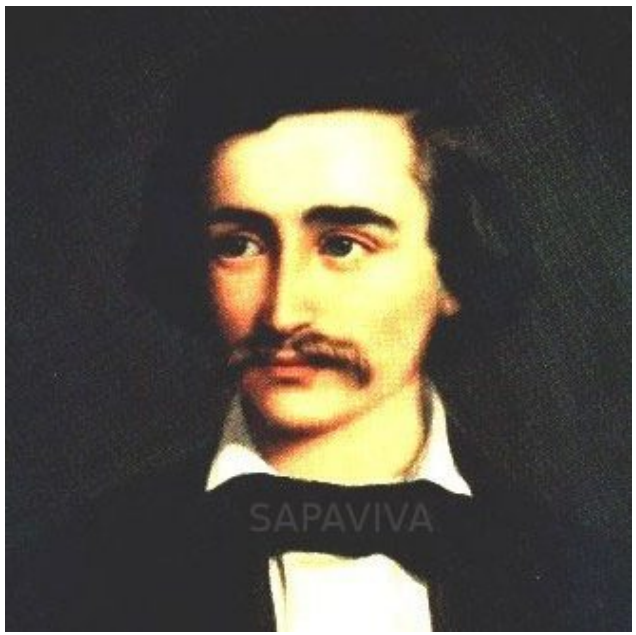
Dedekind domains



A case of Fermat's Last Theorem

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$.

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime.

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime. Except, there ARE solutions when $n = 2$,

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime. Except, there ARE solutions when $n = 2$, so suffices to prove no nontrivial integer solutions when $n = 4$ or $n =$ odd prime.

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime. Except, there ARE solutions when $n = 2$, so suffices to prove no nontrivial integer solutions when $n = 4$ or $n =$ odd prime. Euler showed that there are no nontrivial integer solutions when $n = 3, 4$.

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime. Except, there ARE solutions when $n = 2$, so suffices to prove no nontrivial integer solutions when $n = 4$ or $n =$ odd prime. Euler showed that there are no nontrivial integer solutions when $n = 3, 4$. Let's consider the equation $x^n + y^n = z^n$ when $n = p > 3$ is an odd prime.

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime. Except, there ARE solutions when $n = 2$, so suffices to prove no nontrivial integer solutions when $n = 4$ or $n =$ odd prime. Euler showed that there are no nontrivial integer solutions when $n = 3, 4$. Let's consider the equation $x^n + y^n = z^n$ when $n = p > 3$ is an odd prime. We may assume that $\{x, y, z\}$ are pairwise relative prime.

A case of Fermat's Last Theorem

If (x, y, z) is a nontrivial integer solution to $x^{mn} + y^{mn} = z^{mn}$, then (x^m, y^m, z^m) is a nontrivial solution to $x^n + y^n = z^n$. Thus, if one wants to show that there are no nontrivial integer solutions to $x^n + y^n = z^n$, it suffices to establish it when n is prime. Except, there ARE solutions when $n = 2$, so suffices to prove no nontrivial integer solutions when $n = 4$ or $n =$ odd prime. Euler showed that there are no nontrivial integer solutions when $n = 3, 4$. Let's consider the equation $x^n + y^n = z^n$ when $n = p > 3$ is an odd prime. We may assume that $\{x, y, z\}$ are pairwise relative prime. We consider only "Case 1": p divides none of x, y, z.

A case of Fermat's Last Theorem, II

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z,

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$. Since $(x^p-1) = (x-1)(x^{p-1}+\cdots+1)$,

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$. Since $(x^p-1) = (x-1)(x^{p-1}+\cdots+1)$, we get $(x-\omega)\cdots(x-\omega^{p-1}) = (x^{p-1}+\cdots+1)$, so

$$(1-\omega)\cdots(1-\omega^{p-1}) = p.$$

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$. Since $(x^p-1) = (x-1)(x^{p-1}+\cdots+1)$, we get $(x-\omega)\cdots(x-\omega^{p-1}) = (x^{p-1}+\cdots+1)$, so

$$(1-\omega)\cdots(1-\omega^{p-1}) = p.$$

Hence $y\omega^i(1-\omega^{j-i})$ divides yp.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$. Since $(x^p-1) = (x-1)(x^{p-1}+\cdots+1)$, we get $(x-\omega)\cdots(x-\omega^{p-1}) = (x^{p-1}+\cdots+1)$, so

$$(1-\omega)\cdots(1-\omega^{p-1}) = p.$$

Hence $y\omega^i(1-\omega^{j-i})$ divides yp. Now π divides $\gcd(z, yp) = 1$.

