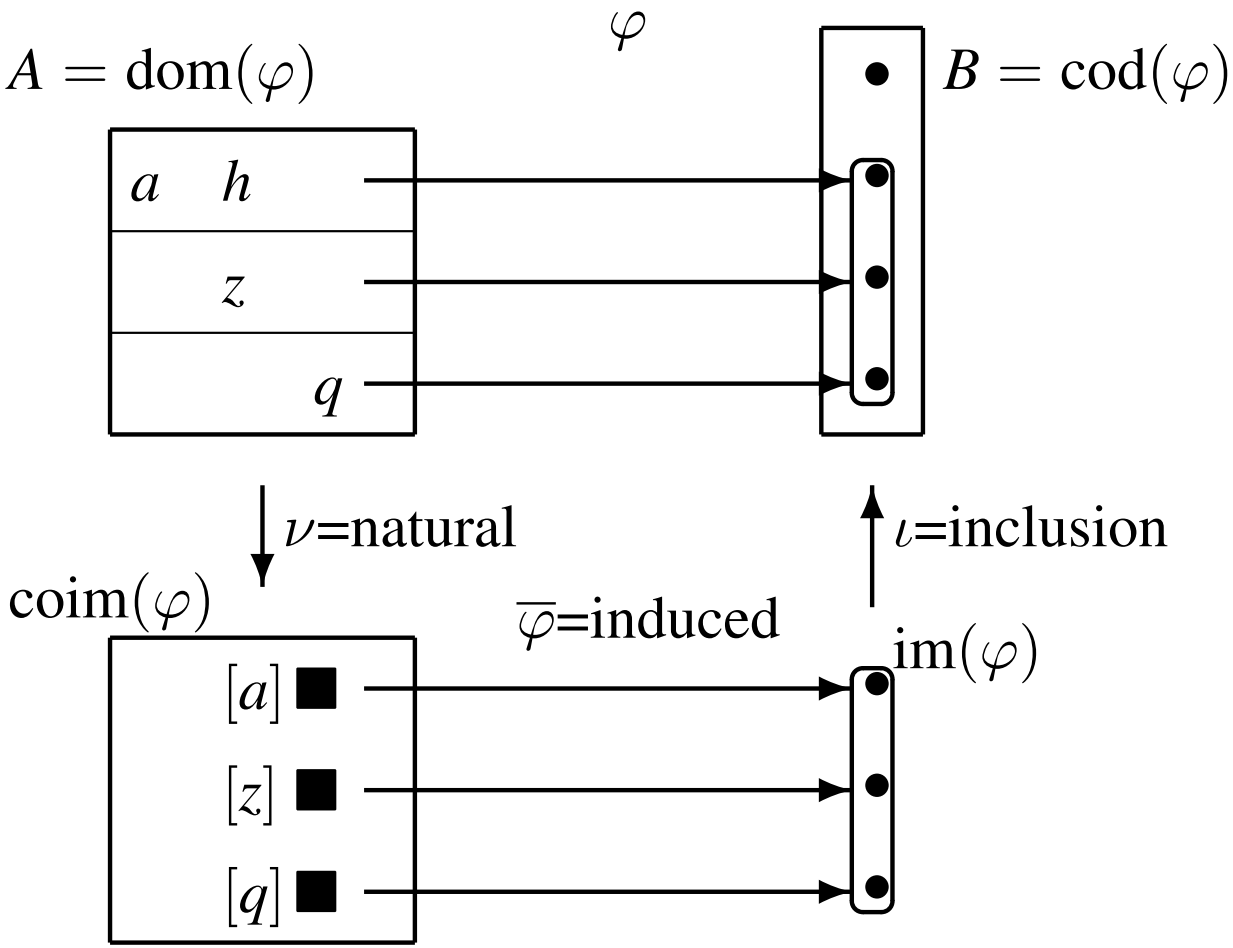
Rings, ideals

Modern Algebra 1

Fall 2016

Rings: $R = \langle R; \cdot, 1, +, -, 0 \rangle$

Rings: $R = \langle R; \cdot, 1, +, -, 0 \rangle$



We know what "homomorphism, kernel, image, coimage, subring, and quotient ring" should mean.

