Polynomial rings

Modern Algebra 1

Fall 2016

$\mathbb{Z}[x], \mathbb{F}[x, y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1 x + \cdots + a_n x^n$, $a_i \in R$.

$\mathbb{Z}[x], \mathbb{F}[x, y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting.
(Elements are normal forms for words.)

$\mathbb{Z}[x], \mathbb{F}[x,y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting.
(Elements are normal forms for words.)
More precisely, every word in $X = \{x\}$ in the language of commutative rings can be reduced to a unique word of the form $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{Z}$.

$\mathbb{Z}[x], \mathbb{F}[x,y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting. (Elements are normal forms for words.)
More precisely, every word in $X = \{x\}$ in the language of commutative rings can be reduced to a unique word of the form $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{Z}$.
$\mathbb{Z}[x]$ is the free ring over $\{x\}$. The universal property is verified by **evaluation**:

$\mathbb{Z}[x], \mathbb{F}[x, y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting. (Elements are normal forms for words.)
More precisely, every word in $X = \{x\}$ in the language of commutative rings can be reduced to a unique word of the form $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{Z}$.
$\mathbb{Z}[x]$ is the free ring over $\{x\}$. The universal property is verified by **evaluation**:

Any function $\{x\} \to R\colon x \mapsto r$ extends uniquely to a ring homomorphism

$$\mathbf{eval}_r\colon \mathbb{Z}[x] \to R\colon p(x) \mapsto p(r).$$

$\mathbb{Z}[x], \mathbb{F}[x,y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting.
(Elements are normal forms for words.)
More precisely, every word in $X = \{x\}$ in the language of commutative rings can be reduced to a unique word of the form $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{Z}$.
$\mathbb{Z}[x]$ is the free ring over $\{x\}$. The universal property is verified by **evaluation**:

Any function $\{x\} \to R\colon x \mapsto r$ extends uniquely to a ring homomorphism

$$\mathbf{eval}_r\colon \mathbb{Z}[x] \to R\colon p(x) \mapsto p(r).$$

If $X = \{x_1, x_2, \ldots\}$, then $\mathbb{Z}[X]$ is the free commutative ring over X.

$\mathbb{Z}[x], \mathbb{F}[x,y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting. (Elements are normal forms for words.)
More precisely, every word in $X = \{x\}$ in the language of commutative rings can be reduced to a unique word of the form $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{Z}$.
$\mathbb{Z}[x]$ is the free ring over $\{x\}$. The universal property is verified by **evaluation**:

Any function $\{x\} \to R \colon x \mapsto r$ extends uniquely to a ring homomorphism

$$\mathbf{eval}_r \colon \mathbb{Z}[x] \to R \colon p(x) \mapsto p(r).$$

If $X = \{x_1, x_2, \ldots\}$, then $\mathbb{Z}[X]$ is the free commutative ring over X. $R[X]$ is the free commutative R-algebra over X.

$\mathbb{Z}[x], \mathbb{F}[x,y], R[X]$, Chap 9

Book's definition: a *polynomial* over R in the variable x is a formal expression $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in R$.
What they are trying to express is that $R[x]$ is a free object in some setting. (Elements are normal forms for words.)
More precisely, every word in $X = \{x\}$ in the language of commutative rings can be reduced to a unique word of the form $a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{Z}$.
$\mathbb{Z}[x]$ is the free ring over $\{x\}$. The universal property is verified by **evaluation**:

Any function $\{x\} \to R\colon x \mapsto r$ extends uniquely to a ring homomorphism

$$\mathbf{eval}_r\colon \mathbb{Z}[x] \to R\colon p(x) \mapsto p(r).$$

If $X = \{x_1, x_2, \ldots\}$, then $\mathbb{Z}[X]$ is the free commutative ring over X. $R[X]$ is the free commutative R-algebra over X.

If R is a domain, then $R[x]$ is a domain.

Ideals of $\mathbb{F}[x]$

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$.

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$.

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \dots \rangle, \quad \text{for} \quad I = (p_1, p_2, \dots).$$

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$),

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$ (α algebraic/$\mathbb{F}$),

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$ (α algebraic/$\mathbb{F}$), in either case I is principal,

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$ (α algebraic/$\mathbb{F}$), in either case I is principal, and in (ii) the principal generator can be taken to be a monic, irreducible (=nonfactorable) polynomial over $\mathbb{F}$.

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$ (α algebraic/$\mathbb{F}$), in either case I is principal, and in (ii) the principal generator can be taken to be a monic, irreducible (=nonfactorable) polynomial over $\mathbb{F}$.

What we know at this point is that I is prime.

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\}\rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots\rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$ (α algebraic/$\mathbb{F}$), in either case I is principal, and in (ii) the principal generator can be taken to be a monic, irreducible (=nonfactorable) polynomial over $\mathbb{F}$.