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$. Since $(x^p-1) = (x-1)(x^{p-1}+\cdots+1)$, we get $(x-\omega)\cdots(x-\omega^{p-1}) = (x^{p-1}+\cdots+1)$, so

$$(1-\omega)\cdots(1-\omega^{p-1}) = p.$$

Hence $y\omega^i(1-\omega^{j-i})$ divides yp. Now π divides $\gcd(z, yp) = 1$. $\square$

A case of Fermat's Last Theorem, II

The fact that $x^p - 1$ factors as $(x-1)(x-\omega)\cdots(x-\omega^{p-1})$ for $\omega = e^{\frac{2\pi i}{p}}$ implies that

$$z^p = x^p - (-y)^p = (x+y)(x+\omega y)(x+\omega^2 y)\cdots(x+\omega^{p-1}y).$$

This factorization takes place in $A = \mathbb{Z}[\omega]$.

Assume that $\mathbb{Z}[\omega]$ is a UFD.

Claim. Distinct factors $f_i = x + \omega^i y$ and $f_j = x + \omega^j y$ are relatively prime.

Proof. If π is prime dividing $x+\omega^i y$ and $x+\omega^j y$, then (i) π divides z, and (ii) π divides $f_i - f_j = y\omega^i(1-\omega^{j-i})$. Since $(x^p-1) = (x-1)(x^{p-1}+\cdots+1)$, we get $(x-\omega)\cdots(x-\omega^{p-1}) = (x^{p-1}+\cdots+1)$, so

$$(1-\omega)\cdots(1-\omega^{p-1}) = p.$$

Hence $y\omega^i(1-\omega^{j-i})$ divides yp. Now π divides $\gcd(z, yp) = 1$. $\square$

This forces $(x+\omega y) = u\alpha^p$ for some $u, \alpha \in \mathbb{Z}[\omega]$, u a unit.

A case of Fermat's Last Theorem, III

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω.

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$.

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$.

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$.

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$. Thus $x^p + y^p = z^p$ reduces mod p to $x^p + x^p \equiv (-x)^p \pmod{p}$,

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$. Thus $x^p + y^p = z^p$ reduces mod p to $x^p + x^p \equiv (-x)^p \pmod{p}$, or $p \mid 3x^p$.

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$. Thus $x^p + y^p = z^p$ reduces mod p to $x^p + x^p \equiv (-x)^p \pmod{p}$, or $p \mid 3x^p$. But p does not divide 3 or x^p,

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$. Thus $x^p + y^p = z^p$ reduces mod p to $x^p + x^p \equiv (-x)^p \pmod{p}$, or $p \mid 3x^p$. But p does not divide 3 or x^p, contradiction.

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$. Thus $x^p + y^p = z^p$ reduces mod p to $x^p + x^p \equiv (-x)^p \pmod{p}$, or $p \mid 3x^p$. But p does not divide 3 or x^p, contradiction. $\square$

A case of Fermat's Last Theorem, III

Kummer's Lemma. If u is a unit in $\mathbb{Z}[\omega]$, then $\omega/\overline{\omega}$ is a power of ω. Hence, if $p \geq 5$ and $(x + \omega y) \equiv u\alpha^p \pmod{p}$, then $x \equiv y \pmod{p}$. (See *Number fields, by Daniel Marcus.*)

Thus $x \equiv y \pmod{p}$. The same argument applied to $x^p + (-z)^p = (-y)^p$ implies that $x \equiv -z \pmod{p}$. Thus $x^p + y^p = z^p$ reduces mod p to $x^p + x^p \equiv (-x)^p \pmod{p}$, or $p \mid 3x^p$. But p does not divide 3 or x^p, contradiction. $\square$

Conclusion. There are no Case 1 solutions to $x^p + y^p = z^p$ if $p \geq 5$ and $\mathbb{Z}[\omega_p]$ is a UFD.

A case of Fermat's Last Theorem, IV

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime":

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p$

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$,

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$, so $(x+\omega y) = u\alpha^p$.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$, so $(x+\omega y) = u\alpha^p$. If p is a regular prime, then we can follow the same argument and prove that there are no Case 1 solutions.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$, so $(x+\omega y) = u\alpha^p$. If p is a regular prime, then we can follow the same argument and prove that there are no Case 1 solutions.

