PMATH 345 Lecture 1: September 14, 2009

~pmat345

- $\mathbb{Z}$ Integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $C[0,1]$ all continuous functions $f\colon [0,1] \to \mathbb{R}$

In both cases:
can "add": $(f+g)\colon [0,1] \to \mathbb{R}$, $x \mapsto f(x) + g(x)$
can "multiply": $(fg)\colon [0,1] \to \mathbb{R}$, $x \mapsto f(x)g(x)$
both 0 and 1

figure: 0 function and 1 function

Definition: A *ring* R is a set with two distinguished elements, 0 and 1, and two binary functions

$$+\colon R^2 \to R$$
$$\times\colon R^2 \to R$$

i.e., given two elements x, y we can add them $x + y \in R$, we can multiply them $xy \in R$[1)]
such that: for all $x, y, z \in R$,

1. Associativity of addition:
$$(x+y)+z = x+(y+z)\text{[2)]}$$

2. Commutativity of addition:
$$x + y = y + x$$

3. Neutrality of zero:
$$x + 0 = x\text{[3)]}$$

4. Existence of additive inverse:
For all $x \in R$ there is some $y \in R$ such that
$$x + y = 0\text{[4)]}$$

5. Associativity of multiplication:
$$(xy)z = x(yz)\text{[5)]}$$

6. Neutrality of one:
$$x1 = x = 1x$$

7. Distributivity:
$$(x+y)z = xz + yz$$
$$z(x+y) = zx + zy$$

Remarks:

1. **WARNING:** What we call a ring here is a "ring with identity" for some people.
For us rings always have 1.
Example: $2\mathbb{Z}$ set of even integers
For Dummit and Foote this is a ring, for us it is *not*.

2. **Notation:** $x - y$ means $x + (-y)$

---

1) Note: drop the $\times$ sometimes.
2) Note: so we just write $x + y + z$
3) zero is also called "additive identity"
4) Note: We write $-x$ for y here and call it the negative of x
5) we just write xyz

3. We don't ask $\times$ to be commutative. Why?
   Example: $M_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{R} \right\}$

   - $0 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$
   - $1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$
   - $+$ matrix addition
   - $\times$ matrix multiplication

   Check: This is a *ring*. $\times$ is not commutative.

   Why should $+$ be commutative?
   Because it is *forced* by the other axioms.

$$\begin{aligned}
(\overset{x}{1} + \overset{y}{1})(a \overset{z}{+} b) &= 1(a+b) + 1(a+b) \\
&= (a+b) + (a+b) \\
(1 \overset{z}{+} 1)(\overset{x}{a} + \overset{y}{b}) &= (1+1)a + (1+1)b \\
&= (1a + 1a) + (1b + 1b) \\
&= (a+a) + (b+b) \\
(a+b) + (a+b) &= (a+a) + (b+b) \\
a + b + a + b &= a + a + b + b
\end{aligned}$$

   add $(-a)$ to both sides on the left

$$b + a + b = a + b + b$$

   add $(-b)$ to both sides on the right

$$b + a = a + b$$

PMATH 345 Lecture 2: September 16, 2009

Definition: A ring R is *commutative* if for all $x, y \in R$, $xy = yx$.

Proposition: Let R be a ring.

(a) If $x + z = y + z$ then $x = y$.

(b) For all y there is a *unique* y such that $x + y = 0$.
(We call y the *additive inverse* of x, denote it by $-x$).

(c) For all x, $-(-x) = x$.

(d) If $x \in R$, $0x = 0 = x0$.

(e) $(-1)x = -x = x(-1)$.

(f) $(-x)y = -(xy) = x(-y)$

(g) $(-x)(-y) = xy$

Proof:

(a) $x + z = y + z$
Let u be such that $z + u = 0$.

$$\begin{aligned}
\implies x + z + u &= y + z + u \\
\implies x + 0 &= y + 0 \\
\implies x &= y
\end{aligned}$$

(b) By existence of additive inverses there is a $y \in R$ such that $x + y = 0$. Suppose $x + y' = 0$ also.

$$x + y = x + y'$$

By part (a) and commutativity

$$y = y'.$$

(c) $x + (-x) = 0$ since $-x$ is the additive inverse of x.
Therefore x must be the additive inverse of $(-x)$.
i.e., $x = -(-x)$.

(d) $0 + 0x =^{6)} 0x =^{7)} (0 + 0)x =^{8)} 0x + 0x$
Therefore by (a), $0 = 0x$.
Similarly $x0 = 0$.

(e) $x + (-1)x =^{9)} 1x + (-1)x =^{10)} (1 + (-1))x = 0x =^{11)} 0$
Therefore $(-1)x = -x$.

(f) $(-x)y =^{12)} ((-1)x)y =^{13)} (-1)(xy) =^{14)} -(xy)$
Similarly for $x(-y)$.

(g) $(-x)(-y) =^{15)} -(x(-y)) =^{16)} -(-(xy)) =^{17)} xy$.

Examples:

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

not a ring: positive integers; no additive inverse.

$C[0, 1]$
Definition: Given any ring R and nonempty set X let $\mathrm{Fun}(X, R)$ be the set of all functions from X to R.

$(f + g)(x) := f(x) + g(x)$, here $f: X \to R$, $g: X \to R$
$(fg)(x) := f(x)g(x)$
$0(x) = 0$ for all $x \in X$
$1(x) = 1$ for all $x \in X$
Check: $\mathrm{Fun}(X, R)$ is a ring. Its commutative iff R is commutative.

not a ring: set of monotonic $f: [0, 1] \to \mathbb{R}$ with usual $+$, $\times$ on functions; not closed under $\times$

$M_2(\mathbb{R})$
Definition: Given any ring R, $n \geq 1$, $M_n(R) =$ set of all $n \times n$ matrices with entries in R

Usual matrix addition and multiplication formulas.
0 matrix.
1 matrix.

check: $M_n(R)$ is a ring. Even if R is commutative, this need not be.

not a ring: $\mathrm{GL}_n(\mathbb{R}) = n \times n$ matrices with det $\neq 0$; not preserved by matrix addition

---

[6] neutrality of 0
[7] since $0 = 0 + 0$ by neutrality
[8] distributitivity
[9] neutrality of 1
[10] distributivity
[11] (d)
[12] (e)
[13] associativity
[14] (e)
[15] (f)
[16] (f)
[17] (c)

Definition: Given rings R, S with $+_R, \times_R, 0_R, 1_R$ the ring structure on R and $+_S, \times_S, 0_S, 1_S$ the ring structure on S.

The *direct product* of R and S is:

$$\begin{aligned} R \times S &= \{ (a,b) : a \in R, b \in S \} \\ (a,b) + (a',b') &= (a +_R a', b +_S b')^{18)} \\ (a,b)(a',b') &= (a \times_R a', b \times_S b')^{19)} \\ 0 &\quad (0_R, 0_S) \\ 1 &\quad (1_R, 1_S) \end{aligned}$$

check: that $R \times S$ is a ring, commutative iff both R and S are.

Example: $\mathbb{Z}_n$. $n \geq 2$, *residues modulo* n
$a, b \in \mathbb{Z}$ are *congruent modulo* n if $n \mid (a - b)$, $a \equiv b \pmod{n}$.
Congruence is an equivalence relation on $\mathbb{Z}$.
$a \in \mathbb{Z}$, let $\overline{a} =$ equivalence class of $a = \{ b \in \mathbb{Z} : a \equiv b \pmod{n} \} =:$ *residue* of $a \pmod{n}$
$\mathbb{Z}_n$ is $\{ \overline{a} : a \in \mathbb{Z} \} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$
Note: $\overline{a} = \overline{b} \iff a \equiv b \pmod{n}$

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a+b} \\ \overline{a}\overline{b} &:= \overline{ab} \end{aligned}$$

Warning: Check this is *well-defined*!
i.e., if $\overline{a} = \overline{a'}$ then need $\overline{ab} = \overline{a'b'}$
similarly for $+$.
zero is $\overline{0}$
one is $\overline{1}$
Check: This is a commutative ring.

PMATH 345 Lecture 3: September 18, 2009

Aside: **Remark:** R is a ring. Then 0, 1 are unique.

a) If $a \in R$ such that $a + x = x$ for all x, then $a = 0$

b) If $a \in R$ such that $ax = x$ for all x, then $a = 1$

Proof:

a) $a + x = x \implies a + 0 = 0$
$\implies a = 0$, since $a + 0 = a$

b) $ax = x \implies a1 = 1$
$\implies a = 1$

Note: In fact, if $a + x = x$ for any x, then $a = 0$ since $a + x = x = 0 + x$
$\implies a = 0$
Note: If R is such that $0 = 1$, then $R = \{0\}$
Proof: If $x \in R$, then

$$\begin{aligned} x &= 1x \\ &= 0x \\ &= 0 \end{aligned}$$

Therefore $x = 0$.
$R = \{0\}$ is called the trivial ring.

18) "co-ordinate addition"
19) "co-ordinate multiplication"

For $\mathbb{Z}_n$, $n \geq 2$, given $a \in \mathbb{Z}$, then the *residue* of a,

$$\begin{aligned}\overline{a} &= \{\, b \in \mathbb{Z} : a \equiv b \pmod{n} \,\} \\ &= \{\, a + rn : r \in \mathbb{Z} \,\} \subseteq \mathbb{Z}\end{aligned}$$

Note: $\overline{a} \cap \overline{b} = \emptyset$ or $\overline{a} = \overline{b}$
Note: For all $x \in \mathbb{Z}$, $x \in \overline{a}$ for some $a \in \{0, \ldots, n-1\}$

$$\begin{aligned}\text{Therefore } \mathbb{Z}_n &= \{\, \overline{a} : a \in \mathbb{Z} \,\} \text{ is \textit{finite}.} \\ &= \{\overline{0}, \ldots, \overline{n-1}\}\end{aligned}$$

Definition: Let R be a ring. A *subring* of R is a set $S \subseteq R$ which is preserved by $+$ and $\times$ and $-$ and contains 0 and 1.
i.e., if $a, b \in S \implies a + b \in S$
and $a, b \in S \implies ab \in S$, then S is a subring and $-a \in S$.
$*$ different from textbook for us, $\{0\}$ is not a subring of R unless $R = \{0\}$.
Note: S is a ring, we call it the "induced ring".
Example: $\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of $\mathbb{R}$ which is a subring of $\mathbb{C}$.
Example: The Gaussian integers $\mathbb{Z}[i] = \{\, a + bi : a, b \in \mathbb{Z} \,\}$ is a subring of $\mathbb{C}$.

Units and Zero Divisors
Definition: Let R be a ring. An element of $a \in R$ is a *unit* if there exists $b \in R$ such that $ab = 1$ and $ba = 1$
Remark: b is unique
Proof: If $ac = 1$ and $ca = 1$,
therefore $ac = ab$
$\implies cac = cab$
$\implies 1c = 1b \implies c = b$
Such a b is called the multiplicative inverse of a and is denoted a^{-1}.
Definition: A *field* is a commutative ring where $0 \neq 1$ and every nonzero element is a unit.
Note: If $0x = 1$, then since $0x = 0$, we have $0 = 1$.
So, in a nontrivial ring, 0 is *not* a unit.
Example: $\mathbb{Z}$ is *not* a field, $\mathbb{Q}$ is a field.
Definition: Let R be a ring. An element $a \in R$, $a \neq 0$ is a *zero divisor* if there exists $b \in R$, $b \neq 0$ such that

$$ab = 0 \qquad \text{or} \qquad ba = 0$$

b is not necessarily unique.
Definition: An *integral domain* is a commutative ring with $0 \neq 1$ and there are no zero divisors.
Example: $\mathbb{Z}$, $\mathbb{Q}$ are integral domains
$\mathbb{Z} \times \mathbb{Z}$ is not an integral domain, as $(a, 0) \cdot (0, a) = (0, 0)$, so $(a, 0)$ is a zero divisor for $a \neq 0$.

PMATH 345 Lecture 4: September 21, 2009

Proposition: R ring, $a \in R$, $a \neq 0$ *a is not a zero divisor* if and only if whenever

$$\begin{gathered}\text{if } ab = ac \text{ for some } b, c \in R \text{ then } b = c, \\ \textit{and} \text{ if } ba = ca \text{ for some } b, c \in R \text{ then } b = c\end{gathered} \tag{$*$}$$

Proof: Suppose a is *not a zero divisor.*
Suppose $ab = ac$.

$$\begin{aligned}&\implies ab - ac = 0 \\ &\implies a(b - c) = 0\end{aligned}$$

Since a is not a zero divisor and $a \neq 0$,

$$\begin{aligned}b - c &= 0 \\ \implies b &= c\end{aligned}$$

Similarly if $ba = ca$ then

$$\begin{aligned} ba - ca &= 0 \\ \implies (b-c)a &= 0 \\ \implies b - c &= 0 \\ \implies b &= c \end{aligned}$$

Conversely suppose $(*)$ is true of a.
If $ab = 0 = a0$ then by $(*)$ $b = 0$.
If $ba = 0 = 0a$ by $(*)$ $b = 0$.
So a is *not* a zero divisor.

Corollary: Units are never zero divisors.
Proof: Suppose u is a unit in R.
If $ub = uc$ then multiply both sides by u^{-1}.

$$\begin{aligned} u^{-1}ub &= u^{-1}uc \\ \implies 1b &= 1c \\ \implies b &= c \end{aligned}$$

Similarly $bu = cu$, $\implies b = c$.
So by proposition, u is *not* a zero divisor.

Example: In the direct product $\mathbb{Z} \times \mathbb{Z}$, $(1,2)$ is not a unit.

$$\begin{aligned} (1,2)(a,b) &= (1,1) \\ \implies (a,2b) &= (1,1) \\ \implies a &= 1 \\ 2b &= 1^{20)} \end{aligned}$$

Also *not* a zero divisor.

$$\begin{aligned} (1,2)(a,b) &= (0,0) \\ (a,2b) &= (0,0) \\ \implies a &= 0 \\ 2b &= 0 \\ \implies b &= 0 \end{aligned}$$

So $(a,b) = (0,0)$.
Corollary: Every field is an integral domain[21)].

Example: $\mathbb{Z}$ is an integral domain but *not* a field.

Theorem: If R is finite then every nonzero element is either a unit or a zero divisor.

Proof: Suppose $a \in R$, $a \neq 0$, is not a zero divisor. Consider the function

$$\begin{aligned} f_a \colon R &\to R \\ b &\mapsto ab \end{aligned}$$

By the proposition since a is not a zero divisor if $f_a(b) = f_a(c)$ then $ab = ac$ then $b = c$.
So f_a is injective.
R finite $\implies$ f_a is also surjective.

---

20) contradiction

21) $0 \neq 1$, commutative

So there is a $c \in R$ such that $f_a(c) = 1$, i.e., $ac = 1$.
Repeating the argument with

$$\begin{aligned} g_a \colon R &\to R \\ b &\mapsto ba \end{aligned}$$

we get a $c' \in R$ such that $c'a = 1$.

$$\begin{aligned} c' = c'1 &= c'(ac) \\ &= (c'a)c \\ &= 1c \\ &= c \end{aligned}$$

So $c = a^{-1}$ is the inverse, i.e., a is a unit.

$\mathbb{Z}_n$ is a finite commutative ring (fixed $n \geq 2$).
Every residue by the theorem is either 0, or zero divisor or a unit.
Which are which?
Recall: $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, are called *coprime* if $\gcd(a, b) = 1$.
FACT: $\gcd(a, b) = 1 \iff$ there are x, y such that $ax + by = 1$, $a, b \in \mathbb{Z}$

Proposition: Suppose $a \in \mathbb{Z}$, $a \neq 0$.
$\overline{a}$ is a unit in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$.
(So by the theorem the zero divisors are the $\overline{b}$ where $\gcd(b, n) \neq 1$.)

Proof: Suppose $\gcd(a, n) = 1$, so $ax + ny = 1$ for some $x, y \in \mathbb{Z}$.

$$\begin{gathered} \overline{ax +^{22)} ny} = \overline{1} \\ \overline{ax} +^{23)} \overline{ny} = \overline{1} \\ \overline{ax} + \overline{ny} = \overline{1} \\ ny \equiv 0 \pmod{n} \implies \overline{ny} = \overline{0} \\ \implies \overline{ax} = \overline{1} \end{gathered}$$

So $\overline{x} = \overline{a}^{-1}$ and $\overline{a}$ is a unit.
Conversely, suppose $\overline{a} \in \mathbb{Z}_n$ is a unit.
Want: $\gcd(a, n) = 1$.
Let $\overline{a}^{-1} \in \mathbb{Z}_n$, $\overline{a}^{-1} = \overline{x}$ for some $x \in \mathbb{Z}$.

$$\begin{gathered} \overline{a}\overline{a}^{-1} = \overline{1} \\ \overline{a}\overline{x} = \overline{1} \\ \overline{ax} = \overline{1} \\ ax \equiv 1 \pmod{n} \end{gathered}$$

there there is a $y \in \mathbb{Z}$ such that

$$\begin{gathered} 1 - ax = ny \\ 1 = ax + ny \\ {}^{24)} \gcd(a, d) = 1 \end{gathered}$$

Corollary: $\mathbb{Z}_n$ is a field iff n is prime.

Proof: $\mathbb{Z}_n$ is a field iff every nonzero $\overline{a}$ is a unit iff *every nonzero a,* $\gcd(a, n) = 1$ iff n is prime

---

[22] in $\mathbb{Z}$
[23] in $\mathbb{Z}_n$
[24] fact

Example: $\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{8}\}$
units: $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$
zero divisors: $\overline{3}, \overline{6}$

Let $\phi(n) = \#$ of units in $\mathbb{Z}_n$, $\phi(9) = 6$.
When n is a prime, $\phi(n)$[25] $= n - 1$ By proposition

$$\phi(n) = \# \text{ of nonzero integers } 2n \text{ which are coprime to } n$$

Application: Theorem: If $a \neq 0$, $a \in \mathbb{Z}$, $n \geq 2$, $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.
So: $5^6 \equiv 1 \pmod{n}$, $8^6 \equiv 1 \pmod{n}$, $n = 9$

PMATH 345 Lecture 5: September 23, 2009

Euler's Theorem: $a \in \mathbb{Z}$, $a \neq 0$, $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$
$\phi(n) = \#$ of nonnegative integers $< n$ that are coprime with n

Need **Lemma:** R commutative ring, with a *finite* set of units, say m of them. Then if $a \in R$ is a unit then a^m[26] $= 1$.

Proof: a a unit. Consider $f_a : R \to R$ by $b \mapsto ab$. Since a is not a zero divisor, f_a is injective.
Note that the product of units is a unit.
If $U =$ set of units in $R = \{u_1, u_2, \ldots, a_m\}$, then $f_a(U) = U$.
i.e., $f_a|_U : U \to U$ injective, hence bijective since U is finite.
$U = \{u_1, \ldots, u_m\}$
$U = f_a(U) = \{au_1, au_2, \ldots, au_m\}$
$\{u_1, \ldots, u_m\} = \{au_1, \ldots, au_m\}$, so

$$\begin{aligned} \prod_{i=1}^{m} u_i{}^{27)} = \prod_{i=1}^{m} au_i &= (au_1)(au_2)\cdots(au_m) \\ &= a^m(u_1 u_2 \cdots u_m) \\ &= a^m \prod_{i=1}^{m} u_i \end{aligned}$$

Therefore $1 \prod_i = a^m \prod_i u_i$. Since $\prod_i u_i$ is also a unit it is not a zero divisor and hence we can cancel $\implies 1 = a^m$.

Proof of Euler's theorem:
$n \geq 2$, $a \neq 0$, $\gcd(a, n) = 1$.
$R = \mathbb{Z}_n$.
$U =$ set of units in $\mathbb{Z}_n$ has $\phi(n)$ many elements in it by the previous propositions.
$\overline{b}$ is a unit in $\mathbb{Z}_n \iff \gcd(b, n) = 1$
$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \#$ of units $= \phi(n)$
$\overline{a} \in \mathbb{Z}_n$ is a unit.
$\#$ of units in $\mathbb{Z}_n$ is $\phi(n)$ so by the lemma

$$\begin{aligned} &\overline{a}^{\phi(n)} = \overline{1}^{28)} \\ \implies &\overline{a^{\phi(n)}} = \overline{1} \\ \implies &a^{\phi(n)} \equiv 1 \pmod{n} \end{aligned}$$

What are the units/zero divisors in $\mathbb{Z}[i] = \{\, a + bi : a, b \in \mathbb{Z} \,\}$?
zero divisors: *none*.

---

[25] Euler's function
[26] $\underbrace{a \cdot a \cdot a \cdots a}_{m \text{ times}}$
[27] $u_1 u_2 \cdots u_m$
[28] in $\mathbb{Z}_n$

$\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ and $\mathbb{C}$ have no zero divisors.
($u, v \in \mathbb{C}$, $uv = 0 \implies u = 0$ or $v = 0$, i.e., $\mathbb{C}$ is an integral domain)
units: units in $\mathbb{C}$ are $\mathbb{C} \setminus \{0\}$ (i.e., $\mathbb{C}$ is a field.)
$*$ This does *not* mean that $\mathbb{Z}[i]$ is a field. Example: 2 is a unit in $\mathbb{Q}$ but not in $\mathbb{Z}$.

units: ± 1, $\pm i$
claim: these are the only units
Proof: $z \in \mathbb{Z}[i]$, $z = a + bi$
$|z| = \sqrt{a^2 + b^2}$
$N(z) = |z|^2 = a^2 + b^2 \in \mathbb{Z}$
$z, w \in \mathbb{Z}$, $N(zw) = N(z)N(w)$
If z is a unit in $\mathbb{Z}[i]$, let $w = z^{-1} \in \mathbb{Z}[i]$,
$1 = zw \implies N(1)$[29] $= N(zw) = N(z)N(w)$
$N(w) = N(z)^{-1}$,
i.e., $N(z)$ is a *unit* in $\mathbb{Z}$.
$\implies N(z) = \pm 1$
$\implies a^2 + b^2 = \pm 1$
$\implies a^2 + b^2 = 1$
$\implies a = \pm 1$ and $b = 0$
or
$a = 0$ and $b = \pm 1$
$z = 1, -1, i, -i$

Exercise: $\text{Fun}([0,1], \mathbb{R})$. What are the zero-divisors and the units?

Polynomials:
Definition: R commutative ring. Let x be an indeterminate (i.e., a variable), i.e., x is just a symbol.
A *polynomial in x over R* is a formal expression[30] of the form

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

where a_is are in R *and* all but finitely many of the a_is are 0.

$$a_0 + a_1 x + a_2 x^2 + \cdots = b_0 + b_1 x + b_2 x^2 + \cdots$$

if and only if each $a_i = b_i$ in R.

Notational conventions:

1. We use series notation:
$$a_0 + a_1 x + a_2 x^2 + \cdots =: \sum_{i=0}^{\infty} a_i x^i$$

2. We often *drop* the $a_i x^i$ if $a_i = 0$.
So for example when $R = \mathbb{Z}$, we write:
$$x^2 - 2x^4 + x^6$$
rather than
$$0 + 0x + 1x^2 + 0x^3 + (-2)x^4 + 1x^6 + 0x^7 + 0x^8 + \cdots$$

3. we also write $x^2 - 2x^4$ instead of $x^2 + (-2)x^4$

Let $R[x]$ denote the *set* of all polynomials in x over R.

[29] 1
[30] formal expression means it is just a string of symbols

Check: $R[x]$ is a ring with

$$0 = \sum_{i=1}^{\infty} 0x^i$$

$$1 = 1 + 0x + 0x^2 + \cdots$$

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) \coloneqq \sum_{i=0}^{\infty} (a_i + b_i)^{31)} x^i$$

$$\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) \coloneqq \sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} a_{i-j}{}^{32)} b_j\right) x^i$$

PMATH 345 Lecture 6: September 25, 2009

R commutative
$R[x]$ ring of polynomials
$P \in R[x]$, $P = \sum_{i=0}^{\infty} a_i x^i$ formal expression

- $a_i \in R$
- all but finitely many are 0.

