Integral Dependence

Integral elements

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial.

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup.

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$$

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2 + 1 = 0$, $\sqrt[3]{2}$ is a root of $x^3 - 2 = 0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2+1=0$, $\sqrt[3]{2}$ is a root of $x^3-2=0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle f_1, f_2, \ldots, f_n \rangle_{\text{AbGrp}}$,

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2+1=0$, $\sqrt[3]{2}$ is a root of $x^3-2=0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle f_1, f_2, \ldots, f_n \rangle_{\text{AbGrp}}$, then

$$(\exists m) \qquad \langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{m-1} \rangle_{\text{AbGrp}},$$

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2+1=0$, $\sqrt[3]{2}$ is a root of $x^3-2=0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle f_1, f_2, \ldots, f_n \rangle_{\text{AbGrp}}$, then

$$(\exists m) \qquad \langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{m-1} \rangle_{\text{AbGrp}},$$

so $\alpha^m = b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$,

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2+1=0$, $\sqrt[3]{2}$ is a root of $x^3-2=0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle f_1, f_2, \ldots, f_n \rangle_{\text{AbGrp}}$, then

$$(\exists m) \qquad \langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{m-1} \rangle_{\text{AbGrp}},$$

so $\alpha^m = b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$, so α satisfies $x^m = b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$.

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2+1=0$, $\sqrt[3]{2}$ is a root of $x^3-2=0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle f_1, f_2, \ldots, f_n \rangle_{\text{AbGrp}}$, then

$$(\exists m) \qquad \langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{m-1} \rangle_{\text{AbGrp}},$$

so $\alpha^m = b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$, so α satisfies $x^m = b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. $\square$

Integral elements

Recall that an element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic integer polynomial. (E.g., i is a root of $x^2+1=0$, $\sqrt[3]{2}$ is a root of $x^3-2=0$.)

This property is equivalent to the property that the subring $\langle \alpha \rangle_{\text{Rng}}$ of $\mathbb{C}$ that is generated by α has a finitely generated additive subgroup. (I.e., the *additive reduct* $\langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}}$ is finitely generated.)

Proof of equivalence:
If α satisfies $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then for all k we have $\alpha^{n+k} = a_{n-1}\alpha^{n+k-1} + \cdots + a_1\alpha^{k+1} + a_0\alpha^k$, so

$$\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\text{AbGrp}}$$

Conversely, if $\langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\text{AbGrp}} = \langle f_1, f_2, \ldots, f_n \rangle_{\text{AbGrp}}$, then

$$(\exists m) \qquad \langle \alpha \rangle_{\text{Rng}} = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{m-1} \rangle_{\text{AbGrp}},$$

so $\alpha^m = b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$, so α satisfies $x^m = b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. $\square$

Generalization

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A:

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A:

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Proof. If $A[b] = \langle 1, b, \ldots, b^{m-1} \rangle_{A-\text{Mod}}$,

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Proof. If $A[b] = \langle 1, b, \ldots, b^{m-1} \rangle_{A-\text{Mod}}$, $A[c] = \langle 1, c, \ldots, c^{n-1} \rangle_{A-\text{Mod}}$,

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Proof. If $A[b] = \langle 1, b, \ldots, b^{m-1} \rangle_{A-\text{Mod}}$, $A[c] = \langle 1, c, \ldots, c^{n-1} \rangle_{A-\text{Mod}}$, then $A[b+c], A[bc] \leq A[b,c] = \langle \{b^i c^j | i < m, j < n\} \rangle_{A-\text{Mod}}$

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Proof. If $A[b] = \langle 1, b, \ldots, b^{m-1} \rangle_{A-\text{Mod}}$, $A[c] = \langle 1, c, \ldots, c^{n-1} \rangle_{A-\text{Mod}}$, then $A[b+c], A[bc] \leq A[b,c] = \langle \{b^i c^j | i < m, j < n\} \rangle_{A-\text{Mod}}$ ($= C$ from (3)).

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Proof. If $A[b] = \langle 1, b, \ldots, b^{m-1} \rangle_{A-\text{Mod}}$, $A[c] = \langle 1, c, \ldots, c^{n-1} \rangle_{A-\text{Mod}}$, then $A[b+c], A[bc] \leq A[b,c] = \langle \{b^i c^j | i < m, j < n\} \rangle_{A-\text{Mod}}$ ($= C$ from (3)). $\square$

Df. The set of elements of B integral over A is the *integral closure* of A in B.