$p = 23$ is regular, $\mathbb{Z}[\omega_{23}]$ is not a UFD, yet $\mathbb{Z}[\omega_{23}]$ has unique factorization of ideals.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$, so $(x+\omega y) = u\alpha^p$. If p is a regular prime, then we can follow the same argument and prove that there are no Case 1 solutions.

$p = 23$ is regular, $\mathbb{Z}[\omega_{23}]$ is not a UFD, yet $\mathbb{Z}[\omega_{23}]$ has unique factorization of ideals. So we understand FLT for more primes this way.

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$, so $(x+\omega y) = u\alpha^p$. If p is a regular prime, then we can follow the same argument and prove that there are no Case 1 solutions.

$p = 23$ is regular, $\mathbb{Z}[\omega_{23}]$ is not a UFD, yet $\mathbb{Z}[\omega_{23}]$ has unique factorization of ideals. So we understand FLT for more primes this way.

[Note: The above argument is based on Kummer's "Main Argument".

A case of Fermat's Last Theorem, IV

The previous argument explains why, if $\mathbb{Z}[\omega_p]$ is a UFD, there can be no Case 1 solutions to $x^p + y^p = z^p$. Unique factorization was use to deduce from $z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$ that $x + \omega y = u\alpha^p$. Suppose we have unique factorization of ideals rather than elements. We could deduce from

$$(z^p) = (z)^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

that $(x+\omega y) = I^p$. Now suppose that p is a "regular prime": If $I \lhd \mathbb{Z}[\omega_p]$ and I^p is principal, then I is principal. In particular, if $(x+\omega y) = I^p$, then $(x+\omega y) = I^p = (\alpha)^p = (\alpha^p)$, so $(x+\omega y) = u\alpha^p$. If p is a regular prime, then we can follow the same argument and prove that there are no Case 1 solutions.

$p = 23$ is regular, $\mathbb{Z}[\omega_{23}]$ is not a UFD, yet $\mathbb{Z}[\omega_{23}]$ has unique factorization of ideals. So we understand FLT for more primes this way.

[Note: The above argument is based on Kummer's "Main Argument". He also proved that FLT holds for regular primes in Case 2, where $p \mid z$.]

Dedekind domains

Dedekind domains

Definition 1.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.
2. D is integrally closed.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.
2. D is integrally closed.
3. D has Krull dimension one.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.
2. D is integrally closed.
3. D has Krull dimension one.

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.
2. D is integrally closed.
3. D has Krull dimension one.

Important examples:

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.
2. D is integrally closed.
3. D has Krull dimension one.

Important examples:

1. The ring of integers $\mathcal{O}_K$ of an algebraic number field K (= finite extension of the rationals).

Dedekind domains

Definition 1. An integral domain D is a Dedekind domain if every nonzero ideal factors uniquely into primes ideals.

Fields are considered to be Dedekind domains.

Definition 2. Let D be an integral domain that is not a field. D is a Dedekind domain if

1. D is Noetherian.
2. D is integrally closed.
3. D has Krull dimension one.

Important examples:

1. The ring of integers $\mathcal{O}_K$ of an algebraic number field K (= finite extension of the rationals).
2. the coordinate ring $k[C]$ of a nonsingular curve.

Dedekind domains = robust generalization of PIDs

Dedekind domains = robust generalization of PIDs

"Like a PID"

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

$$\text{torsion free} \oplus \text{torsion} = ((\oplus_{i=1}^{r} D) \oplus I) \oplus (D/P_1^{e_1} \oplus \cdots \oplus D/P_s^{e_s})$$

where the P_j are nonzero primes.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

$$\text{torsion free} \oplus \text{torsion} = ((\oplus_{i=1}^{r} D) \oplus I) \oplus (D/P_1^{e_1} \oplus \cdots \oplus D/P_s^{e_s})$$

where the P_j are nonzero primes.

"Robust generalization"

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

$$\text{torsion free} \oplus \text{torsion} = ((\oplus_{i=1}^{r} D) \oplus I) \oplus (D/P_1^{e_1} \oplus \cdots \oplus D/P_s^{e_s})$$

where the P_j are nonzero primes.

"Robust generalization"

1. If D is a Dedekind domain, B a domain, $D \leq_{\text{int}} B$ is a finite integral extension, then B is a Dedekind domain.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

$$\text{torsion free} \oplus \text{torsion} = ((\oplus_{i=1}^{r} D) \oplus I) \oplus (D/P_1^{e_1} \oplus \cdots \oplus D/P_s^{e_s})$$

where the P_j are nonzero primes.