Homomorphisms

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$:

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^{-}\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^{-}\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^{-}\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-)

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^{-}\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-) Verify by checking $\overline{1} = 1$, $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, $\overline{w + z} = \overline{w} + \overline{z}$.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^-\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-) Verify by checking $\overline{1} = 1$, $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, $\overline{w + z} = \overline{w} + \overline{z}$.
2. For any ring R, there is a unique homomorphism $\iota\colon \mathbb{Z} \to R$.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^-\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-) Verify by checking $\overline{1} = 1$, $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, $\overline{w + z} = \overline{w} + \overline{z}$.
2. For any ring R, there is a unique homomorphism $\iota\colon \mathbb{Z} \to R$.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^-\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-) Verify by checking $\overline{1} = 1$, $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, $\overline{w + z} = \overline{w} + \overline{z}$.
2. For any ring R, there is a unique homomorphism $\iota\colon \mathbb{Z} \to R$. Determined by $1_{\mathbb{Z}} \mapsto 1_R$.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^-\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-) Verify by checking $\overline{1} = 1$, $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, $\overline{w + z} = \overline{w} + \overline{z}$.
2. For any ring R, there is a unique homomorphism $\iota\colon \mathbb{Z} \to R$. Determined by $1_{\mathbb{Z}} \mapsto 1_R$. $\mathbb{Z}$ is the free ring over $X = \emptyset$.

Homomorphisms

Recall that a function $\varphi\colon G \to H$ between additive groups is a homomorphism iff it preserves addition. Preservation of $-$ and 0 are automatic. No extra automatic preservation for a ring homomorphism $\varphi\colon R \to S$: must check that $1, \cdot, +$ are preserved. Homomorphisms preserve multiplicative inverses, when they exist.

Examples.

1. $^{-}\colon \mathbb{C} \to \mathbb{C}\colon a + bi \mapsto a - bi$ is a homomorphism. (auto-) Verify by checking $\overline{1} = 1$, $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, $\overline{w + z} = \overline{w} + \overline{z}$.
2. For any ring R, there is a unique homomorphism $\iota\colon \mathbb{Z} \to R$. Determined by $1_{\mathbb{Z}} \mapsto 1_R$. $\mathbb{Z}$ is the free ring over $X = \emptyset$.
3. For any field $\mathbb{F}$, there is at most one homomorphism $\varphi\colon \mathbb{Q} \to \mathbb{F}$.

Kernels

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$.

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1.

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1. Any equivalence relation is compatible with 1.

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1. Any equivalence relation is compatible with 1. For an equivalence relation θ to be compatible with $F(x_1, \ldots, x_n)$, it suffices for θ to be compatible with all unary "basic translations": $F(r_1, \ldots, x, \ldots, r_n)$

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1. Any equivalence relation is compatible with 1. For an equivalence relation θ to be compatible with $F(x_1, \ldots, x_n)$, it suffices for θ to be compatible with all unary "basic translations": $F(r_1, \ldots, x, \ldots, r_n)$ $= F_{i,\mathbf{r}}(x)$.

For $F(x, y) = x \cdot y$ this means $a \equiv b \pmod{\theta}$ implies $ra \equiv rb \pmod{\theta}$ and $as \equiv bs \pmod{\theta}$ for all $r, s \in R$.

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1. Any equivalence relation is compatible with 1. For an equivalence relation θ to be compatible with $F(x_1, \ldots, x_n)$, it suffices for θ to be compatible with all unary "basic translations": $F(r_1, \ldots, x, \ldots, r_n)$ $=F_{i,\mathbf{r}}(x)$.

For $F(x, y) = x \cdot y$ this means $a \equiv b \pmod{\theta}$ implies $ra \equiv rb \pmod{\theta}$ and $as \equiv bs \pmod{\theta}$ for all $r, s \in R$.

Moving everything to one side and writing i for $a - b$, this condition is: $i \equiv 0 \pmod{\theta}$ implies $ri \equiv 0 \pmod{\theta}$ and $is \equiv 0 \pmod{\theta}$ for all $r, s \in R$.

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1. Any equivalence relation is compatible with 1. For an equivalence relation θ to be compatible with $F(x_1, \ldots, x_n)$, it suffices for θ to be compatible with all unary "basic translations": $F(r_1, \ldots, x, \ldots, r_n)$ $= F_{i,\mathbf{r}}(x)$.

For $F(x, y) = x \cdot y$ this means $a \equiv b \pmod{\theta}$ implies $ra \equiv rb \pmod{\theta}$ and $as \equiv bs \pmod{\theta}$ for all $r, s \in R$.

