PMATH 345 Lecture 1: May 3, 2010

PMath 345
David McKinnon
http://www.student.math.uwaterloo.ca/~pmat345

Rings
A ring is a bunch of things you can add, subtract and multiply in a reasonable way.

Example: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}[x] = \{\text{polynomials in } x \text{ with real coefficients}\}$, $\mathbb{R}[x_1, \dots, x_n] = \{\text{polynomials in } x_1, \dots, x_n \text{ with real coefficients}\}$, $M_n(\mathbb{Z}) = \{n \times n \text{ matrices with } \mathbb{Z} \text{ coefficients}\}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}[i] = \{\, a + bi : a, b \in \mathbb{Z} \,\}$ = "Gaussian integers"

Definition: A ring is a set R with two functions $+\colon R \times R \to R$ and $\cdot\colon R \to R$ satisfying the following properties for all a, b, $c \in R$:

(1) $(a + b) + c = a + (b + c)$

(2) $a + b = b + a$

(3) There exists $0 \in R$ such that $a + 0 = a$

(4) There exists $-a \in R$ such that $a + (-a) = 0$

(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(6) $a \cdot b = b \cdot a$ $\leftarrow$ Not really a ring axiom

(7) There exists a $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$. Controversial! rng

(8) $a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$

$$0_{\text{Paul}} = 0_{\text{Paul}} + 0_{\text{Ringo}} = 0_{\text{Ringo}}$$

Definition: Let R be a ring. A subring of R is a subset $S \subset R$ which is a ring using the $+$ and $\cdot$ of R.
Example: $\mathbb{Q}$ is a subring of $\mathbb{C}$.
$\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Theorem: (Subring Theorem) Let R be a ring. $S \subset R$ a subset. Then S is a subring of R *iff*

(1) $0, 1 \in S$

(2) If a, $b \in S$, then $a - b \in S$.

(3) If a, $b \in S$, then $a \cdot b \in S$.

PMATH 345 Lecture 2: May 5, 2010

Definition: A ring is a set R with 2 operations $+\colon R \times R \to R$, $\cdot\colon R \times R \to R$ satisfying for all a, b, $c \in R$:

(1) $(a + b) + c = a + (b + c)$
(2) $a + b = b + a$
(3) There is $0 \in R$ such that $a + 0 = a$ $\forall a \in R$
(4) There is $-a \in R$ such that $a + (-a) = 0$
(5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(6) $a \cdot b = b \cdot a$
(7) There is $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$
(8) $a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$

Theorem: (Subring Theorem)
Let R be a ring. $S \subset R$ any subset. Then S is a subring of R *iff*:

(1) $0,\, 1 \in S$

(2) If $a,\, b \in S$ then $a - b \in S$

(3) If $a,\, b \in S$ then $ab \in S$

Proof: Forwards is trivial.
Backwards: Assume S satisfies (1), (2), and (3) from the theorem. We need to check that $+$ and $\cdot$ are well defined from $S \times S \to S$, and we need to check (1)–(8).

The fact that $\cdot$ is from $S \times S \to S$ is precisely (3). For $+$, first note that (1) means that $0, 1 \in S$. By (2), we find $0 - 1 = -1 \in S$. Thus, if $a,\, b \in S$, then by (3), $(-1) \cdot b \in S$ so since $(-1) \cdot b = -b$, we get $-b \in S$.

$$\begin{aligned}
(-1) \cdot b + b &= (-1 + 1) \cdot b \\
&= 0 \cdot b \\
&= 0 \\
\text{follows from: } 0 \cdot b &= (0 + 0) \cdot b \\
&= 0 \cdot b + 0 \cdot b \\
\implies -0 \cdot b + 0 \cdot b &= -0 \cdot b + 0 \cdot b + 0 \cdot b \\
\implies 0 &= 0 \cdot b
\end{aligned}$$

We want to show that $a + b \in S$. Well, $-b \in S$, so $a - (-b) \in S$ by (2), so $a + b \in S$.
(1), (2), (5), (6), (8): Trivial for S
(3), (7): By (1)
(4): Already done □

