive integer, and $k \in \mathbb{N}$. The factorization is unique in the following sense; if $r = v \prod_{i=1}^{\ell} q_i^{f_i}$ for some unit v, primes q_i, positive integers f_i, and $\ell \in \mathbb{N}$, then $k = \ell$ and up to re-indexing, $p_i = u_i q_i$ with u_i a unit and $e_i = f_i$ for all i.

Proof. Math 332.

PID $\Rightarrow$ UFD

Proposition. Let R be a principal ideal domain. Then R is a *unique factorization domain* (UFD): Let $r \in R$. Then r has a factorization

$$r = u \prod_{n=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are prime, each e_i is a positive integer, and $k \in \mathbb{N}$. The factorization is unique in the following sense; if $r = v \prod_{i=1}^{\ell} q_i^{f_i}$ for some unit v, primes q_i, positive integers f_i, and $\ell \in \mathbb{N}$, then $k = \ell$ and up to re-indexing, $p_i = u_i q_i$ with u_i a unit and $e_i = f_i$ for all i.

Proof. Math 332.

So a PID is a UFD and there is no difference between primes and irreducibles.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done. Otherwise, let a be the smallest positive element of I.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done. Otherwise, let a be the smallest positive element of I. Given any element $b \in I$, apply the division algorithm to find $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done. Otherwise, let a be the smallest positive element of I. Given any element $b \in I$, apply the division algorithm to find $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$. Since $a, b \in I$, and I is an ideal,

$$r = b - aq \in I.$$

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done. Otherwise, let a be the smallest positive element of I. Given any element $b \in I$, apply the division algorithm to find $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$. Since $a, b \in I$, and I is an ideal,

$$r = b - aq \in I.$$

By the definition of a, it follows that $r = 0$.

$\mathbb{Z}$ is a PID

Proposition. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done. Otherwise, let a be the smallest positive element of I. Given any element $b \in I$, apply the division algorithm to find $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$. Since $a, b \in I$, and I is an ideal,

$$r = b - aq \in I.$$

By the definition of a, it follows that $r = 0$. Hence, $b = aq$. We have shown that $I = (a)$.

Division algorithm in $K[x]$

Proposition. (Division algorithm) Let K be a field, and let $f, g \in K[x]$ with $f \neq 0$. Then there exists $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

Division algorithm in $K[x]$

Proposition. (Division algorithm) Let K be a field, and let $f, g \in K[x]$ with $f \neq 0$. Then there exists $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

Proof. Math 332.

Division algorithm in $K[x]$

Proposition. (Division algorithm) Let K be a field, and let $f, g \in K[x]$ with $f \neq 0$. Then there exists $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

Proof. Math 332.

Example (on board). Let $g = x^4 + x^3 + 4x^2 + 1$ and $f = x^2 + 1$ in $\mathbb{Q}[x]$. Find $q, r \in \mathbb{Q}[x]$ such that $g = fq + r$ with $0 \leq \deg(r) < \deg(f)$.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K,

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0. So there exists an element f in I of smallest positive degree.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0. So there exists an element f in I of smallest positive degree. Given $g \in I$, apply the division algorithm to find $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0. So there exists an element f in I of smallest positive degree. Given $g \in I$, apply the division algorithm to find $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$. Since I is and ideal and $f, g \in I$, it follows that

$$r = g - fq \in I.$$

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0. So there exists an element f in I of smallest positive degree. Given $g \in I$, apply the division algorithm to find $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$. Since I is and ideal and $f, g \in I$, it follows that

$$r = g - fq \in I.$$

By definition of f, it follows that $\deg(r) = 0$.

$K[x]$ is a PID

Proposition. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0. So there exists an element f in I of smallest positive degree. Given $g \in I$, apply the division algorithm to find $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$. Since I is and ideal and $f, g \in I$, it follows that

$$r = g - fq \in I.$$

By definition of f, it follows that $\deg(r) = 0$. Hence, $r \in K \cap I = \{0\}$, i.e., $r = 0$. It follows that $g = fq$. We have shown that $I = (f)$.