Moving everything to one side and writing i for $a - b$, this condition is: $i \equiv 0 \pmod{\theta}$ implies $ri \equiv 0 \pmod{\theta}$ and $is \equiv 0 \pmod{\theta}$ for all $r, s \in R$.

Df. A *left ideal* of a ring R is an additive subgroup $I \leq R$ such that $RI \subseteq I$. (Right ideal, 2-sided ideal, $I \lhd R$.)

Kernels

Any kernel of a map $\varphi\colon R \to S$ is a congruence on the ring R, hence on the group $\langle R; +, -, 0\rangle$. Beyond being a group congruence it must be compatible with $\cdot$ and 1. Any equivalence relation is compatible with 1. For an equivalence relation θ to be compatible with $F(x_1, \ldots, x_n)$, it suffices for θ to be compatible with all unary "basic translations": $F(r_1, \ldots, x, \ldots, r_n)$ $=F_{i,\mathbf{r}}(x)$.

For $F(x, y) = x \cdot y$ this means $a \equiv b \pmod{\theta}$ implies $ra \equiv rb \pmod{\theta}$ and $as \equiv bs \pmod{\theta}$ for all $r, s \in R$.

Moving everything to one side and writing i for $a - b$, this condition is: $i \equiv 0 \pmod{\theta}$ implies $ri \equiv 0 \pmod{\theta}$ and $is \equiv 0 \pmod{\theta}$ for all $r, s \in R$.

Df. A *left ideal* of a ring R is an additive subgroup $I \leq R$ such that $RI \subseteq I$. (Right ideal, 2-sided ideal, $I \lhd R$.)

So, $I \lhd R$ iff $\exists S, \exists \varphi(\varphi^{\mathsf{hom}}\colon R \to S)$ such that $I = \varphi^{-1}(0)$.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal. (2-sided)

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal. (2-sided)
3. If $R = C([0,1]) = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$ and $x_0 \in [0,1]$, then the set $I = \{f \mid f(x_0) = 0\}$ of functions that vanish at x_0 is an ideal.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal. (2-sided)
3. If $R = C([0,1]) = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$ and $x_0 \in [0,1]$, then the set $I = \{f \mid f(x_0) = 0\}$ of functions that vanish at x_0 is an ideal.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal. (2-sided)
3. If $R = C([0,1]) = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$ and $x_0 \in [0,1]$, then the set $I = \{f \mid f(x_0) = 0\}$ of functions that vanish at x_0 is an ideal. (2-sided)

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal. (2-sided)
3. If $R = C([0,1]) = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$ and $x_0 \in [0,1]$, then the set $I = \{f \mid f(x_0) = 0\}$ of functions that vanish at x_0 is an ideal. (2-sided)

Generally, if $X \subseteq R$, then the ideal generated by X is the set (X) or $\langle X \rangle$ of all elements of the form

$$r_1 x_1 s_1 + r_2 x_2 s_2 + \cdots + r_k x_k s_k$$

where $r_i, s_i \in R$ and $x_i \in X$.

Examples

1. The set I of matrices of the form $\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ is a left ideal that is not a right ideal in $M_2(\mathbb{R})$. But I is a 2-sided ideal of the subring of upper triangular matrices of $M_2(\mathbb{R})$!
2. Given $n \in \mathbb{Z}$, the set $I = \{m \mid n \text{ divides } m\}$ of multiples of n is an ideal. (2-sided)
3. If $R = C([0,1]) = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$ and $x_0 \in [0,1]$, then the set $I = \{f \mid f(x_0) = 0\}$ of functions that vanish at x_0 is an ideal. (2-sided)

Generally, if $X \subseteq R$, then the ideal generated by X is the set (X) or $\langle X \rangle$ of all elements of the form

$$r_1 x_1 s_1 + r_2 x_2 s_2 + \cdots + r_k x_k s_k$$

where $r_i, s_i \in R$ and $x_i \in X$. (X) is *principal* if $X = \{x\}$.

Ideal lattices.

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons).

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal.

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$,

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$, but there is a third important operation, ideal product: $IJ = \langle \{ i \cdot j \mid i \in I, j \in J \} \rangle$.

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$, but there is a third important operation, ideal product: $IJ = \langle \{ i \cdot j \mid i \in I, j \in J \} \rangle$.