Example: Prove $\mathbb{Z}[\sqrt{17}] = \{\, a + b\sqrt{17} : a, b \in \mathbb{Z} \,\}$ is a subring of $\mathbb{R}$.
Solution: $\mathbb{Z}[\sqrt{17}] \subset \mathbb{R}$ clearly. By Subring Theorem:

(1) $0 = 0 + 0\sqrt{17} \in \mathbb{Z}[\sqrt{17}]$
$1 = 1 + 0\sqrt{17} \in \mathbb{Z}[\sqrt{17}]$

(2) $a + b\sqrt{17} \in \mathbb{Z}[\sqrt{17}]$
$c + d\sqrt{17} \in \mathbb{Z}[\sqrt{17}]$
$\implies (a + b\sqrt{17}) - (c + d\sqrt{17}) = (a - c) + (b - d)\sqrt{17} \in \mathbb{Z}[\sqrt{17}]$

(3) Similarly, $(a + b\sqrt{17})(c + d\sqrt{17}) = (ac + 17bd) + (ad + bc)\sqrt{17} \in \mathbb{Z}[\sqrt{17}]$ so we're done.

Definition: Let R be a ring, $r \in R$ any element. Then:

r is a zero divisor *iff* $ra = 0$ for some $a \in R$, $a \neq 0$, provided $r \neq 0$. r is a unit *iff* there is an element $1/r \in R$ such that $r(1/r) = 1$.
r is nilpotent *iff* $r^n = 0$ for some positive integer n $(r \neq 0)$.

Definition: A ring R is called an (integral) domain *iff* it contains no zero divisors.

A ring R is a field *iff* every nonzero element is a unit.
A ring R is reduced *iff* it contains no nilpotent elements.

$\mathbb{Z}/4\mathbb{Z}$ is not reduced: $2^2 = 0$, $2 \neq 0$
$\mathbb{Z}/6\mathbb{Z}$ is reduced, but not a domain: $2 \cdot 3 = 0$, $2, 3 \neq 0$
$\mathbb{Z}/7\mathbb{Z}$ is a field: every nonzero element is a unit: $1 \cdot 1 = 1$, $2 \cdot 4 = 1$, $3 \cdot 5 = 1$, $6 \cdot 6 = 1$

$\mathbb{Z}$ is a domain that's not a field.
Theorem: Let R be a ring, $r \in R$ any element. Then r cannot be both a zero divisor and a unit.
Proof: Say r is a unit. Then $r \cdot (1/r) = 1$. If r is also a zero divisor, then $ra = 0$ for some $a \neq 0$, so:

$$\begin{aligned}
ar(1/r) &= a \\
\implies 0 &= a
\end{aligned}$$

Bad! □

Definition: Let R, S be rings. Their direct sum is the ring $R \oplus S$. The elements of $R \oplus S$ are the elements of $R \times S$, and the $+$ and $\cdot$ are:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$$

Theorem: $R \oplus S$ is a ring.
Proof: Dull.

$$0 \leftrightarrow (0, 0)$$
$$1 \leftrightarrow (1, 1)$$

□

$(1, 0) \cdot (0, 1) = (0, 0)$
If R, S are nonzero, then $0 \neq 1$, so $R \oplus S$ is not an integral domain.

PMATH 345 Lecture 3: May 7, 2010

Definition: Let R be a ring. A subring of R is a set $S \subset R$ such that S is a ring using the same operations as R *and* $1 \in S$.

Example: $R = \mathbb{Z}/6\mathbb{Z}$
$S = \{0, 3\}$
S is a ring using $+$ and $\cdot$ as R, but the multiplicative identity of S is not $1 \in R$.
$S \subset R$, S closed under $+, \cdot, -$, and has $z \in S$ such that $z + r = r$ for all $r \in S$.
$\implies z = 0$ ✓.

Theorem: Let $n \geq 1$ be an integer. Then $\mathbb{Z}/n\mathbb{Z}$ is:

(1) A field *iff* n is prime

(2) Reduced *iff* n is squarefree

Proof:

(1) If n is prime, then every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is represented by an integer coprime to n. Thus, every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is a unit, so $\mathbb{Z}/n\mathbb{Z}$ is a field.

Conversely, if $\mathbb{Z}/n\mathbb{Z}$ is a field, then every nonzero element is coprime to n, so n is prime.

