Math 361

March 3, 2023

Today

- Operations on ideals.
- Example of using ideals to recapture uniqueness of factorization.

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Let R be a ring (commutative, with 1).

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Let R be a ring (commutative, with 1).

A nonempty subset $I \subseteq R$ is an *ideal* if it is closed under addition ($a, b \in I \Rightarrow a + b \in I$) and

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Let R be a ring (commutative, with 1).

A nonempty subset $I \subseteq R$ is an *ideal* if it is closed under addition ($a, b \in I \Rightarrow a + b \in I$) and "inside-out" multiplication ($r \in R, a \in I \Rightarrow ra \in I$).

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Let R be a ring (commutative, with 1).

A nonempty subset $I \subseteq R$ is an *ideal* if it is closed under addition ($a, b \in I \Rightarrow a + b \in I$) and "inside-out" multiplication ($r \in R, a \in I \Rightarrow ra \in I$).

Equivalently, I is an R-submodule of R.

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Let R be a ring (commutative, with 1).

A nonempty subset $I \subseteq R$ is an *ideal* if it is closed under addition ($a, b \in I \Rightarrow a + b \in I$) and "inside-out" multiplication ($r \in R, a \in I \Rightarrow ra \in I$).

Equivalently, I is an R-submodule of R.

An ideal I is *finitely generated* if it is finitely generated as an R-module.

Review

Motivation: Although integers in a ring do not necessarily factor uniquely into primes, we can recapture unique factorization by replacing integers with ideals.

Recall:

Let R be a ring (commutative, with 1).

A nonempty subset $I \subseteq R$ is an *ideal* if it is closed under addition ($a, b \in I \Rightarrow a + b \in I$) and "inside-out" multiplication ($r \in R, a \in I \Rightarrow ra \in I$).

Equivalently, I is an R-submodule of R.

An ideal I is *finitely generated* if it is finitely generated as an R-module. This means that there exist $a_1, \ldots, a_k \in R$ for some k such that

$$I = (a_1, \ldots, a_k) := \{\textstyle\sum_{i=1}^{k} r_i a_i : r_1, \ldots, r_k \in R\}.$$

Operations on ideals

Definition. The *sum* and *product* of ideals I and J of R are defined as follows:

Operations on ideals

Definition. The *sum* and *product* of ideals I and J of R are defined as follows:

$$I + J = \{a + b : a \in I \text{ and } b \in J\},$$

Operations on ideals

Definition. The *sum* and *product* of ideals I and J of R are defined as follows:

$$I + J = \{a + b : a \in I \text{ and } b \in J\},$$

$$IJ = \{\textstyle\sum_{i=1}^{k} a_i b_i : k \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \text{ for all } i\}.$$

Operations on ideals

Definition. The *sum* and *product* of ideals I and J of R are defined as follows:

$$I + J = \{a + b : a \in I \text{ and } b \in J\},$$

$$IJ = \{\textstyle\sum_{i=1}^{k} a_i b_i : k \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \text{ for all } i\}.$$

Exercise: These are ideals.

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J + K) = IJ + IK$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J + K) = IJ + IK$,
2. $(IJ)K = I(JK)$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J + K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J + K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J + K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J+K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,
6. $(a_1, \ldots, a_k) + (b_1, \ldots, b_\ell) = (a_i + b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J+K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,
6. $(a_1, \ldots, a_k) + (b_1, \ldots, b_\ell) = (a_i + b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
7. $(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (a_i b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J+K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,
6. $(a_1, \ldots, a_k) + (b_1, \ldots, b_\ell) = (a_i + b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
7. $(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (a_i b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
8. $(a) \subseteq (b)$ if and only if $b|a$,

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J+K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,
6. $(a_1, \ldots, a_k) + (b_1, \ldots, b_\ell) = (a_i + b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
7. $(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (a_i b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
8. $(a) \subseteq (b)$ if and only if $b|a$, (to contain is to divide) and

Operations on ideals

Proposition. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J+K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,
6. $(a_1, \ldots, a_k) + (b_1, \ldots, b_\ell) = (a_i + b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
7. $(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (a_i b_j : 1 \leq i \leq k, 1 \leq j \leq \ell)$,
8. $(a) \subseteq (b)$ if and only if $b|a$, (to contain is to divide) and
9. if R is a domain, then $(a) = (b)$ if and only if $a = ub$ for some unit u.

Prime ideals

Definition. Let P be an ideal of R. Then

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition.

1. P is prime if and only if for all ideals I and J such $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition.

1. P is prime if and only if for all ideals I and J such $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.
2. If P is maximal, then P is prime.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition.

1. P is prime if and only if for all ideals I and J such $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.
2. If P is maximal, then P is prime.
3. P is prime if and only if R/P is a domain.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition.

1. P is prime if and only if for all ideals I and J such $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.
2. If P is maximal, then P is prime.
3. P is prime if and only if R/P is a domain.
4. P is maximal if and only if R/P is a field.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition.

