Unique factorization

Modern Algebra 1

Fall 2016

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial.

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.)

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.)
How do we recognize such p?

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.)
How do we recognize such p?

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order.

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD.

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. ($\mathbb{Z}$,

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. ($\mathbb{Z}$, $\mathbb{Z}[i]$,

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. ($\mathbb{Z}, \mathbb{Z}[i], \mathbb{F}[x]$)

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. ($\mathbb{Z}, \mathbb{Z}[i], \mathbb{F}[x]$)

Gauss' Lemma. If Z is a UFD and $Q = \text{FracField}(Z)$, then any primitive $p(x) \in Z[x]$ is irreducible in $Z[x]$ iff it is irreducible in $Q[x]$.

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. ($\mathbb{Z}, \mathbb{Z}[i], \mathbb{F}[x]$)

Gauss' Lemma. If Z is a UFD and $Q = \text{FracField}(Z)$, then any primitive $p(x) \in Z[x]$ is irreducible in $Z[x]$ iff it is irreducible in $Q[x]$.

Thm. If Z is UFD then $Z[x]$ is a UFD.

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. ($\mathbb{Z}, \mathbb{Z}[i], \mathbb{F}[x]$)

Gauss' Lemma. If Z is a UFD and $Q = \text{FracField}(Z)$, then any primitive $p(x) \in Z[x]$ is irreducible in $Z[x]$ iff it is irreducible in $Q[x]$.

Thm. If Z is UFD then $Z[x]$ is a UFD. ($\mathbb{Z}[x]$,

Factorization in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Recall that if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[x]/(p(x))$ where $p(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. ($p(x) = \min_{\alpha,\mathbb{Q}}(x)$.) How do we recognize such p?

Df. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit has a finite factorization into irreducible elements, $a = q_1 \cdots q_k$, and the irreducible factors q_i are unique up to associates and order. (Any field is a UFD!)

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Thm. Every PID is a UFD. $(\mathbb{Z}, \mathbb{Z}[i], \mathbb{F}[x])$

Gauss' Lemma. If Z is a UFD and $Q = \text{FracField}(Z)$, then any primitive $p(x) \in Z[x]$ is irreducible in $Z[x]$ iff it is irreducible in $Q[x]$.

Thm. If Z is UFD then $Z[x]$ is a UFD. $(\mathbb{Z}[x], \mathbb{F}[x,y,z] = ((\mathbb{F}[x])[y])[z])$

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc$

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n]$

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$,

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$
$= (q_{i_1}) \cdots (q_{i_m})$

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$. There can be only finitely many choices for (b).

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$. There can be only finitely many choices for (b).

[UFD $\Rightarrow$ (ii)] Suppose that $q \mid ab$, say $qc = ab$.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$. There can be only finitely many choices for (b).

[UFD $\Rightarrow$ (ii)] Suppose that $q \mid ab$, say $qc = ab$. Equate factorizations and learn that $(q) = (p)$ for some irreducible factor of a or b.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$. There can be only finitely many choices for (b).

[UFD $\Rightarrow$ (ii)] Suppose that $q \mid ab$, say $qc = ab$. Equate factorizations and learn that $(q) = (p)$ for some irreducible factor of a or b. Thus $q \mid a$ or $q \mid b$.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$. There can be only finitely many choices for (b).

[UFD $\Rightarrow$ (ii)] Suppose that $q \mid ab$, say $qc = ab$. Equate factorizations and learn that $(q) = (p)$ for some irreducible factor of a or b. Thus $q \mid a$ or $q \mid b$.

[(i)&(ii) $\Rightarrow$ UFD] ACC on principal ideals implies each nonunit has a finite factorization into irreducibles.

Characterization of UFDs

Thm. Z is a UFD iff (i) Z has ACC on principal ideals and (ii) irreducible elements are prime.

[UFD $\Rightarrow$ (i)] Suppose Z contains $a = q_1 \cdots q_k$ and $(a) \subsetneq (b)$. There is a nonunit c such that $a = bc = [b][c] = [r_1 \cdots r_m][s_1 \cdots s_n] = q_1 \cdots q_k$. For each r_j there is a q_{i_j} such that $(r_j) = (q_{i_j})$, so $(b) = (r_1) \cdots (r_m)$ $= (q_{i_1}) \cdots (q_{i_m})$ is a subproduct of $(a) = (q_1) \cdots (q_k)$. There can be only finitely many choices for (b).

[UFD $\Rightarrow$ (ii)] Suppose that $q \mid ab$, say $qc = ab$. Equate factorizations and learn that $(q) = (p)$ for some irreducible factor of a or b. Thus $q \mid a$ or $q \mid b$.