(2) Assume $p^2 \mid n$, $p > 1$. Then $n/p \neq 0$, $n/p \in \mathbb{Z} \implies n/p$ is well defined mod n, but

$$\left(\frac{n}{p}\right)^2 = \frac{n^2}{p^2} = \left(\frac{n}{p^2}\right)n = 0.$$

So $\mathbb{Z}/n\mathbb{Z}$ is not reduced, since n/p is nilpotent.

Finally, assume that m is nilpotent mod n. We want to show that n is not squarefree. Well, $m \neq 0$ mod n, but $m^a = 0$ mod m. As integers, write ${}^{m = p_1^{a_1} \cdots p_r^{a_r}}_{n = p_1^{b_1} \cdots p_r^{b_r}}$ where, in principle, some of the a_i, b_i may be 0.

Since $n \nmid m$, we get $n \nmid m$, we get $b_i > a_i$ for some i. Since $n \mid m^a$, we get $b_i \leq a a_i$. Note $b_i > a_i \geq 0$, and $b_i \leq a a_i$, so $a_i > 0$. So $b_i > a_i \geq 1$, and so $b_i \geq 2$. Thus, $p_i^2 \mid n$, and n is not squarefree. □

Homomorphisms
Definition: Let R, S be rings. A homomorphism from R to S is a function $f\colon R \to S$ satisfying:

(1) $f(1) = 1$

(2) $f(a + b) = f(a) + f(b)$

(3) $f(ab) = f(a)f(b)$

Example: $f\colon \mathbb{C} \to \mathbb{C}$, $f(a+bi) = a - bi$
Example: $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
$f(r) = r \bmod n$
Example: $f\colon \mathbb{Q}[x] \to \mathbb{Q}$
$f(p(x)) = p(3\frac{1}{2})$
$f(x-7) = -3\frac{1}{2}$
$f(x^2+2x+3) = \frac{49+28+12}{4} = \frac{89}{4}$
$f(6) = 6$
"Plugging in" homomorphism:

$$f\colon R[x_1, \ldots, x_n] \to T$$

where R is a ring, $R \subset T$, and:

$$f(p(x_1, \ldots, x_n)) = p(t_1, \ldots, t_n)$$

where $t_1, \ldots, t_n \in T$ are any fixed elements of T.

Example: $f\colon \mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}$
$f(a+bi) = a + 2b \bmod 5$

(1) $f(1) = 1 \bmod 5$ ✓

(2) $f((a+bi)+(c+di)) = f((a+c)+(b+d)i) = a+c+2(b+d) \bmod 5$
$f(a+bi)+f(c+di) = a+2b+c+2d \bmod 5$. Same.

(3)
$$f(a+bi)f(c+di) = (a+2b)(c+2d) = ac+4bd+2ad+2bc \bmod 5$$
$$f((a+bi)(c+di)) = f(ac-bd+bci+adi) = ac-bd+2(ad+bc) \bmod 5$$

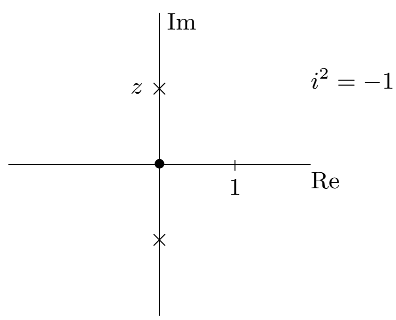
These are the same, so $\square$.

PMATH 345 Lecture 4: May 10, 2010

$\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} =$ "Integers mod 3"

Definition: Let R, S be rings, $f\colon R \to S$ a homomorphism. Then f is an isomorphism *iff* there is another homomorphism $g\colon S \to R$ such that $f \circ g = \text{id}$ and $g \circ f = \text{id}$.

Example: $f\colon \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$. This is an isomorphism; the inverse of f is f.



To prove $z = i$, we'd have to have some relationship between z, real numbers, and $+$ and $\cdot$:

$$a_n z^n + \cdots + a_1 z + a_0 = 0$$

where $a_i \in \mathbb{R}$. Then:

$$a_n \overline{z}^n + \cdots + a_1 \overline{z} + a_0 = 0$$

So there's no way to tell the difference between i and $-i$.