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i \left(a_i + b_i\right) x^i \in R[x] \tag{A}$$

$$\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) = \sum_i \left(\sum_{j=0}^{i} a_{i-j} b_j\right) x^i \in R[x] \tag{B}$$

note: x is the usual "collecting terms" rule.
In $\mathbb{Z}[x]$,

$$\begin{aligned} PQ &= (x^2 + 2x^3 - 7x^6)(-x + x^2) \\ &= -x^3 - 2x^4 + 7x^7 + x^4 + 2x^5 - 7x^8 \\ &= -x^3 - x^4 + 2x^5 + 7x^7 - 7x^8 \end{aligned}$$

Remark: Given $P \in R[x]$ it induces a function

$$f_P \colon R \to R$$

by "substitution".

$$P = \sum_i a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots$$

$$f_P(r) = \sum_i a_i r^i = a_0 + a_1 r + a_2 r^2 + \cdots^{33)} \in R$$

for any $r \in R$

Warning: Then maybe $P \neq Q$ in $R[x]$ such that as *functions*, $f_P \neq f_Q$.
So you *cannot* identify the polynomial with the function it induces.
Example: $\mathbb{Z}_2[x]$

$$P = 0 = \sum_i 0x^i \in \mathbb{Z}_2[x]$$

$$Q = x + x^2 = 0 + 1x + 1x^2 + 0x^3 + 0x^4 + \cdots$$

---

31) in R
32) in R
33) finite sum

$P \neq Q$ but $0 \neq 1$ in $\mathbb{Z}_2$
$f_P \colon \mathbb{Z}_2 \to \mathbb{Z}_2$, $f_P(\overline{0}) = f_P(\overline{1}) = \overline{0}$
$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$
$f_Q(\overline{0}) = \overline{0} + \overline{0}^2 = \overline{0}$
$f_Q(\overline{1}) = \overline{1} + \overline{1}^2 = \overline{1} + \overline{1} = \overline{2} = \overline{0}$
As functions $f_P = f_Q$.

Definition: R commutative ring.
The *power series* ring, $R[[x]]$ is the ring whose elements are formal expressions

$$\sum_{i=0}^{\infty} a_i x^i, \qquad \text{where } a_i \in R$$

(maybe infinitely many nonzero a_is)
where $+$ and $\times$ are given by the rules (A) and (B) (same as in $R[x]$).

Exercise: $R[x]$ is a *subring* of $R[[x]]$.

Definition: R commutative. $P \in R[x]$, $P = \sum_{i=0}^{\infty} a_i x^i$

(a) For any $m \geq 0$, the *coefficient of x^m in P* is a_m.

(b) If $P \neq 0$ then the *degree of P* is the highest power of x that occurs with a nonzero coefficient.

$$\deg P = \max\{\, m : a_m \neq 0 \,\}$$

[the 0 polynomial has no degree]

(c) If $P \neq 0$ then the *leading coefficient of P* is a_n where $n = \deg P$.

(d) If $P \neq 0$ then the *leading term* of P is $a_n x^n$ where $n = \deg P$.

(e) Each summand $a_i x^i$ is called a *monomial* of P.

(f) A *term of P* is a monomial $a_i x^i$ where $a_i \neq 0$ (polynomials have only finitely many terms)[34)]

Note: $\deg P = 0 \implies P = r + 0x + 0x^2 + \cdots$ where $r \neq 0$.
So if $P \neq 0$, $P \in R[x]$, and $n = \deg P$ then we can write

$$P = a_0 + a_1 x + \cdots + a_n x^n$$

Remark: Every element of R can be viewed as a polynomial on R.

$$r = r + 0x + 0x^2 + \cdots$$

Under this identification, R becomes a subring of $R[x]$.

$$R = 0 \cup \{\text{degree 0 polynomials of } R[x]\}$$

Call these *constant polynomial*[35)]

Example: $Q = x + x^2 \in \mathbb{Z}_2[x]$. $\deg Q = 2$, Q is not a constant polynomial.
But as a function $\mathbb{Z}_2 \to \mathbb{Z}$ it is a constant function (it's th zero function).

Proposition: R commutative. $P, Q \in R[x]$. $P \neq 0, Q \neq 0$.

1. If $\deg P \neq \deg Q$ then $\deg(P+Q) = \max\{\deg P, \deg Q\}$
2. If $\deg P = \deg Q$ then $\deg(P+Q) \leq \deg P$
3. If $PQ \neq 0$, $\deg(PQ) \leq \deg P + \deg Q$

---

34) not completely standard
35) a constant polynomial is the 0 polynomial or a polynomial of degree 0

4. If R is an integral domain then so is $R[x]$ and $\deg(PQ) = \deg P + \deg Q$

Proof: 1, 2 exercises.

(3) $\deg P = n$, $\deg Q = m$

$$\begin{aligned} P &= a_0 + a_1x + \cdots + a_nx^n \qquad a_n \neq 0 \\ Q &= b_0 + b_1x + \cdots + b_mx^m \qquad b_m \neq 0 \\ PQ &= \cdots + \cdots + a_nb_mx^{m+n} \\ &\implies \deg(PQ) \leq m + n \end{aligned}$$

But *maybe* $a_nb_m = 0$ so you don't in general get equality.
If R is an integral domain then $a_nb_m \neq 0$.
So $PQ \neq 0$. Hence $R[x]$ is also integral domain.
Moreover we have shown in this case that $\deg(PQ) = m + n$.

PMATH 345 Lecture 7: September 28, 2009

Definition: R commutative ring, $P \in R[x]$
Suppose S is an extension of R
Given that $s \in S$, we can *substitute s for x*

$P(s) \in S$ as follows:
if $P = a_0 + a_1x + \cdots + a_nx^n$, $n = \deg P$
then $P(s) = \underbrace{a_0 + a_1s + a_2s^2 + \cdots + a_ns^n}_{36)}$

each $a_i \in R \subseteq S$
$s \in S$

Another way of describing this is:
R is a subring of S
so $R[x]$ is a subring of $S[x]$ (check)
so $P \in S[x]$ and consider
$f_P \colon S \to S$
Then $P(s) := f_P(s)$
"*P evaluated at s*"

Homomorphisms
Definition: R, S rings. A *homomorphism* $\phi\colon R \to S$ is a function with

$$\begin{aligned} \phi(1) &= 1^{37)} \\ {}^{38)}\phi(a+b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \end{aligned}$$

Remark: If ϕ is a homomorphism, then $\phi(0) = 0$ and $\phi(a) = -\phi(a)$.
Proof:

$$\begin{aligned} 0 + \phi(0) &= \phi(0+0) = \phi(0) + \phi(0) \\ &\implies 0 = \phi(0) \\ \varphi(-a) + \varphi(a) &= \varphi(-a+a) \\ &= \varphi(0) = 0 \\ &\implies \phi(-a) = -\phi(a) \end{aligned}$$

The *image* of $\phi\colon R \to S$

$$\phi(R) = \{\, \phi(a) : a \in R \,\} \subseteq S$$

36) $+$ and $-$ are happening in S
37) $*$ Different from text
38) a, $b \in R$

Check: $\phi(R)$ is a subring of S.

The *kernel* of ϕ
$$\ker\phi = \{\, a \in R : \varphi(a) = 0 \,\} \subseteq R$$

Remark: $\ker\phi$ is a subring $\iff$ $\ker\phi = R$ $\iff$ $S = \{0\}$.
As long as S is nontrivial, here it is *not* a subring.[39)]

Example:

(a) R is a subring of S and

$$\begin{aligned} \phi\colon R &\to S && \text{is the inclusion} \\ r &\mapsto r && \phi \text{ is a homomorphism} \end{aligned}$$

When $R = S$ we call this the identity homomorphism

(b)

$$\begin{aligned} \phi\colon \mathbb{C} &\to \mathbb{C} && \text{homomorphisms} \\ z &\mapsto \overline{z} && \text{conjugation map} \end{aligned}$$

$z = r + si$, $\overline{z} = r - si$

(c)

$$\begin{aligned} \operatorname{res}\colon \mathbb{Z} &\to \mathbb{Z}_n, && n \text{ fixed} \geq 2 \\ a &\mapsto \overline{a} = \{\, b \in \mathbb{Z} : a \equiv b \pmod{n} \,\} \end{aligned}$$

homomorphism

$$\begin{gathered} \operatorname{res}(1) = \overline{1} = \text{identity in } \mathbb{Z}_n \\ \operatorname{res}(ab) = \overline{ab} = \overline{a}\overline{b} \\ \operatorname{res}(a+b) = \overline{a+b} = \overline{a} + \overline{b} \end{gathered}$$

(d) What about homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$?
Suppose $\phi\colon \mathbb{Z}_n \to \mathbb{Z}$ was a homomorphism, then:

$$\begin{aligned} \phi(\overline{1}) &= 1 \\ \phi(\overline{1} + \overline{1}) &= \phi(\overline{1}) + \phi(\overline{1}) = 1 + 1 = 2 \\ &\vdots \\ 0 = \phi(\overline{0}) = \phi(\overline{n}) = \phi(\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n \text{ times}}) &= n \qquad \text{in } \mathbb{Z}^{40)} \end{aligned}$$

No homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}$.

(e) Fix any ring R, what are the homomorphisms from $\mathbb{Z}$ to R?

Consider $\phi\colon \mathbb{Z} \to R$ $a > 0$ in $\mathbb{Z}$, $\phi(a) \coloneqq \overbrace{1_R +_R + \cdots +_R 1_R}^{a \text{ times}}$
$a < 0$ in $\mathbb{Z}$, $\phi(a) = -\phi(a)$
$\phi(0) = 0$

check: ϕ is a homomorphism
This is the *only* possible since if $\psi\colon \mathbb{Z} \to R$ is any other my homomorphism.

[39)] (for us, different in DF)

then for $a > 0$,

$$\begin{aligned}\psi(a) &= \psi(\underbrace{1 + \cdots + 1}_{a \text{ times}}) \\ &= \psi(1) + \cdots + \psi(1) \\ &= 1_R + \cdots + 1_r = \phi(a)\end{aligned}$$

Hence $\psi = \phi$.

Point: For any R there is a unique homomorphism in $\mathbb{Z}$ to R.

Definition: $\phi\colon R \to S$ a ring homomorphism

1. ϕ is *injective* if ϕ is 1-to-1.
   Also called *embedding*, *monomorphism*
2. ϕ is a *surjective homomorphism* if
   $$\phi(R) = S$$
   Also called a *epimorphism*.
3. If $R = S$, then a homomorphism $\phi\colon R \to R$ is called *endomorphism*
4. An *isomorphism* is an injective *and* surjective homomorphism.
5. If $\phi\colon R \to R$ is an isomorphism we call it an *automorphism*.

Suppose $\phi\colon R \to R$ is a homomorphism.
Lemma: $\phi\colon R \to S$ is an endomorphism iff $\ker\phi = \{0\}$.
Proof: If ϕ is an embedding and $\phi(a) = 0 = \phi(0) \implies a = 0$,
i.e., $\ker\phi = \{0\}$.
Conversely, suppose $\ker\phi = \{0\}$.

$$\begin{aligned}\phi(a) &= \phi(b) \\ \phi(a) - \phi(b) &= 0 \\ \phi(a) + -(\phi(b)) &= 0 \\ \phi(a) + \phi(-b) &= 0 \\ \phi(a + (-b)) &= 0 \\ a + (-b) &\in \ker\phi = \{0\} \\ \implies a + (-b) &= 0 \\ \implies a &= b\end{aligned}$$

Ideals and Quotients
Definition: An ideal I of a ring R is a *nonempty* subset such that

1. $a, b \in I$, $(a + b) \in I$
2. for any $r \in R$ and $a \in I$, $ra \in I$ and $ar \in I$ in R

Remark: $0 \in I$
let $a \in I$, $-a = (-1)a$

PMATH 345 Lecture 8: September 30, 2009

$$\begin{aligned}e &= (f + f) \\ (1 + e)^{-1} &\overset{\times}{=} (1 - f)^{41)} \\ &= (1 - ef)\end{aligned}$$

40) contradiction

Example: Any R, (0) trivial ideal $= \{0\}$

Example: $\phi\colon R \to S$ homomorphism of rings
$\ker\phi$ is an ideal of R.

Proof:

$$\begin{matrix}\phi(a)=0\\ \phi(b)=0\end{matrix} \implies \phi(a+b)=\phi(a)+\phi(b)=0$$

$\ker\phi \neq 0$ since $0 \in \ker\phi$
$a \in \ker\phi$, $r \in R$, $\phi(ra)=\phi(r)\phi(a)=\phi(r)0=0$
Similarly $\phi(ar)=0 \longrightarrow ar, ra \in \ker\phi$

Example: What are the ideals of $\mathbb{Z}$?
Suppose $I \neq (0)$ ideal in $\mathbb{Z}$.
$\implies I$ has positive elements (since $a \in I \implies -a \in I$)
Let c be the *least* positive integer *in* I.
Let $J = c\mathbb{Z} \coloneqq \{\, ca : a \in \mathbb{Z} \,\} = \{\text{integers divisible by } c\}$

Check: J is an ideal "ideal generated by c"
$J \subseteq I$ since $c \in I$, all $ca \in I$

Claim: $J = I$.
Proof: Suppose not.
There is $a \in I \setminus J$.
If $-a \in J$ then $-(-a) = a \in J$.
But $a \notin J$, so $-a \notin J$.
But $-a \in I$. So $-a \in I \setminus J$.
$I \setminus J$ has a positive integer.
Let b be the *least* positive integer in $I \setminus J$.
$\implies b = qc + r$ where $q \in \mathbb{Z}$, $0 < r < c$.
$r = b - qc = b + (-q)c \in I$ since $b, c \in I$, therefore $r \in I$.
Note $b \geq c$ by choice of c.
$\implies r < c \leq b$, therefore $r < b$
And $0 < r < c$, $c \nmid r \implies r \notin J$.
Contradiction to minimal choice of b.

Every ideal in $\mathbb{Z}$ is of the form $c\mathbb{Z}$ for some $c \geq 0$.

Definition: R commutative ring. A *principal ideal* is one of the form

$$cR \coloneqq \{\, ca : a \in R \,\}$$

where $c \in R$.

(Exercise: cR is the smallest ideal containing c.)

R is a *principal ideal domain* (pid) if it is an integral domain and *every* ideal of R is principal.
So $\mathbb{Z}$ is a pid.

R commutative ring. I an ideal of R. $a \in R$, $\overline{a} \coloneqq a + I \coloneqq \{\, a + b : b \in I \,\} \subseteq R$.

residue a mod I
$R/I \coloneqq \{\, \overline{a} : a \in R \,\}$.

Quotient of R modulo I
Elements of R/I are called *cosets* of I.

Lemma: If $a, b \in R$, either $\overline{a} = \overline{b}$ or $\overline{a} \cap \overline{b} = \emptyset$.

[41] f is unique $\iff 2 = 1 + 1$ is not a zero divisor

Proof: Suppose $z \in \overline{a} \cap \overline{b}$.

$$\begin{aligned} z &= a + x \\ z &= b + y \end{aligned} \qquad \text{for some } x, y \in I$$

$\implies a = b + (y - x)$
Hence for any $u \in I$,

$$\begin{aligned} a + u &= b + \underbrace{(y - x) + u}_{\text{in } I} \\ &\in b + I = \overline{b} \end{aligned}$$

therefore $\overline{a} \subseteq \overline{b}$. Similarly $\overline{b} \subseteq \overline{a}$.

Note: If $a \in R$ then $a \in \overline{a} = a + I$
Hence R is partitioned into disjoint cosets of I.
(Possibly *infinite* partitioning of R).

figure: I subset of R

Proposition: R/I is a commutative ring with:

$$\begin{aligned} 0 &= 0 + I \\ 1 &= 1 + I \\ (a + I) + (b + I) &= (a + b) + I \\ (a + I)(b + I) &= (ab) + I \end{aligned}$$

Proof: Need to prove that $+$ and $\times$ on R/I are well-defined operations.

Note: A coset $a + I$ is not uniquely represented by this notation. In fact if $b \in a + I$ then $a + I = b + I$.
(by the lemma)
(conversely $a + I = b + I \implies b \in a + I$).

Every element of a coset represents that coset.
$+$ should depend only on the cosets *not* on the representatives.
need: If $a + I = a' + I$
$b + I = b' + I$
then $(a + b) + I = (a' + b') + I$.
Proof:

$$\begin{aligned} a' + I = a + I &\implies a' \in a + I \\ &\implies a' = a + x \text{ for some } x \in I \\ b' + I = b + I &\implies b' \in b + I \\ &\implies b' = b + y \text{ for some } y \in I \\ \implies (a' + b') &= (a + b) + \underbrace{(x + y)}_{\text{in } I} \\ &\in (a + b) + I \\ \text{therefore } (a' + b') + I &= (a + b) + I \end{aligned}$$

Similarly check $\times$ is well-defined.
Check: R/I is a commutative ring.

Example: Consider $\mathbb{Z}$ and the ideal $n\mathbb{Z} = \{ na : a \in \mathbb{Z} \}$, $n \geq 2$
Check: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$
$a \in \mathbb{Z}$. $\text{res}(a) = a + n\mathbb{Z}$
$\mathbb{Z}_n$ is the quotient of $\mathbb{Z}$ mod $n\mathbb{Z}$
missing: $n = 0$, $n = 1$, $0\mathbb{Z} = (0)$, $\mathbb{Z}/(0) = \{ a + (0) = \{a\} : a \in \mathbb{Z} \}$
$\mathbb{Z}/1\mathbb{Z}$ trivial ring

PMATH 345 Lecture 9: October 2, 2009

$n \geq 2$, $\mathbb{Z}/n\mathbb{Z} = \{\, a + n\mathbb{Z} : a \in \mathbb{Z} \,\} = \mathbb{Z}_n$
$\mathbb{Z}/1\mathbb{Z} = 0 + 1\mathbb{Z}$ trivial
In general, R/R is the trivial ring.
$\mathbb{Z}/0\mathbb{Z} = \{\, a + (0) : a \in \mathbb{Z} \,\}$

$$a + (0) = \{a + 0\} = \{a\}$$

Exercise: $\mathbb{Z}/0\mathbb{Z} \approx \mathbb{Z}$ by $\mathbb{Z}/0\mathbb{Z} \to \mathbb{Z}$, $a + (0) \mapsto a$
In general, $R/(0) \approx R$ in the canonical way. That is

$$\begin{aligned} \phi \colon R/(0) &\to R \\ a + (0) &\mapsto a \end{aligned}$$

is a bijective homomorphism.
Example: $\mathbb{R}[x]$

$$\begin{aligned} I &= (x^2 + 1)\mathbb{R}[x] \\ &= \left\{\, (x^2 + 1)P : P \in \mathbb{R}[x] \,\right\} \end{aligned}$$

Consider $\mathbb{R}[x]/I$

$$(x + I)^2 = x^2 + I$$

since $x^2 + 1 \in I$

$$x^2 + I = -1 + I = -(1 + I) = -1_{R/I}$$

In $\mathbb{R}[x]/I$, $(x + I)$ is a square root of -1.

Lemma: R commutative ring, I ideal of R.

$$\underbrace{a + I = b + I}_{\text{inside } R/I} \iff a - b \in I.$$

Proof: $a + I = b + I$, so

$$\begin{aligned} a \in b + I &\implies a = b + x \qquad \text{for some } x \in I \\ &\implies a - b = x \in I \end{aligned}$$

If $a - b \in I$, so $a - b = x$, for some $x \in I$.

$$\begin{aligned} &\implies a = b + x \in b + I \\ &\implies a \in a + I \\ &\implies (a + I) \cap (b + I) \neq \emptyset \\ &\implies a + I = b + I. \end{aligned}$$

$$\begin{aligned} \text{Also } \phi \colon \mathbb{R} &\to \mathbb{R}[x]/I \\ r &\mapsto r + I \end{aligned}$$

is an embedding.

Proof: Clearly a homomorphism,
Suppose $r + I = 0_{R/I}$, i.e., $r \in \ker(\phi)$
$r + I = 0 + I$
$\implies r \in I$
But in I the only constant polynomial is 0. Therefore $r = 0$.

Aside: The above argument works for any integral domain R. That is,

$$\phi \colon R \to R[x]/(x^2 + 1)\mathbb{R}[x]$$

is an embedding and in $R[x]/I$, $(x + I)^2 = -1$.

Identify $\mathbb{R}$ with its image in $\mathbb{R}[x]$.

$$\begin{array}{rl} \mathbb{C} \approx^{[42]} & \mathbb{R}[x]/I^{[43]} \\ & \mid \\ & \mathbb{R} \end{array}$$

Notation: In any ring R, by (a) we mean aR, the ideal generated by a in R, $a \in R$.

First isomorphism theorem: R, T commutative rings. $\phi\colon R \to T$ homomorphism.
$\mathrm{Im}(\phi)$ is isomorphic to $R/\mathrm{Im}(\ker\phi)$. $\operatorname{im}\phi \coloneqq \phi(R)$

Proof:

$$\begin{aligned} \text{Define } \psi\colon R/\ker\phi &\to \operatorname{Im}\phi \\ a + \ker\phi &\mapsto \phi(a) \end{aligned}$$

Note if $b + \ker\phi = a + \ker\phi$ then by lemma $a - b \in \ker\phi$
$\phi(a-b) = 0$
$\implies \phi(a) - \phi(b) = 0$
$\implies \phi(a) = \phi(b)$
So ψ is well-defined.
Let's write $\overline{a} = a + \ker\phi$.

$$\begin{aligned} \psi(\overline{a} + \overline{b}) &= \psi(\overline{a+b}) \text{ by definition of } + \text{ in } R/\ker\phi \\ &= \phi(a+b) \text{ by definition of } \psi \\ &= \phi(a) + \phi(b) = \psi(\overline{a}) + \psi(\overline{b}) \end{aligned}$$

Similarly $\psi(\overline{a}\overline{b}) = \psi(\overline{a})\psi(\overline{b})$.
And $\phi(\overline{1}) = \phi(1) = 1$.
So ψ is a homomorphism.
Surjective: $x \in \operatorname{Im}\phi$

$$\begin{aligned} x &= \phi(a) \text{ for some } a \in R \\ &= \psi(\overline{a}) \in \operatorname{Im}\psi \end{aligned}$$

therefore ψ is surjective
Injective: $x \in \ker(\psi)$. $\psi(x) = 0$.
$x \in R/\ker\phi$ so $x = \overline{a}$ for some $a \in R$.
$\phi(a) = \psi(\overline{a}) = 0$
therefore $a \in \ker\phi$

Example: $\phi\colon \mathbb{R}[x] \to \mathbb{C}$
the "evaluation at i" map,
i.e., $\phi(P) \coloneqq P(i) \in \mathbb{C}$
Check: ϕ is a homomorphism.

$\ker\phi = ?$
Suppose $P \in \ker\phi$.
So $P(i) = 0$.
That is i is a root of P.
In $\mathbb{C}[x]$, $(x - i)$ is a factor, $(x + i)$ is a factor
since P is *actually* real.
$\implies (x+i)(x-i) = x^2 + 1$ is a factor
therefore (x^2+1) is a factor of P in $\mathbb{R}[x]$.
i.e., $P \in (x^2+1) = (x^2+1)\mathbb{R}[x]$

[42] we will see this
[43] in here -1 has a square

Conversely if $Q \in (x^2+1)$
then $Q = (x^2+1)Q'$
so $Q(i) = 0 \cdot Q'(i) = 0$.
$\implies Q \in \ker\phi$.
therefore $\ker\phi = (x^2+1)$.
What is $\operatorname{Im}\phi = ?$
Let $a + bi \in \mathbb{C}$. $a, b \in \mathbb{R}$
$a + bi = P(i) \qquad P = a + bx \in \mathbb{R}[x]$
therefore ϕ is surjective.
Hence $\mathbb{C} \approx \mathbb{R}[x]/(x^2+1)$.
Moreover this isomorphism is given by

$$\begin{aligned} \phi\colon \mathbb{R}[x]/(x^2+1) &\to \mathbb{C} \\ P + (x^2 = 1) &\mapsto P(i) \end{aligned}$$

PMATH 345 Lecture 10: October 5, 2009

$R/I \quad 0_{R/I} = 0_R + I = I$
$a + I = b + I \iff a - b \in I$
$I = R$
$0_{R/R} = R$
elements in R/R is $a + R$ some $a \in R$
$a \in R \implies a + R = 0 + R = R = 0_{R/R}$

R commutative ring, I an ideal

Quotient ring: R/I.
It's elements are called *cosets of* I, $a + I = \{\, a + b : b \in I \,\}$
Sometimes use $\overline{a}$ to denote $a + I$

$$\begin{aligned} \textit{Quotient map} \text{ is the function } \pi\colon R &\to R/I \\ a &\mapsto a + I \end{aligned}$$

Note: π is a surjective ring homomorphism.
Proof: $\alpha \in R/I$,

$$\begin{aligned} \alpha &= a + I \text{ for some } a \in R \\ &= \pi(a) \text{ therefore } \pi \text{ is onto} \\ \pi(a+b) = (a+b) + I &= (a+I) + (b+I) \\ &= \pi(a) + \pi(b) \\ \pi(ab) &= ab + I \\ &= (a+I)(b+I) \\ &= \pi(a)\pi(b) \\ \pi(1_R) &= 1_R + I \\ &= 1_{R/I} \\ \ker(\pi) &= I \\ \pi(a) = 0_{R/I} &= 0 + I \\ &\Updownarrow \\ a + I &= 0 + I \\ &\Updownarrow \\ a &\in I \end{aligned}$$

Suppose $\phi\colon R \to S$ ring homomorphism of commutative rings.
Then there is a *commutative diagram*[44] of homomorphism:

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & S \\ & R/\ker\phi \arrow[ur, "\psi"'] & \end{tikzcd}$$

where π is the quotient map
and $\psi(a + \ker\phi) := \phi(a)$
In the proof of the 1st Isomorphism Theorem we saw that ψ *is* well-defined and a homomorphism *and* its image is $\phi(R)$.
Note: ψ is the *unique* homomorphism from $R/\ker\phi$ to S which makes the diagram commute.
Point: Every ring homomorphism $\phi\colon R \to S$ of commutative rings factors canonically through $\pi\colon R \to R/\ker\phi$.