Generalization

Df. If $A \leq B$ are commutative rings, then $b \in B$ is *integral* over A if any of the following equivalent conditions is satisfied.

1. b satisfies a monic polynomial over A: $p(b) = 0, p(x) \in A[x]$.
2. The A-algebra $A[b] \leq B$ is finitely generated as an A-module.
3. There exists an A-algebra C with $A[b] \subseteq C \subseteq B$ where C is finitely generated as an A-module.

Thm. The set of elements of B integral over A is closed under plus and times.

Proof. If $A[b] = \langle 1, b, \ldots, b^{m-1} \rangle_{A-\text{Mod}}$, $A[c] = \langle 1, c, \ldots, c^{n-1} \rangle_{A-\text{Mod}}$, then $A[b+c], A[bc] \leq A[b,c] = \langle \{b^i c^j | i < m, j < n\} \rangle_{A-\text{Mod}}$ ($= C$ from (3)). $\square$

Df. The set of elements of B integral over A is the *integral closure* of A in B. (Leave off the phrase "in B" if A is an integral domain and B is its field of fractions.)

Some properties

Some properties

Transitivity of Integrality.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Quotients.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Quotients. If $A \leq_{\text{int}} B$ and $I \lhd B$, then $A/I^c \leq_{\text{int}} B/I$.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Quotients. If $A \leq_{\text{int}} B$ and $I \lhd B$, then $A/I^c \leq_{\text{int}} B/I$.

Proof.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Quotients. If $A \leq_{\text{int}} B$ and $I \lhd B$, then $A/I^c \leq_{\text{int}} B/I$.

Proof. Similar to the previous one.

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Quotients. If $A \leq_{\text{int}} B$ and $I \lhd B$, then $A/I^c \leq_{\text{int}} B/I$.

Proof. Similar to the previous one. $\square$

Some properties

Transitivity of Integrality. If $A \leq_{\text{int}} B \leq_{\text{int}} C$, then $A \leq_{\text{int}} C$.

Proof. If $c \in C$, then $c^n = b_{n-1}c^{n-1} + \cdots + b_0$. Assume that $b_r^{k_r} = a_{r,k_r-1}b_r^{k_r-1} + \cdots + a_{r,0}$. Then $A[c]$ is an A-submodule of $\langle \{c^i \mid i < n\} \cup \{b_r^j \mid j < k_r, r < n\} \rangle$. $\square$

Localization. If $A \leq_{\text{int}} B$ and $S \subseteq A$ is multiplicatively closed, then $S^{-1}A \leq_{\text{int}} S^{-1}B$.

Proof. Choose $b/s \in S^{-1}B$. If $b^n = a_{n-1}b^{n-1} + \cdots + a_0$, then $(b/s)^n = (a_{n-1}/s)(b/s)^{n-1} + \cdots + (a_0/s^n)$. $\square$

Quotients. If $A \leq_{\text{int}} B$ and $I \lhd B$, then $A/I^c \leq_{\text{int}} B/I$.

Proof. Similar to the previous one. $\square$

Integral closure: Algebraic number rings

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in* K.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in* K.

Examples.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
   2. If $m \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
   2. If $m \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.
2. If ω is a root of unity and $K = \mathbb{Q}[\omega]$, then $\mathcal{O}_K = \mathbb{Z}[\omega]$.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
   2. If $m \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.
2. If ω is a root of unity and $K = \mathbb{Q}[\omega]$, then $\mathcal{O}_K = \mathbb{Z}[\omega]$.
3. The integral closure of $\mathbb{Z}[2i]$ is $\mathbb{Z}[i]$.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
   2. If $m \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.
2. If ω is a root of unity and $K = \mathbb{Q}[\omega]$, then $\mathcal{O}_K = \mathbb{Z}[\omega]$.
3. The integral closure of $\mathbb{Z}[2i]$ is $\mathbb{Z}[i]$.
4. Every UFD is integrally closed.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
   2. If $m \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.
2. If ω is a root of unity and $K = \mathbb{Q}[\omega]$, then $\mathcal{O}_K = \mathbb{Z}[\omega]$.
3. The integral closure of $\mathbb{Z}[2i]$ is $\mathbb{Z}[i]$.
4. Every UFD is integrally closed.