What we know at this point is that I is prime. We also want to show that in case (ii) I is maximal.

Ideals of $\mathbb{F}[x]$

If $\mathbb{F} \leq \mathbb{K}$ are fields, and $\alpha \in \mathbb{K} - \mathbb{F}$, then we are interested in the structure of $\mathbb{F}[\alpha] = \langle \mathbb{F} \cup \{\alpha\} \rangle$. This is $\cong \mathbb{F}[x]/I$ where $I = \ker(\mathbf{eval}_\alpha)$. Hence $\mathbb{F}[\alpha]$ has a commutative $\mathbb{F}$-algebra presentation

$$\langle x \mid p_1(x) = 0, p_1(x) = 0, \ldots \rangle, \quad \text{for} \quad I = (p_1, p_2, \ldots).$$

Our goal is to show that either (i) $I = (0)$ (α transcendental/$\mathbb{F}$), or (ii) $I = (p(x))$ (α algebraic/$\mathbb{F}$), in either case I is principal, and in (ii) the principal generator can be taken to be a monic, irreducible (=nonfactorable) polynomial over $\mathbb{F}$.

What we know at this point is that I is prime. We also want to show that in case (ii) I is maximal. So if α is algebraic over $\mathbb{F}$, then $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$ is a field.

Stage I: $\mathbb{F}[x]$ is a Euclidean Domain

Stage I: $\mathbb{F}[x]$ is a Euclidean Domain

Df. An integral domain D is *Euclidean* if it "possesses a division algorithm": there is a function $N\colon D \to \mathbb{Z}^{\geq 0}$ satisfying $N(0) = 0$ such that whenever $a, b \in D$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $N(r) < N(b)$.

Stage I: $\mathbb{F}[x]$ is a Euclidean Domain

Df. An integral domain D is *Euclidean* if it "possesses a division algorithm": there is a function $N\colon D \to \mathbb{Z}^{\geq 0}$ satisfying $N(0) = 0$ such that whenever $a, b \in D$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $N(r) < N(b)$.

1. $N(x) = |x|$ is a norm on $\mathbb{Z}$.

Stage I: $\mathbb{F}[x]$ is a Euclidean Domain

Df. An integral domain D is *Euclidean* if it "possesses a division algorithm": there is a function $N\colon D \to \mathbb{Z}^{\geq 0}$ satisfying $N(0) = 0$ such that whenever $a, b \in D$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $N(r) < N(b)$.

1. $N(x) = |x|$ is a norm on $\mathbb{Z}$.
2. $N(p(x)) = \deg(p(x))$ is a norm on $\mathbb{F}[x]$.

Stage I: $\mathbb{F}[x]$ is a Euclidean Domain

Df. An integral domain D is *Euclidean* if it "possesses a division algorithm": there is a function $N\colon D \to \mathbb{Z}^{\geq 0}$ satisfying $N(0) = 0$ such that whenever $a, b \in D$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $N(r) < N(b)$.

1. $N(x) = |x|$ is a norm on $\mathbb{Z}$.
2. $N(p(x)) = \deg(p(x))$ is a norm on $\mathbb{F}[x]$.

Stage I: $\mathbb{F}[x]$ is a Euclidean Domain

Df. An integral domain D is *Euclidean* if it "possesses a division algorithm": there is a function $N\colon D \to \mathbb{Z}^{\geq 0}$ satisfying $N(0) = 0$ such that whenever $a, b \in D$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $N(r) < N(b)$.

1. $N(x) = |x|$ is a norm on $\mathbb{Z}$.
2. $N(p(x)) = \deg(p(x))$ is a norm on $\mathbb{F}[x]$.

Note: $N(r) = 0$ implies $r = 0$ or r is a unit.

Stage II: Euclidean Domains are PID's (*)

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*).

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

If $N(b) = 0$, then b is a unit, so $R = (b) \subseteq I$, and I is principal.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

If $N(b) = 0$, then b is a unit, so $R = (b) \subseteq I$, and I is principal.

Else $N(b)$ is positive.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

If $N(b) = 0$, then b is a unit, so $R = (b) \subseteq I$, and I is principal.

Else $N(b)$ is positive. Choose any $a \in I$ and write $a = qb + r$ with $N(r) < N(b)$.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

If $N(b) = 0$, then b is a unit, so $R = (b) \subseteq I$, and I is principal.

Else $N(b)$ is positive. Choose any $a \in I$ and write $a = qb + r$ with $N(r) < N(b)$.

$r = a - qb \in I$ has smaller norm, so $r = 0$.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

If $N(b) = 0$, then b is a unit, so $R = (b) \subseteq I$, and I is principal.

Else $N(b)$ is positive. Choose any $a \in I$ and write $a = qb + r$ with $N(r) < N(b)$.

$r = a - qb \in I$ has smaller norm, so $r = 0$.
So $a = qb \in (b)$.