Ideal product is a direct analogue of the group commutator, and therefore has predictable properties, e.g.:

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$, but there is a third important operation, ideal product: $IJ = \langle \{ i \cdot j \mid i \in I, j \in J \} \rangle$.

Ideal product is a direct analogue of the group commutator, and therefore has predictable properties, e.g.:

1. $IJ = JI \subseteq I \cap J$,

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$, but there is a third important operation, ideal product: $IJ = \langle \{ i \cdot j \mid i \in I, j \in J \} \rangle$.

Ideal product is a direct analogue of the group commutator, and therefore has predictable properties, e.g.:

1. $IJ = JI \subseteq I \cap J$,
2. $I(J + K) = IJ + IK$.

Ideal lattices.

From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$, but there is a third important operation, ideal product: $IJ = \langle \{ i \cdot j \mid i \in I, j \in J \} \rangle$.

Ideal product is a direct analogue of the group commutator, and therefore has predictable properties, e.g.:

1. $IJ = JI \subseteq I \cap J$,
2. $I(J + K) = IJ + IK$.

Ideal lattices.

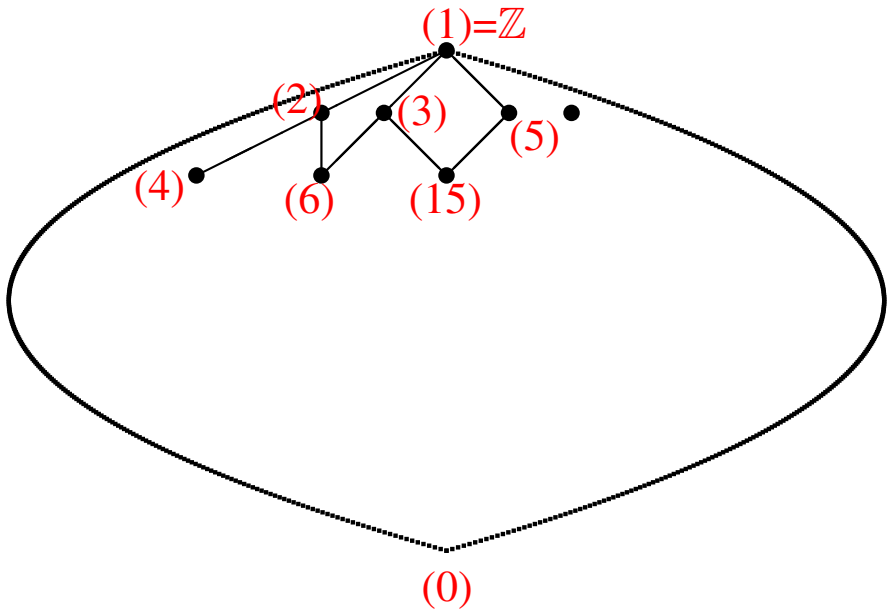
From now on, rings are commutative, but please ask about the differences for noncommutative rings.
The lattice of ideals of a ring is modular (no pentagons). The least and largest ideals are (0), the *trivial* ideal, and $(1) = R$, the *improper* ideal. The lattice operations are $I \vee J = I + J$, $I \wedge J = I \cap J$, but there is a third important operation, ideal product: $IJ = \langle \{ i \cdot j \mid i \in I, j \in J \} \rangle$.

Ideal product is a direct analogue of the group commutator, and therefore has predictable properties, e.g.:

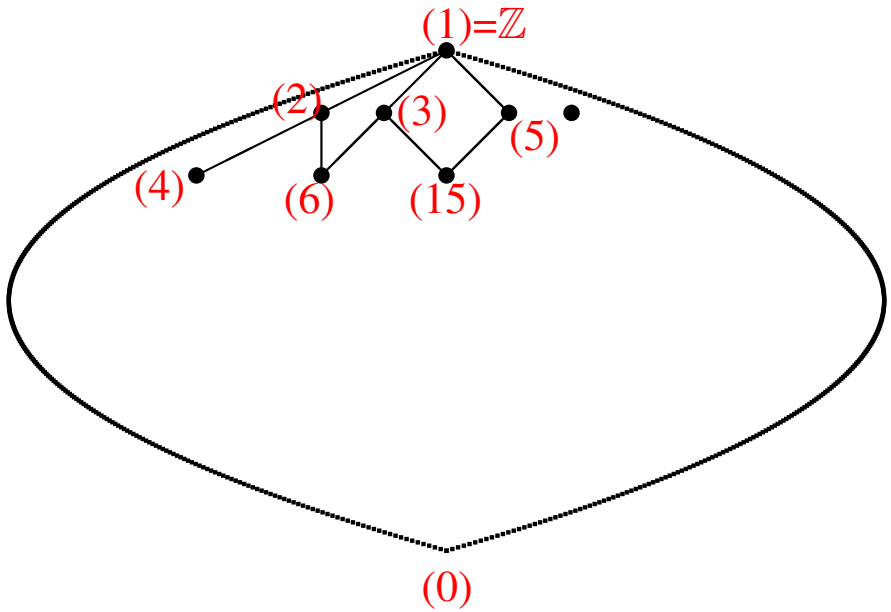
1. $IJ = JI \subseteq I \cap J$,
2. $I(J + K) = IJ + IK$.