Ring homomorphisms

Definition. A mapping $\phi\colon R \to S$ between rings R and S is a *(ring) homomorphism* if it preserves the ring operations, i.e., for all $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

Ring homomorphisms

Definition. A mapping $\phi\colon R \to S$ between rings R and S is a *(ring) homomorphism* if it preserves the ring operations, i.e., for all $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

In that case, the *kernel* of ϕ is

$$\ker(\phi) := \{r \in R : \phi(r) = 0\},$$

Ring homomorphisms

Definition. A mapping $\phi\colon R \to S$ between rings R and S is a *(ring) homomorphism* if it preserves the ring operations, i.e., for all $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

In that case, the *kernel* of ϕ is

$$\ker(\phi) := \{r \in R : \phi(r) = 0\},$$

and the *image* of ϕ is

$$\operatorname{im}(\phi) := \phi(R) := \{\phi(r) : r \in R\}.$$

The homomorphism ϕ is an *isomorphism* if it is bijective.

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism.

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).
2. The kernel of ϕ is an ideal of R.

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).
2. The kernel of ϕ is an ideal of R.
3. The image of ϕ is not necessarily an ideal of S.

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).
2. The kernel of ϕ is an ideal of R.
3. The image of ϕ is not necessarily an ideal of S.
4. ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).
2. The kernel of ϕ is an ideal of R.
3. The image of ϕ is not necessarily an ideal of S.
4. ϕ is injective if and only if $\ker(\phi) = \{0\}$.
5. ϕ is an isomorphism if and only if its kernel is trivial (i.e., equal to $\{0\}$) and its image is S.

Ring homomorphisms

Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).
2. The kernel of ϕ is an ideal of R.
3. The image of ϕ is not necessarily an ideal of S.
4. ϕ is injective if and only if $\ker(\phi) = \{0\}$.
5. ϕ is an isomorphism if and only if its kernel is trivial (i.e., equal to $\{0\}$) and its image is S.
6. If ϕ is bijective, its inverse (as a mapping of sets) is necessarily a ring homomorphism.

Quotient rings

Definition. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a + I := \{a + i : i \in I\}$ for each $a \in R$.

Quotient rings

Definition. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a + I := \{a + i : i \in I\}$ for each $a \in R$. The collection of cosets naturally forms a ring where

$$(a + I) + (b + I) := (a + b) + I \quad \text{and} \quad (a + I)(b + I) := ab + I.$$

Quotient rings

Definition. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a + I := \{a + i : i \in I\}$ for each $a \in R$. The collection of cosets naturally forms a ring where

$$(a + I) + (b + I) := (a + b) + I \quad \text{and} \quad (a + I)(b + I) := ab + I.$$

This ring of cosets is called a *quotient ring* and is denoted R/I.

Quotient rings

Definition. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a + I := \{a + i : i \in I\}$ for each $a \in R$. The collection of cosets naturally forms a ring where

$$(a + I) + (b + I) := (a + b) + I \quad \text{and} \quad (a + I)(b + I) := ab + I.$$

This ring of cosets is called a *quotient ring* and is denoted R/I.

Example. Describe the elements of $\mathbb{Q}[x]/(x^2 + 1)$.

Quotient rings

Definition. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a + I := \{a + i : i \in I\}$ for each $a \in R$. The collection of cosets naturally forms a ring where

$$(a + I) + (b + I) := (a + b) + I \quad \text{and} \quad (a + I)(b + I) := ab + I.$$

This ring of cosets is called a *quotient ring* and is denoted R/I.

Example. Describe the elements of $\mathbb{Q}[x]/(x^2 + 1)$.

$$\mathbb{Q}[x]/(x^2 + 1) = \{a + bx : a, b \in \mathbb{Q}\} \quad \text{with} \quad x^2 = -1.$$

Quotient rings

Definition. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a + I := \{a + i : i \in I\}$ for each $a \in R$. The collection of cosets naturally forms a ring where

$$(a + I) + (b + I) := (a + b) + I \quad \text{and} \quad (a + I)(b + I) := ab + I.$$

This ring of cosets is called a *quotient ring* and is denoted R/I.