Stage II: Euclidean Domains are PID's (*)

Df. R a PID $\Leftrightarrow$ R is an integral domain where every ideal is principal.

Proof of (*). Let D be Euclidean and $I \lhd D$, $I \neq (0)$.

Choose $b \in I - \{0\}$ of least norm.

If $N(b) = 0$, then b is a unit, so $R = (b) \subseteq I$, and I is principal.

Else $N(b)$ is positive. Choose any $a \in I$ and write $a = qb + r$ with $N(r) < N(b)$.

$r = a - qb \in I$ has smaller norm, so $r = 0$.
So $a = qb \in (b)$. So $I = (b)$. $\square$

Elements versus ideals

Throughout, D is an integral domain.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.
6. a and b are associate (=differ by a unit) iff $(a) = (b)$

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.
6. a and b are associate (=differ by a unit) iff $(a) = (b)$
7. a is associate to $b_1 b_2 \ldots b_k$ iff $(a) = (b_1 b_2 \cdots b_k) = (b_1)(b_2) \cdots (b_k)$

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.
6. a and b are associate (=differ by a unit) iff $(a) = (b)$
7. a is associate to $b_1 b_2 \ldots b_k$ iff $(a) = (b_1 b_2 \cdots b_k) = (b_1)(b_2) \cdots (b_k)$
8. Given $a, b \in D$, if (d) is the smallest principal ideal satisfying $(a) + (b) \subseteq (d)$, then $d = \gcd(a, b)$.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.
6. a and b are associate (=differ by a unit) iff $(a) = (b)$
7. a is associate to $b_1 b_2 \ldots b_k$ iff $(a) = (b_1 b_2 \cdots b_k) = (b_1)(b_2) \cdots (b_k)$
8. Given $a, b \in D$, if (d) is the smallest principal ideal satisfying $(a) + (b) \subseteq (d)$, then $d = \gcd(a, b)$.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.
6. a and b are associate (=differ by a unit) iff $(a) = (b)$
7. a is associate to $b_1 b_2 \ldots b_k$ iff $(a) = (b_1 b_2 \cdots b_k) = (b_1)(b_2)\cdots(b_k)$
8. Given $a, b \in D$, if (d) is the smallest principal ideal satisfying $(a) + (b) \subseteq (d)$, then $d = \gcd(a, b)$.

If D is a PID, gcd's exist, and if $d = \gcd(a, b)$ then $d = au + bv$ for some $u, v \in D$.

Elements versus ideals

Throughout, D is an integral domain.

1. u is a unit iff $(u) = R$.
2. A nonzero nonunit p is a prime iff (p) is a nonzero prime ideal.
3. A nonzero nonunit q is irreducible iff (q) is maximal among nonzero proper principal ideals.
4. Fact: primes are irreducible.
5. Fact: in a PID, irreducibles are prime.
6. a and b are associate (=differ by a unit) iff $(a) = (b)$
7. a is associate to $b_1 b_2 \dots b_k$ iff $(a) = (b_1 b_2 \cdots b_k) = (b_1)(b_2)\cdots(b_k)$
8. Given $a, b \in D$, if (d) is the smallest principal ideal satisfying $(a) + (b) \subseteq (d)$, then $d = \gcd(a, b)$.

If D is a PID, gcd's exist, and if $d = \gcd(a, b)$ then $d = au + bv$ for some $u, v \in D$. If D is Euclidean with effective division algorithm, then u, v, d can be computed algorithmically with the Euclidean algorithm.

Prime ideals in $\mathbb{F}[x]$

1. Every nonzero polynomial in $\mathbb{F}[x]$ is associate to a monic polynomial.

Prime ideals in $\mathbb{F}[x]$

1. Every nonzero polynomial in $\mathbb{F}[x]$ is associate to a monic polynomial.
2. $I \lhd \mathbb{F}[x]$ is prime iff $I = (0)$ or $I = (p(x))$ for some monic irreducible $p(x) \in \mathbb{F}[x]$

Prime ideals in $\mathbb{F}[x]$

1. Every nonzero polynomial in $\mathbb{F}[x]$ is associate to a monic polynomial.
2. $I \lhd \mathbb{F}[x]$ is prime iff $I = (0)$ or $I = (p(x))$ for some monic irreducible $p(x) \in \mathbb{F}[x]$

Prime ideals in $\mathbb{F}[x]$

1. Every nonzero polynomial in $\mathbb{F}[x]$ is associate to a monic polynomial.
2. $I \lhd \mathbb{F}[x]$ is prime iff $I = (0)$ or $I = (p(x))$ for some monic irreducible $p(x) \in \mathbb{F}[x]$ $I = (0)$ or I is maximal.
3. If $p(x)$ is a monic irreducible, then $\mathbb{F}[x]/(p)$ is a field.