Definition: Let $f\colon R \to S$ be a homomorphism. The image of f is the set:

$$\begin{aligned}\text{im}(f) &= \{\, f(x) : x \in R \,\}\\ &= \text{range of } f\end{aligned}$$

and the kernel of f:

$$\ker(f) = \{ x \in R : f(x) = 0 \}$$

Theorem: Let $f \colon R \to S$ be a homomorphism. Then f is 1–1 *iff* $\ker(f) = \{0\}$.
Proof: Forwards is trivial, because $f(0) = 0$.
Backwards: Assume $\ker f = \{0\}$. We want to show f is 1–1. If $f(a) = f(b)$, then $f(a - b) = 0$, so $a - b \in \ker f$, so $a - b = 0 \implies a = b$. □

Theorem: Let $f \colon R \to S$ be a homomorphism. Then:

(1) $f(0) = 0$

(2) The composition of homomorphisms is a homomorphism

(3) If x is a unit, then so is $f(x)$.

Theorem: Let $f \colon R \to S$ be a homomorphism. Then $\ker f$ is usually not a subring of R. In fact, $\ker f$ is a subring of R *iff* $\ker f = R$.

Definition: Let R be a ring. An ideal of R is a subset $I \subset R$ satisfying:

(1) $0 \in I$

(2) If a, $b \in I$ then $a - b \in I$

(3) If $a \in I$, $r \in R$, then $ar \in I$.

Theorem: Let $f \colon R \to S$ be a homomorphism. Then $\ker f$ is an ideal of R.
Proof:

(1) $f(0) = 0 \implies 0 \in \ker f$.

(2) If a, $b \in \ker f$, then $f(a) = f(b) = 0$. We want $a - b \in \ker f$, i.e., $f(a - b) = 0$. This is trivial.

(3) If $a \in \ker f$, $r \in R$, then $f(a) = 0$, so $f(ra) = f(r)f(a) = f(r) \cdot 0 = 0$. So $ra \in \ker f$. □

Example: What are the ideals of $\mathbb{Z}$?
$\{0\}$ is the trivial or zero ideal.
$\mathbb{Z}$ is the improper or unit ideal.
$I = \{\text{even integers}\}$ is an ideal, often written $2\mathbb{Z}$.
In fact, $\{\text{multiples of } n\} = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
Better yet, every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Definition: Let R be a ring, $a \in R$ any element. The principal ideal of R generated by a is the set:

$$(a) = aR = \{ aR : r \in R \}.$$

Theorem: (a) is an ideal of R.
Proof: Easy. □

PMATH 345 Lecture 5: May 12, 2010

Claim: The ideals of $\mathbb{Z}$ are precisely the sets $n\mathbb{Z} = \{ nr : r \in \mathbb{Z} \}$.
Proof: First, $n\mathbb{Z}$ is an ideal by a quick check of the definition. It only remains to show that every ideal is of the form $n\mathbb{Z}$. Thus, say $I \subset \mathbb{Z}$ is an ideal. It could be that $I = \{0\} = 0\mathbb{Z}$. Otherwise, I must contain some nonzero integer, which we may assume is positive. Let n be the smallest positive element of I. We will show that $I = (n) = n\mathbb{Z}$. Clearly $n\mathbb{Z} \subset I$, since $n \in I$. Thus, $x \in I$. We want to show $x \in n\mathbb{Z}$. After long division:

$$x = qn + r$$

where q, $r \in \mathbb{Z}$, $0 \leq r < n$. But $r = x - qn \in I$, so by minimality of n, we get $r = 0$, and hence $x = qn \in n\mathbb{Z}$. Thus, $I = n\mathbb{Z}$. □

Definition: Let R be a ring, $a_1, \ldots, a_n \in R$ any elements. The ideal generated by $a_1, \ldots, a_n$ is:

$$(a_1, \ldots, a_n) = \{ r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R \}$$

It is easy to see that this is an ideal.

Example: $(6, 8) \subset \mathbb{Z}$

$$\begin{aligned} &= \{ 6a + 8b : a, b \in \mathbb{Z} \} \\ &= \{ 2(3a + 4b) : a, b \in \mathbb{Z} \} \end{aligned}$$

so $2 \in (6, 8)$. This immediately means that $(2) \subset (6, 8)$.