Integral closure: Algebraic number rings

Assume that K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is written $\mathcal{O}_K$ and is called the *ring of integers in K*.

Examples.

1. Assume that $K = \mathbb{Q}[\sqrt{m}]$ where $m \in \mathbb{Z}$ is square-free.
   1. If $m \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
   2. If $m \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.
2. If ω is a root of unity and $K = \mathbb{Q}[\omega]$, then $\mathcal{O}_K = \mathbb{Z}[\omega]$.
3. The integral closure of $\mathbb{Z}[2i]$ is $\mathbb{Z}[i]$.
4. Every UFD is integrally closed. (Rational root theorem.)

$\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ when $\alpha : A \overset{\text{int}}{\hookrightarrow} B$

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
2. (Incomparability) If $\alpha^*(\mathfrak{q}) = \alpha^*(\mathfrak{r})$, then $\mathfrak{q}$ and $\mathfrak{r}$ are incomparable.

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
2. (Incomparability) If $\alpha^*(\mathfrak{q}) = \alpha^*(\mathfrak{r})$, then $\mathfrak{q}$ and $\mathfrak{r}$ are incomparable.

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
2. (Incomparability) If $\alpha^*(\mathfrak{q}) = \alpha^*(\mathfrak{r})$, then $\mathfrak{q}$ and $\mathfrak{r}$ are incomparable.
3. (Going up) Any finite ascending chain of primes of A is the contraction of a finite ascending chain of primes of B.

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
2. (Incomparability) If $\alpha^*(\mathfrak{q}) = \alpha^*(\mathfrak{r})$, then $\mathfrak{q}$ and $\mathfrak{r}$ are incomparable.
3. (Going up) Any finite ascending chain of primes of A is the contraction of a finite ascending chain of primes of B.

Cohen-Seidenberg Theorems. If $\alpha : A \overset{\text{int}}{\hookrightarrow} B$, then

1. (Lying over) $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
2. (Incomparability) If $\alpha^*(\mathfrak{q}) = \alpha^*(\mathfrak{r})$, then $\mathfrak{q}$ and $\mathfrak{r}$ are incomparable.
3. (Going up) Any finite ascending chain of primes of A is the contraction of a finite ascending chain of primes of B.
4. (Going down) Any finite descending chain of primes of A is the contraction of a finite descending chain of primes of B, provided A and B are domains and A is integrally closed.

Preparing for Incomparability/Lying Over

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol. $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$,

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol. $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it $b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol. $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it $b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. Then
$a^{-1} = -(a_{n-1} \cdot 1 + \cdots + a_0 a^{n-1}) \in A$.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. Then
$a^{-1} = -(a_{n-1} \cdot 1 + \cdots + a_0 a^{n-1}) \in A$. $\square$

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. Then
$a^{-1} = -(a_{n-1} \cdot 1 + \cdots + a_0 a^{n-1}) \in A$. $\square$

Lm. If $A \leq_{\text{int}} B$ and $\mathfrak{q} \lhd B$ is prime, then $\mathfrak{q}^c$ is maximal iff $\mathfrak{q}$ is maximal.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. Then
$a^{-1} = -(a_{n-1} \cdot 1 + \cdots + a_0 a^{n-1}) \in A$. $\square$

Lm. If $A \leq_{\text{int}} B$ and $\mathfrak{q} \lhd B$ is prime, then $\mathfrak{q}^c$ is maximal iff $\mathfrak{q}$ is maximal.

Proof.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. Then
$a^{-1} = -(a_{n-1} \cdot 1 + \cdots + a_0 a^{n-1}) \in A$. $\square$

Lm. If $A \leq_{\text{int}} B$ and $\mathfrak{q} \lhd B$ is prime, then $\mathfrak{q}^c$ is maximal iff $\mathfrak{q}$ is maximal.

Proof. $A/\mathfrak{q}^c \leq_{\text{int}} B/\mathfrak{q}$.

Preparing for Incomparability/Lying Over

Lm. If $A \leq_{\text{int}} B$ are integral domains, then A is a field iff B is a field.

Proof. $[\Rightarrow]$ Choose $b \in B - \{0\}$, and find least-degree monic pol.
$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Then $a_0 \neq 0$, so multiply by b^{-1} & solve for it
$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B$.