Example. Describe the elements of $\mathbb{Q}[x]/(x^2 + 1)$.

$$\mathbb{Q}[x]/(x^2 + 1) = \{a + bx : a, b \in \mathbb{Q}\} \quad \text{with} \quad x^2 = -1.$$

So $\mathbb{Q}[x]/(x^2 + 1) \approx \mathbb{Q}(i)$.

Quotient mapping

Definition. If I is an ideal of R, define the *(canonical) quotient mapping*

$$\begin{aligned} \pi \colon R &\to R/I \\ a &\mapsto \overline{a} = a + I. \end{aligned}$$

Quotient mapping

Definition. If I is an ideal of R, define the *(canonical) quotient mapping*

$$\begin{aligned} \pi \colon R &\to R/I \\ a &\mapsto \overline{a} = a + I. \end{aligned}$$

It is a surjective homomorphism with kernel I.

Quotient mapping

Definition. If I is an ideal of R, define the *(canonical) quotient mapping*

$$\begin{aligned} \pi\colon R &\to R/I \\ a &\mapsto \overline{a} = a + I. \end{aligned}$$

It is a surjective homomorphism with kernel I.

If $\phi\colon R \to S$ is a ring homomorphism, then $\mathrm{im}(\phi)$ is a ring with unity $\phi(1)$, and there is a well-defined isomorphism

$$\begin{aligned} \overline{\phi}\colon R/\ker(\phi) &\to \mathrm{im}(\phi) \\ a + \ker(\phi) &\mapsto \phi(a). \end{aligned}$$

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition. Let R be a PID, and let $a, b \in R$. Then

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition. Let R be a PID, and let $a, b \in R$. Then

1. There exists a greatest common divisor d of a, b.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition. Let R be a PID, and let $a, b \in R$. Then

1. There exists a greatest common divisor d of a, b.
2. $(a, b) = (d)$.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition. Let R be a PID, and let $a, b \in R$. Then

1. There exists a greatest common divisor d of a, b.
2. $(a, b) = (d)$.
3. There exist $m, n \in R$ such that $ma + nb = d$.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition. Let R be a PID, and let $a, b \in R$. Then

1. There exists a greatest common divisor d of a, b.
2. $(a, b) = (d)$.
3. There exist $m, n \in R$ such that $ma + nb = d$.
4. The greatest common divisors of a, b are exactly the elements of the form ud where u is a unit.

GCDs

Definition. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition. Let R be a PID, and let $a, b \in R$. Then

1. There exists a greatest common divisor d of a, b.
2. $(a, b) = (d)$.
3. There exist $m, n \in R$ such that $ma + nb = d$.
4. The greatest common divisors of a, b are exactly the elements of the form ud where u is a unit.
5. If a, b have no prime factors in common, there exist $m, n \in R$ such that $ma + nb = 1$.

Maximal ideals

Definition. An ideal I in a ring R is *maximal* if $I \neq R$, and the only ideal of R properly containing I is R, itself.

Maximal ideals

Definition. An ideal I in a ring R is *maximal* if $I \neq R$, and the only ideal of R properly containing I is R, itself. In other words, if J is an ideal of R and $J \supsetneq I$, then $J = R$.

Maximal ideals

Definition. An ideal I in a ring R is *maximal* if $I \neq R$, and the only ideal of R properly containing I is R, itself. In other words, if J is an ideal of R and $J \supsetneq I$, then $J = R$.

Facts:

- I is maximal if and only if R/I is a field.

Maximal ideals

Definition. An ideal I in a ring R is *maximal* if $I \neq R$, and the only ideal of R properly containing I is R, itself. In other words, if J is an ideal of R and $J \supsetneq I$, then $J = R$.

Facts:

- I is maximal if and only if R/I is a field.
- In a PID, $I = (a)$ is maximal if and only if a is irreducible (and, hence, if and only if a is prime).

Maximal ideals

Definition. An ideal I in a ring R is *maximal* if $I \neq R$, and the only ideal of R properly containing I is R, itself. In other words, if J is an ideal of R and $J \supsetneq I$, then $J = R$.

Facts:

- I is maximal if and only if R/I is a field.
- In a PID, $I = (a)$ is maximal if and only if a is irreducible (and, hence, if and only if a is prime). Thus, for example, $\mathbb{Z}/(n)$ is a field if and only if n is prime.