Furthermore, ideals under product forms a commutative monoid with unit $(1) = R$.

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$

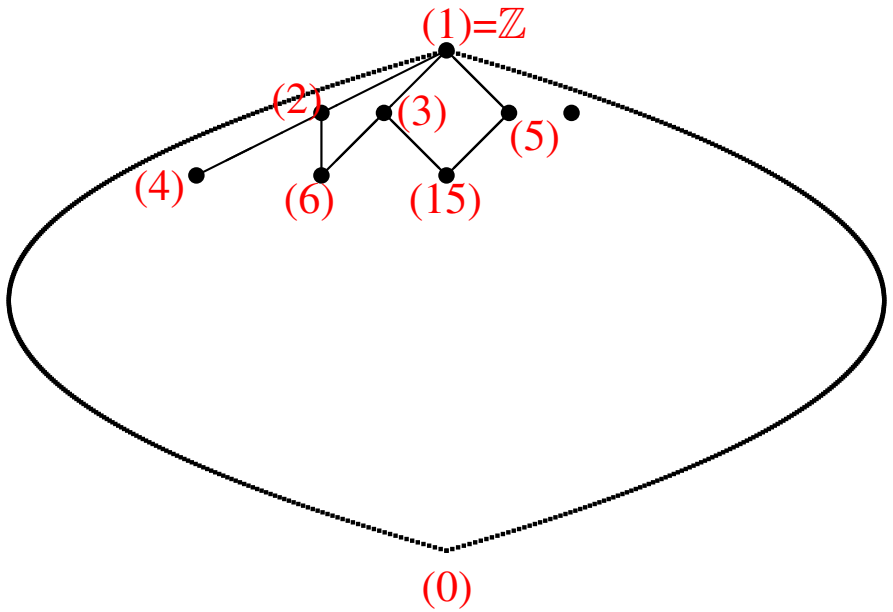


The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



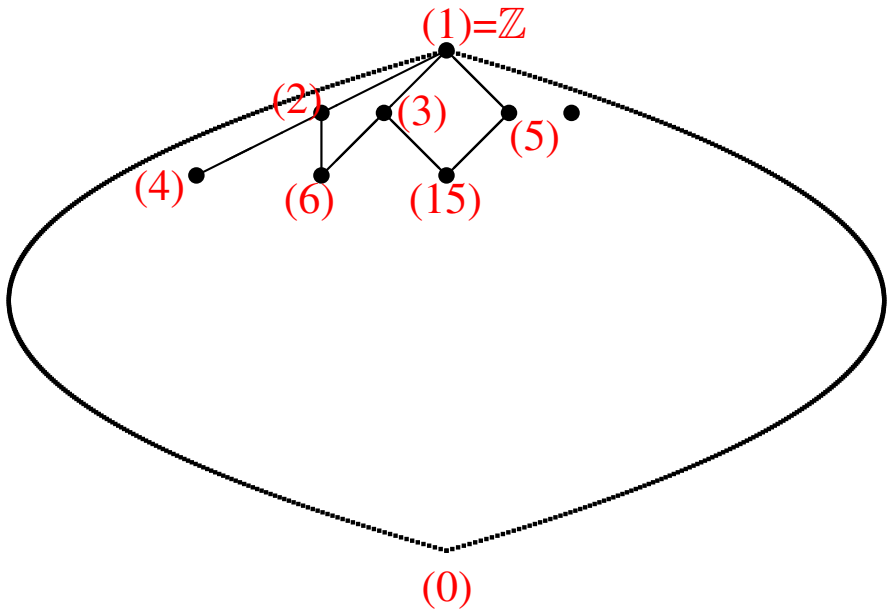
1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