$[\Leftarrow]$ Choose $a \in A - \{0\}$. Then $a^{-1} \in B$, so $\exists$ pol.
$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$. Then
$a^{-1} = -(a_{n-1} \cdot 1 + \cdots + a_0 a^{n-1}) \in A$. $\square$

Lm. If $A \leq_{\text{int}} B$ and $\mathfrak{q} \lhd B$ is prime, then $\mathfrak{q}^c$ is maximal iff $\mathfrak{q}$ is maximal.

Proof. $A/\mathfrak{q}^c \leq_{\text{int}} B/\mathfrak{q}$. $\square$

Incomparability

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B.

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof.

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{p}'$ be the extension of $\mathfrak{p}$ to $A_{\mathfrak{p}}$, and let $\mathfrak{q}' \subseteq \mathfrak{r}'$ be the extensions of $\mathfrak{q} \subseteq \mathfrak{r}$ to $B_{\mathfrak{p}}$.

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{p}'$ be the extension of $\mathfrak{p}$ to $A_{\mathfrak{p}}$, and let $\mathfrak{q}' \subseteq \mathfrak{r}'$ be the extensions of $\mathfrak{q} \subseteq \mathfrak{r}$ to $B_{\mathfrak{p}}$. Necessarily $(\mathfrak{q}')^c = \mathfrak{p}' = (\mathfrak{r}')^c$,

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{p}'$ be the extension of $\mathfrak{p}$ to $A_{\mathfrak{p}}$, and let $\mathfrak{q}' \subseteq \mathfrak{r}'$ be the extensions of $\mathfrak{q} \subseteq \mathfrak{r}$ to $B_{\mathfrak{p}}$. Necessarily $(\mathfrak{q}')^c = \mathfrak{p}' = (\mathfrak{r}')^c$, so $\mathfrak{q}' = \mathfrak{r}'$,

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{p}'$ be the extension of $\mathfrak{p}$ to $A_{\mathfrak{p}}$, and let $\mathfrak{q}' \subseteq \mathfrak{r}'$ be the extensions of $\mathfrak{q} \subseteq \mathfrak{r}$ to $B_{\mathfrak{p}}$. Necessarily $(\mathfrak{q}')^c = \mathfrak{p}' = (\mathfrak{r}')^c$, so $\mathfrak{q}' = \mathfrak{r}'$, so $\mathfrak{q} = \mathfrak{r}$.

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{p}'$ be the extension of $\mathfrak{p}$ to $A_{\mathfrak{p}}$, and let $\mathfrak{q}' \subseteq \mathfrak{r}'$ be the extensions of $\mathfrak{q} \subseteq \mathfrak{r}$ to $B_{\mathfrak{p}}$. Necessarily $(\mathfrak{q}')^c = \mathfrak{p}' = (\mathfrak{r}')^c$, so $\mathfrak{q}' = \mathfrak{r}'$, so $\mathfrak{q} = \mathfrak{r}$. $\square$

Incomparability

Thm. Assume that $A \leq_{\text{int}} B$ and $\mathfrak{q} \subseteq \mathfrak{r}$ are primes of B. If $\mathfrak{q}^c = \mathfrak{r}^c =: \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{r}$.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{p}'$ be the extension of $\mathfrak{p}$ to $A_{\mathfrak{p}}$, and let $\mathfrak{q}' \subseteq \mathfrak{r}'$ be the extensions of $\mathfrak{q} \subseteq \mathfrak{r}$ to $B_{\mathfrak{p}}$. Necessarily $(\mathfrak{q}')^c = \mathfrak{p}' = (\mathfrak{r}')^c$, so $\mathfrak{q}' = \mathfrak{r}'$, so $\mathfrak{q} = \mathfrak{r}$. $\square$

Lying Over

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof.

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{r}$ be a maximal ideal of $B_{\mathfrak{p}}$.

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{r}$ be a maximal ideal of $B_{\mathfrak{p}}$. Restrict $\mathfrak{r}$ to A in two ways.

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{r}$ be a maximal ideal of $B_{\mathfrak{p}}$. Restrict $\mathfrak{r}$ to A in two ways. If $\mathfrak{q} = \mathfrak{r}^c \lhd B$, then $\mathfrak{q}^c = \mathfrak{p}$.

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{r}$ be a maximal ideal of $B_{\mathfrak{p}}$. Restrict $\mathfrak{r}$ to A in two ways. If $\mathfrak{q} = \mathfrak{r}^c \lhd B$, then $\mathfrak{q}^c = \mathfrak{p}$. $\square$

Lying Over

Thm. If $A \leq_{\text{int}} B$ and $\mathfrak{p}$ is a prime of A, then $\mathfrak{p} = \mathfrak{q}^c$ for some prime $\mathfrak{q}$ of B.