1st Isomorphism Theorem tells us more: ψ is an embedding whose image is $\phi(R)$. *In part*, if ϕ is surjective then ψ is an isomorphism.

Definition: R ring, I an ideal.

1. I is a *prime ideal* if $I \neq R$ and for all
$$a, b \in R, \qquad \text{if } ab \in I \text{ then either } a \in I \text{ or } b \in I$$
2. I is a *maximal* ideal if
   - $I \neq R$
   - If $J \subsetneq R$ is a proper ideal and $I \subseteq J$ then $I = J$.
     i.e., there is *no* ideal properly in between $I \subseteq R$.

Examples:

(a) R commutative ring
$$(0) \text{ is prime} \iff R \text{ integral domain}$$

(b) $R = \mathbb{Z}$.
Ideals in $\mathbb{Z}$ are all of the form $(n) = n\mathbb{Z}$ where $n \geq 0$.
(0) is prime by part (a)
(1) is neither prime nor maximal because $(1) = \mathbb{Z}$.
$n \geq 2$,
$$(n) \text{ is prime ideal} \iff n \text{ is prime number}$$

Proof: Suppose (n) prime ideal. Let p be a prime number.
Suppose $n = ab \in (n)$
$\implies a \in (n)$ or $n \in (n)$
$n \mid a$ or $n \mid b$
$\implies a = 1$ or $b = 1$
Consequently n prime number.

$$\begin{aligned} ab \in (n) &\iff n \mid ab \\ &\iff n \mid a \text{ or } n \mid b \text{ as } n \text{ is prime} \\ &\iff a \in (n) \text{ or } b \in (n) \\ (n) \text{ maximal} &\iff n \text{ is a prime number} \end{aligned}$$

[44] i.e., for $a \in R$
$$\phi(a) = \psi(\pi(a))$$
Proof: $\psi(\pi(a)) = \phi(a + \ker\phi) = \phi(a)$

Proof: ($\Longrightarrow$) (0) not maximal

$$(0) \subsetneq (2) \subsetneq \mathbb{Z}.$$

($\Longleftarrow$) Suppose p is a prime number

$$(p) \subseteq I^{45)} \subseteq \mathbb{Z}^{46)}$$

$\Longrightarrow p \in (n) \Longrightarrow n \mid p \Longrightarrow n = 1$ or $n = p$
$\Longrightarrow I = (p)$ or $I = \mathbb{Z}$.

Theorem: Let I be an ideal in a commutative ring R. Then:

1. I is prime $\iff R/I$ is an integral domain
2. I is maximal $\iff R/I$ is a field

In particular: maximal ideals are prime
(since ideals are integral domains)

PMATH 345 Lecture 11: October 7, 2009

Corrected:

1. Assume in (a), (b) that ϕ *is surjective*
   (a) Just do *maximal*, not prime

Bonus: Counterexample to (b) if ϕ is *not* surjective

Counterexample to (a) for *prime*

Theorem: R commutative ring. I an ideal.

(a) I is prime $\iff R/I$ is an integral domain

(b) I is maximal $\iff R/I$ is a field

Proof:

(a) Suppose I is prime. $\overline{a} := a + I$.

$$\overline{a}, \overline{b} \in R/I \qquad \begin{aligned} \overline{a} &\neq 0_{R/I} \\ \overline{b} &\neq 0_{R/I} \end{aligned}$$

$$\begin{aligned} \overline{a} \neq 0 &\Longrightarrow a \notin I \\ \overline{b} \neq 0 &\Longrightarrow b \notin I \\ &\Longrightarrow ab \notin I \text{ as } I \text{ is prime} \\ &\Longrightarrow \overline{ab} \neq 0_{R/I} \\ &\Longrightarrow \overline{a} \cdot \overline{b} \neq 0_{R/I} \end{aligned}$$

Therefore R/I is an integral domain.
(Note prime ideals *are* proper so R/I is not trivial.)

Suppose R/I is an integral domain.

$$R/I \text{ maximal} \Longrightarrow I \text{ proper}.$$

$a, b \in R$, suppose $ab \in I$.

$$\begin{aligned} \overline{ab} &= 0_{R/I} \\ \Longrightarrow \overline{a}\overline{b} &= 0_{R/I} \\ \Longrightarrow \text{either } \overline{a} = 0 &\text{ or } \overline{b} = 0 \text{ in } R/I \end{aligned}$$

45) $= (n)$
46) uses next theorem

as R/I is an integral domain
$\implies a \in I$ or $b \in I$.

(b) Suppose I is maximal.
Let $\overline{a} \neq \overline{0}$ in R/I. **Need:** $\overline{a}$ is invertible in R/I.
Consider: $(a) + I$ in R.

$$J := (a) + I = \{\, ar + b : r \in R, b \in I \,\}$$

Check: In any commutative ring S, given ideals A and B,

$$A + B := \{\, a + b : a \in A,\, b \in B \,\}$$

$A + B$ is an ideal[47]

Note: $I \subseteq (a) + I$. If $b \in I$, then $I \subseteq J$.
$b = a \cdot 0 + b \in (a) + I$
I maximal $\implies \cancel{J = I}$ or $J = R$.
But $a = a \cdot 1 + 0 \in J$ but $\overline{a} \neq \overline{0}$ so $a \notin I$.
Therefore $J = R$.
In particular there is $r \in R$, $b \in I$ such that $ar + b = 1$

$$\begin{aligned} &\implies ar - 1 = -b \in I \\ &\implies \overline{ar} = \overline{1} \\ &\implies \overline{ar} = \overline{1} = 1_{R/I} \end{aligned}$$

Therefore $\overline{a}$ is invertible.
Therefore R/I is a field.

Suppose R/I is a field.
Suppose there exists an ideal J such that

$$I \subsetneq J \subseteq R.$$

Let $a \in J \setminus I$.
$\overline{a} \neq \overline{0}$.
$\implies$ there is $\overline{b} \in R/I$ such that[48]

$$\overline{a} \cdot \overline{b} = \overline{1} \text{ in } R/I$$

$\implies ab - 1 \in I \subseteq J$
Also $a \in J \implies ab \in J$ so

$$1 = \underbrace{-(ab-1)}_{\text{in } J} + \underbrace{ab}_{\text{in } J} \implies 1 \in J$$

For any $r \in R$,

$$r = r \cdot 1 \in J$$

i.e., $J = R$
i.e., I is maximal.

Corollary: All maximal ideals are prime.

Existence?

Zorn's Lemma
Definition: A *partially ordered set* is a nonempty set P with a binary relation, $\leq$, that is reflexive, transitive, anti-symmetric.
i.e.,

1. For all $a \in P$, $a \leq a$

[47] **Exercise:** $A + B$ is the smallest ideal containing A and B
[48] R/I a field

2. If $a, b, c \in P$,
$$a \leq b \text{ and } b \leq c \implies a \leq c$$
3. If $a \leq b$ and $b \leq a \implies a = b$

Typical example: X nonempty set,
Let $\emptyset \neq \mathcal{S}$[49] $\subseteq \mathcal{P}(X)$
$(\mathcal{S}, \subseteq)$ is a poset.

Definition: Suppose $(P, \leq)$ is a poset.
A *chain* in $(P, \leq)$ (or a *totally ordered subset*) is a subset $C \subseteq P$ such that for all $a, b \in C$, either $a \leq b$ or $b \leq a$.

Zorn's lemma: Suppose $(P, \leq)$ is a poset where $C \subseteq P$ is a chain, there exists $a \in P$ such that $a \geq b$ for *all* $b \in C$. (a is an *upper bound* for C).
Then $(P, \leq)$ has a *maximal* element i.e., there exists $d \in P$ such that if $a \in P$, $d \leq a$, then $a = d$. (Nothing strictly bigger than d in P.)
We will assume this.

Theorem: Let R be a ring. I a *proper* ideal. Then I is contained in a maximal ideal.

Proof: Let $\mathcal{S} =$ set of all proper ideals in R containing I.
$$\mathcal{S} \subseteq \mathcal{P}(R) \qquad I \in \mathcal{S}$$
So $(\mathcal{S}, \subseteq)$ is a poset.
Let C be a chain in $\mathcal{S}$.
So $C = \{\, J_i : i \in \kappa \,\}$
$$\begin{aligned} \text{Let } J^* &= \bigcup C \\ &= \{\, a \in R : a \in J_i \text{ for some } i \in \kappa \,\} \end{aligned}$$
Exercise: Show J^* is a proper ideal.
$$J^* = R \iff 1 \in J^* \iff 1 \in J_i \text{ for some } i \iff J_i = R \text{ for some } i$$
Note $I \subseteq J^*$. So $J^* \in \mathcal{S}$.
Hence by Zorn's Lemma, $(\mathcal{S}, \subseteq)$ has a *maximal* element, i.e., there exists a proper ideal M containing I such that if $M \subseteq J \subsetneq R$ where $J \neq R$ ideal containing I then $M = J$.
i.e., M is a maximal ideal.

PMATH 345 Lecture 12: October 9, 2009

My name is Collis Roberts. I'm a PhD student in Pure Math, and your PMath 345 TA.

Chinese Remainder Theorem
Recall: For a positive integer n, the *Euler function* $\phi(n)$, is the # of positive integers ($\leq n$) coprime to n (i.e., that have gcd $= 1$ with n).
$$\phi(n) = \# \text{ of units in } \mathbb{Z}_n = \mathbb{Z}/(n).$$
If p is prime then
$$\begin{aligned} \phi(p) &= p - 1 \\ \phi(p^e) &= p^e - p^{e-1} = p^e\left(1 - \tfrac{1}{p}\right) \end{aligned}$$ [50]

Goal for today: Develop a "nice" formula for $\phi(n)$ when n has multiple prime factors.

[49] a collection of subsets of X
[50] (the only divisors of p^e are powers of p)

Proposition: (Chinese Remainder Theorem)
For positive integers m, n: If $\gcd(m, n) = 1$, then

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$$

Proof: Let

$$\begin{aligned} \sigma_m \colon \mathbb{Z} &\to \mathbb{Z}_m \\ k &\mapsto \overline{k} \end{aligned} \qquad\qquad \begin{aligned} \sigma_n \colon \mathbb{Z} &\to \mathbb{Z}_n \\ k &\mapsto \overline{k} \end{aligned}$$

be the residue maps: these are homomorphisms.

Define:

$$\begin{aligned} \sigma \colon \mathbb{Z} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ k &\mapsto (\sigma_m(k), \sigma_n(k)) \end{aligned}$$

a homomorphism since σ_m, σ_n are.

1st Isomorphism Theorem: $\mathbb{Z}/\ker\sigma \simeq \operatorname{im}\sigma$.

So we're done if we can prove:

- $\ker\sigma = (mn)$
- $\operatorname{im}\sigma = \mathbb{Z}_m \times \mathbb{Z}_n$

Proof that $\ker\sigma = (mn)$:
($(mn) \subseteq \ker\sigma$): $\sigma(mn) = (\sigma_m(mn), \sigma_n(mn)) = (\overline{0}, \overline{0})$ in $\mathbb{Z}_m \times \mathbb{Z}_n$
($\ker\sigma \subseteq (mn)$): Let $k \in \ker\sigma$ be arbitrary. $\iff$ $\sigma(k) = (\overline{0}, \overline{0})$. $\implies$ $(\overline{0}, \overline{0}) = (\sigma_m(k), \sigma_n(k))$ $\implies$ $m \mid k$ and $n \mid k$.
Since $\gcd(m, n) = 1$, there exists integers u, v such that $1 = um + vn$.
Multiplying by k gives: $k = umk + vnk$.
Since $m \mid k$ and $n \mid k$, mn divides the RHS.
$\implies$ $mn \mid k$ $\implies$ $k \in (mn)$. Therefore ($\ker\sigma = (mn)$).

Proof that $\operatorname{im}\sigma = \mathbb{Z}_m \times \mathbb{Z}_n$:
By definition, $\operatorname{im}\sigma \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$. We need to check the containment cannot be proper.
It's clear that $\mathbb{Z}_m \times \mathbb{Z}_n$ contains mn elements.
1st Isomorphism Theorem now says: $\mathbb{Z}_{mn} = \mathbb{Z}/(mn) \simeq \operatorname{im}\sigma$.
This isomorphism guarantees $\operatorname{im}\sigma$ contains mn elements.
$\implies$ $\operatorname{im}\sigma = \mathbb{Z}_m \times \mathbb{Z}_n$.
So finally, $\mathbb{Z}_{mn} = \mathbb{Z}/(mn) = \mathbb{Z}/\ker\sigma \simeq \operatorname{im}\sigma = \mathbb{Z}_m \times \mathbb{Z}_n$.

Corollary: If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.
Proof: By previous proposition, $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.
\# of units in $\mathbb{Z}_{mn}$ is $\phi(mn)$ $\implies$ # of units in $\mathbb{Z}_m \times \mathbb{Z}_n$ is $\phi(mn)$.
So we just need to count the units of $\mathbb{Z}_m \times \mathbb{Z}_n$ another way.
An element (a, b) of $\mathbb{Z}_m \times \mathbb{Z}_n$ is a unit $\iff$

- a is a unit in $\mathbb{Z}_m$ ($\phi(m)$ of these) AND
- b is a unit in $\mathbb{Z}_n$ ($\phi(n)$ of these)

Therefore there are $\phi(m)\phi(n)$ units in $\mathbb{Z}_m \times \mathbb{Z}_n$.

Example: Instead of using brute force, we can now compute

$$\phi(637) = \phi(7 \cdot 91) = \phi(\underbrace{7^2}_{m} \cdot \underbrace{13}_{n}) = \phi(7^2)\phi(13) = 7^2\big(1 - \tfrac{1}{7}\big)(12) = 504.$$

Recall that every positive integer n has a unique factorization into distinct primes: $n = p_1^{e_1} \cdots p_k^{e_k}$. We can now state our formula for $\phi(n)$.

Proposition: If the prime factorization for n is $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\phi(n) = n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_k}\right)$$

Proof: Since $p_1^{e_1}$ is coprime to $p_2^{e_2} \cdots p_k^{e_k}$, previous corollary says:

$$\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2} \cdots p_k^{e_k}) = p_1^{e_1}\left(1 - \tfrac{1}{p_1}\right)\phi(p_2^{e_2} \cdots p_k^{e_k})$$

(Repeat the argument for $p_2^{e_2}$ to get)

$$= p_1^{e_1}\left(1 - \tfrac{1}{p_1}\right)p_2^{e_2}\left(1 - \tfrac{1}{p_2}\right)\phi(p_3^{e_3} \cdots p_k^{e_k})$$

Continue until all prime factors are exhausted. Get

$$\begin{aligned} &= (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_k}\right) \\ &= n\left(1 - \tfrac{1}{p_1}\right) \cdots \left(1 - \tfrac{1}{p_k}\right) \end{aligned}$$

Final Observation: Euler's Formula
Suppose $n = p^e$ for some prime p. Then:

$$\begin{aligned} n = p^e &= (p^e - p^{e-1}) + (p^{e-1} - p^{e-2}) + \cdots + (p^1 - p^0) + 1 \\ &= \phi(p^e) + \phi(p^{e-1}) + \cdots + \phi(p^1) + \phi(1) \\ &= \sum_{d|n, d>0} \phi(d) \end{aligned}$$

Remark: This holds when n has multiple prime factors also.
Sadly, we don't have time to prove it today.

PMATH 345 Lecture 13: October 14, 2009

In class midterm Monday Oct. 16.

Localizations and Function Fields

R commutative ring
$S \subseteq R$ subset such that

1. $1 \in S$
2. $a, b \in S \implies ab \in S$ (S is multiplicatively closed)
3. S contains *no* zero divisors, or zero

Consider the Cartesian product $R \times S$ and define on it a relation as follows:
Definition: $(a, s) \sim (b, t)$ if $at = bs$

Lemma: $\sim$ is an equivalence relation on $R \times S$
Proof:

1. Reflexive: $a \in R$, $s \in S$,
$$(a, s) \sim (a, s)$$
2. Symmetric: $a, b \in R$, $s, t \in S$
If $(a, s) \sim (b, t)$ then $(b, t) \sim (a, s)$
3. Transitivity: $a, b, c \in R$, $s, t, u \in S$
Need: If $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$ then $(a, s) \sim (c, u)$
$$\begin{matrix} at = bs \\ bu = ct \end{matrix} \implies atu = bsu = bus = cts$$
$\implies aut = cst$, t is not a zero divisor and $t \neq 0$
$\implies au = cs$, i.e., $(a, s) \sim (c, u)$

So we can form the equivalence classes $a \in R, s \in S$.

$$[(a,s)] \coloneqq \{\, (b,t) : b \in R, t \in S, (b,t) \sim (a,s) \,\}$$

Note: $[(a,s)] = [(b,t)] \iff (a,s) \sim (b,t)$

Definition: The *localization of R at S* is

$$R_S \coloneqq R \times S/\sim = \{\, [(a,s)] : (a,s) \in R \times S \,\}.$$

Notation: We often write an element $[(a,s)]$ as $\frac{a}{s}$.
Note: In R_S, $\frac{a}{t} = \frac{b}{s} \iff as = bt$ $(*)$

Proposition: The following operations make R_S into a commutative ring:

$$0_{R_S} = \tfrac{0}{1} \qquad 1_{R_S} = \tfrac{1}{1}$$

$$\left(\begin{aligned} \tfrac{0}{1} = [(0,1)] &= \{\, (b,t) : (b,t) \sim (0,1) \,\} \\ &= \{\, (0,t) : t \in S \,\} \end{aligned} \right) \qquad \left(\begin{aligned} \tfrac{1}{1} = [(1,1)] &= \{\, (b,t) : (b,t) \sim (1,1) \,\} \\ &= \{\, (t,t) : t \in S \,\} \end{aligned} \right)$$

$$\frac{a}{s} + \frac{b}{t} \coloneqq \frac{at+bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} \coloneqq \frac{ab}{st}$$

(note $st \in S$)
Proof: Well-defined.
Suppose $\frac{a}{s} = \frac{a'}{s'} \implies as' = a's$
$a', b' \in R$, $s', t' \in S$, $\frac{b}{t} = \frac{b'}{t'} \implies bt' = b't$

$$\begin{aligned} (a't' + b's')st &= a't'st + b's'st \\ &= as't't + bt's's \\ &= (at+bs)s't' \\ \frac{a't' + b's'}{s't'} &= \frac{at+bs}{st} \qquad \text{by } (*) \end{aligned}$$

Therefore $\frac{a'}{s'} + \frac{b'}{t'} = \frac{a}{s} + \frac{b}{t}$, so $+$ is well defined.
$(a'b')(st) = as'bt' = (ab)(s't')$
$\implies \frac{a'b'}{s't'} = \frac{ab}{st}$
$\implies \left(\frac{a'}{s'}\right)\left(\frac{b'}{t'}\right) = \left(\frac{a}{s}\right)\left(\frac{b}{t}\right)$
therefore $\cdot$ is well-defined.
Check that this makes R_S into a commutative ring.
Example: Existence of additive inverse:

$$-\left(\frac{a}{s}\right) = \frac{-a}{s}$$

Proof:

$$\left(\frac{a}{s}\right) + \left(\frac{-a}{s}\right) = \frac{as + (-a)s}{s^2} = \frac{as - as}{s^2} = \frac{0}{s^2} = \frac{0}{1} = 0_{R_S}$$

Point: R_S is the "smallest" extension of R in which every element of S is a unit.
Proposition: The function

$$\begin{aligned} R &\xrightarrow{\rho} R_S \\ a &\mapsto \tfrac{a}{1} \end{aligned}$$

is an embedding with the property that $\rho(s)$ is a unit in R_S for all $s \in S$.
If $\rho \colon R \to T$ is an embedding with the property that for all $s \in S$, $\rho(s)$ is a unit in T then there exists

a unique embedding $\psi\colon R_S \to T$ such that

$$\begin{tikzcd}
R \arrow[rr, "\phi"] \arrow[dr, "\rho"'] & \arrow[d, phantom, "\circlearrowleft"] & T \\
& R_S \arrow[ur, "\psi"'] &
\end{tikzcd}$$

Proof: $\rho(1) = \frac{1}{1} = 1_{R_S}$

$$\rho(a+b) = \tfrac{a+b}{1} = \tfrac{a}{1} + \tfrac{b}{1} = \rho(a) + \rho(b)$$

$$\rho(ab) = \tfrac{ab}{1} = \left(\tfrac{a}{1}\right)\left(\tfrac{b}{1}\right) = \rho(a)\rho(b)$$

$a \in \ker\rho \implies \rho(a) = 0_{R_S} \implies \frac{a}{1} = \frac{0}{1}$
$\implies a = 0$, therefore ρ is an embedding.

Given $s \in S$,

$$\tfrac{1}{s} \cdot \tfrac{s}{1} = \tfrac{s}{s} = \tfrac{1}{1} = 1_{R_S}$$

therefore $\frac{1}{s}$ is the inverse of $\rho(s)$ in R_S
$\implies \rho(s)$ is a unit in R_S

Given $\phi\colon R \to T$ with these properties then define

$$\psi\colon R_S \to T$$

by

$$\tfrac{a}{s} \mapsto \phi(a) \cdot \phi(s)^{-1}$$

for $a \in R$, $s \in S$.

PMATH 345 Lecture 14: October 16, 2009

Proof that ψ is well-defined. Let $\frac{a}{s} = \frac{a'}{s'}$.

$$\begin{aligned}
&\implies as' = a's \\
&\implies \phi(as') = \phi(a's) \\
&\implies \phi(a)\phi(s') = \phi(a')\phi(s) \\
&\implies \phi(a)\phi(s)^{-1} = \phi(a')\phi(s')^{-1} \\
&\implies \psi(\tfrac{a}{s}) = \psi(\tfrac{a'}{s'}), \text{ so } \psi \text{ is well-defined.}
\end{aligned}$$

Check: ψ is a homomorphism
Now, show ψ in injective. Let $\frac{a}{s} \in \ker\psi$

$$\begin{aligned}
&\implies \psi(\tfrac{a}{s}) = 0 \\
&\implies \phi(a)\phi(s)^{-1} = 0 \\
&\implies \phi(a) = 0, \text{ since } \phi(s) \text{ is a unit} \\
&\implies a = 0^{51)} \implies \tfrac{a}{s} = 0, \text{ so } \psi \text{ is an embeddding}
\end{aligned}$$

Now, we will show $\psi(\phi(a)) = \phi(a)$

$$\begin{aligned}
\psi(\phi(a)) &= \psi(\tfrac{a}{1}) \\
&= \phi(a)\phi(1)^{-1} \\
&= \phi(a)1^{-1} \\
&= \phi(a), \text{ as required}
\end{aligned}$$

51) since ϕ is an embedding

Lastly, we will show ψ in unique.
Suppose $\psi'\colon R_S \to T$ is an embedding such that $\psi' \circ \rho = \phi$. Let $\frac{a}{s} \in R_S$.
Then, $\psi'(\frac{a}{1}) = \psi'(\rho(a)) = \phi(a)$
And, $1 = \psi'(1) = \psi'(\frac{s}{1} \cdot \frac{1}{s}) = \psi'(\frac{s}{1})\psi'(\frac{1}{s}) = \phi(s)\psi'(\frac{1}{s})$, so $\psi'(\frac{1}{s}) = \phi(s)^{-1}$
So, $\psi'(\frac{a}{1})\psi'(\frac{1}{s}) = \phi(a)\phi(s)^{-1}$
$\implies \psi'(\frac{a}{1} \cdot \frac{1}{s}) = \phi(a)\phi(s)^{-1}$
$\implies \psi'(\frac{a}{s}) = \phi(a)\phi(s)^{-1}$
$\implies \psi'(\frac{a}{s}) = \psi(\frac{a}{s})$. So ψ is unique.