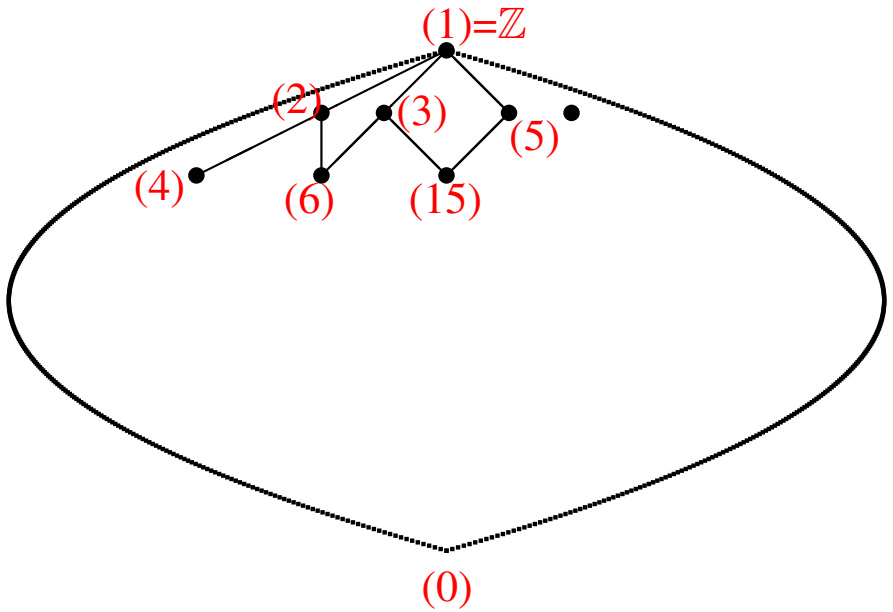
1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$
2. Inclusion order is reverse of divisibility: $(n) \subseteq (m)$ iff m divides n.

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



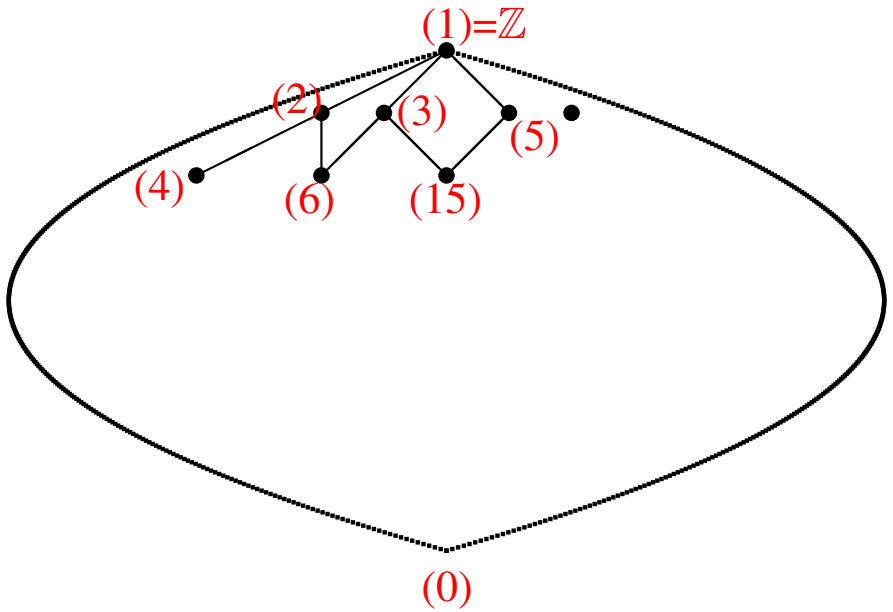
1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$
2. Inclusion order is reverse of divisibility: $(n) \subseteq (m)$ iff m divides n.
3. Maximal ideals are (p) for p prime.