"Robust generalization"

1. If D is a Dedekind domain, B a domain, $D \leq_{\text{int}} B$ is a finite integral extension, then B is a Dedekind domain.

Dedekind domains = robust generalization of PIDs

"Like a PID"

1. Unique factorization of ideals.
2. Every ideal I of a Dedekind domain D can be $1\frac{1}{2}$-generated: for all nonzero $a \in I$, there exists b such that $I = (a, b)$.
3. Finitely generated modules over a Dedekind domain are uniquely expressible as

$$\text{torsion free} \oplus \text{torsion} = ((\oplus_{i=1}^{r} D) \oplus I) \oplus (D/P_1^{e_1} \oplus \cdots \oplus D/P_s^{e_s})$$

where the P_j are nonzero primes.

"Robust generalization"

1. If D is a Dedekind domain, B a domain, $D \leq_{\text{int}} B$ is a finite integral extension, then B is a Dedekind domain.
2. If D is a domain, then $D_{\mathfrak{m}}$ is a PID/DD for each maximal $\mathfrak{m}$ iff D is a Dedekind domain.

Our main goals

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain.

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain.

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain. (Assuming $[\mathbb{Q} : K] < \infty$!)

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain. (Assuming $[\mathbb{Q} : K] < \infty$!)
2. Prove the equivalence of the two definitions.

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain. (Assuming $[\mathbb{Q} : K] < \infty$!)
2. Prove the equivalence of the two definitions.

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain. (Assuming $[\mathbb{Q} : K] < \infty$!)

2. Prove the equivalence of the two definitions. (That is, show that an integral domain has unique factorization of ideals iff it is Noetherian, integrally closed, and has Krull dimension 1.)

Our main goals

1. Prove that $\mathcal{O}_K$ is a Dedekind domain. (Assuming $[\mathbb{Q} : K] < \infty$!)
2. Prove the equivalence of the two definitions. (That is, show that an integral domain has unique factorization of ideals iff it is Noetherian, integrally closed, and has Krull dimension 1.)
3. (If time) Discuss the ideal class group.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

Claim 3. $\mathcal{O}_K$ is Noetherian.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

Claim 3. $\mathcal{O}_K$ is Noetherian. (We will prove later that the additive group of $\mathcal{O}_K$ is finitely generated as an abelian group.)

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

Claim 3. $\mathcal{O}_K$ is Noetherian. (We will prove later that the additive group of $\mathcal{O}_K$ is finitely generated as an abelian group.)

Proof.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

Claim 3. $\mathcal{O}_K$ is Noetherian. (We will prove later that the additive group of $\mathcal{O}_K$ is finitely generated as an abelian group.)

Proof. Since $\mathbb{Z}$ is Noetherian, and $\mathcal{O}_K$ is finitely generated as an abelian group, $\mathcal{O}_K$ is has ACC on additive subgroups.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

Claim 3. $\mathcal{O}_K$ is Noetherian. (We will prove later that the additive group of $\mathcal{O}_K$ is finitely generated as an abelian group.)

Proof. Since $\mathbb{Z}$ is Noetherian, and $\mathcal{O}_K$ is finitely generated as an abelian group, $\mathcal{O}_K$ is has ACC on additive subgroups. Hence it has ACC in ideals.

$\mathcal{O}_K$ is a Dedekind domain: "easy part"

Claim 1. $\mathcal{O}_K$ is integrally closed.

Proof. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. $\square$

Claim 2. $\mathcal{O}_K$ has Krull dimension 1.

Proof. $(\dim(\mathbb{Z}) = 1) + (\mathbb{Z} \leq_{\text{int}} \mathcal{O}_K)$+Incomparability+Going Up. $\square$

Claim 3. $\mathcal{O}_K$ is Noetherian. (We will prove later that the additive group of $\mathcal{O}_K$ is finitely generated as an abelian group.)