Convention: We usually identify R with its image under ρ in R_S, i.e., we view R as a subring of R_S, with $a = \frac{a}{1}$
Definition: Suppose R is an integer domain, and let $S = R \setminus \{0\}$. Then R_S is called the *field of fractions of* R, and we will denote it by $Q(R)$.

The obvious example is $Q(\mathbb{Z}) = \mathbb{Q}$.
Note: $Q(R)$ is a field.
Proof: Let $\frac{a}{b} \in Q(R) \implies a \in R,\, b \neq 0 \in R$
If $\frac{a}{b} \neq 0$, then $a \neq 0$, then $\frac{b}{a} \in Q(R)$
And, $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1$
So $\frac{a}{b}$ is a unit. Therefore $Q(R)$ is a field.
Example: Let R be an integral domain.
$R[x]$ is an integral domain.

$$\begin{aligned} Q(R[x]) &= \{\, f/g : f, g \in R[x],\, g \neq 0 \,\} \\ &:= R(x) \text{ called } \textit{rational functions} \text{ on } R \end{aligned}$$

Perhaps later we will talk about $Q(R[[x]])$, called the set of *Laurent series*.
Proposition: Let R be a principal ideal domain, (respectively integral domain) and let $S \subseteq R$ satisfy the properties.
Then R_S is a principal ideal domain. (respectively integral domain)
Proof: R is not trivial $\implies R_S$ is not trivial.
And, R_S is commutative.
Suppose $\frac{a}{s}, \frac{b}{t} \in R_S$

$$\begin{aligned} \frac{ab}{st} = 0 = \frac{0}{1} &\implies ab = 0 \\ &\implies a = 0 \text{ or } b = 0, \text{ since } R \text{ is an integral domain} \\ &\implies \tfrac{a}{s} = 0 \text{ or } \tfrac{b}{t} = 0 \end{aligned}$$

And, recall that principal ideal domains are all integral domains.
Let $I \subseteq R_S$ be an ideal in R_S.
Identify $R \subseteq R_S$, and let $I^* = I \cap R$.
Check: I^* is an ideal in R.
Thus, $I^* = cR$ for some $c \in R$
Suppose $\frac{a}{s} \in I$.
Then, $a = s(\frac{a}{s}) \in I \cap R = I^*$
$\implies a = cr$ for some $r \in R$
$\implies \frac{a}{s} = \frac{cr}{s} = c\frac{r}{s} \in cR$
$\implies I \subseteq cR_S$
And, since $c \in I$, $cR_S \subseteq I$.
Therefore $I = cR_S$, so R_S is a principal ideal domain.

PMATH 345 Lecture 15: October 19, 2009

1. Preliminaries
2. Units/Zero Divisors
3. Polynomials

4. Homomorphisms
5. Ideals and Quotients
6. Localization and fields of fractions
7. *Euclidean domains*

Recall the division algorithm for $\mathbb{Z}$.
Given $a, b \in \mathbb{Z}$, $a \neq 0$ there exists $q, r \in \mathbb{Z}$ such that

$$b = qa + r$$

and

$$|r| < |a|.$$

Definition: An integral domain R is an *Euclidean domain* if there exists a function $N\colon R \to \mathbb{N}$ with $N(0) = 0$[52], such that given $a, b \in R$, $a \neq 0$, there exists $q, r \in R$ with

$$b = qa + r \qquad \text{and} \qquad N(r) < N(a).$$

Example: $R = \mathbb{Z}$, $N(a) = |a|$.
Such an N is often referred to as a Euclidean norm for R.

Proposition: F a field. Given $f, g \in F[x]$, $f \neq 0$. There exist $q, r \in F[x]$ such that $g = qf + r$ where either $r = 0$ or $\deg(r) < \deg(f)$.
Corollary: $F[x]$ is a Euclidean domain (F a field) with

$$N := \begin{cases} 0 & \text{if } f = 0 \\ \deg(f) + 1 & \text{if } f \neq 0 \end{cases}.$$

Proof: If $g = 0$ then let $q = r = 0$. ✓
Assume $g \neq 0$.
If $\deg(g) < \deg(f)$ then let $q = 0$, $r = g$. ✓
Assume $\deg(g) \geq \deg(f)$.
Induction on $\deg(g)$.

$$\deg(g) = 0 \implies \deg(f) = 0.$$

Therefore $f, g \in F$, so units in F.

$$g = \left(\frac{g}{f}\right) f + 0 \quad \checkmark$$

$\deg(g) = n$:

$$\begin{aligned} g &= b_0 + b_1 x + \cdots + b_n x^n & b_n &\neq 0 \\ f &= a_0 + a_1 x + \cdots + a_m x^m & a_m &\neq 0 \end{aligned}$$

$m \leq n$
Consider $g^* = g - \underbrace{f \cdot \left(\frac{b_n}{a_m} x^{n-m}\right)}$. OK since $a_m \neq 0$ in a field F.
The underbrace has leading term $(a_m x^m)(\frac{b_n}{a_m} x^{n-m}) = b_n x^n =$ leading term of g.
So $\deg(g^*) < \deg(g) = n$. By Induction Hypothesis,

$$g^* = q^* f + r \text{ where either } r = 0 \text{ or } \deg(r) < \deg(f).$$

$$g - f \cdot \left(\frac{b_n}{a_m} x^{n-m}\right) = q^* f + r$$

Corollary: (Factor Theorem): F a field, $g \in F[x]$, $\lambda \in F$
If $g(\lambda) = 0$ (i.e., λ is a *root* of g)

[52] for convenience

then $(x - \lambda)$ is a *factor* of g.
(i.e., $g = (x - \lambda)f$, for some $f \in F[x]$)
The converse is true as well.

Proof: If $g = (x - \lambda)f$, $g(\lambda) = (\lambda - \lambda)f = 0f = 0$ ✓
Conversely, suppose λ is a root of g.
By the proposition, there exists $f, r \in F[x]$ such that

$$g = (x - \lambda)f + r$$

(we are dividing g by $(x - \lambda)$)
with $N(r) < N(x - \lambda) = 2$
$\implies N(r) = 0$ or 1.

If $N(r) = 1$ then $\deg r = 0$ so $r = a_0 \in F$, $a_0 \neq 0$.

$$g = (x - \lambda)f + a_0$$
$$g(\lambda) = 0 \cdot f + a_0 = a_0 \neq 0$$

contradiction. Therefore $N(r) = 0$, therefore $r = 0$, therefore $g = (x - \lambda)f$.
Corollary: F field.
$g \in F[x]$, $\deg(g) = n$ $(g \neq 0)$
Then g has at most n roots.

Proof: Induction on n.
$n = 0$: g is nonzero constant polynomial $\implies g$ has no roots
$n > 0$: $\lambda_1, \ldots, \lambda_l$ be distinct roots of g.
Divide $(x - \lambda_l)$ into g to get
$g = (x - \lambda_l)q$ (by previous corollary)
But $\deg(q) = n - 1$ (since F is an integral domain $\deg(PQ) = \deg(P) + \deg(Q)$)
For each $i < l$,

$$0 = g(\lambda_i) = \underbrace{(\lambda_i - \lambda_l)}_{\neq 0 \text{ since } \lambda_i \neq \lambda_l} q(\lambda_i)$$

By Induction Hypothesis, $l - 1 \leq n - 1 \implies l \leq n$.

PMATH 345 Lecture 16: October 21, 2009

Theorem: Every Euclidean domain is a pid.
Proof: $I \subseteq R$, R Euclidean domain $I \neq (0)$.
Let $N \colon R \to \mathbb{N}$ be a Euclidean norm on R.
Let $a \in I \setminus \{0\}$ be of least norm.
Show: $I = (a)$. Clearly $(a) \subseteq I$.
If not, let $b \in I \setminus (a)$.
Divide b by a to get

$$b = aq + r \qquad q, r \in R$$
$$N(r) < N(a)$$
$$r = b - aq \in I$$

By minimality of $N(a)$
$\implies r = 0$
$\implies b = aq$
$\implies b \in (a)$ Contradiction.
Therefore $I = (a)$.
Therefore R is a pid.
Corollary: $F[x]$ is a pid if F is a field.

Definition: R integral domain.
$a, b \in R$, $a \mid b$ mean a *divides* b which means there is $r \in R$ such that $b = ar$.

(**Note:** $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$.)
(**Note:** units divide everything: take $r = \frac{b}{a}$. 0 divides only 0.)
A nonzero and nonunit $a \in R$ is called *prime* if whenever $a \mid bc$, either $a \mid b$ or $a \mid c$.
A nonzero nonunit $a \in R$ is called *irreducible* if whenever $a = bc$, either $a \mid b$ or $a \mid c$.
Example: In $\mathbb{Z}$, prime = irreducible (= prime #s)

Note: prime $\implies$ irreducible
Example: (prime $\neq$ irreducible)
F field. $F[x]$.
$R \subseteq F[x]$ be the subring of polynomials with no linear term.
i.e., coefficient of x is 0.

Example: R *is* a subring of $F[x]$.
Consider x^2.
Claim: x^2 is irreducible in R.
Proof: $x^2 = fg$, $f, g \in R$
$2 = \deg f + \deg g$.
Since $f, g \in R$, $\deg f \neq 1$, $\deg g \neq 1$
Without loss of generality, $f = a \in F \setminus \{0\}$
$g = \frac{1}{a}x^2$
$\implies x^2 \mid g$.

Claim: x^2 is not prime in R.
Proof: $x^2 \mid x^4 \cdot x^2 = x^6 = x^3 \cdot x^3$
but if $x^2 \mid x^3$ then $x^3 = x^2 f$ for some $f \in R$
$\implies \deg f = 1$, contradiction. So $x^2 \nmid x^3$.

Proposition: If R is a pid then prime = irreducible.
Proof: Need irreducible $\implies$ prime.
$a \in R$ be *irreducible*. Suppose $a \mid bc$. Assume $a \nmid b$.
$I = (a) + (b) = \{\, ar + bs : r, s \in R \,\} = (a, b)$
R pid $\implies I = (d)$, for some $d \in R$.
$d \mid a$ and $d \mid b$
$\Downarrow$
$a = du$ for some $u \in R$
$a \nmid d$ (else $a \mid b$)
$\implies a \mid u$ as a is irreducible
$\implies u = ar$ for some $v \in R$
$\implies a = ard \implies 1 = vd \implies d$ is a unit
therefore $I = R$
there exists $r, s \in R$

$$ar + bs = 1$$
$$acr + cbs = c$$

$a \mid cbs$ as $a \mid bc$
$a \mid acr$ ✓
$\implies a \mid c$ [end of midterm material]

Corollary: In $F[x]$, prime = irreducible, F a field.

Definition: R integral domain is a *Unique Factorization Domain* (UFD) if every nonzero nonunit is a product of primes.

Definition: A ring R is *Noetherian* if there does not exist any infinite *increasing* sequence of ideals. i.e., *cannot* have $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$

Theorem: If R is a Noetherian integral domain then every nonzero nonunit is a product of irreducibles.

Corollary: A noetherian pid is a ufd.

Lemma: pids are always noetherian.

Corollary: pid $\implies$ ufd

PMATH 345 Lecture 17: October 23, 2009

Office Hours Today: 11:30–12, 1:15–2:25, 3:30–4:30

Definition: A commutative ring R is *Noetherian* if there *does not exist* an infinite increasing sequence of ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots .$$

Lemma: pid $\implies$ Noetherian
Proof: Suppose we have a sequence

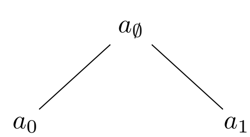
$$(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots .$$

Let $I = \bigcup_i (a_i)$.
Exercise: I is an ideal.
(**Note:** unions of ideals are *not* generally ideals.)

$$\begin{aligned} R \text{ pid} &\implies I = (b) \\ &\implies \text{for some } i,\, b \in (a_i) \\ &\implies I \subseteq (a_i) \\ &\implies (a_j) \subseteq (a_i) \text{ for all } j \geq i \\ &\implies (a_j) = (a_i) \text{ for all } j \geq i \end{aligned}$$

Therefore R is Noetharianity.

Proposition: R Noetharian integral domain.
Every nonzero nonunit is a finite product of irreducibles.
Proof: $a \in R$, $a \neq 0$, a *not* a unit.
We build tree starting with $a = a_\emptyset$
(We will index this tree by finite sequences of 0s and 1s, i.e., by elements of $2^{<\omega}$.)
If a is irreducible then ✓.
If not then $a = a_0 \cdot a_1$ such that $a \nmid a_0$ *and* $a \nmid a_1$.



If a *is irreducible*, *stop* that branch. Otherwise write $a_0 = a_{00} \cdot a_{01}$ where

$$a_0 \nmid a_{00} \qquad \text{and} \qquad a_0 \nmid a_{01}.$$

Continue in this way.
If the tree is *finite*, then a is the product of all the "leaves" of the tree and these elements are irreducible. So we are done.

If the tree is infinite there must exist an infinite branch (König's Lemma). So we have $\alpha \in 2^\omega$, an infinite sequence of 0s and 1s and for each i,

$$a_{\alpha\restriction_{i+1}} \mid a_{\alpha\restriction_i} \qquad \text{but} \qquad a_{\alpha\restriction_i} \nmid a_{\alpha\restriction_{i+1}}$$

$$(a_{\alpha\restriction_i}) \subsetneq (a_{\alpha\restriction_{i+1}})$$

$$(a_\emptyset) \subsetneq (a_{\alpha\restriction_1}) \subsetneq (a_{\alpha\restriction_2}) \subsetneq \cdots$$

Contradiction to Noetheranity.
Hence the tree *is* finite and a is a product of finitely many irreducibles.

Recall: An integral domain R is a *Unique factorization domain* if every nonzero nonunit is a product of primes.
Corollary: pid $\implies$ ufd
Proof: By the lemma pid is Noetharian. By a proposition last time in a pid irreducible = prime. Hence pid $\implies$ ufd by the previous proposition.

$$\text{fields} \subsetneq^{53)} \text{Euclidean domains} \subsetneq^{54)} \text{pids} \subsetneq^{55)} \text{ufds} \subsetneq^{56)} \text{integral domains}$$

Lemma: R integral domain. $a, b \in R$, $u \in R$ a unit.
Then $a \mid b \iff a \mid bu$.
Proof:

$$\begin{aligned} a \mid b &\iff b = ax \text{ for some } x \in R \\ &\iff bu = ay \text{ for some } y \in R \end{aligned}$$

for $\implies$ let $y = xu$
for $\impliedby$ let $x = yu^{-1}$

Lemma: R integral domain, a irreducible in R and u a unit in R. Then au is irreducible.
Proof: Suppose $au = bc$
$\implies a = bcu^{-1} = (b)(cu^{-1})$
$\implies a \mid b$ or $a \mid cu^{-1}$
$\overset{\text{Ex.}}{\implies} au \mid b$ or $a \mid c$ ($\implies au \mid c$).
Lemma+

Lemma: R integral domain, $a \in R$ irreducible, $b \mid a$ *then* either b is a unit or $b = au$ for some unit u. (in particular in the second case, b is also irreducible by the previous lemma.)
Proof: $b \mid a \implies a = bx$ for some $x \in R$.
Exercise: a irreducible $\implies$ either b is a unit of x is a unit.

Definition: R integral domain, $a, b \in R$ irreducibles. We say a and b are *associate* if $a = bu$ for some unit $u \in R$.

Theorem: R a unique factorization domain, $a \in R$ nonzero. Then up to associates and rearrangement there is a unique factorization of a,

$$a = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$$

where $p_1, \ldots, p_l$ are distinct irreducibles and $e_1, \ldots, e_l$ are positive integers.

PMATH 345 Lecture 18: October 28, 2009

median	18.5	74%
mean	17.5	70%

$$\text{fields} \subseteq \text{euclidean domains} \subseteq \text{pids} \subseteq \text{ufds} \subsetneq \text{integral domains}$$

Definition: $a, b \in R$ integral domain. a, b irreducibles. We say a and b are *associate* if $a = bu$ for some unit u.

Exercises:

1. Being associate is an equivalence relation among the irreducibles.
2. If a is irreducible/prime then au is irreducible/prime if u is a unit.
3. a is *irreducible* iff whenever $a = bc$ either b or c is a unit.
4. a, b irreducibles. a and b are associate $\iff a \mid b$

53) $\mathbb{Z}$
54) example?
55) example: $\mathbb{Z}[x]$, why?
56) ?

Lemma: In a unique factorization domain, irreducible = prime.
Proof: Recall R unique factorization domain means a is nonzero nonunit then a is a finite product of primes.

$$\text{prime} \implies \text{irreducible} \quad \checkmark$$

Conversely let a be an irreducible. $a = p_1 \cdots p_n$ where p_i are prime.
Each $p_i \mid a \implies p_i = au_i$ for some u_i.
Exercise: If a product of elements is a unit then so is each factor.

$a = p_i v$, v is a unit

$$\begin{aligned} \text{cancellation} &\implies v = p_1 \cdots \cancel{p_i}^{57)} \cdots p_n \\ &\implies^{58)} \ n = 1 \\ &\implies a \text{ is prime} \end{aligned}$$

Corollary: There are integral domains that are *not* unique factorization domains.
Proof: We have seen an example of an integral domain where irreducible $\not\Longrightarrow$ prime.
Theorem: (Unique factorization theorem):
R unique factorization domain. a nonzero nonunit.

$$\begin{aligned} a &= p_1 \cdots p_n \\ a &= q_1 \cdots q_l \end{aligned} \qquad \text{where the } p_i\text{s and } q_j\text{s are prime}$$

Then $n = l$ and after re-indexing each p_i is associate to q_i.
Proof: By induction on n.
$n = 1$:

$$p_1 = a = q_1 \cdots q_l$$

$\implies l = 1$ and $p_1 = q_1$ as before
$p_1 \mid q_1 \implies p_1 = q_1 u$

$$q_1 u = q_1 q_2 \cdots q_l$$

$\implies u = q_2 \cdots q_l{}^{59)} \implies l = 1 \checkmark$

$n > 1$:

$$p_1 \cdots p_n = a = q_1 \cdots q_l$$

$$p_1 \mid \text{LHS} \implies \begin{matrix} p_1 \mid q_1 \\ \text{or} \\ p_1 \mid (q_2 \cdots q_l) \end{matrix} \overset{p_1 \nmid q_1}{\Longrightarrow} \begin{matrix} p_1 \mid q_2 \\ \text{or} \\ p_1 \mid (q_3 \cdots q_l) \end{matrix} \overset{p_1 \nmid q_2}{\Longrightarrow} \cdots$$

$\implies p_1 \mid q_i$ for some $i = 1, \ldots, l$.
After re-indexing without loss of generality let $i = 1$.
$\implies p_1 \mid q_1 \implies q_1 = p_1 u$, u unit.

$$\begin{aligned} \cancel{p_1} \cdots p_n &= u\cancel{p_1} q_2 \cdots q_l \\ p_2 \cdots p_n &= u q_2 \cdots q_l \end{aligned}$$

Replacing q_2 by an associate (namely uq_2) we may assume without loss of generality

$$p_2 \cdots p_n = q_2 \cdots q_l$$

$\overset{\text{IH}}{\Longrightarrow} n = l$ and after re-indexing p_j *is associate to* q_j $j = 2, \ldots, n = l$.

57) remove p_i
58) by previous exercise
59) contradiction

Example: (non-ufd)
$\mathbb{Z}[2i]$ subring of Gaussian integers

$$\mathbb{Z}[2i] = \{\, a + 2bi : a, b \in \mathbb{Z} \,\}$$

$i = \sqrt{-1}$
Fails unique factorization:

$$4 = 2 \cdot 2v$$
$$4 = (-2i) \cdot (2i)$$

$2, 2i \in \mathbb{Z}[i]$
Need:

1. $2, 2i$ are irreducibles
2. 2 and $2i$ are *not* associate

This leads to two non-associate factorizations of 4 into irreducibles
$\implies \mathbb{Z}[2i]$ *not* unique factorization domain
Claim: 2 is irreducible
Proof:

$$\begin{aligned} 2 &= (a + 2bi)(c + 2di) \qquad a, b, c, d \in \mathbb{Z} \\ &= (ac - 4bd) + 2(ad + bc)i \end{aligned}$$

$\implies$ (1) $ad = -bc$ and
(2) $ac - 4bd = 2$
Assume $bd \neq 0$. Then $ac \neq 0$.
$\implies \operatorname{sgn}(ac) = \text{positive} \implies \operatorname{sgn}(bd) = \text{negative}$ by (1) $\implies$ contradiction (2)
$\implies \operatorname{sgn}(bd) = \text{positive} \implies \operatorname{sgn}(ac) = \text{negative}$ by (1) $\implies$ contradiction (2)

Theorem: (Unique factorization theorem)
R ufd. a nonzero nonunit.
$\implies$ 2 is irreducible ✓
Similarly $2i$ is irreducible ✓
Only units in $\mathbb{Z}[i]$ are $1, -1, -i$[60], i[61]
Only units in $\mathbb{Z}[2i]$ are $1, -1$
$\implies 2, 2i$ are non-associates.

PMATH 345 Lecture 19: October 30, 2009

R ufd
Association is an equivalence relation on the set of primes in R.
We choose and fix once and for all, one prime from each class: P_R is the set of these primes.

- If $p \in R$ is a prime then p is associate to exactly one prime in P_R.
- Any two distinct primes $p, q \in P_R$ are non-associate.

Corollary: (of unique factorization). Given $a \in R$ nonzero nonunit, a can be written uniquely (up to rearrangements) as

$$a = u p_1^{a_1} \cdots p_l^{a_l}$$

where u is a unit, $p_1, \ldots, p_l$ are distinct primes from P_R, $a_1, \ldots, a_l$ are positive integers.
Proof: Exercise.
Remark: Given $a, b \in R$ nonzero we can write

$$a = u p_1^{a_1} \cdots p_l^{a_l}$$
$$b = v p_1^{b_1} \cdots p_l^{b_l}$$

[60] not in R
[61] not in R

where $p_1, \dots, p_l$ are distinct primes from P_R, u, v units, $a_1, \dots, a_l, b_1, \dots, b_l$ non-negative integers.

8. Factoring in polynomials rings.

Definition: R ufd, P_R as above, $a, b \in R$ nonzero nonunits

$$\left.\begin{aligned} a &= up_1^{a_1} \cdots p_l^{a_l} \quad a_1, \dots, a_l \geq 0 \\ b &= vp_1^{b_1} \cdots p_l^{b_l} \quad b_1, \dots, b_l \geq 0 \end{aligned}\right. \quad \text{prime factorizations}$$

The $\gcd(a,b) \coloneqq p_1^{\min\{a_1,b_1\}} \cdot p_2^{\min\{a_2,b_2\}} \cdots p_l^{\min\{a_l,b_l\}}$ greatest common divisor.
Note: This depends on P_R.

Lemma: $d = u\gcd(a,b)$, u a unit[62] $\iff$ $d \mid a$, $d \mid b$ and whenever $e \mid a$, $e \mid b \implies e \mid d$.