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



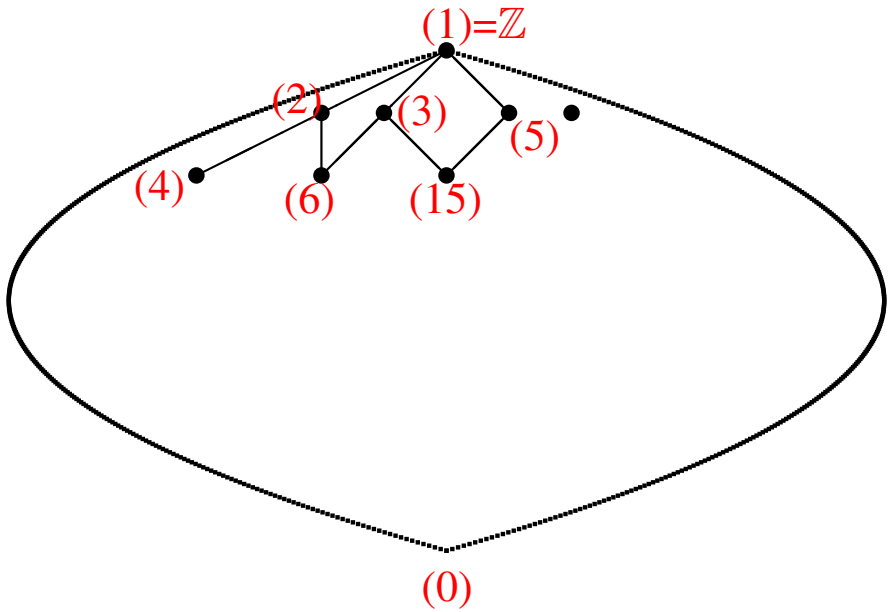
1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$
2. Inclusion order is reverse of divisibility: $(n) \subseteq (m)$ iff m divides n.
3. Maximal ideals are (p) for p prime.
4. $(m) + (n) = (d)$ for $d = \gcd(m, n)$.

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



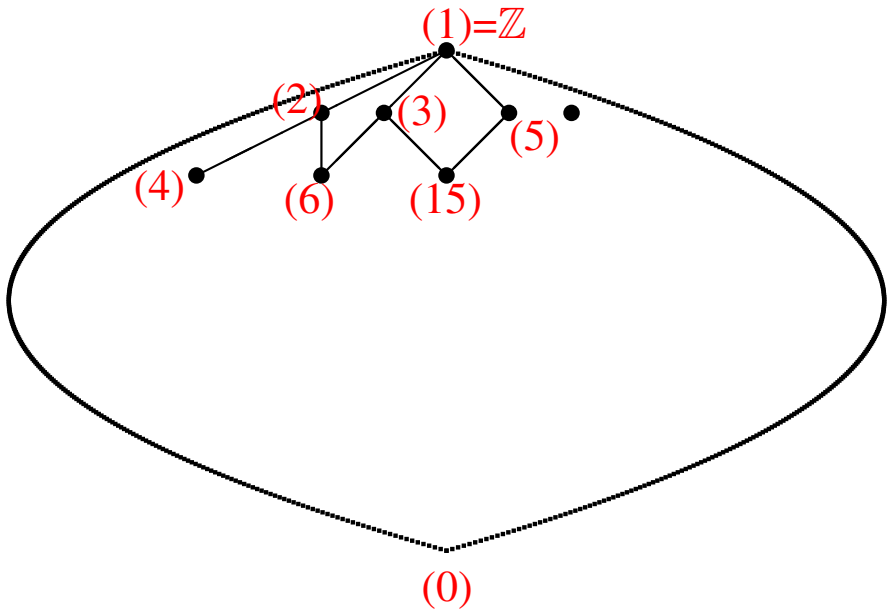
1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$
2. Inclusion order is reverse of divisibility: $(n) \subseteq (m)$ iff m divides n.
3. Maximal ideals are (p) for p prime.
4. $(m) + (n) = (d)$ for $d = \gcd(m, n)$.
5. $(m) \cap (n) = (\ell)$ for $\ell = \mathrm{lcm}(m, n)$.

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$
2. Inclusion order is reverse of divisibility: $(n) \subseteq (m)$ iff m divides n.
3. Maximal ideals are (p) for p prime.
4. $(m) + (n) = (d)$ for $d = \gcd(m, n)$.
5. $(m) \cap (n) = (\ell)$ for $\ell = \mathrm{lcm}(m, n)$.
6. $(m) \cdot (n) = (mn)$.