Proof. Consider commutative

$$\begin{array}{ccc} A & \xrightarrow{\text{int}} & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \xrightarrow{\text{int}} & B_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{r}$ be a maximal ideal of $B_{\mathfrak{p}}$. Restrict $\mathfrak{r}$ to A in two ways. If $\mathfrak{q} = \mathfrak{r}^c \lhd B$, then $\mathfrak{q}^c = \mathfrak{p}$. $\square$

Going Up

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof.

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step,

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$.

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$. Let $\overline{B} = B/\mathfrak{q}_1$ and $\overline{A} = A/\mathfrak{q}_1^c = A/\mathfrak{p}_1$.

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$. Let $\overline{B} = B/\mathfrak{q}_1$ and $\overline{A} = A/\mathfrak{q}_1^c = A/\mathfrak{p}_1$. We still have $\overline{A} \leq_{\text{int}} \overline{B}$, but now we focus on primes $(0) \subsetneq \overline{\mathfrak{p}}_2$ in $\overline{A}$, and (0) in $\overline{B}$.

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$. Let $\overline{B} = B/\mathfrak{q}_1$ and $\overline{A} = A/\mathfrak{q}_1^c = A/\mathfrak{p}_1$. We still have $\overline{A} \leq_{\text{int}} \overline{B}$, but now we focus on primes $(0) \subsetneq \overline{\mathfrak{p}}_2$ in $\overline{A}$, and (0) in $\overline{B}$. Any prime $\overline{\mathfrak{q}}_2 \lhd \overline{B}$ that lies over $\overline{\mathfrak{p}}_2$ yields a prime $\mathfrak{q}_2 \lhd B$ satisfying $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2^c = \mathfrak{p}_2$.

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$. Let $\overline{B} = B/\mathfrak{q}_1$ and $\overline{A} = A/\mathfrak{q}_1^c = A/\mathfrak{p}_1$. We still have $\overline{A} \leq_{\text{int}} \overline{B}$, but now we focus on primes $(0) \subsetneq \overline{\mathfrak{p}}_2$ in $\overline{A}$, and (0) in $\overline{B}$. Any prime $\overline{\mathfrak{q}}_2 \lhd \overline{B}$ that lies over $\overline{\mathfrak{p}}_2$ yields a prime $\mathfrak{q}_2 \lhd B$ satisfying $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2^c = \mathfrak{p}_2$. $\square$

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$. Let $\overline{B} = B/\mathfrak{q}_1$ and $\overline{A} = A/\mathfrak{q}_1^c = A/\mathfrak{p}_1$. We still have $\overline{A} \leq_{\text{int}} \overline{B}$, but now we focus on primes $(0) \subsetneq \overline{\mathfrak{p}}_2$ in $\overline{A}$, and (0) in $\overline{B}$. Any prime $\overline{\mathfrak{q}}_2 \lhd \overline{B}$ that lies over $\overline{\mathfrak{p}}_2$ yields a prime $\mathfrak{q}_2 \lhd B$ satisfying $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2^c = \mathfrak{p}_2$. $\square$

Cor. If $A \leq_{\text{int}} B$ and either has finite Krull dimension, then both have the same Krull dimension.

Going Up

Thm. If $A \leq_{\text{int}} B$,

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. Suffices to show how to increment one step, so assume $m = 1, n = 2$. Let $\overline{B} = B/\mathfrak{q}_1$ and $\overline{A} = A/\mathfrak{q}_1^c = A/\mathfrak{p}_1$. We still have $\overline{A} \leq_{\text{int}} \overline{B}$, but now we focus on primes $(0) \subsetneq \overline{\mathfrak{p}}_2$ in $\overline{A}$, and (0) in $\overline{B}$. Any prime $\overline{\mathfrak{q}}_2 \lhd \overline{B}$ that lies over $\overline{\mathfrak{p}}_2$ yields a prime $\mathfrak{q}_2 \lhd B$ satisfying $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2^c = \mathfrak{p}_2$. $\square$

Cor. If $A \leq_{\text{int}} B$ and either has finite Krull dimension, then both have the same Krull dimension. (So any number ring has Krull dimension 1.)