Note: RHS does *not* depend on P_R.
Proof: ($\Longrightarrow$) without loss of generality $d = \gcd(a,b)$.
$d \mid a$, $d \mid b$ by definition of gcd.
Suppose $e \mid a$ and $e \mid b$.
Write $e = wp_1^{e_1} \cdots p_l^{e_l}$: this is possible after increasing l.

$$e \mid a \iff a = ex \iff up_1^{a_1} \cdots p_l^{a_l} = wp_1^{e_1} \cdots p_l^{e_l} x \qquad \text{for some } x \in R,\ x \neq 0$$

Again increasing l if necessary, write $x = w' p_1^{x_1} \cdots p_l^{x_l}$, $x_1, \dots, x_l \geq 0$.

$$\begin{aligned} &\implies up_1^{a_1} \cdots p_l^{a_l} = \underbrace{ww'}_{\text{unit}} p_1^{e_1+x_1} \cdots p_l^{e_l+x_l} \\ &\implies a_i = e_i + x_i \qquad \text{for all } i = 1, \dots, l \\ &\implies e_i \leq a_i \qquad i = 1, \dots, l \end{aligned}$$

Similarly $e_i \leq b_i$ for all $i = 1, \dots, l$.
Therefore $e_i \leq \min\{a_i, b_i\} \coloneqq 1, \dots, l$
$e \frac{1}{w} p_1^{\min\{a_1,b_1\}-e_1} \cdots p_l^{\min\{a_l,b_l\}-e_l} = d$
$\implies e \mid d$.
Conversely, let's prove ($\Longleftarrow$), assume RHS. $d \mid a$, $d \mid b$, and when $e \mid a$ and $e \mid b \implies e \mid d$.
Let $e = \gcd(a,b)$
$\implies \gcd(a,b) \mid d$.
On the other hand, from ($\Longrightarrow$) we know that $\gcd(a,b)$ satisfies RHS.
$\implies d \mid \gcd(a,b)$
$xd = \gcd(a,b) = xy\gcd(a,b) \implies xy = 1 \implies x$ is a unit.
Therefore $d = \frac{1}{x}\gcd(a,b)$.

Definition: R ufd, P_R as above.
Consider $R[x]$, $f \in R[x]$, $f \neq 0$.
Write $f = a_0 + a_1 x + \cdots + a_n x^n$ where $n = \deg(f)$: so $a_n \neq 0$.
The *content* of f is

$$G(f) = \gcd(a_i : i = 0, \dots, n,\ a_i \neq 0)$$

Example: In $\mathbb{Z}[x]$, $f = 2 + 12x + 4x^3$
$G(f) = \gcd(2, 12, 4) = 2$.

Theorem: $f, g \in R[x]$ nonzero.

$$G(fg) = G(f)G(g)$$

Start with a lemma.
Lemma: If $G(f) = G(g) = 1$ then $G(fg) = 1$.

Proof of theorem from Lemma
Given any $f \in R[x]$, $f \neq 0$,

$$f = G(f) \cdot \hat{f}$$

[62] i.e., there is a unit u such that $d = u\gcd(a,b)$

where $\hat{f} \in R[x]$ has content 1. $\to$ Exercise.

$$\begin{aligned}
fg &= G(f)\hat{f} \cdot G(g) \cdot \hat{g} \\
fg &= G(f)G(g) \cdot \hat{f}\hat{g} \\
G(fg) &= G(G(f)G(g)\hat{f}\hat{g}) \\
&= G(f)G(g) \cdot G(\hat{f}\hat{g}) =^{63)} G(g)G(f)
\end{aligned}$$

Example: for any $cP \in R[x]$, $c \in R$, $c \neq 0$,

$$G(cP) = cG(P)$$

PMATH 345 Lecture 20: November 2, 2009

(corrected exercise)
Claim: R ufd, $0 \neq P \in R[x]$, $r \in R$,
$G(rP) = urG(P)$ for some unit u
Proof: $P = a_0 + a_1 x + \cdots + a_n x^n$, $n = \deg P$
write $a_i = u_i p_1^{a_{i1}} p_2^{a_{i2}} \dots p_l^{a_{il}}$
$p_1, \dots, p_n$ distinct primes in P_R
$a_{i1}, \dots, a_{il}$ non-negative integers
$rR = ra_0 + ra_1 x + \cdots + ra_n x^n$
write $r = wp_1^{r_1} \cdots p_l^{r_l}$

$$\begin{aligned}
G(rP) &= \gcd\{\, ra_i : i = 1, \dots, l, a_i \neq 0 \,\} \\
&= p_1^{\min\{\, a_{i1}+r_1 : i=1,\dots,l, a_i \neq 0 \,\}} \cdots p_l^{\min\{\, a_{li}+r_l : i=1,\dots,l, a_i \neq 0 \,\}} \\
&= p_1^{e_1} \cdots p_l^{e_l} \\
e_j &= \min\{\, a_{ij} + r_j : i = 1, \dots, l, a_i \neq 0 \,\} \\
&= r_j + \min\{\, a_{ij} : i = 1, \dots, l, a_i \neq 0 \,\} \\
\implies G(rP) &= p_1^{r_1} \cdots p_l^{r_l} \cdot \gcd\{\, a_i : i = 1, \dots, l, a_i \neq 0 \,\} \\
&= \tfrac{1}{w} r \cdot G(P)
\end{aligned}$$

Lemma: R ufd, $f, g \in R[x] \setminus \{0\}$.

$$G(f) = G(g) = 1 \qquad \text{then} \qquad G(fg) = 1.$$

Proof: Suppose $G(fg) \neq 1$, let $p \in P_R$ such that $p \mid G(fg)$
i.e., p appears in the factorization of $G(fg)$ with a positive exponent.

$$\begin{aligned}
f &= a_0 + \cdots + a_n x^n \qquad & n &= \deg f \\
g &= b_0 + \cdots + b_n x^m \qquad & m &= \deg g
\end{aligned}$$

$p \nmid G(f) \implies$ there is a least $r \geq 0$ such that $p \nmid a_r$.
$p \nmid G(g) \implies$ there is a least $s \geq 0$ such that $p \nmid b_s$.
Consider the coefficient of x^{r+s} in fg:

$$\sum_{i=1}^{r+s} a_{r+s-i} b_i$$

If $i < s \implies p \mid b_i \implies p \mid a_{r+s-i} b_i$
If $i > s \implies r + s - i < r \implies p \mid a_{r+s-i} \implies p \mid a_{r+s-i} b_i$

63) Lemma

If $i = s \implies p \nmid a_r, p \nmid a_s \underset{\text{prime}}{\implies} p \nmid a_r a_s$.

Since

$$\sum_{i=1}^{r+s} a_{r+s-i} b_i - \underbrace{\left(\sum_{\substack{i=1 \\ i \neq s}}^{r+s} a_{r+s-i} b_i \right)}_{p \text{ divides}} = \underbrace{a_r b_s}_{p \text{ does not divide}}$$

Therefore $p \nmid$ coefficients of x^{r+s} in fg. Contradiction.

Theorem: R ufd, $f, g \in R[x] \setminus \{0\}$.
$G(fg) = G(f)G(g)$
Proof: First, need to show (exercise):

$$f = G(f) \cdot \hat{f} \qquad G(\hat{f}) = 1$$
$$g = G(g) \cdot \hat{g} \qquad G(\hat{g}) = 1$$

$$fg = G(f)G(g)\hat{f}\hat{g}$$

$$G(fg) = G(\underbrace{G(f)G(g)}_{r} \underbrace{\hat{f}\hat{g}}_{p}) \overset{\substack{\text{exercise} \\ \text{correcting lemma}}}{\implies} G(fg) = urG(\hat{r}\hat{g}) = ur = uG(f)G(g)$$

$$G(fg) = p_1^{e_1} \cdots p_l^{e_l}$$

p_is in P_R, $e_i \geq 0$
Similarly for $G(f)$ and $G(g)$.
Hence for $G(f)G(g)$.
Therefore $u = 1$.

R ufd.

$$R[x] \overset{\text{subring}}{\subseteq} F[x] \qquad F = Q(R) \text{ factor field}$$

Lemma: R ufd, $F = Q(R)$, $f \in F[x]$. There exist $a, b \in R$, $\gcd(a, b) = 1$, and $\hat{f} \in R[x]$, $G(\hat{f}) = 1$ such that $f = \frac{a}{b}\hat{f}$
Proof: $c =$ product of all denominators appearing in the nonzero coefficients of f
$f = a_0 + \cdots + a_n x^n \qquad n = \deg f$, $a_i \in F = Q(R)$
write each $a_i = \frac{b_i}{c_i}$, $b_i, c_i \in R$

$$\prod_{\substack{i=0 \\ b_i \neq 0}}^{n} c_i =: c \neq 0$$

In $R[x]$
$\implies cf \in R[x]$. Write $cf = G(cf) \cdot \hat{f}$ where $\hat{f} \in R[x]$, $G(\hat{f}) = 1$
In $F[x]$,

$$f = \frac{G(cf)}{c}\hat{f}$$

Let $r = \gcd(G(cf), c)$.
$G(cf) = r \cdot a$ for some $a \in R$
$c = r \cdot b$ for some $b \in R$
$\implies \gcd(a, b) = 1$

$$\frac{G(cf)}{c} = \frac{a}{b}$$

Example:

$$\tfrac{5}{6} + \tfrac{25}{4}x + \tfrac{5}{8}x^3 \in \mathbb{Q}[x]$$
$$= \tfrac{5}{24}(\underbrace{4 + 5x + 3x^3}_{\text{in } \mathbb{Z}[x]})$$

PMATH 345 Lecture 21: November 4, 2009

R ufd, $F = Q(R)$, everything today.

Lemma: If $\alpha \in F[x]$ then $\alpha \frac{a}{b} f$ where $f \in R[x]$, $G(f) = 1$, $a, b \in R$, $\gcd(a,b) = 1$
Gauss' Lemma: $f, g \in R[x]$, $G(f) = 1$. $f \mid g$ in $F[x] \implies f \mid g$ in $R[x]$
Proof: $g = f\alpha$ for some $a \in F[x]$. Write $\alpha = \frac{a}{b}h$, $h \in R[x]$, $G(h) = 1$, $\gcd(a,b) = 1$
$\implies g = \frac{a}{b} fh \implies bg = afh$ in $R[x]$
$\implies G(bg) = G(afh) \implies ubG(g) = va\overbrace{G(fh)}^{=1} = va$ in R, u, v units
$\implies b \mid va \implies b \mid a$ in $R \implies \frac{a}{b} \in R \implies \alpha \in R[x]$.
Note: $2x(\frac{1}{2}x) = x^2$ in $\mathbb{Q}[x]$
$2x \mid x^2$ in $\mathbb{Q}[x]$ *not* in $\mathbb{Z}[x]$

Definition: $g \in \mathbb{R}[x]$, $\deg g > 0$, g *factors properly* if $g = h_1 h_2$ where $h_i \in R[x]$, $\deg h_i > 0$

$2 + 2x = 2(1 + x)$ factors in $\mathbb{Z}[x]$ but not properly
Proposition: $g \in R[x]$, $\deg g > 0$
If g does not factor properly in $R[x]$ then g is irreducible in $F[x]$.
Proof: Contrapositive. Suppose $g = \alpha_1\alpha_2$ in $F[x]$, such that *neither* α_1 nor α_2 *is a unit* in $F[x]$
$\implies \deg \alpha_i > 0$.
Write $\alpha_i = \frac{a_i}{b_i} f_i$, $\gcd(a_i, b_i) = 1$, $f_i \in R[x]$, $G(f_i) = 1$, $i = 1, 2$.

$$\begin{aligned} g &= \frac{a_1 a_2}{b_1 b_2} f_1 f_2 \\ \implies b_1 b_2 g &= a_1 a_2 f_1 f_2 \qquad (*) \\ \implies u b_1 b_2 G(g) &= v a_1 a_2 G(f_1 f_2) \\ &= v a_1 a_2 \qquad \text{in } R \end{aligned}$$

u, v units
$\implies b_1 b_2 \mid a_1 a_2$
$b_1 b_2 = w p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ prime factorization, $p_1, \ldots, p_l$ distinct primes in P_R $a_1 = w_1 p_1^{f_1} \cdots p_l^{f_l}$
$a_2 = w_2 p_1^{g_1} \cdots p_l^{g_l}$
Since $b_1 b_2 \mid a_1 a_2$, $e_i \le f_i + g_i$ for $i = 1, \ldots, l$. ...

Claim: Since $b_1 b_2 \mid a_1 a_2$ there exists b_1', b_2' such that $b_1 b_2 = b_1' b_2'$, $b_1' \mid a_1$, $b_2' \mid a_2$ *in* R.
Proof: next time.

By the *claim*,

$$\begin{aligned} b_1' b_2' g = b_1 b_2 g &\overset{(*)}{=} a_1 a_2 f_1 f_2 \\ \implies g &= \left(\frac{a_1}{b_1'} f_1\right)\left(\frac{a_2}{b_2'} f_2\right) \end{aligned}$$

Since $b_i' \mid a_i$ in R,

$$\frac{a_i}{b_i'} \in R \implies \left(\frac{a_i}{b_i'} f_i\right) \in R[x]$$

$$g = \left(\frac{a_1}{b_1'} f_1\right)\left(\frac{a_2}{b_2'} f_2\right) \text{ in } R[x]$$

$$\deg f_i > 0 \qquad i = 1, 2$$

$\implies g$ factors properly.

Corollary: $f \in R[x]$, $\deg f > 0$. If f does not factor properly in $R[x]$ and $G(f) = 1$, then f is prime in $R[x]$.
Proof: By previous proposition, f is irreducible in $F[x]$, hence prime ($F[x]$ is a pid)

R ufd, $F = Q(R)$
Suppose $f \mid gh$ in $R[x]$, $g, h \in R[x]$
$\implies f \mid gh$ in $F[x]$

$$\implies \begin{matrix} f \mid g \text{ in } F[x] \\ \text{or} \\ f \mid h \text{ in } F[x] \end{matrix} \underset{\text{Gauss' Lemma}}{\implies} \begin{matrix} f \mid g \text{ in } R[x] \\ \text{or} \\ f \mid h \text{ in } R[x] \end{matrix}$$

Theorem: R ufd $\implies R[x]$ ufd
Proof: $f \in R[x]$, $f \neq 0$, non-unit
want to write f as a product of primes in $R[x]$.
Case 1: $\deg f = 0$, $f \in R$
R ufd $\implies f = p_1 \cdots p_l$ where p_is are primes in R
Exercise: primes of R are primes in $R[x]$
Case 2: $\deg f > 0$
Suppose there exists a polynomial in $R[x]$ of positive degree that is *not* a product of primes. Let f be of least positive degree. Let f be of least positive degree. Seek a contradiction. If f factors properly then $f = gh$, $\deg g > 0$, $\deg h > 0$
$\implies \deg g < \deg f$, $\deg h < \deg f$
$\implies$ each of g, h must factor into primes, contradiction.

We may assume that f does *not* factor properly.
Write $f = G(f) \cdot \hat{f}$, $G(\hat{f}) = 1$
Then $\hat{f}$ also does not factor properly.
$\implies \hat{f}$ is prime in $R[x]$
and $G(f) \in R$ so by case 1,
$G(f)$ is a product of primes in $R[x]$
therefore f is a product of primes in $R[x]$
Contradiction.

PMATH 345 Lecture 22: November 6, 2009

Claim: Let R be a ufd. Let $a_1, a_2, b_1, b_2 \in R$ and $b_1 b_2 \mid a_1 a_2$. Then there exists b_1', b_2' such that $b_1 b_2 = b_1' b_2'$, and $b_1' \mid a_1$ and $b_2' \mid a_2$.
Proof: Fix P_R for R. Factorize.

$$\begin{aligned} b_1 &= u p_1^{e_1} \cdots p_l^{e_l} \quad &\text{and} \quad b_2 &= v p_1^{f_1} \cdots p_l^{f_l} \\ a_1 &= w p_1^{g_1} \cdots p_l^{g_l} \quad &\text{and} \quad a_2 &= x p_1^{h_1} \cdots p_l^{h_l} \end{aligned}$$

Then $b_1 b_2 \mid a_1 a_2 \implies uvp_1^{e_1+f_1} \cdots p_l^{e_l+f_l} \mid wxp_1^{g_1+h_1} \cdots p_l^{g_l+h_l}$
So, $e_i + f_i \leq g_i + h_i$
So, let e_i' and f_i' be such that $e_i' + f_i' = e_i + f_i$ and $e_i' \leq g_i$ and $f_i' \leq h_i$
Then, let $b_1' = up_1^{e_1'} \cdots p_l^{e_l'}$ and $b_2 = vp_1^{f_1} \cdots p_l^{f_l'}$
Then, it is clear that $b_1' \mid a_1$ and $b_2' \mid a_2$, and also that $b_1' b_2' = b_1 b_2$
So, from theorem, R ufd $\implies R[x]$ ufd.
Examples: $\mathbb{Z}[x]$ is a ufd
$F[x]$ is a ufd for any field F.
But recall that $\mathbb{Z}[x]$ is not a pid, since $(2, x)$ has no principal ideal. Thus, pids $\subsetneq$ ufds

Observe: R pid $\not\Longrightarrow R[x]$ pid
R Euclidean domain $\not\Longrightarrow R[x]$ Euclidean domain

Definition: Let R be a commutative ring. The *polynomial ring in variables* $x_1, \ldots, x_n$ denoted by $R[x_1, \ldots, x_n]$ is the following ring:
Elements are formal expressions of

$$\sum_{\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

where $a_\alpha \in R$, and all but finitely many a_αs are zero.
If we relax the requirement that all but finitely many are zero, then we get $R[[x_1, \ldots, x_n]]$, the power series in n variables.

Multiindex Notation: $\overline{x} = (x_1, \ldots, x_n)$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$

$$\begin{aligned} \text{Then, } \overline{x}^\alpha &:= x_1^{\alpha_1} \cdots x_n^{\alpha_n} \\ |\alpha| &:= \alpha_1 + \cdots + \alpha_n \\ \alpha + \beta &:= (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) \end{aligned}$$

Then, in this ring,

$$\begin{aligned} 0 &= \sum_\alpha 0\overline{x}^\alpha \\ 1 &= 1x_1^0 \cdots x_n^0 + \sum_{\alpha \neq (0,0,\ldots,0)} 0\overline{x}^\alpha \\ \left(\sum_\alpha \overline{x}^\alpha\right) + \left(\sum_\alpha b_\alpha \overline{x}^\alpha\right) &= \sum_\alpha (a_\alpha + b_\alpha)\overline{x}^\alpha \\ \left(\sum_\alpha a_\alpha \overline{x}^\alpha\right)\left(\sum_\alpha b_\alpha \overline{x}^\alpha\right) &= \sum_\alpha \left(\sum_{\substack{\gamma,\delta \in \mathbb{N}^n \\ \gamma+\delta=\alpha}} a_\gamma b_\delta\right)\overline{x}^\alpha \end{aligned}$$

Check: $R[x_1, \ldots, x_n]$ is a commutative ring and it is a subring of the commutative ring $R[[x_1, \ldots, x_n]]$
Example:

a) $R[x_1, \ldots, x_n]$ is isomorhpic to $\underbrace{\underbrace{\underbrace{R[x_1]}[x_2]} \cdots [x_n]}_{\text{These are all rings}}$

b) R embeds in $R[x_1, \ldots, x_n]$

Corollary: R ufd $\implies$ $R[x_1, \ldots, x_n]$ is a ufd

Theorem: R ufd. The irreducibles of $R[x]$ are

i) irreducibles of R

ii) $f \in R[x]$, $\deg f > 0$, $G(f) = 1$ and f is irreducible in $F[x]$, $F = Q(R)$

Proof: If $f \in R$ irreducible in $R \implies f$ irreducible in $R[x]$
If f is of type 2, f does not factor properly in $R[x] \implies f$ irreducible in $R[x]$
So, i) and ii) are both irreducible. Now, we will show these are the *only* irreducibles.
Suppose $f \in R[x]$ is irreducible, and $f \notin R$
therefore $\deg f > 0$. So, $f = G(f)\hat{f}$, where $G(\hat{f}) = 1$.
Since $\deg \hat{f} = \deg f > 0$, $\hat{f}$ is not a unit in $R[x]$
$\implies G(f)$ is a unit in $\hat{f}$, since f is irreducible.
But $G(f) = p_1^{e_1} \cdots p_l^{e_l}$, $\implies e_1 = e_2 = \cdots = e_l = 0$.

$$\implies G(f) = 1 \tag{1}$$

Also, since f is irreducible, f does not factor properly in $R[x]$.

$$\implies f \text{ is irreducible in } F[x] \tag{2}$$

By (1) and (2), f is in category ii)

Theorem: (Eisenstein Criterion)
Let R be a ufd, $f \in R[x]$

$$f = a_0 + a_1x + \cdots + a_nx^n, \qquad n = \deg f > 0$$

Suppose there exists an irreducible $p \in R$ such that

i) $p \nmid a_n$

ii) $p \mid a_i$, $i = 0, \dots, n-1$

iii) $p^2 \nmid a_0$

Then, f is irreducible in $F[x]$, $F = Q(R)$
Hence, if $G(f) = 1$, then f is irreducible in $R[x]$.
Proof: It suffices to prove that f does not factor properly in $R[x]$.
Suppose $f = gh$ with $\deg g, \deg h > 0$
Then,

$$\begin{aligned} g &= b_0 + \cdots + b_m x^m \quad 0 < m < n \\ n &= c_0 + \cdots + c_l x^l \quad\ \ 0 < l < n \end{aligned} \qquad \text{and } m + l = n$$

Then, $a_n = b_m c_l$, so since $p \nmid a_n$, then $p \nmid b_m$ and $p \nmid c_l$.
$p \mid a_0 \implies p \mid b_0 c_0 \implies p \mid b_0$ or $p \mid c_0$
And, since $p^2 \nmid b_0 c_0$, then p does not divide both.
Then, without loss of generality assume $p \mid b_0$ and $p \nmid c_0$.
Let k be least integer such that $p \nmid b_k$, $0 < k \leq m$

$$\begin{aligned} \text{Consider } [x^k]f &= a_k \\ &= b_k c_0 + b_{k-1} c_1 + \cdots + b_1 c_{k-1} + b_0 c_k \end{aligned}$$

Since k is minimal, $p \mid b_{k-1} c_1, \dots, p \mid b_0 c_k$
And, we know $p \mid a_k$, since $k < n$
Therefore $p \mid b_k c_0$. But $p \nmid b_k$ and $p \nmid c_0$, contradiction.

PMATH 345 Lecture 23: November 9, 2009

Examples: R is a ufd, working in $R[x]$

a) $a + x^n$, where a is a product of distinct primes is irreducible in $R[x]$
as long as the factors of a are all distinct (because $8 + x^3$ can be factored in $\mathbb{Z}[x]$)

b) Let p be a prime number $\in \mathbb{Z}$
Then $f = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbb{Q}[x]$
Proof: By Einsenstein, $g = p + \binom{p}{2}x + \binom{p}{3}x^2 + \cdots + \binom{p}{p-2}x^{p-3} + px^{p-2} + x^{p-1}$ is irreducible, since $p \mid \binom{p}{i}$, $p \nmid 1$, and $p^2 \nmid p$

$$\begin{aligned} \text{Consider } \sigma \colon \mathbb{Q}[x] &\to \mathbb{Q}[x] \\ h &\mapsto h(x+1) \end{aligned}$$

[We showed this in an assignment. We can use $R[x]$ to send any extension of R, called S, to S. In this case, $S = R[x]$.]
So if $h = a_0 + \cdots + a_n x^n$, $a_n \neq 0$, then

$$\sigma(h) = a_0 + a_1(x+1) + \cdots + a_n(x+1)^n$$

Note that the leading term is still $a_n x^n$
Thus, $\ker \sigma = \{0\}$[64] and σ perserves degree.
Also, σ is surjective, since given h,

$$\sigma(a_0 + a_1(x-1) + a_2(x-1)^2 + \cdots + a_n(x-1)^n) = h$$

So, σ is an automorphism that preserves degree.

Exercise: Given any automorphism, if h is irreducible, then σh is irreducible.
→ This is true for all automorphisms on integral domains.