The ideal lattice of $\mathbb{Z}$ = subgroup lattice of $\mathbb{Z}$



1. $\forall I \lhd \mathbb{Z}$, $I = (n)$ for some $n \in \mathbb{Z}_{\geq 0}$
2. Inclusion order is reverse of divisibility: $(n) \subseteq (m)$ iff m divides n.
3. Maximal ideals are (p) for p prime.
4. $(m) + (n) = (d)$ for $d = \gcd(m, n)$.
5. $(m) \cap (n) = (\ell)$ for $\ell = \mathrm{lcm}(m, n)$.
6. $(m) \cdot (n) = (mn)$.
7. (m) and (n) *comaximal* $\overset{df}{\iff} (m) + (n) = (1) \iff \gcd(m, n) = 1$.

Some properties of comaximal (= “relatively prime”) pairs

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$.

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

CRT. Assume $I, J \lhd R$ are comaximal. For any $a, b \in R$ there is an $r \in R$ such that $x = r$ is a solution to the system

$$\begin{aligned} x &\equiv a \pmod{I}, \\ x &\equiv b \pmod{J}. \end{aligned}$$

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

CRT. Assume $I, J \lhd R$ are comaximal. For any $a, b \in R$ there is an $r \in R$ such that $x = r$ is a solution to the system

$$\begin{aligned} x &\equiv a \pmod{I}, \\ x &\equiv b \pmod{J}. \end{aligned}$$

Proof.

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

CRT. Assume $I, J \lhd R$ are comaximal. For any $a, b \in R$ there is an $r \in R$ such that $x = r$ is a solution to the system

$$\begin{aligned} x &\equiv a \pmod{I}, \\ x &\equiv b \pmod{J}. \end{aligned}$$

Proof. (Same as before.)

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

CRT. Assume $I, J \lhd R$ are comaximal. For any $a, b \in R$ there is an $r \in R$ such that $x = r$ is a solution to the system

$$\begin{aligned} x &\equiv a \pmod{I}, \\ x &\equiv b \pmod{J}. \end{aligned}$$

Proof. (Same as before.) Since $a - b \in R = I + J$, $a - b = i + j$ with $i \in I$ and $j \in J$.

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

CRT. Assume $I, J \lhd R$ are comaximal. For any $a, b \in R$ there is an $r \in R$ such that $x = r$ is a solution to the system

$$\begin{aligned} x &\equiv a \pmod{I}, \\ x &\equiv b \pmod{J}. \end{aligned}$$

Proof. (Same as before.) Since $a - b \in R = I + J$, $a - b = i + j$ with $i \in I$ and $j \in J$. Choose $r = a - i = b + j$. $\square$

Some properties of comaximal (= "relatively prime") pairs

Fact. If $I, J \lhd R$ are comaximal, then $I \cap J = IJ$.

Proof. $IJ \subseteq (I \cap J) = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. $\square$

Fact. If $I, J, K \lhd R$ are pairwise comaximal, then $I \cap J$ and K are comaximal.

Proof. $R = RR = (I+K)(J+K) = IJ + (IK + JK) \subseteq IJ + K$. So $R = IJ + K = (I \cap J) + K$. $\square$

CRT. Assume $I, J \lhd R$ are comaximal. For any $a, b \in R$ there is an $r \in R$ such that $x = r$ is a solution to the system

$$\begin{aligned} x &\equiv a \pmod{I}, \\ x &\equiv b \pmod{J}. \end{aligned}$$

Proof. (Same as before.) Since $a - b \in R = I + J$, $a - b = i + j$ with $i \in I$ and $j \in J$. Choose $r = a - i = b + j$. $\square$

Can extend to more congruences using above Facts.

Simple commutative rings = fields

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*.

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Related terminology.

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Related terminology.

1. zero divisor

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Related terminology.

1. zero divisor
2. integral domain

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Related terminology.

1. zero divisor
2. integral domain

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Related terminology.

1. zero divisor
2. integral domain

Fact. R is a subring of a field iff R is an integral domain.

Simple commutative rings = fields

Df. An element of a ring with a 2-sided inverse is called a *unit*. A nontrivial commutative ring in which all nonzero elements are units is called a *field*. (nontrivial $\Leftrightarrow |R| > 1 \Leftrightarrow 0_R \neq 1_R$)

Observation. If R is commutative and $u \in R$, then u is a unit iff $(u) = R$.

Thm. A nontrivial commutative ring is simple iff it is a field.

Proof. R is simple iff its only ideals are (0) and R iff R is a field. $\square$

Related terminology.

1. zero divisor
2. integral domain

Fact. R is a subring of a field iff R is an integral domain. **Proof?**