Conversely, 6, $8 \in (2)$, so $(6, 8) \subset (2)$, and hence $(2) = (6, 8)$.

Fact: Given an ideal I and elements $a_1, \ldots, a_n \in R$, if $a_1, \ldots, a_n \in I$ then $(a_1, \ldots, a_n) \subset I$.

Example: $(x, y) \subset \mathbb{Q}[x, y]$

$$\begin{aligned} (x, y) &= \{ xp(x, y) + yq(x, y) : p, q \in \mathbb{Q}[x, y] \} \\ &= \{ r(x, y) : r(0, 0) = 0 \} \end{aligned}$$

Definition: Let I, J be ideals. Then these are ideals:

$$\begin{aligned} I + J &= \{ a + b : a \in I, b \in J \} \\ \text{and } IJ &= \{ a_1 b_1 + \cdots + a_n b_n : a_i \in I, b_i \in J \} \end{aligned}$$

$$\begin{aligned} (a_1, \ldots, a_n) + (b_1, \ldots, b_m) &= (a_1, \ldots, a_n, b_1, \ldots, b_m) \\ (a_1, \ldots, a_n)(b_1, \ldots, b_m) &= (a_1 b_1, a_1 b_2, \ldots, a_1 b_m, a_2 b_1, \ldots, a_2 b_m, \ldots, a_n b_1, \ldots, a_n b_m) \\ &= (a_i b_j)_{\substack{i \in \{1, \ldots, n\} \\ j \in \{1, \ldots, m\}}} \end{aligned}$$

Example: In $\mathbb{Q}[x, y]$:

$$(x, y^2) \cdot (x - y, y^3 - y) = (x^2 - xy, xy^2 - y^3, xy^3 - xy, y^5 - y^3)$$

If R is a ring, then $R^* =$ group of units of R

Theorem: Let I be an ideal of a ring R. Then $I = (1) = R$ *iff* I contains some unit of R.
Proof: Forwards is trivial. For backwards, assume $u \in I$ is a unit. Then $1 = uu^{-1} \in I \implies I = (1)$. $\square$

Theorem: Let R be a ring, $R \neq \{0\}$. Then R is a field *iff* it has exactly two ideals, (0) and (1).
Proof: Forwards: Assume R is a field, $I \subset R$ any ideal. If $I = (0)$, we're done. If not, I contains some $x \in R$, $x \neq 0$. Since R is a field, x is a unit, so $I = (1)$.

Backwards: Let $x \in R$ be any nonzero element. We want to show $x \in R^*$. Well, $(x) \subset R$ is an ideal with $(x) \neq (0)$, so by assumption $(x) \neq (1)$. This means $1 \in (x) = \{ xr : r \in R \}$

$$\implies 1 = rx \text{ for some } r \in R$$

so $x \in R^*$ and R is a field. $\square$

Quotient rings
Let R be a ring, $I \subset R$ an ideal. (e.g., $R = \mathbb{Z}$, $I = (n)$)
We want to build a ring R/I and a homomorphism $q\colon R \to R/I$ such that $\ker q = I$.

If we had such a thing, then $q(x) = q(y) \iff x - y \in \ker q = I$.

Thus, elements of R/I ought to be equivalence classes of elements of R under the equivalence relation

$$x \equiv y \bmod I \quad \textit{iff} \quad x - y \in I.$$

PMATH 345 Lecture 6: May 14, 2010

Theorem: A homomorphism $f\colon R \to S$ is an isomorphism *iff* it's 1–1 and onto.
Proof: Forwards is trivial.
Backwards: Assume f is 1–1 and onto. We want to show that $f^{-1}\colon S \to R$ is a homomorphism.