[64] $\implies$ σ is injective

Claim: $\sigma(f) = g$
$(-1+x)(1+x+\cdots+x^{p-1}) = (-1+x^p)$

$$\begin{aligned}
\text{Thus, } \sigma((-1+x)(1+\cdots+x^{p-1})) &= \sigma(-1+x^p) \\
\implies \sigma(-1+x)\sigma(1+\cdots+x^{p-1}) &= \sigma(-1+x^p) \\
x\sigma(1+\cdots+x^{p-1}) &= -1+(x+1)^p \\
&= px + \tbinom{p}{2}x^2 + \tbinom{p}{3}x^3 + \cdots + \tbinom{p}{p-2}x^{p-2} + px^{p-1} + x^p \\
\implies \sigma(1+\cdots+x^{p-1}) &= p + \tbinom{p}{2}x + \cdots + \tbinom{p}{p-2}x^{p-3} + px^{p-2} + x^{p-1} \\
\implies \sigma(f) &= g
\end{aligned}$$

So f is irreducible, since g is.

Fields
Let R be an integral domain. Then, there is a unique homomorphism

$$\begin{aligned}
\phi\colon \mathbb{Z} &\to R \\
n &\mapsto \underbrace{1+\cdots+1}_{n} \quad n \geq 0 \\
-n &\mapsto -\phi(n)
\end{aligned}$$

Recall: R integral domain $\implies \ker\phi$ is a prime ideal.
$\implies \ker(\phi) = (0)$ or $\ker(\phi) = (p)$, p is prime

Definition: If, as above, $\ker\phi = (0)$, then we say R is at *characteristic 0.* ($\iff \underbrace{1+1+\cdots+1}_{n} \neq 0$ in R for all $n \in \mathbb{Z}$)
If $\ker\phi = (p)$, we say *characteristic of R is p.* ($\iff \underbrace{1+1+\cdots+1}_{p} = 0$ in R)

Remark: If $R = F$ is a field then,

a) $\operatorname{char} F = 0 \implies \phi$ extends to an embedding of $\mathbb{Q}$ in F (by the universal property, or by showing directly)

$$\begin{aligned}
\hat{\phi}\colon \mathbb{Q} &\to F \\
\tfrac{n}{m} &\mapsto \phi(n)\phi(m)^{-1}
\end{aligned}$$

b) $\operatorname{char} F = p \implies$ we have an embedding (by 1st isomorphism theorem, oy by showing directly)

$$\text{also an embedding } \begin{cases} \hat{\phi}\colon \mathbb{Z}_p = \mathbb{Z}/(p) \to F \\ \quad n + (p) \mapsto \underbrace{1+\ldots+1}_{n} \end{cases}$$

Definition: A subfield of a field is a subring that is a field.
Therefore every field has a subfield isomorphic to $\mathbb{Q}$ ($\operatorname{char} F = 0$) or $\mathbb{Z}_p$ ($\operatorname{char} F = p$)

Convention: Idenitify $\mathbb{Q}$ and $\mathbb{Z}_p$ with their images in F.
So $\mathbb{Q} = \left\{ \phi(n)\phi(m)^{-1} : n, m \in \mathbb{Z},\, m \neq 0 \right\} \subseteq F$ for $\operatorname{char} F = 0$ and $\mathbb{Z}_p = \{0, 1, 1{+}1, \ldots, \underbrace{1+1+\cdots+1}_{p-1}\} \subseteq F$ for $\operatorname{char} F = p$

Definition: The set above is the *prime subfield* of F.
Exercise: The prime subfield of F is the unique smallest subfield of F.
Notation: $\mathbb{F}$ is the prime subfield of F.

PMATH 345 Lecture 24: November 11, 2009

$F \subseteq L$ *field extension*: F is a subfield of L. Call F the *base field.*
We can view L as an F-vector space.
zero vector: $0 \in L$

vector sum: $+$
$r \in F$, scalar multiplication by r: given $a \in L$, $r \cdot a = ra$.

Linear Algebra $\implies$ L has an F-basis: $B \subseteq L$ such that every $a \in L$ is of the form

$$a = r_1 b_1 + r_2 b_2 + \cdots + r_l b_l$$

where $r_1, \ldots, r_l \in F$, $b_1, \ldots, b_l \in B$.
Moreover this is a unique representation of a.

Also **Fact:** $B \subseteq L$ is a basis $\iff$ B is a maximal F-linearly independent set $\iff$ B is F-linearly independent and

$$L = \operatorname{span}_F(B) = \{\, r_1 b_1 + \cdots + r_l b_l : b_1, \ldots, b_l \in B,\, r_1, \ldots, r_l \in F \,\}$$

Fact 2: Any two bases for L over F are of the same *cardinality*, called the *dimension*. That is, there exists a bijection between any two bases.

Definition: $F \subseteq L$ field extension.
The *degree of L over F* is the dimension of L as an F-vector space, denoted $[L : F]$
When $[L : F] \in \mathbb{N}$ we say that L is a *finite extension.*
Example: $\mathbb{R} \subseteq \mathbb{C}$ finite extension, $[\mathbb{C} : \mathbb{R}] = 2$

Remark: $[L : F] = 1 \iff L = F$

Lemma: $n, m \in \mathbb{N}$, field extensions $[L : K] = n$, $[K : F] = m$

$$\underbrace{L \overset{\deg n}{\supseteq} K \overset{\deg m}{\supseteq} F}_{\deg nm}$$

Then $[L : F] = nm$.
Proof: Let $\{u_1, \ldots, u_m\} \subseteq K$ be an F-basis for K
Let $\{v_1, \ldots, v_n\} \subseteq L$ be an K-basis for L
Let $B = \{\, u_i v_j : i = 1, \ldots, m, j = 1, \ldots, n \,\}$
$|B| = nm$. We claim B is an F-basis for L.
$\operatorname{span}_F(B) = L$ ✓
Let $a \in L$ we can write

$$a = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

where $\lambda_1, \ldots, \lambda_n \in K$.
Write each

$$\lambda_i = \alpha_{i,1} u_1 + \alpha_{i,2} u_2 + \cdots + \alpha_{i,m} u_m$$

where $\alpha_{i,j} \in F$

$$\begin{aligned} a &= \sum_{i=1}^{n} \lambda_i v_i \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{i,j} u_j \right) v_i \\ a &= \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{i,j} u_j v_i \in \operatorname{span}_F(B) \end{aligned}$$

B is linearly independent over F
Suppose $\sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{i,j} u_j v_i = 0$ where $\alpha_{i,j} \in F$

$$\implies \sum_{i=1}^{n} \underbrace{\left(\sum_{j=1}^{m} \alpha_{i,j} u_j \right)} v_i = 0$$

since $u_j \in K$, $\alpha_{i,j} \in F$, the underbrace $\implies \sum_{j=1}^m \alpha_{i,j} u_j \in K$
Since $\{v_1, \dots, v_n\}$ are K-linearly independent
$\implies \sum_{j=1}^m \alpha_{i,j} u_j = 0$ for all $i = 1, \dots, n$.

Definition: $F \subseteq L$ field extension, $a \in L$.
a is *algebraic over* F if there exists a polynomial $f \in F[x]$ which is *nonzero* and such that $f(a) = 0$. If every $a \in L$ is algebraic over F then we say that $F \subseteq L$ is an *algebraic extension*.
If $a \in L$ is not algebraic over F then we say it is *transcendental over* F.

Example:

(a) If $a \in F$ then a is F-algebraic, take $f = -a + x \in F[x]$

(b) $\mathbb{Q} \subseteq \mathbb{C}$, i is algebraic over $\mathbb{Q}$ since $f = 1 + x^2 \in \mathbb{Q}[x]$ vanishes at i

(c) In fact $\mathbb{R} \subseteq \mathbb{C}$ is an algebraic extension.

$\rightarrow$ $a + bi$, $a, b \in \mathbb{R}$, is a root of
$$f = (x - a)^2 + b^2 \in \mathbb{R}[x]$$

(d) Let F be any field.
Let $L = F(x) =$ fraction field of $F[x]$
$$\underbrace{F \subseteq F[x] \subseteq F(x) = L}_{\text{field extension}}$$

$a = x \in L$ is transcendental over F

$\rightarrow$ Suppose $f \in F[x]$, such that $f(a) = 0$[65]
$f(a) = f(x)$, i.e., $f = a_0 + a_1 x + \cdots + a_n x^n$
$f(a) = a_0 + a_1 x + \cdots + a_n x^n = 0$ in $F[x]$
So f is the zero polynomial.

Theorem: Every finite extension of fields is an algebraic extension.

PMATH 345 Lecture 25: November 13, 2009

Proposition: Every finite field extension is algebraic.
Proof: $F \subseteq L$, $[L : F] = n$
Let $a \in L$.
Consider $\{a^0 = 1, a, a^2, \dots, a^n\} = X \subseteq L$

case 1: some $a^i = a^j$, $i \neq j$, $0 \leq i < j \leq n$
$\implies 1 = a^{j-1}$
$\implies -1 + a^{j-i} = 0$
$\implies f(a) = 0$ where f[66] $= -1 + x^{j-i} \in F[x]$
Therefore a is algebraic over F. ✓
(in fact a is algebraic over $\mathbb{F}$.)

case 2: otherwise X has $n + 1$ many elements in it $\implies$ X is F-linearly dependent
Therefore there exist $a_0, \dots, a_{n+1} \in F$ not *all* zero such that
$$a_0 \cdot 1 + a_1 \cdot a + a_2 \cdot a^2 + \cdots + a_n \cdot a^n = 0$$

Let $g = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$
Then $g \neq 0$ but $g(a) = 0$.
Therefore a is algebraic over F.

Definition: A *monic polynomial* is a polynomial with leading coefficient $= 1$.

---
[65] in L
[66] $\neq 0$

Proposition/Definition: $F \subseteq L$ field extension, $a \in L$ algebraic over F. There exists a *unique* monic polynomial $h \in F[x]$ of minimal degree such that $h(a) = 0$. This h is called the *minimal polynomial of a over F*.
Proof: Note since a is algebraic over F, there exists $g \neq 0$, $g(a) = 0$, $g \in F[x]$.
Let $c =$ leading coefficient of $g \neq 0$, $c \in F$ and let $g' = \frac{1}{c} g$.
Then g' is monic, and $g' \neq 0$, and $g'(a) = \frac{1}{c} g(a) = 0$.
Hence there exists a monic polynomial $h \in F[x]$ of minimal degree, say n, such that $h(a) = 0$.
Uniqueness: Suppose $f \in F[x]$ monic also of degree n, also $f(a) = 0$.
By the division algorithm (i.e., $F[x]$ is a Euclidean domain) we can write

$$f = hq + r \qquad q, r \in F[x]$$

and either $r = 0$ or $\deg r < \deg h = n$[67].

$$\begin{aligned} \text{But } r(a) &= f(a) - hq(a) \\ &= f(a)^{68)} - h(a)^{69)} q(a) = 0 \end{aligned}$$

Therefore $r = 0$. So $f = hq$

$$\begin{aligned} n = \deg f &= \deg h + \deg q \\ &= n + \deg q \\ \implies \deg q &= 0 \\ \implies q &\in F \setminus \{0\} \end{aligned}$$

leading coefficient(h)[70] $=$ leading coefficient(f)[71] $\cdot\, q$
Therefore $q = 1$, therefore $f = h$.

Proposition: $F \subseteq L$ field extension, $a \in L$ algebraic over F, $h =$ minimal polynomial of a over $F \in F[x]$. Then:

(a) h is irreducible

(b) If $g \in F[x]$ and $g(a) = 0$ then $h \mid g$. (Hence a polynomial vanishes at $a \iff h$ divides it.)

(c) If $g \in F[x]$, monic and irreducible and $g(a) = 0$ then $g = h$.

Proof:

(a) Suppose $h = fg$. $h(a) = 0 \implies f(a)g(a) = 0$

$$\implies f(a) = 0^{72)} \implies \deg f = \deg h \text{ by minimality}^{73)} \implies \deg g = 0^{74)} \implies g \text{ is a unit}^{75)}$$

But $\deg f \leq \deg h$, $\deg g \leq \deg h$.
Therefore h is irreducible.

(b) Suppose $g(a) = 0$, $g \neq 0$

$$g = hq + r \qquad q, r \in F[x]$$

either $r = 0$ or $\deg r < \deg h$.
Again by minimality of $\deg h$, and as $r(a) = 0$

$$\begin{aligned} &\implies r = 0 \\ &\implies g - hq \implies h \mid g \quad \checkmark \end{aligned}$$

[67] By minimality of n this can't happen
[68] $= 0$
[69] $= 0$
[70] $= 1$
[71] $= 1$

(c) $g \in F[x]$, monic, irreducible, $g(a) = 0$.
By (b), $h \mid g \implies g = hf$ for some $f \in F[x]$.
g irreducible $\implies$ h or f is a unit
Since $h(a) = 0$, h is not a nonzero constant polynomial
$\implies$ h is *not* a unit
$\implies$ f is a unit, $\deg f = 0$, $f \in F$. Since

$$\begin{aligned} 1 &= \text{leading coefficient of } g \\ &= \text{leading coefficient of } h \\ \implies f &= 1 \end{aligned}$$

Therefore $g = h$.

Remark: $a \in L \supseteq F$, F-algebraic

$$I = \left\{ f \in F[x] : f(a)^{76)} = 0 \right\} \text{ ideal in } F[x]$$

(b) says $I = (h)$
where $h =$ minimal polynomial of a over F.

Example: $\mathbb{Q} \subseteq \mathbb{R}$, $\sqrt{2}$
$x^2 - 2$ vanishes at $\sqrt{2}$ and monic, is irreducible in $\mathbb{Q}[x]$ by Eisenstein
$\implies$ $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$.

Definition: $L \supseteq F$, $a \in L$ algebraic over F.

$$\deg(a/F)^{77)} = \text{degree of the minimal polynomial}$$

Corollary: $F \subseteq K \subseteq L$, $a \in L$ algebraic over F.

$$\deg(a/F) \geq \deg(a/K)$$

Proof:

$$\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array}$$

$$\begin{aligned} h_1 &= \text{minimal polynomial of } a \text{ over } F \in F[x] \\ h_2 &= \text{minimal polynomial of } a \text{ over } K \in K[x] \end{aligned}$$

$$\begin{aligned} h_1 \in K[x], h_1(a) = 0 &\overset{(b)}{\implies} h_2 \mid h_1 \\ &\implies \deg h_2{}^{78)} \leq \deg h_1{}^{79)} \end{aligned}$$

PMATH 345 Lecture 26: November 16, 2009

72) or $g(a) = 0$
73) or $\deg g = \deg h$ by minimality
74) or $\deg f = 0$
75) or f is a unit
76) $I(a/F)$
77) *degree of a over F*
78) $= \deg(a/K)$
79) $= \deg(a/F)$

Definition: $F \subseteq L$ field extension.
Let $R \subseteq F$ subring of F such that
$F = Q(R)$ (special case: $R = F$)
$a_1, \ldots, a_n \in L$

$$\begin{aligned}
R[a_1, \ldots, a_n] &= \textit{The subring of } L \textit{ generated by } a_1, \ldots, a_n \textit{ over } \mathbb{R} \\
&= \text{intersection of all subrings of } L \text{ that contain } R \text{ and } a_1, \ldots, a_n \\
F(a_1, \ldots, a_n) &= \textit{the subfield of } L \textit{ generated by } a_1, \ldots, a_n \textit{ over } F \\
&= \text{fraction field of } R[a_1, \ldots, a_n]
\end{aligned}$$

$$\begin{tikzcd}
L \arrow[r, dash] & F(a_1, \ldots, a_n) \arrow[r, dash] \arrow[dr, dash] & R[a_1, \ldots, a_n] \arrow[r, dash] & R \arrow[dl, dash] \\
& & F &
\end{tikzcd}$$

Exercises:

(a) $R[a_1, \ldots, a_n]$ is a subring of L

(b) $F(a_1, \ldots, a_n)$ is the intersection of all subfields of L with respect to $a_1, \ldots, a_n$ and F.

(c) $R[a_1, \ldots, a_n] = \{ f(a_1, \ldots, a_n) : f \in R[a_1, \ldots, a_n]$[80] $\} \subseteq L$
Need:

- Show $\supseteq$
- Show RHS is a subring of L and contains R, $a_1, \ldots, a_n$

(d)
$$F(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} : f, g \in F[x_1, \ldots, x_n],\, g(a_1, \ldots, a_n) \neq 0 \right\}$$

Theorem: $F \subseteq L$ field extension, $a \in L$, F-algebraic, $h =$ minimal polynomial of a over F

$$F[x]/(h) \simeq F[a] = F(a)$$

and $[F(a) : F] = \deg h$
Proof: Consider

$$\begin{aligned}
\phi\colon F[x] &\to F[a] \\
f &\mapsto f(a)
\end{aligned}$$

"evaluation at a map" ring homomorphism
By exercise (c), ϕ is surjective

$$\xRightarrow{\text{1st iso. thm.}} F[x]/\ker\phi \simeq F[a]$$

If $h \mid f$ then $f = hg$

$$\begin{aligned}
&\implies f(a) = h(a)g(a) = 0 \\
&\implies f \in \ker\phi
\end{aligned}$$

We have proved the reverse: if $f(a) = 0$ then $h \mid f$.
Therefore $\ker\phi = (h)$, therefore $F[x]/(h) \simeq F[a]$

$$\begin{aligned}
h \text{ irreducible nonzero } &\implies (h) \neq (0) \text{ is prime in } F[x],\ F[x] \text{ pid} \\
&\implies (h) \text{ is maximal} \\
&\implies F[a] \text{ is a field} \\
&\implies F[a] = F(a)
\end{aligned}$$

[80] polynomial ring

[Why? $(h) \subseteq (f) \subseteq F[x]$
$\implies h = fg$ for some g
$\implies f$ is a unit $\implies (f) = F[x]$
  or
  g is a unit $\implies f = g^{-1}h \implies f \in (h) \implies (f) = (h)$
$h = a_0 + a_1 x + \cdots + a_m x^m$
$m = \deg h$, $a_m \neq 0$
$B = \{1, a, a^2, \ldots, a^{m-1}\} \subseteq F(a)$

$$\begin{tikzcd} L \arrow[r, dash] \arrow[rr, dash, bend right] & F(a) \arrow[r, dash] & F \end{tikzcd}$$

Claim: B is F-linearly independent
Proof: $r_0 \cdot 1 + r_1 \cdot a + \cdots + r_{m-1}a^{m-1} = 0$, $r_i \in F$
$\implies f(a) = 0$ where $f = r_0 + r_1 x + \cdots + r_{m-1}x^{m-1}$
$m =$ smallest degree of a nonzero polynomial vanishing at a
$\implies f = 0 \implies r_i = 0$: Claim 1

Claim 2: $\operatorname{span}_F(B) = F(a)$
Proof: $b \in F(a) = F[a]$
$\implies b = f(a)$ for some $f \in F[x]$
$f = r_0 + r_1 x + \cdots + r_n x^n$
$n = \deg f \qquad r_n \neq 0$
Show $f(a) \in \operatorname{span}_F(B)$ by induction on n.

$n < m$: $f(a) = r_0 + r_1 a + \cdots + r_n a^n \in \operatorname{span}_F(B)$
since $1, a, \cdots, a^n \in B$ ✓

$n = m$: $b = f(a) = r_0 + \cdots + r_m a^m$

$$\implies a_m = -\left(\frac{r_0}{r_m} + \frac{r_1}{r_m}a + \cdots + \frac{r_{m-1}}{r_m}a^{m-1}\right) \in \operatorname{span}_F(B)$$

Therefore $1, a, \ldots, a^m \in \operatorname{span}_F(B)$
$\implies b = r_0 + r_1 a + \cdots + r_m a^m \in \operatorname{span}_F(B)$

$n > m$: Induction Hypothesis: $1, a, \ldots, a^{n-1} \in \operatorname{span}_B(F)$

$$\begin{aligned} a^n = a(a^{n-1}) &= a(s_0 + s_1 a + \cdots + s_{m-1}a^{m-1}) \\ &= s_0 a + s_1 a^2 + \cdots + s_{m-1}a^m \\ &\in \operatorname{span}_F\{a, a^2, \ldots, a^m\} \subseteq \operatorname{span}_F(B) \end{aligned}$$

since $B = \{1, \ldots, a^{m-1}\}$ and $a^m \in \operatorname{span}_F(B)$ by case $m = n$
$b = f(a) = r_0 + r_1 a + \cdots + r_n a^n \in \operatorname{span}_F(B)$: Claim 2

$$[F(a) : F] = |B| = m = \deg h$$

Corollary: The above proof shows more:
$F \subseteq L$ field extension, $a \in L$ algebraic over F, $\deg(a/F) = m$ *then* $\{1, a, \ldots, a^{m-1}\}$ is an F-basis for $F(a)$.

$$\begin{tikzcd} & a \in L \arrow[dl, dash] \arrow[dr, dash] & \\ F \arrow[rr, dash, "\text{deg}=\deg(a/F)"'] & & F(a) \end{tikzcd}$$

PMATH 345 Lecture 27: November 18, 2009

Last time: $F \subseteq L$, $a \in L$, F-algebraic. $\deg(a/F) = m$.
$\{1, a\}$ is an F-basis for $F(a)$.
Example:

$$\begin{array}{c} \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} \deg(i/\mathbb{Q}) = 2 \\ \{1, i\} \text{ is a } \mathbb{Q}\text{-basis} \end{array} \qquad x^2 + 1$$

$\mathbb{Q}(i)$[81] $= \{\, a + bi : a, b \in \mathbb{Q} \,\}$

$\mathbb{Q}(\sqrt{2})$[82]

$$\begin{array}{c} \phantom{\mathbb{Q}} \\ | \,\}2 \\ \mathbb{Q} \end{array} \qquad \text{Basis: } \{1, \sqrt{2}\}$$

$$\mathbb{Q}(\sqrt{2}) = \left\{\, a + b\sqrt{2} : a, b \in \mathbb{Q} \,\right\} \overset{\text{def/ex}}{=} \left\{\, f(\sqrt{2}) : f \in \mathbb{Q}[x] \,\right\}$$

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}) \\ | \,\}3 \\ \mathbb{Q} \end{array} \qquad \mathbb{Q}\text{-basis: } \{1, 2^{1/3}, 2^{2/3}\} \qquad x^3 - 2$$

Corollary: $F \subseteq K$ algebraic extension of fields
$K \subseteq L$ algebraic extension of fields
Then L is algebraic over F.

$$\begin{array}{l} L \\ |\ \text{alg} \\ K \\ |\ \text{alg} \\ F \end{array}$$

Proof: $a \in L$, a is algebraic over K
$\implies h(a) = 0$ for some $h = b_0 +_1 x + \cdots + b_n x^n \in K[x]$, $b_n \neq 0$
b_is are in K hence algebraic over F.

$$\begin{array}{c} F(b_0)(b_1)(b_2)\cdots(b_n) \underset{\text{Ex}}{=} F(b_0, \ldots, b_n) \\ \vdots \\ F(b_0)(b_1) \\ \text{finite}\ | \\ F(b_0) \\ \mathbb{N} \ni \deg(b_0/F)\ | \\ F \end{array}$$

Therefore $[F(b_0, \ldots, b_n) : F] \in \mathbb{N}$.

$$\begin{array}{c} F(b_0, \ldots, b_n)(a) \\ \| \\ F(b_0, \ldots, b_n, a) \\ |\ \text{finite} \\ F(b_0, \ldots, b_n) \\ |\ \text{finite} \\ F \end{array}$$

a is algebraic over $F(b_0, \ldots, b_n)$ since $h \in F(b_0, \ldots, b_n)[x]$, $h(a) = 0$
Therefore $[F(b_0, \ldots, b_n, a) : F] \in \mathbb{N}$
$\implies F(b_0, \ldots, b_n, a)$ is algebraic over F
$\implies a$ is algebraic over F.