1. P is prime if and only if for all ideals I and J such $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.
2. If P is maximal, then P is prime.
3. P is prime if and only if R/P is a domain.
4. P is maximal if and only if R/P is a field.

We will prove 2 and 3.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$. Suppose $ab \in P$ with $a \notin P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$. Suppose $ab \in P$ with $a \notin P$.

Then $P \subsetneq (a) + P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$. Suppose $ab \in P$ with $a \notin P$.

Then $P \subsetneq (a) + P$.

By maximality, $(a) + P = R$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$. Suppose $ab \in P$ with $a \notin P$.

Then $P \subsetneq (a) + P$.

By maximality, $(a) + P = R$.

Thus, $1 \in (a) + P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$. Suppose $ab \in P$ with $a \notin P$.

Then $P \subsetneq (a) + P$.

By maximality, $(a) + P = R$.

Thus, $1 \in (a) + P$.

Take $r \in R$ and $p \in P$ such that $1 = ra + p$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. Suppose P is maximal. Then P is prime.

Proof. Let $a, b \in R$. Suppose $ab \in P$ with $a \notin P$.

Then $P \subsetneq (a) + P$.

By maximality, $(a) + P = R$.

Thus, $1 \in (a) + P$.

Take $r \in R$ and $p \in P$ such that $1 = ra + p$.

Multiplying by b, we find $b = rab + bp \in P$. $\square$

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

($\Leftarrow$) Suppose that R/P is a domain and that $ab \in P$ with $a \notin P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

($\Leftarrow$) Suppose that R/P is a domain and that $ab \in P$ with $a \notin P$. It follows that $\overline{ab} = \overline{a}\,\overline{b} = 0 \in R/P$ and $\overline{a} \neq 0$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

($\Leftarrow$) Suppose that R/P is a domain and that $ab \in P$ with $a \notin P$. It follows that $\overline{ab} = \overline{a}\,\overline{b} = 0 \in R/P$ and $\overline{a} \neq 0$. Since R/P is a domain, $\overline{b} = 0 \in R/P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

($\Leftarrow$) Suppose that R/P is a domain and that $ab \in P$ with $a \notin P$. It follows that $\overline{ab} = \overline{a}\,\overline{b} = 0 \in R/P$ and $\overline{a} \neq 0$. Since R/P is a domain, $\overline{b} = 0 \in R/P$. Hence, $b \in P$.

Prime ideals

Definition. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and
2. P is *maximal* if $P \neq R$ and if Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition. The ideal P is prime if and only if R/P is a domain.

Proof. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

($\Leftarrow$) Suppose that R/P is a domain and that $ab \in P$ with $a \notin P$. It follows that $\overline{ab} = \overline{a}\,\overline{b} = 0 \in R/P$ and $\overline{a} \neq 0$. Since R/P is a domain, $\overline{b} = 0 \in R/P$. Hence, $b \in P$. We have shown that P is prime.

Recapturing unique factorization using ideals

Let $K = \mathbb{Q}(\sqrt{-5})$. Then in $\mathfrak{O}_K$ we have seen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

where $2, 3, 1 \pm \sqrt{-5}$ are non-associated irreducibles, and none are prime.

Recapturing unique factorization using ideals

Let $K = \mathbb{Q}(\sqrt{-5})$. Then in $\mathfrak{O}_K$ we have seen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

where $2, 3, 1 \pm \sqrt{-5}$ are non-associated irreducibles, and none are prime.

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

Recapturing unique factorization using ideals

Let $K = \mathbb{Q}(\sqrt{-5})$. Then in $\mathfrak{O}_K$ we have seen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

where $2, 3, 1 \pm \sqrt{-5}$ are non-associated irreducibles, and none are prime.

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

These ideals are prime, and

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

We have the prime factorization of ideals:

$$(6) = (2)(3)$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

We have the prime factorization of ideals:

$$(6) = (2)(3) = (P_1)^2 (P_2 P_3) = P_1^2 P_2 P_3$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

We have the prime factorization of ideals:

$$\begin{aligned}(6) = (2)(3) &= (P_1)^2 (P_2 P_3) = P_1^2 P_2 P_3 \\ &= (1 + \sqrt{-5})(1 - \sqrt{-5})\end{aligned}$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

We have the prime factorization of ideals:

$$\begin{aligned}(6) = (2)(3) = (P_1)^2(P_2 P_3) = P_1^2 P_2 P_3 \\ = (1 + \sqrt{-5})(1 - \sqrt{-5}) = (P_1 P_2)(P_1 P_3)\end{aligned}$$

Recapturing unique factorization using ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

$$P_1^2 = (2), \quad P_2 P_3 = (3), \quad P_1 P_2 = (1+\sqrt{-5}), \quad P_1 P_3 = (1-\sqrt{-5}).$$

We have the prime factorization of ideals:

$$\begin{aligned}(6) = (2)(3) = (P_1)^2(P_2 P_3) = P_1^2 P_2 P_3 \\ = (1 + \sqrt{-5})(1 - \sqrt{-5}) = (P_1 P_2)(P_1 P_3) = P_1^2 P_2 P_3.\end{aligned}$$