First, $f^{-1}(1) = 1$ because $f(1) = 1$. Next, let $a, b \in S$ be any elements. We want to show that

$$f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b).$$

Since f is 1–1 and onto, we can find $A, B, C \in R$ such that $f(A) = a$, $f(B) = b$, and $f(C) = a + b$. Then: $f(A) + f(B) = f(A + B) = a + b$

$$\implies A + B = f^{-1}(a+b)$$

But $C = f^{-1}(a + b)$ by definition of C

$$\begin{aligned} &\implies A + B = C \\ &\implies f^{-1}(a) + f^{-1}(b) = f^{-1}(a+b) \end{aligned}$$

as desired.
Proving $f^{-1}(a)f^{-1}(b) = f^{-1}(ab)$ is exactly similar. □

We've got: a ring R, an ideal $I \subset R$
We want: a ring $R/I =$ "$R \bmod I$" an onto homomorphism $q\colon R \to R/I$ with $\ker q = I$.

$$R/I = \{\text{equivalence classes of elements of } R\}$$

where $r_1 \equiv r_2 \bmod I$ *iff* $r_1 - r_2 \in I$

$$= \{\, r + I^{1)} : r \in R \,\}$$

Addition: $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$
Multiplication: $(r_1 + I)(r_2 + I) = (r_1 r_2 + I)$
One: $1 + I$
We need to check that these definitions are well defined.

If $r_1 \equiv r_1' \bmod I$ and $r_2 \equiv r_2' \bmod I$, we must check that $r_1 + r_2 \equiv r_1' + r_2' \bmod I$ and $r_1' r_2' \equiv r_1 r_2 \bmod I$.

If $a_1 = r_1 - r_1' \in I$, $a_2 = r_2 - r_2' \in I$, then

$$(r_1 + r_2) - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in I$$

$$\begin{aligned} \text{and } r_1 r_2 - r_1' r_2' &= r_1 r_2 - (r_1 - a_1)(r_2 - a_2) \\ &= \cancel{r_1 r_2 - r_1 r_2} + a_1 r_2 + a_2 r_1 - a_1 a_2 \\ &\in I \end{aligned}$$

Checking that R/I is a ring is tedious but straight forward.

It's clear from the construction that the map

$$\begin{aligned} q\colon R &\to R/I \\ \text{given by } q(r) &= r \bmod I \\ &= r + I \end{aligned}$$

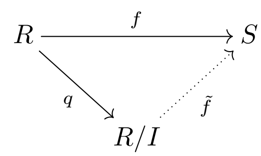
is a surjective homomorphism. The map q is called the "reduction mod I" homomorphism.

1) "coset of I"
$r + I = \{\, r + a : a \in I \,\}$

Example: $R = \mathbb{Z}$, $I = (n)$
Then $R/I = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
Example: $\mathbb{C}[x]/(x)$ should be isomorphic to $\mathbb{C}$.
Example: $\mathbb{R}[x]/(x^2+1)$ should be isomorphic to $\mathbb{C}$.[2)]

$$\mathbb{C}[x,y,z]/(x^2 - x + 3yz, x^3 z + 4y)$$

Theorem: (Universal Property of Quotients)
Let R, S be rings, $I \subset R$ an ideal, $f\colon R \to S$ a homomorphism, $q\colon R \to R/I$ the "reduce mod I" homomorphism.

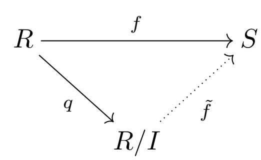


There exists a homomorphism $\tilde{f}\colon R/I \to S$ with $\tilde{f} \circ q = f$ *iff* $I \subset \ker f$.

Remark: This theorem says that if you can find a homomorphism $f\colon R \to S$ with $I \subset \ker f$, then f "makes sense mod I".

PMATH 345 Lecture 7: May 17, 2010

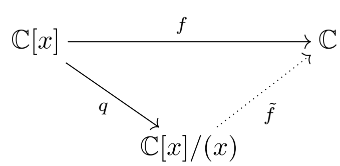
Theorem: (UPQ) Let R, S be rings, $I \subset R$ an ideal, $f\colon R \to S$ a homomorphism, $q\colon R/I$ the quotient homomorphism



Then there exists a homomorphism $\tilde{f}\colon R/I \to S$ with $f = \tilde{f} \circ q$ *iff* $I \subset \ker f$.

Example: Find an isomorphism from $\mathbb{C}[x]/(x)$ to $\mathbb{C}$.