[(i)&(ii) $\Rightarrow$ UFD] ACC on principal ideals implies each nonunit has a finite factorization into irreducibles. Finite factorizations into primes are unique up to associates and order. $\square$

PIDs are UFDs (*)

Proof of (*):

PIDs are UFDs (*)

Proof of (*):

(i) If $I_0 < I_1 < \cdots$ is any strictly increasing ω-chain of ideals in a ring, then $I = \bigcup I_j$ cannot be finitely generated.

PIDs are UFDs (*)

Proof of (*):

(i) If $I_0 < I_1 < \cdots$ is any strictly increasing ω-chain of ideals in a ring, then $I = \bigcup I_j$ cannot be finitely generated. Hence $(a_0) < (a_1) < \cdots$ is impossible in a PID.

PIDs are UFDs (*)

Proof of (*):

(i) If $I_0 < I_1 < \cdots$ is any strictly increasing ω-chain of ideals in a ring, then $I = \bigcup I_j$ cannot be finitely generated. Hence $(a_0) < (a_1) < \cdots$ is impossible in a PID.

(ii) q is irreducible iff (q) is maximal among principal ideals.

PIDs are UFDs (*)

Proof of (*):

(i) If $I_0 < I_1 < \cdots$ is any strictly increasing ω-chain of ideals in a ring, then $I = \bigcup I_j$ cannot be finitely generated. Hence $(a_0) < (a_1) < \cdots$ is impossible in a PID.

(ii) q is irreducible iff (q) is maximal among principal ideals. In a PID, this means (q) is a maximal ideal, hence prime. Therefore q is prime. $\square$

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.
   p prime. If $p \nmid a_n$; $p | a_m$, $m < n$; $p^2 \nmid a_0$, then $a_0 x^n + \cdots + a_0$ irred.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.
   p prime. If $p \nmid a_n$; $p | a_m$, $m < n$; $p^2 \nmid a_0$, then $a_0 x^n + \cdots + a_0$ irred.
   E.g., $x^5 + 2x^4 - 4x + 2$ is irreducible.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.
   p prime. If $p \nmid a_n$; $p | a_m$, $m < n$; $p^2 \nmid a_0$, then $a_0 x^n + \cdots + a_0$ irred.
   E.g., $x^5 + 2x^4 - 4x + 2$ is irreducible.
5. Shifting.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.
   p prime. If $p \nmid a_n$; $p | a_m$, $m < n$; $p^2 \nmid a_0$, then $a_0 x^n + \cdots + a_0$ irred.
   E.g., $x^5 + 2x^4 - 4x + 2$ is irreducible.
5. Shifting.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.
   p prime. If $p \nmid a_n$; $p | a_m$, $m < n$; $p^2 \nmid a_0$, then $a_0 x^n + \cdots + a_0$ irred.
   E.g., $x^5 + 2x^4 - 4x + 2$ is irreducible.
5. Shifting. $f(x) = g(x)h(x)$ iff $f(x + a) = g(x + a)h(x + a)$.

Irreducibility in $\mathbb{Q}[x]$ vs $\mathbb{Z}[x]$

Fact. Z a UFD $\Rightarrow$ primitive $f(x) \in Z[x]$ is irred. in $Q[x]$ iff irred. in $Z[x]$.

Irreducibility tests. $f(x) \in Z[x]$, Z a UFD, Q = fraction field.

1. Root Theorem.
   $f(r) = 0$ iff $f(r) = (x - r)g(x)$. E.g., $x^5 + x^3 - x^2 - 1$ is reducible.
2. Rational Root Theorem.
   If $r = s/t$ is a root of $a_n x^n + \cdots + a_0$, $(s,t) = 1$, then $s \mid a_0$ and $t \mid a_n$.
3. Reduction modulo a prime ideal.
   If $f(x) = g(x)h(x)$, then $f(x) \equiv g(x)h(x) \pmod{P}$.
   E.g. $301x^3 + 202x^2 + 103x + 9999$ is irred in $\mathbb{Z}[x]$.
4. Eisenstein's Criterion.
   p prime. If $p \nmid a_n$; $p | a_m$, $m < n$; $p^2 \nmid a_0$, then $a_0 x^n + \cdots + a_0$ irred.
   E.g., $x^5 + 2x^4 - 4x + 2$ is irreducible.
5. Shifting. $f(x) = g(x)h(x)$ iff $f(x+a) = g(x+a)h(x+a)$.
   E.g., $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + 1$ is irred, by E's Crit applied to $\Phi_p(x+1) = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}$.