Proof. Since $\mathbb{Z}$ is Noetherian, and $\mathcal{O}_K$ is finitely generated as an abelian group, $\mathcal{O}_K$ is has ACC on additive subgroups. Hence it has ACC in ideals. $\square$

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory,

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K:

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d} \bigoplus^n \mathbb{Z}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d} \bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j \beta_j$, $x_j \in \mathbb{Q}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m\beta$ satisfies $x^m + a_m a_{m-1}x^{m-1} + \cdots + a_m^{m-1}a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d}\bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j\beta_j$, $x_j \in \mathbb{Q}$. Apply each σ_i: $\sigma_i(\gamma) = \sum_{j=1}^n x_j\sigma_i(\beta_j)$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m\beta$ satisfies $x^m + a_m a_{m-1}x^{m-1} + \cdots + a_m^{m-1}a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d}\bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j\beta_j$, $x_j \in \mathbb{Q}$. Apply each σ_i: $\sigma_i(\gamma) = \sum_{j=1}^n x_j\sigma_i(\beta_j)$. Cramer's Rule implies $x_j = |A_j|/|B| = (|A_j||B|)/|B|^2$ where $|A_j|, |B| \in \mathcal{O}_K$ and $|B|^2 =: d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. (Check!)

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m\beta$ satisfies $x^m + a_m a_{m-1}x^{m-1} + \cdots + a_m^{m-1}a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d}\bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j\beta_j$, $x_j \in \mathbb{Q}$. Apply each σ_i: $\sigma_i(\gamma) = \sum_{j=1}^n x_j\sigma_i(\beta_j)$. Cramer's Rule implies $x_j = |A_j|/|B| = (|A_j||B|)/|B|^2$ where $|A_j|, |B| \in \mathcal{O}_K$ and $|B|^2 =: d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. (Check!) Hence $dx_j \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m\beta$ satisfies $x^m + a_m a_{m-1}x^{m-1} + \cdots + a_m^{m-1}a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d}\bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j\beta_j$, $x_j \in \mathbb{Q}$. Apply each σ_i: $\sigma_i(\gamma) = \sum_{j=1}^n x_j\sigma_i(\beta_j)$. Cramer's Rule implies $x_j = |A_j|/|B| = (|A_j||B|)/|B|^2$ where $|A_j|, |B| \in \mathcal{O}_K$ and $|B|^2 =: d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. (Check!) Hence $dx_j \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Hence $x_j \in \frac{1}{d}\mathbb{Z}$.

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m\beta$ satisfies $x^m + a_m a_{m-1}x^{m-1} + \cdots + a_m^{m-1}a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d}\bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j\beta_j$, $x_j \in \mathbb{Q}$. Apply each σ_i: $\sigma_i(\gamma) = \sum_{j=1}^n x_j\sigma_i(\beta_j)$. Cramer's Rule implies $x_j = |A_j|/|B| = (|A_j||B|)/|B|^2$ where $|A_j|, |B| \in \mathcal{O}_K$ and $|B|^2 =: d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. (Check!) Hence $dx_j \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Hence $x_j \in \frac{1}{d}\mathbb{Z}$. $\square$

$\mathcal{O}_K$ is a Dedekind domain: "hard part"

From field theory, if $[\mathbb{Q} : K] = n$, then there is a $\mathbb{Q}$-basis for K: $\{\beta_1, \ldots, \beta_n\}$. There exist n $\mathbb{Q}$-independent field embeddings $\sigma : K \to \mathbb{C}$.

Claim 1. We can choose the β's from $\mathcal{O}_K$.

Proof. If β satisfies $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\alpha := a_m \beta$ satisfies $x^m + a_m a_{m-1} x^{m-1} + \cdots + a_m^{m-1} a_1 x + a_m^n a_0 \in \mathbb{Z}[x]$. Hence any $\beta \in K$ has the form α/k for some $\alpha \in \mathcal{O}_K$, $k \in \mathbb{Z}$. Use the α's to replace the β's if necessary. $\square$

Claim 2. There is an integer d such that $\mathcal{O}_K \leq \frac{1}{d} \bigoplus^n \mathbb{Z}$.

Proof. For $\gamma \in \mathcal{O}_K$, write $\gamma = \sum_{j=1}^n x_j \beta_j$, $x_j \in \mathbb{Q}$. Apply each σ_i: $\sigma_i(\gamma) = \sum_{j=1}^n x_j \sigma_i(\beta_j)$. Cramer's Rule implies $x_j = |A_j|/|B| = (|A_j||B|)/|B|^2$ where $|A_j|, |B| \in \mathcal{O}_K$ and $|B|^2 =: d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. (Check!) Hence $dx_j \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Hence $x_j \in \frac{1}{d}\mathbb{Z}$. $\square$

Cor. Additively, $\mathcal{O}_K$ is free of rank n.