$\mathbb{C}[x]$[3)] $/(x)$[4)] to $\mathbb{C}$[5)]



$$f(p(x)) = p(0)$$

This is a homomorphism, and $x \in \ker f$, so $(x) \subset \ker f$, so by the UPQ, f "makes sense" as a homomorphism from $\mathbb{C}[x]/(x) \to \mathbb{C}$. That is, f induces a homomorphism $\tilde{f}\colon \mathbb{C}[x]/(x) \to \mathbb{C}$.

$$\tilde{f}(p(x) \bmod I) = p(0).$$

It's onto because $\tilde{f}(z) = z$ for any $z \in \mathbb{C}$, so we just need to check 1–1. To do this, we show that $\ker \tilde{f} = (0) \iff \ker f = (x)$.
We already know $(x) \subset \ker f$, so let $p(x) \in \ker f$. Then $f(p(x)) = p(0) = 0$, so $x \mid p(x)$, and so $p(x) \in (x)$ and we're done.

Proof of UPQ: Forwards: We have $\tilde{f} \circ q = f$, so if $r \in I$, we compute $f(r) = \tilde{f}(q(r)) = \tilde{f}(0) = 0$, so $r \in \ker f$.

---

2) Aside: Show: $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \oplus \mathbb{R}$
3) R
4) I
5) S

Backwards: Assume $I \subset \ker f$. We want $\tilde{f}\colon R/I \to S$ such that $\tilde{f} \circ q = f$
Define

$$\tilde{f}(r \bmod I) = f(r)$$

To check that this is well defined, we check that if $r_1 \equiv r_2 \bmod I$, then $\tilde{f}(r_1 \bmod I) = \tilde{f}(r_2 \bmod I)$. That is, we check that $f(r_1) = f(r_2)$.

Well, $f(r_1) - f(r_2) = f(r_1 - r_2) = 0$ since $r_1 - r_2 \in I \subset \ker f$.

We check that $\tilde{f}$ is a homomorphism:

$$\tilde{f}(1 \bmod I) = f(1) = 1 \quad \checkmark$$
$$\tilde{f}(a + b \bmod I) = f(a+b) = f(a) + f(b) = \tilde{f}(a \bmod I) + \tilde{f}(b \bmod I) \quad \checkmark$$
$$\tilde{f}(ab \bmod I) = f(ab) = f(a)f(b) = \tilde{f}(a \bmod I)\tilde{f}(b \bmod I) \quad \checkmark \quad \square$$

Facts: $\ker \tilde{f} = \ker f \bmod I$
$\operatorname{im} \tilde{f} = \operatorname{im} f$

Theorem: (First Isomorphism Theorem) Let $f\colon R \to S$ be a homomorphism. Then $\operatorname{im} f \cong^{6)} R/\ker f$.
Proof: Straight from UPQ. $\square$

Theorem: Let $f\colon R \to S$ be a homomorphism, $I \subset R$ an ideal, $J \subset S$ an ideal. Then:

(1) $f^{-1}(J) = \{\, r \in R : f(r) \in J \,\}$ = preimage of J is an ideal of R

(2) If f is onto, then
$$f(I) = \{\, f(r) : r \in I \,\}$$
is an ideal of S.

Proof:

(1) $0 \in f^{-1}(J)$ because $f(0) = 0 \in J$. If $a, b \in f^{-1}(J)$, then $f(a), f(b) \in J$, so $f(a-b) = f(a) - f(b) \in J$, and hence $a - b \in f^{-1}(J)$.

Finally, if $a \in f^{-1}(J)$, $r \in R$, then $f(ra) = f(r)f(a) \in J$, so $ra \in f^{-1}(J)$.

(2) $0 \in f(I)$ because $f(0) = 0$. If $a, b \in f(I)$. Then $a = f(r)$, $b = f(s)$ for $r, s \in I$, so $a - b = f(r) - f(s) = f(r - s)$, so $a - b \in f(I)$.

Finally, let $a \in f(I)$, $r \in S$. Since f is onto, we write $r = f(t)$ and $a = f(u)$ for $t \in R$, $u \in I$.

Then $tu \in I$ and $f(tu) = ra$, so $ra \in f(I)$. $\square$

Definition: Let R be a ring, $I \subset R$ an ideal. Then I is prime *iff* $I \neq R$ and for all $a, b \in R$, if $ab \in I$ then either $a \in I$ or $b \in I$.
I is maximal *iff* the only ideal J with $I \subsetneq J$ is $J = R$ and $I \neq R$.