Going Down

Going Down

Thm. Assume that $A \leq_{\text{int}} B$ are integral domains and A is integrally closed. If

$$\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Going Down

Thm. Assume that $A \leq_{\text{int}} B$ are integral domains and A is integrally closed. If

$$\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof.

Going Down

Thm. Assume that $A \leq_{\text{int}} B$ are integral domains and A is integrally closed. If

$$\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. See AM Theorem 5.16, or Eisenbud Theorem 13.9.

Going Down

Thm. Assume that $A \leq_{\text{int}} B$ are integral domains and A is integrally closed. If

$$\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$$

is a chain of primes in A, and

$$\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$$

is a chain of primes in B satisfying $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$ $(\leq n)$, then the $\mathfrak{q}$-chain can be extended to a length-n chain ($\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, n$).

Proof. See AM Theorem 5.16, or Eisenbud Theorem 13.9. □

Df. A ring extension $A \leq B$ has the "going up" or "going down" property if chains or primes can be extended as appropriate.

Noether Normalization

Noether Normalization

Thm. Let k be a field and let B be a finitely generated k-algebra.

Noether Normalization

Thm. Let k be a field and let B be a finitely generated k-algebra. There exists $A \leq_{\text{int}} B$ with $A \cong k[y_1, \ldots, y_d]$, $d =$ Krull dimension of B.

Noether Normalization

Thm. Let k be a field and let B be a finitely generated k-algebra. There exists $A \leq_{\text{int}} B$ with $A \cong k[y_1, \ldots, y_d]$, $d =$ Krull dimension of B. (B is integral-extension-of-free.)

Noether Normalization

Thm. Let k be a field and let B be a finitely generated k-algebra. There exists $A \leq_{\text{int}} B$ with $A \cong k[y_1, \ldots, y_d]$, $d =$ Krull dimension of B. (B is integral-extension-of-free.)

Proof.

Noether Normalization

Thm. Let k be a field and let B be a finitely generated k-algebra. There exists $A \leq_{\text{int}} B$ with $A \cong k[y_1, \ldots, y_d]$, $d =$ Krull dimension of B. (B is integral-extension-of-free.)

Proof. See AM Exercise 5.16, or Eisenbud Theorem 13.3.

Noether Normalization

Thm. Let k be a field and let B be a finitely generated k-algebra. There exists $A \leq_{\text{int}} B$ with $A \cong k[y_1, \ldots, y_d]$, $d =$ Krull dimension of B. (B is integral-extension-of-free.)

Proof. See AM Exercise 5.16, or Eisenbud Theorem 13.3. □

Zariski's Lemma

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$,

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$, so K is integral over $A[1/c]$,

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$, so K is integral over $A[1/c]$, so $A[1/c]$ is a field.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$, so K is integral over $A[1/c]$, so $A[1/c]$ is a field. But $A = k[a_1] \cong k[x]$ is a PID with infinitely many primes, so $A[1/c]$ cannot be a field.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$, so K is integral over $A[1/c]$, so $A[1/c]$ is a field. But $A = k[a_1] \cong k[x]$ is a PID with infinitely many primes, so $A[1/c]$ cannot be a field. $\square$

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$, so K is integral over $A[1/c]$, so $A[1/c]$ is a field. But $A = k[a_1] \cong k[x]$ is a PID with infinitely many primes, so $A[1/c]$ cannot be a field. $\square$

Cor. A finitely generated ring that is a field is a finite field.

Zariski's Lemma

Lemma. Let K/k be an extension of fields. If K is finitely generated as a k-algebra, then K is finitely generated as a k-module. (That is, K an algebraic extension of k.)

Proof. Assume that $K = k[a_1, \ldots, a_t, \ldots, a_n]$ where $a_1, \ldots, a_t$ are a transcendence base for K over k. Replace k by $k(a_1, \ldots, a_{t-1})$ to reduce to the case $t = 1$. If $A = k[a_1]$, then $\exists c \in k[a_1] - \{0\}$ such that all a's are integral over $A[1/c]$, so K is integral over $A[1/c]$, so $A[1/c]$ is a field. But $A = k[a_1] \cong k[x]$ is a PID with infinitely many primes, so $A[1/c]$ cannot be a field. $\square$

Cor. A finitely generated ring that is a field is a finite field. (Equivalently, every maximal ideal of $\mathbb{Z}[x_1, \ldots, x_n]$ has finite index.)