Example:

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[dr, dash, "2"] \arrow[dd, dash, "4"] & \\ \mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

[81] $=$ fraction field of $\mathbb{Z}[i]$ = Gaussian integers
[82] $\subseteq \mathbb{R}$

$$x^2 - 2 = \text{minimal polynomial of } \sqrt{2} \text{ over } \mathbb{Q}$$
$$x^2 - 3 = \text{minimal polynomial of } \sqrt{3} \text{ over } \mathbb{Q}$$
$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$$
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = \deg(\sqrt{3}/\mathbb{Q}(\sqrt{2})) \leq \deg(\sqrt{3}/\mathbb{Q}) = 2$$

If $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1 \implies \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})$
$\implies \sqrt{3} \in \mathbb{Q}(\sqrt{2}) \implies \sqrt{3} = a + b\sqrt{2},\ a, b \in \mathbb{Q}$
$\implies 3 = a^2 + 2ab\sqrt{2} + 2b^2 \implies ab = 0 \implies 3 = 2b^2$ or $3 = a^2$, contradiction
Therefore $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$
Therefore $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

Example: Suppose $F \subseteq L$ field extension
$a, b \in L$, F-algebraic

$$\begin{aligned} \deg(a/F) &= m \\ \deg(b/F) &= n \end{aligned} \qquad \gcd(m, n) = 1$$

Then: $[F(a,b) : F] = nm$

$$\begin{tikzcd}[column sep=small] & F(a,b) = F(a)(b) \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\ F(b) \arrow[dr, dash, "n"'] & & F(a) \arrow[dl, dash, "m"] \\ & F & \end{tikzcd}$$

n and m must divide $[F(a,b) : F]$
$\implies nm \mid [F(a,b) : F] \implies F[F(a,b) : F] \geq nm$

$$\begin{aligned} [F(a,b) : F] &= [F(a,b) : F(a)] \cdot [F(a) : F] \\ &= \deg(b/F(a)) \cdot \deg(a/F) \\ &\leq n \cdot m \end{aligned}$$

F field. $g \in F[x]$ irreducible
(g) is a nonzero prime ideal in the pid $F[x]$
$\implies (g)$ is maximal ideal
$L := F[x]/(g)$ is a field

$$\begin{aligned} \phi\colon F &\to L \\ r &\mapsto r + (g) \end{aligned} \qquad \text{homomorphism}$$

Claim: ϕ is en embedding
Proof:

$$\begin{aligned} r \in F,\ r \neq 0,\ \phi(r) = 0 &\implies r + (g) = 0 \text{ in } L \\ &\implies r \in (g) \implies (g) = F[x] \text{ contradiction} \end{aligned}$$

Identify F with $\phi(F)$ and we have a field extension

$$\begin{tikzcd} L = F[x]/(g) \arrow[d, dash] \\ F \end{tikzcd}$$

Proposition: F field, $g \in F[x]$ irreducible. $L = F[x]/(g)$
Then $[L : F] = \deg g$
Proof:

$$\begin{aligned} \text{Let } a &:= x + (g) \qquad \text{Call } (g) = I. \\ &= x + I \in L \end{aligned}$$

Claim: $L = F(a)$
Proof: Let $\alpha \in L$. $\alpha = f + I$ for some $f \in F[x]$
While $f = a_0 + a_1 x + \cdots + a_n x^n$, a_is $\in F$.

$$\begin{aligned} \alpha = f + I &= (a_0 + \cdots + a_n x^n) + I \qquad \text{in } L \\ &= a_0 + a_1(x + I) + a_2(x + I)^2 + \cdots + a_n(x + I)^n \\ &= f(a) \end{aligned}$$

Therefore $L = F[a] = F(a)$.

Claim 2: $g(a) = 0$ in L
Proof:

$$\begin{aligned} g &= b_0 + b_1 x + \cdots + b_m x^m \qquad m = \deg g \\ g(a) &= b_0 + b_1 a + \cdots + b_m a^m \\ &= b_0 + (b_1 x + I) + \cdots + (b_m x^m + I) \\ &= (b_0 + b_1 x + \cdots + b_m x^m) + I \\ &= g + I = g + (g) \\ &= 0 \text{ in } L \end{aligned}$$

Therefore $\min(a/F) = \frac{1}{bm} \cdot g$

$$\begin{aligned} \text{Therefore } [L : F] &= \deg(\tfrac{1}{bm} g) \\ &= \deg g \end{aligned}$$

PMATH 345 Lecture 28: November 20, 2009

Kronecker's Theorem: F field, $f \in F[x]$, $\deg f > 0$.
There exists a field extension $L \supseteq F$ in which f has a root, and $[L : F] \leq \deg f$.
Proof: Let $g \in F[x]$ be irreducible and $g \mid f$

$$\begin{array}{c} L = F[x]/(g) \\ | \\ F \end{array}$$

By the previous proposition, $[L : F] = \deg g \leq \deg f$ and if

$$a := x + (g) \in L$$

then $g(a) = 0$
$\implies f(a) = 0$.

Corollary: F field, $f \in F[x]$ monic, $\deg f = n > 0$. There exists a field extension $L \supseteq F$ such that

(i) $f = (x - a_1)(x - a_2) \cdots (x - a_n)$ in $L[x]$ where $a_1, \ldots, a_n \in L$

(ii) $[L : F] \leq n!$

Proof: Apply Kronecker's to f get $\begin{array}{c} L_1 \\ | \\ F \end{array}$ in which f has a root, say a_1. By factor theorem, $f = (x - a_1) f_1$ in $L_1[x]$

$$f_1 \in L_1[x] \qquad \deg f_1 = n - 1.$$

Iterate, $n - 1$ times to get

$$f = (x - a_1)(x - a_2) \cdots (x - a_{n-1}) f_{n-1}$$

where $a_i \in L_i,\ f_{n-1} \in L_{n-1}[x]$

$$\begin{array}{r@{}l} & L_{n-1} \\ & \ \vdots \\ {\scriptstyle n-1}\,\{ & L_2 \\ & \ | \\ {\scriptstyle n}\,\{ & L_1 \\ & \ | \\ & F \end{array}$$

$\implies \deg f_{n-1} = 1$ and monic
$\implies f_{n-1} = (x - a_n)$ for some $a_n \in L_{n-1}$

$$[L_{i+1} : L_i] \leq \deg f_i = n - i$$

$L \coloneqq L_{n-1}$ then $[L : F] = n!$ and L works.

Definition: F field, $f \in F[x]$, $\deg f > 0$, a *splitting field of f over F* is a minimal field extension $L \supseteq F$ over which $f = c(x - a_1)(x - a_2)\cdots(x - a_n)$, $c, a_1, \ldots, a_n \in L$
(i.e., f factors into a product of linear polynomials.)

Example:

(i) Suppose $L \supseteq F$ and in $L[x]$, $f = c(x - a_1)\cdots(x - a_n)$ then $F(a_1, \ldots, a_n)$ is a splitting field

(ii) If $L \supseteq F$ is the splitting field of f over F then, $L = F(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in L$ are the roots of f.

Note:

- The roots may *repeat*
- As $L[x]$ is a ufd, this factorization is unique

Definition: $f \in F[x]$ has *repeated roots* if in some extension $L \supseteq F$, $f = (x - a)^2 g$ for some $a \in L$, $g \in L[x]$.
Example: f has repeated roots if and only if it has a repeated root in a splitting field.
Theorem: F field, $f \in F[x]$, $\deg f > 0$.
f has repeated roots if and only if $\gcd(f, f') = 1$[83] where f' is the *formal derivative* of f with respect to x. So

$$f = a_0 + a_1 x + \cdots + a_n x^n \qquad n = \deg f$$
$$f' \coloneqq a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1} \qquad \text{in } L[x]$$

Remark: A natural choice of representatives of association classes of primes in $F[x]$ is the set of monic irreducible polynomials: $\mathcal{P}$.
Proof: Let L be a splitting field for f over F.
If $f = (x - a)^2 g$, $g \in L[x]$, $a \in g$
then $f' = 2(x - a)g + (x - a)^2 g' \to$ exercise
$f'(a) = 0$ also.
Let $I = (f, f')$ in $F[x]$.
Since $f(a) = f'(a) = 0$[84] $\implies$ for all $h \in I$, $h(a) = 0$[85] $\implies 1 \notin I \implies I \subsetneq L[x]$.
$F[x]$ is a pid $\implies I = (h)$ for some nonzero *nonunit* h.
$f, f' \in (h)$
$\implies h \mid f$ and $h \mid f'$

---

[83] in $F[x]$
[84] in L
[85] in L

$\implies \gcd(f, f') \neq 1$
Conversely, suppose $a_1, \dots, a_n \in L$, roots of f, are all distinct

$$\begin{aligned} f &= c(x-a_1)(x-a_2)\cdots(x-a_n) \qquad \text{in } L[x] \\ f' &= \sum_{i=1}^{n} \frac{f}{(x-a_i)} \\ &= c\big((x-a_2)(x-a_3)\cdots(x-a_n) + (x-a_1)(x-a_3)\cdots(x-a_n) + \cdots (x-a_1)\cdots(x-a_{n-1})\big) \end{aligned}$$

Since $a_i \neq a_j$ for all $i \neq j$,

$$f'(a_i) \neq 0 \qquad \text{for any} \qquad i = 1, \dots, n.$$

In fact, $f' \neq 0$.
$\gcd(f, f') = ?$
Suppose $g \mid f$ and $g \mid f'$.
$g \in F[x]$, g not a unit
$g \in L[x]$, and $\deg g > 0$

$$\begin{array}{c} L' \\ | \\ L \\ | \\ F \end{array}$$

there is $L' \supseteq L$ with a roots of g in L', say b.
$\implies f(b) = 0 = f'(b)$
But $f(b) = 0 \implies b = a_i$ for some $i = 1, \dots, n$.
Contradiction: $f'(a_i) \neq 0$ for any $i = 1, \dots, n$.

PMATH 345 Lecture 29: November 23, 2009

Definition: F field, $f \in F[x]$ irreducible is *separable* if it has no repeated roots.
Corollary: $f \in F[x]$ irreducible, f separable $\iff f' \neq 0$
Proof: f separable $\implies f' \neq 0$ by the previous theorem
(in fact we showed $f'(a) \neq 0$ for any root a of f in a splitting field of f.)
Suppose $f' \neq 0$ and f has repeated roots.
$\overset{\text{thm}}{\implies} \gcd(f, f') \neq 1$. Since f is irreducible, the prime factorization of f is $f = cg$ where $c \in F \setminus \{0\}$, $g \in F[x]$ monic irreducible
$\gcd(f, f') \neq 1 \implies g \mid f' \implies f \mid f'$. But $\deg f' \leq \deg f - 1 < \deg f$.
Corollary: $\operatorname{char}(F) = 0$, $f \in F[x]$ irreducible, then f is separable.
Proof: $f = a_0 + a_1 x + \cdots + a_n x^n$, $n = \deg f$, $a_n \neq 0$, $n > 0$
$f' = a_1 + 2a_2 + \cdots + n a_n^{n-1}$
$n \neq 0$ in F since $\mathbb{Z}$ embeds in F
(i.e., $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \neq 0$ in F, $na_n = (1 + \cdots + 1)a_n$)
$\implies na_n \neq 0 \implies f' \neq 0$.
Example: $\mathbb{Z}_2$, t indeterminant

$$\begin{array}{c} L = \mathbb{Z}_2(t) \\ | \\ F = \mathbb{Z}_2(t^2) \end{array}$$

$f \in F[x]$
$f = -t^2 + x^2$
Since $t \notin F$ it's not hard to check that t^2 is prime in F. Apply Eisenstein $\implies f$ is irreducible $F[x]$

In L,

$$\begin{aligned} f = x^2 - t^2 &= (x-t)(x+t) \\ &= (x-t)^2 \qquad \text{since } 1 = -1 \text{ in } L \end{aligned}$$

$\implies$ f *not* separable.
Note:

- $f' = 2x = 0$ in F
- f = minimal polynomial of f over F

10. Finite fields
F finite field
$\implies \mathbb{Q} \subsetneq F$
$\implies \operatorname{char}(F) \neq 0$
$\implies \operatorname{char}(F) = p$, p prime
$\mathbb{Z}_p \subseteq F$
Since F is finite $\implies [F : \mathbb{Z}_p] \in \mathbb{N}$
$\implies$ F is an algebraic extension of $\mathbb{Z}_p$
F finite dimensional over $\mathbb{Z}_p$, say $\dim = n$
$\implies$ As vector spaces $F \approx (\mathbb{Z}_p)^n$
$\implies |F| = p^n$
Proposition: F finite field then $\operatorname{char}(F) = p$, p a prime
F is a finite extension of $\mathbb{Z}_p$, and cardinality of F is a power of p.

Suppose $|F| = p^n = q$.
If $a \in F \setminus \{0\}$,

$$\{1, a, a^2, \ldots, a^{q-1}\} \subseteq F \setminus \{0\}$$

$\implies a^i = a^j$ for some $0 \leq i < j \leq q-1$.
$\implies a^{j-i} = 1$, $0 < j - i < q$

Definition: F finite field, $a \in F \setminus \{0\}$
The *order of* a, $o(a)$, is the least positive integer m such that $a^m = 1$.

$\rightarrow$ Always exists by previous remarks, and $o(a) \leq q - 1$

$$q = p^n = |F|$$

Lemma: $|F| = p^n = q$. $a, b \in F \setminus \{0\}$, $k > 0$

(a) $a^k = 1 \implies o(a) \mid k$

(b) $o(a^k) = \frac{o(a)}{\gcd(k, o(a))}$

(c) *If* $\gcd(o(a), o(b)) = 1$ then $o(ab) = o(a) \cdot o(b)$.

Proof:

(a) $k = qo(a) + r$, $0 \leq r < o(a)$

$$1 = a^k = (a^{o(a)})^q \cdot a^r = a^r$$

$\implies r = 0$ ✓

(b) $d = \gcd(k, o(a))$

$$(a^k)^{o(a)/d} = a^{ko(a)/d} = (a^{o(a)})^{k/d} = 1$$

$\overset{\text{(a)}}{\implies} o(a^k) \mid \frac{o(a)}{d}$
On the other hand,

$$a^{k \cdot o(a^k)} = (a^k)^{o(a^k)} = 1$$

$\underset{(a)}{\Longrightarrow} o(a) \mid k \cdot o(a^k)$
$\Longrightarrow \frac{o(a)}{d} \mid \frac{k}{d} \cdot o(a^k)$
since $\gcd(\frac{o(a)}{d}, \frac{k}{d}) = 1$
$\Longrightarrow \frac{o(a)}{d} \mid o(a^k)$
Therefore $o(a^k) = \frac{o(a)}{d}$

(c)

$$\begin{aligned}(ab)^{o(a)\cdot o(b)} &= a^{o(a)\cdot o(b)} \cdot b^{o(a)\cdot o(b)} \\ &= 1\end{aligned}$$

$\overset{(a)}{\Longrightarrow} o(ab) \mid o(a)o(b)$

$$\begin{aligned}a^{o(ab)\cdot o(b)} &= a^{o(ab)\cdot o(b)} \cdot b^{o(ab)\cdot o(b)} \\ &= (ab)^{o(ab)o(b)} = 1\end{aligned}$$

$\Longrightarrow o(a) \mid o(ab) \cdot o(b) \Longrightarrow o(a) \mid o(ab)$
Similarly $o(b) \mid o(ab)$.
Since $\gcd(o(a), o(b)) = 1$
Therefore $o(a)o(b) \mid o(ab)$
Therefore $o(ab) = o(a)o(b)$

Theorem: $|F| = p^n = q$

(a) There exists $a \in F \setminus \{0\}$ such that $o(a) = q - 1 = |F| - 1$.

(b) Every element of F is a root of $x^q - x \in F[x]$

Corollary: $a \in F \setminus \{0\} \Longrightarrow o(a) \mid q - 1$.
Proof: Theorem (b) $\Longrightarrow a^q = a \Longrightarrow a^{q-1} = 1$
$\overset{\text{Lemma (a)}}{\Longrightarrow} o(a) \mid q - 1$.
Definition: $a \in F$ is an *primitive element* if $o(a) = |F| - 1$
Remark: If a is primitive in F, then

$$\{1, a, a^2, \ldots, a^{q-2}\} = F \setminus \{0\} \qquad q = |F|$$

PMATH 345 Lecture 30: November 25, 2009

Theorem: $|F| = p^n = q$ field

(a) There exists: $a \in F \setminus \{0\}$, $o(a) = q - 1$

$\hookrightarrow$ a is called a *primitive element*

(b) Every element of F is a root of $x^q - x$

Remark: If $F = \mathbb{Z}_p$ then (b) is Fermat's little theorem
Proof: Since every element of $F \setminus \{0\}$ has finite order $\leq q - 1$ there exists $m > 0$ such that $u^m = 1$ for all $u \in F \setminus \{0\}$

$$\hookrightarrow \qquad m = \prod_{a \in F\setminus\{0\}} o(a)$$

Let N be *least* such $N \leq \prod_{a\in F\setminus\{0\}} o(a)$
But $x^N - 1$ has at most N roots in F, 0 is not such a root
$\Longrightarrow q - 1 \leq N$
Suppose $N = 1$
$\Longrightarrow F = \mathbb{Z}_2$

$\implies$ (a) is true with $a = 1$

(b) is true as $F = \{0, 1\}$

We may assume $N > 1$
$N = p_1^{k_1} \cdots p_l^{k_l}$ prime factorization

Claim: For any $j = 1, \dots, l$, there is an element $a_j \in F \setminus \{0\}$, $o(a_j) = p_j^{k_j}$
Proof: Fix j. $0 < \frac{N}{p_j} < N$
$\implies$ there is $b_j \in F \setminus \{0\}$

$$b_j^{N/p_j} \neq 1$$

let $a_j = b_j$

$$\begin{aligned} a_j^{p_j^{k_j}} &= b_j^{(N/p_j^{k_j}) p_j^{k_j}} = b_j^N = 1 \xrightarrow{\text{prev. prop}} o(a_j) \mid p_j^{k_j} \\ a_j^{p_j^{k_j-1}} &= b_j^{(N/p_j^{k_j}) p_j^{k_j-1}} = b_j^{N/p_j} \neq 1 \implies o(a_j) \nmid p_j^{k_j-1} \end{aligned}$$

Therefore $o(a_j) = p_j^{k_j}$: claim.

Since $o(a_i)$ is coprime with $o(a_j)$ for all $i \neq j$

$$\begin{aligned} \xrightarrow{\text{prev. prop (c)}} o(a_1 \cdots a_l) &= o(a_1) \cdots o(a_l) \\ &= p_1^{k_1} \cdots p_l^{k_l} = N \end{aligned}$$

Let $a = a_1 \cdots a_l$. $N = o(a) \leq q - 1$
Therefore $N = q - 1$ and a is a prime element.
By choice, $u^N = 1$ for all $u \in F \setminus \{0\}$.
$\implies$ u is a root of $x^N - 1 = x^{q-1} - 1$ for all $u \in F \setminus \{0\}$.
$\implies$ u is a root of $x^q - x$ for all $u \in F$.

Corollary: $f \in \mathbb{Z}_p[x]$ irreducible $\deg f = n$
$\implies$ $f \mid x^{p^n} - x$
Proof: Consider

$$\begin{array}{c} F := \mathbb{Z}_p[x]/(f) \\ | \\ \mathbb{Z}_p \end{array}$$

We know that $F = \mathbb{Z}_p(a)$ where $a := x + (f)$ and a is algebraic over $\mathbb{Z}_p$ and $f =$ minimal polynomial of a over $\mathbb{Z}_p$.
$\implies$ $[F : \mathbb{Z}_p] = n$
$\implies$ $|F| = p^n$
By Theorem (b) every element of F is a root of $x^{p^n} - x$.
$\implies$ $a^{p^n} - a = 0$
$\implies$ $f \mid x^{p^n} - x$

Proposition: $|F| = q = p^n$ field.
There are $\phi(q-1)$ primitive elements in F.

$\hookrightarrow$ ϕ Euler-phi function

Proof: Choose a primitive.

$$F \setminus \{0\} = \{1, a, a^2, \dots, a^{q-2}\}$$

We want to know how many of the a^ks are primitive. a^k primitive if and only if

$$o(a^k) = q - 1 \iff$$

$$\frac{o(a)}{\gcd(k, o(k))} = q - 1 \iff \frac{q-1}{\gcd(k, q-1)} = q - 1$$

$$\iff \gcd(k, q-1) = 1$$

By definition there are $\phi(q-1)$ many such $k < q-1$.

Proposition: Every finite field is a simple algebraic extension of its prime subfield. That is, $F = \mathbb{Z}_p(a)$ where $a \in F$ is algebraic.
Proof: Let $a \in F$ be primitive.

$$\begin{aligned} F &= \{\overset{0}{0}, \overset{1}{1}, \overset{x}{a}, \overset{x^2}{a^2}, \ldots, \overset{x^{q-2}}{a^{q-2}}\} \qquad q = |F| \\ &\implies F \subseteq \mathbb{Z}_p(a) \implies F = \mathbb{Z}_p(a) \end{aligned}$$

Theorem: Let p be a prime, $n > 0$.

(a) There exists a field of size p^n.

(b) Any two fields of size p^n are isomorphic

Proof: $f = x^{p^n} - x \in \mathbb{Z}_p[x]$.

Let $\begin{matrix} L \\ | \\ \mathbb{Z}_p \end{matrix}$ be a splitting field of f over $\mathbb{Z}_p$.

Let $F \subseteq L$ be the *set of roots* of f in L.
Since $f' = p^n x^{p^n - 1} = -1$
$\gcd(f, f') = 1$
$\implies$ f has no repeated roots in L
$\implies |F| = p^n$

We show F is a subfield of L

- $0^{p^n} - 0 = 0 \implies 0 \in F$
- $1^{p^n} - 1 = 0 \implies 1 \in F$
- $$\begin{aligned} (-1)^{p^n} &= \begin{cases} 1 & \text{if } p = 2 \\ -1 & \text{otherwise} \end{cases} \\ &= -1 \implies -1 \in F \end{aligned}$$
- $a, b \in F \implies (ab)^{p^n} = a^{p^n} b^{p^n} = ab \implies ab \in F$
- $a \in F \implies -a = (-1)a \in F$
- $a, b \in F \implies (a+b)^{p^n} = a^{p^n} + b^{p^n} + \binom{p^n}{1} a^{p^n - 1} b + \cdots$
  since $\mathrm{char}(L) = p$
  all the other binomial coefficients being divisible by p are equal to 0.
  $\implies (a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$
  $\implies a + b \in F$
- $a \in F \setminus \{0\} \implies \exists b \in L, b = a^{-1}$

$$\begin{aligned} ab &= 1 \\ (ab)^{p^n} &= 1 \\ a^{p^n} b^{p^n} &= 1 \end{aligned}$$

$\implies b^{p^n} = (a^{p^n})^{-1} = a^{-1} = b \implies b \in F.$

This proves part (a).

PMATH 345 Lecture 31: November 27, 2009

Theorem: p prime, $n > 0$.

(a) There exists a field of size p^n.

(b) Any two fields are isomorphic.

Proof (b): $x^{p^n} - x \in \mathbb{Z}_p[x]$

$$\begin{array}{l} L = \text{splitting field of } x^{p^n} - x \\ | \\ \mathbb{Z}_p \end{array}$$

$$F = \left\{ a \in L : a^{p^n} = a \right\} = \text{roots of } x^{p^n} - x \text{ in } L$$

We proved:

- F is a subfield of L
- $|F| = p^n$

We show that if K a field, $|K| = p^n$ then $K \simeq F$. We know $K = \mathbb{Z}_p(a)$ for some $a \in K$,

$$\deg(a/\mathbb{Z}_p) = n$$

$$\text{So } K \simeq \mathbb{Z}_p[x]/(g)$$

where $g =$ minimal polynomial of $a/\mathbb{Z}_p$.
We show $\mathbb{Z}_p[x]/(g) \simeq F$.
g is irreducible of degree n in $\mathbb{Z}_p[x]$

$$\implies g \mid x^{p^n - x} \qquad \text{previous corollary}$$

Hence g has a root in L, say $b \in L$.
$\implies b^{p^n} = b \implies b \in F$.

$$\begin{aligned} \phi \colon \mathbb{Z}_p[x] &\to F \\ h &\mapsto h(b) \end{aligned}$$

evaluation at b ring homomorphism.
Since $g(b) = 0 \implies g \in \ker(\phi)$
g irreducible, $\mathbb{Z}_p[x]$ pid $\implies (g)$ is maximal
$\implies (g) = \ker(\phi)$
1st isomorphism theorem $\implies \mathbb{Z}_p[x]/(g)$ is isomorphism to a subfield of F.
Both of size $p^n \implies$ this subfield is all of F.
Therefore $K \simeq \mathbb{Z}_p[x]/(g) \simeq F$.

Definition: $\mathbb{F}_{p^n}$ is the unique (up to isomorphism) field of size p^n.

$\rightarrow \mathbb{F}_p = \mathbb{Z}_p$

Corollary: p prime, $n > 0$

(a) There exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$

(b) Given $g, h \in \mathbb{Z}_p[x]$ irreducible of degree n, then

$$\mathbb{Z}_p[x]/(g) \simeq \mathbb{Z}_p[x]/(n).$$

Proof: $\mathbb{F}_{p^n}$ is a simple algebraic extension of $\mathbb{Z}_p$ of degree n.
$\implies \mathbb{F}_{p^n} = \mathbb{Z}_p(a) \simeq \mathbb{Z}_p[x]/(g)$ where $g =$ minimal polynomial of a over $\mathbb{Z}_p$
$\implies g$ is irreducible, $\deg g = n$.

(b) Follows by previous theorem part (b) as both $\mathbb{Z}_p/(g)$ and $\mathbb{Z}_p/(h)$ are degree n extensions of $\mathbb{Z}_p$ and hence of size p^n.

$$\begin{tikzcd}[column sep=small]
\mathbb{F}_{p^2} \arrow[dr, dash] & \mathbb{F}_{p^3} \arrow[d, dash] & \mathbb{F}_{p^4} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
& \mathbb{F}_p & &
\end{tikzcd}$$

Theorem: p prime, $m > 0$, $n > 0$

$\mathbb{F}_{p^2} \not\subseteq \mathbb{F}_{p^3}$ but $\mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^4}$

$$\mathbb{F}_{p^m} \subseteq^{86)} \mathbb{F}_{p^n} \iff m \mid n$$

Proof: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$
$\mathbb{F}_{p^n}$ is an $\mathbb{F}_{p^m}$-vector space of finite dimensional, say dimension d.

$$\mathbb{F}_{p^n} \simeq (\mathbb{F}_{p^m})^d$$

$$|\mathbb{F}_{p^n}| = |(\mathbb{F}_{p^m})^d|$$
$$p^n = (p^m)^d = p^{md}$$
$$\implies n = md \implies m \mid n \quad \checkmark$$

Conversely suppose $m \mid n$.
say $n = md$
L is splitting field of $x^{p^m} - x$ over $\mathbb{F}_{p^n}$
$x^{p^m} - x \in \mathbb{F}_{p^n}[x]$ Let $a \in F$, $a^{p^m} = a$

$$\begin{tikzcd}
L \arrow[d, dash] \\
\mathbb{F}_{p^n}
\end{tikzcd}$$

$$\begin{aligned}
a^{p^n} &= a^{(p^m)^d} \\
&= \left(\cdots\left(\left(a^{p^m}\right)^{p^m}\right)^{p^m}\cdots\right)^{p^m} {}^{87)} \\
&= a
\end{aligned}$$

$\implies$ a is a root of $x^{p^n} - x$.
But $\mathbb{F}_{p^n} \subseteq L$ is the set of *all* roots of $x^{p^n} - x$ since they are roots and there are p^n.
Therefore $a \in \mathbb{F}_{p^n}$
Therefore $F^{88)} \subseteq \mathbb{F}_{p^n}$
Remark: p prime $n > 0$,

$$\mathbb{F}_{p^n} = \text{splitting field of } x^{p^n} - x \text{ over } \mathbb{Z}_p$$

PMATH 345 Lecture 32: November 30, 2009

Addendum to §9: Fields
Notation: $\alpha\colon R \to R'$ isomorphism of rings induces an isomorphism

$$\begin{aligned}
\alpha\colon R[x] &\to R'[x] \\
a_0 + \cdots + a_n x^n &\mapsto \alpha(a_0) + \alpha(a_1)x + \cdots + \alpha(a_n)x^n
\end{aligned}$$

Lemma: $\alpha\colon F \to F'$ isomorphism of fields,
two simple algebraic extensions

$$\begin{tikzcd}
F(a) \arrow[r, dotted, "\beta"] \arrow[d, dash] & F'(b) \arrow[d, dash] \\
F \arrow[r, "\alpha", "\simeq"'] & F'
\end{tikzcd}$$

[86] actually: $\mathbb{F}_{p^m}$ embeds in $\mathbb{F}_{p^n}$
[87] d times
[88] $\simeq \mathbb{F}_{p^m}$

with f = minimal polynomial of a over $F \in F[x]$, such that
$\alpha(f)$ = minimal polynomial of b over $F' \in F'[x]$.
(i.e., α takes minimal polynomial of a/F to minimal polynomial of b/F')
Then, α extends to an isomorphism

$$\beta\colon F(a) \to F'(b)$$

with $\beta(a) = b$.
That is:

- $\beta|_F = \alpha$
- $\beta(a) = b$

Example: converse is also true
Proof: Let $f' = \alpha(f)$ = minimal polynomial of b over F'

$$\begin{tikzcd} F[x] \arrow[r, "\alpha", "\simeq"'] \arrow[d, dash] & F'[x] \arrow[d, dash] \\ F \arrow[r, "\alpha", "\simeq"'] & F' \end{tikzcd}$$

α is an isomorphism

$$\alpha^{-1}(f' \cdot F'[x]) = f \cdot F[x]$$

Then α induces

$$\begin{aligned} \overline{\alpha}\colon f[x]/(f) &\overset{\simeq}{\to} F'[x]/(f') \\ h + (f) &\mapsto \alpha(h) + (f') \end{aligned}$$

check that $\overline{\alpha}$ is indeed an isomorphism.

$$\begin{tikzcd} F(a) & F[x]/(f) \arrow[l, "\simeq"', "\phi"] \arrow[r, "\simeq", "\overline{\alpha}"'] & F'[x]/(f') \arrow[r, "\simeq", "\phi'"'] & F'(b) \arrow[from=1-1, to=1-4, bend left, "\beta"] \end{tikzcd}$$

$$h(a) \longleftarrow\!\shortmid\; h + (f) \qquad\qquad h' + (f') \longmapsto h'(b)$$

$$\beta \coloneqq \phi' \circ \overline{\alpha} \circ \phi^{-1}\colon F(a) \to F'(b)$$

is an isomorphism.
Given $c \in F$,

$$\begin{aligned} \beta(c) &= \phi' \circ \overline{\alpha} \circ \phi^{-1}(c) \\ &= \phi' \circ \overline{\alpha}(c + (f)) \\ &= \phi'(\alpha(c) + (f')) \qquad \alpha(c) \in F' \\ &= \alpha(c) \end{aligned}$$

Therefore $\beta|_F = \alpha$.

$$\begin{aligned} \beta(a) &= \phi' \circ \overline{\alpha} \circ \phi^{-1}(a) \\ &= \phi' \circ \overline{\alpha}(x + (f)) \\ &= \phi'(x + (f')) \\ &= b \end{aligned}$$

Proposition: $\alpha\colon F \to F'$ isomorphism
$f \in F[x]$, $\deg f > 0$.

Let K be a splitting field of f over F
Let K' be a splitting filed of $\alpha(f)$ over F'

$$\begin{tikzcd}
K \arrow[r, dotted, "\beta"] \arrow[d, dash] & K' \arrow[d, dash] \\
F \arrow[r, "\alpha", "\simeq"'] & F'
\end{tikzcd}
\qquad f' = \alpha(f)$$

Then α extends to an isomorphism $\beta\colon K \to K'$.
So $\beta|_F = \alpha$.
Remark: When $F = F'$ and $\alpha = \text{id}$ this proposition says that any two splitting fields of f over F are *isomorphic over* F.
That is, $\beta|_F = \text{id}$.

$$\begin{tikzcd}
K \arrow[rr, dotted] \arrow[dr, dash] & & K' \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

(**Definition:** S and S' extensions of a ring R, are *isomorphic over* R if there is an isomorphism $\beta\colon S \to S'$ such that $\beta|_R = \text{id}$.)
Proof: Induction on $[K : F] = n$.
$n = 1$: $K = F \implies f$ factors completely into linear factors in $F[x]$
$\implies \alpha(f)$ factors into linear factors in $F'[x]$
$\implies K' = F'$
So $\beta = \alpha$ works. ✓
$n > 1$: f must have an irreducible factor $g \in F[x]$ which is *not* linear. $\implies \deg g > 1$
Let $a \in K$ be a root of g.
(exists since $g \mid f$ and $K =$ splitting field of f over F)
Let $g' = \alpha(g) \in F'[x]$.
So $g' \mid \alpha(f) \implies g'$ has a root $b \in K'$.

$$\begin{tikzcd}
K \arrow[r, dotted, "\beta"] \arrow[d, dash] & K' \arrow[d, dash] \\
F(a) \arrow[r, "\beta"] \arrow[d, dash, "\text{minimal polynomial is } g"'] & F'(b) \arrow[d, dash, "\text{minimal polynomial } g' = \alpha(g)"] \\
F \arrow[r, "\alpha", "\simeq"'] & F'
\end{tikzcd}$$

Lemma $\implies$ Can extend α to an isomorphism $\beta\colon F(a) \to F'(b)$ which extends α
But K is still the splitting field of f over $F(a)$
And K' is a splitting field of $\alpha(f)$ over $F'(b)$. Note $\beta(f) = \alpha(f)$

$$[K : F(a)] = \frac{n}{\deg g} < n$$

By Induction Hypothesis β extends to a $\hat{\beta}\colon K \to K'$.

$$\hat{\beta}|_F = \beta|_F = \alpha$$

So $\hat{\beta}$ works.

§10:
Corollary: K, L finite fields, $|K| = |L| = p^n$.

Suppose K, L are both extensions of a finite field F.

$$\begin{tikzcd}
K \arrow[rr, dotted, "\simeq"] \arrow[dr, dash] & & L \arrow[dl, dash] \\
& F \arrow[d, dash] & \\
& \mathbb{Z}_p &
\end{tikzcd}$$

Then K and L are isomorphic over F.
Proof: K and L are both splitting fields of $x^{p^n} - x$ over $\mathbb{Z}_p$, hence also over F.
Apply proposition (in fact the Remark).

PMATH 345 Lecture 33: December 2, 2009

§11 Algebraically Closed Fields
Definition: F field is *algebraically closed* if every polynomial $f \in F[x]$ of $\deg f > 0$ has a root in F.
If $F \subseteq L$, L is an *algebraic closure of* F if L is an *algebraic extension of* F and L is *algebraically closed.*

Proposition: The following are equivalent: F field

(i) F is closed.

(ii) In $F[x]$ every irreducible polynomial is of degree 1.

(iii) F has no proper algebraic extensions.

Proof (i) $\implies$ (ii):
$f \in F[x]$ irreducible
$a \in F$, $f(a) = 0$
$\implies (x - a) \mid f$
f irreducible $\implies f = c(x - a)$, since $c \in F$
(ii) $\implies$ (iii):
Suppose $L \supseteq F$ is an algebraic extension, $a \in L$. $f =$ minimal polynomial of $a/F \in F[x]$
$\overset{(ii)}{\implies} \deg f = 1$ But $[F(a) : F] = \deg f$
$\implies a \in F \implies L = F$
(iii) $\implies$ (i):
To show F is algebraically closed it suffices to show that every irreducible polynomial over F has a root in F.
$f \in F[x]$ irreducible

$$\begin{tikzcd}
L = F[x]/(f) \arrow[d, dash, "\text{algebraic extension, } {[L : F] = \deg f}"] \\
F
\end{tikzcd}$$

(iii) $\implies L = F \implies \deg f = 1$
$f = a$[89]$x + b$ so $b/a \in F$ is a root of f.

Examples:

(a) $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra
Since $[\mathbb{C} : \mathbb{R}] = 2$
$\implies \mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

(b) Let $\overline{\mathbb{Q}} = \{\, a \in \mathbb{C} : a \text{ is } \mathbb{Q}\text{-algebraic} \,\}$

[89] $a \neq 0$

Exercise: $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.
point: $a,\, b \in \overline{\mathbb{Q}}$,

$$\begin{tikzcd}
 & \mathbb{Q}(a,b) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q} \arrow[rr, dash, "\text{alg.}"] & & \mathbb{Q}(a)
\end{tikzcd}$$

Claim: $\overline{\mathbb{Q}}$ algebraically closed
Proof: $f \in \overline{\mathbb{Q}}[x] \subseteq \mathbb{C}[x]$, $\deg f > 0$.
$\implies a \in \mathbb{C},\ f(a) = 0$.
$\implies a$ is $\overline{\mathbb{Q}}$-algebraic

$$\left.\begin{array}{c} \overline{\mathbb{Q}}(a) \\ \big|\ \text{alg} \\ \overline{\mathbb{Q}} \\ \big|\ \text{alg} \\ \mathbb{Q} \end{array}\right\}\text{alg} \qquad \begin{array}{l} \implies a \text{ is } \mathbb{Q}\text{-algebraic} \\ \quad\implies a \in \overline{\mathbb{Q}} \end{array}$$

$\overline{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$.

(c)

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq^{90)} \mathbb{F}_{p^6} \subseteq \cdots \subseteq \mathbb{F}_{p^{n!}} \subseteq^{91)} \mathbb{F}_{p^{(n+1)!}} \subseteq \cdots \subseteq L$$

$$L = \bigcup_n \mathbb{F}_{p^{n!}}$$

Example: L is a field as $n \mid n!$, every $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{n!}} \subseteq L$
Therefore every finite field of characteristic p is a subfield of L.
Claim: L *is algebraically closed* and an algebraic closure of $\mathbb{Z}_p$
Proof: $f \in L[x]$, $\deg f > 0$, irreducible
For some $n > 0$, $f \in \mathbb{F}_{p^{n!}}[x]$ irreducible
Hence $K = \mathbb{F}_{p^{n!}}[x]/(f)$ is a finite field, extending $\mathbb{F}_{p^{n!}}$, say $|K| = p^N$ with $n! \mid N$

$$\begin{tikzcd}
\mathbb{F}_{p^{n!}}[x]/(f) = K \arrow[rr, dash, "\alpha", "\simeq"'] \arrow[dr, dash, "\deg f"'] & & \mathbb{F}_{p^N} \arrow[dl, dash] \\
 & \mathbb{F}_{p^{n!}} &
\end{tikzcd} \qquad \alpha|_{\mathbb{F}_{p^{n!}}} = \mathrm{id}$$

f has a root in K, namely $a = x + (f)$
$\implies \alpha(f)$[92] has a root in $\mathbb{F}_{p^N} \subseteq L$.

Theorem: F field

(a) F has an algebraic closure

(b) Any two algebraic closures of F are isomorphic over F.

Proof:

(a) Let $\mathcal{P}$ be the set of all algebraic extensions of F. Given $K,\, L \in \mathcal{P}$,

$$K \leq L \overset{\text{def}}{\iff} K \text{ is a subfield of } L$$

Then $(\mathcal{P}, \leq)$ is a partially ordered set
Claim: Every chain in $(\mathcal{P}, \leq)$ is bounded.

[90] $2 \mid 6$
[91] $n! \mid (n+1)!$
[92] $= f$

Proof: $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$
all algebraic extensions of F.
Let $L = \bigcup_i K_i$ a field extending F.
Given $a \in L \implies a \in K_i$ for some i
$\implies a$ is F-algebraic.
$\implies L \in \mathcal{P}$ and each $K_i \subseteq L$ ⊣ claim.
By Zorn's Lemma, $\mathcal{P}$ has a maximal element, $L \in \mathcal{P}$.
By maximality, L has no proper algebraic extension, since any such would be in $\mathcal{P}$.
Therefore L is algebraically closed and algebraic over F.

(b)

$$\begin{tikzcd}[column sep=small]
L \arrow[dr, no head] & & L' \arrow[dl, no head] \\
& F &
\end{tikzcd} \qquad \text{algebraic closures of } f$$

$$\mathcal{P} = \left\{ (K, K', \alpha) : \begin{array}{r} F \subseteq K \subseteq L \text{ intermediate field extension} \\ F \subseteq K' \subseteq L' \text{ intermediate field extension} \\ \alpha\colon K \to K' \text{ is an isomorphism over } F \end{array} \right\}$$

$\mathcal{P} \neq \emptyset$ since $(F, F, \mathrm{id}) \in \mathcal{P}$
$(K, K', \alpha) \leq (M, M', \beta)$ in $\mathcal{P}$
if $K \subseteq M$, $K' \subseteq M'$

$$\text{such that} \qquad \begin{tikzcd}[column sep=small]
M \arrow[rr, no head, "\beta"] \arrow[d, no head] & & M' \arrow[d, no head] \\
K \arrow[rr, no head, "\alpha"] \arrow[dr, no head] & & K' \arrow[dl, no head] \\
& F &
\end{tikzcd} \qquad \beta_K = \alpha$$

Example: Check $(\mathcal{P}, \leq)$ is a partially ordered set.
Claim 1: Every chain is bounded in $\mathcal{P}$.
Proof: Take "unions". Exercise. ⊣ Claim 1.
Apply Zorn's Lemma $\implies$ There exists $(k, k', \alpha) \in \mathcal{P}$ which is maximal.
Claim 2: $K = L$.
Proof sketch: $a \in L$

$$f = \text{minimal polynomial of } a/K \in K[x]$$

$$\begin{tikzcd}[column sep=small]
L \arrow[d, no head] & & L' \arrow[d, no head] \\
K(a) \arrow[rr, no head, "\simeq", "\beta"'] \arrow[d, no head] & & K(b) \arrow[d, no head] \\
K \arrow[rr, no head, "\simeq", "\alpha"'] \arrow[dr, no head] & & K' \arrow[dl, no head] \\
& F &
\end{tikzcd}$$

Let $f' = \alpha(f) \in K'[x] \subseteq L'[x]$
As L' is algebraically closed, there is $b \in L'$, $f'(b) = 0$.
$f' =$ minimal polynomial at b over K'

since f' is monic and irreducible
By Lemma last time there is $\beta\colon K(a) \to K(b)$ extending α.

$$(K, K', \alpha) \le (K(a), K'(b), \beta) \text{ in } \mathcal{P}$$

$\implies K(a) = K \implies a \in K$. $\dashv$ Claim.
Example: $K' = L'$
point:

$$K \subseteq \alpha(L)^{93)94)} \subseteq L'$$

PMATH 345 Lecture 34: December 4, 2009

Classical algebraic geometry is the study of simultaneous solutions to systems of polynomial equations.

K algebraically closed field.
$S \subseteq K[x_1, \ldots, x_n]$ a set of polynomials

$$V(S) = \{\, (a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \text{ for } \textit{all } f \in S \,\}$$

affine variety in K^n defined by S

Note: $V(S) = V(S \cdot K[x_1, \ldots, x_n])$ where

$$\begin{aligned} S \cdot K[x_1, \ldots, x_n] &= \text{ideal generated by } S \\ &= \{\, g_1 f_1 + \cdots + g_l f_l : f_1, \ldots, f_l \in S,\, g_1, \ldots, g_l \in K[x_1, \ldots, x_n] \,\} \end{aligned}$$

Therefore all affine varieties are of the form $V(I)$.

Hilbert's Basis Theorem:
R commutative Noetharian ring $\implies R[x]$ is also.

Hence $K[x_1, \ldots, x_n]$ is Noetharian.
$\implies$ every ideal in $K[x_1, \ldots, x_n]$ is finitely generated.

$$\begin{aligned} \text{Therefore } V(S) &= V(S \cdot K[x_1, \ldots, x_n]) \\ &= V(f_1, \ldots, f_l) \end{aligned}$$

where $S \cdot K[x_1, \ldots, x_n] = (f_1, \ldots, f_l)$.
Every affine variety is defined by a finite set of polynomials.

Definition: Given any subset $X \subseteq K^n$

$$I(X) = \{\, f \in K[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, x_n) \in X \,\}$$

This is an ideal, the *ideal of* X.

Remarks: $S, T \subseteq K[x_1, \ldots, x_n] \quad X, Y \subseteq K^n$

(a) $S \subseteq T \implies V(T) \subseteq V(S)$
$X \subseteq Y \implies I(Y) \subseteq T(X)$

(b) $S \subseteq I(V(S))$
$X \subseteq V(I(X))$

(c) $V(S) = V(I(V(S)))$
$I(X) = I(V(I(X)))$

$\to$ exercise

93) a is algebraically closed
94) $= K'$

Hilbert's Nullstellensatz
If $S \cdot K[x_1, \ldots, x_n]$ is a *proper* ideal then $V(S) \neq \emptyset$.

case $n = 1$: $K[x]$ is a pid.
$S \cdot K[x] = (f) \quad f$ if not a *unit* in $K[x]$ since the ideal is proper.
$\implies V(S) = V(f)$

$$\implies \begin{array}{c} f = 0 \implies V(S) = K \\ \text{or} \\ \deg f > 0 \implies \text{since } K \ \textit{algebraically closed} \end{array}$$

f has a root, $a \in K$
$\implies a \in V(S)$.
Note $V(K[x_1, \ldots, x_n]) = \emptyset$

Is $J = I(V(J))$ for all ideals J?
No.
$f \in K[x_1, \ldots, x_n] \quad J = (f^2)$
f^2 vanishes on $V(J)$
$\implies f$ vanishes on $V(J)$
$\implies f \in I(V(J)) \setminus J$
This is the only problem:
Theorem: If J is an ideal in $K[x_1, \ldots, x_n]$, then

$$\begin{aligned} I(V(J)) &= \{\, f \in K[x_1, \ldots, x_n] : f^n \in J \text{ for some } n > 0 \,\} \\ &= \operatorname{Rad} J \end{aligned}$$

Proof: $\supseteq$ is clear.

$$\begin{aligned} f^n \in J &\implies f^n \text{ vanishes on } V(J) \\ &\implies f \text{ vanishes on } V(J) \\ &\implies f \in I(V(J)) \end{aligned}$$

Conversely, $f \in I(V(J))$
Want: $f \in \operatorname{Rad} J$
We may assume $f \neq 0$
HBT $\implies J = (f_1, \ldots, f_l)$
Consider $K[x_1, \ldots, x_n, y]$

$$J' = (f_1, \ldots, f_l, y \cdot f - 1)$$

Suppose $(a_1, \ldots, a_{n+1}) \in V(J')$
$\implies (a_1, \ldots, a_n \in V(J))$

$$\begin{aligned} 0 &= (y \cdot f - 1)(a_1, \ldots, a_{n+1}) \\ &= a_{n+1} \cdot \underbrace{f(a_1, \ldots, a_n)}_{=0 \text{ since } (a_1, \ldots, a_n) \in V(J)} - 1 \\ &= -1 \end{aligned}$$

Contradiction; therefore $V(J') = \emptyset$
HN $\implies J' = K[x_1, \ldots, x_n, y]$

$$1 = g_1 f_1 + \cdots + g_l f_l + h(yf - 1) \text{ where } g_1, \ldots, g_l, h \in K[x_1, \ldots, x_n, y] \qquad (*)$$

$$\begin{gathered} K[x_1, \ldots, x_n, y] \xrightarrow{\phi} K(x_1, \ldots, x_n) \\ g \mapsto g(x_1, \ldots, x_n, 1/f) \end{gathered}$$

Apply ϕ to both sides of $(*)$

$$1 = g_1(x_1, \ldots, x_n, 1/f) f_1 + \cdots + g_l(x_1, \ldots, x_n, 1/f) f_l + h(x_1, \ldots, x_n, 1/f) \cdot 0$$

$$\implies 1 = g_1(x_1, \ldots, x_n, 1/f) f_1 + \cdots + g_l(x_1, \ldots, x_n, 1/f) f_l$$

in $K(x_1, \ldots, x_n)$
clear denominators to get $N > 0$, such that

$$f^N = \overbrace{f^N g_1(x_1, \ldots, x_n, 1/f)}^{95)} f_1 + \cdots + f^N g_l(x_1, \ldots, x_n, 1/f)^{96)} f_l$$

in $K[x_1, \ldots, x_n]$
each $f^N g_i(x_1, \ldots, x_n, 1/f) \in K[x_1, \ldots, x_n]$
$\implies f^N \in (f_1, \ldots, f_l) = J$
$\implies f \in \operatorname{Rad} J$

An ideal J is *radical* if $J = \operatorname{Rad} J$.

We get a 1–1, onto correspondence

$$\begin{gathered} \text{Radical ideals in } K[x_1, \ldots, x_n] \longleftrightarrow \text{affine varieties in } K^n \\ J \longmapsto V(J) \\ I(W) \longleftarrow W \end{gathered}$$

$\rightarrow$ exercises

[95] in $K[x_1, \ldots, x_n]$
[96] in $K[x_1, \ldots, x_n]$