PMATH 345 Lecture 8: May 19, 2010

$\mathbb{Z}_5[x]$: polynomials in x whose coefficients lie in $\mathbb{Z}_5$.
Fact: If $a \in \mathbb{Z}_5$, then $a^5 = a$.
Fact: In $\mathbb{Z}_5[x]$, x^5 and x are *different* polynomials that define the same function $\mathbb{Z}_5 \to \mathbb{Z}_5$.

$$x^5 = (\sqrt{2})^5 = \sqrt{32} = 4\sqrt{2} = -\sqrt{2}$$
$$x = \sqrt{2} \neq 4\sqrt{2}$$

Definition: Let R be a ring, $I \subset R$ an ideal. Then I is prime *iff* every $a, b \in R$ with $ab \in I$ satisfies $a \in I$ or $b \in I$, and $I \neq R$.

Furthermore, I is maximal *iff* $I \neq R$ and the only ideal $J \subset R$ with $I \subsetneq J$ is $J = R$.

6) "is isomorphic to"

Example: What are the prime and maximal ideals of $\mathbb{Z}$?

Well, any ideal of $\mathbb{Z}$ is of the form (n) for $n \in \mathbb{Z}$.

If n is composite, then $n = ab$ for a, $b \in \mathbb{Z}$, a, $b \neq \pm 1$. In that case:

$$(n) \subsetneq (a) \neq (1)$$

so (n) is not a maximal ideal. Also, $a \notin (n)$ and $b \notin (n)$, but $ab \in (n)$, so (n) isn't prime.

(0) is prime but not maximal. If n is prime, then we can call it p. The ideal (p) is maximal and prime. The ideal (p) is prime because $p \mid ab \implies p \mid a$ or $p \mid b$, and (p) is maximal because if $(p) \subsetneq (n)$, then $n \mid p$, so $n = \pm p$ (not possible since $(p) \neq (n)$) or $n = \pm 1$, in which case $(n) = (1)$. Hence (p) is maximal.

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

(1) I is prime *iff* R/I is a domain

(2) I is maximal *iff* R/I is a field

Proof:

(1) Forwards: I is prime. Let a, $b \in R$ be any elements with $ab \equiv 0 \bmod I$. We want to show either $a \equiv 0$ or $b \equiv 0$. Since $ab \equiv 0$, we get $ab \in I$, so either $a \in I$ or $b \in I \implies a \equiv 0$ or $b \equiv 0$.

Backwards: Similar.

(2) Forwards: I is maximal. This means only two ideals of R contain I, namely, I and R.

Now let J be any ideal of R/I, $q\colon R \to R/I$ the quotient homomorphism. Then

$$q^{-1}(J) = \{\, r \in R : q(r) \in J \,\}$$

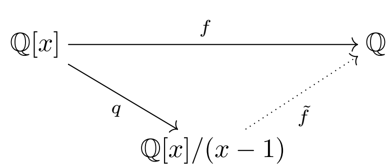
is an ideal of R that contains I.

So $q^{-1}J = I$ or R, so $J = (0)$ or (1). Thus, R/I has exactly 2 ideals, and so must be a field.

Backwards: Similar. □

Corollary: Every maximal ideal is prime.
Proof: Every field is a domain. □

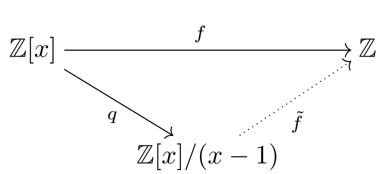
Example: Is $(x-1)$ a prime ideal of $\mathbb{Q}[x]$? How about $\mathbb{Z}[x]$?



$f(p(x)) = p(1)$. By UPQ, this induces $\tilde{f}\colon \mathbb{Q}[x]/(x-1) \to \mathbb{Q}$ because $f(x-1) = 1 - 1 = 0$.
We see that $\tilde{f}$ is onto, since $f(c) = c$ for all $c \in \mathbb{Q}$. Moreover, $\tilde{f}$ is 1–1 because $f(p(x)) = 0 \iff p(1) = 0 \iff x - 1 \mid p(x) \iff p(x) \in (x-1)$. That is, $\ker f = (x-1) \iff \ker \tilde{f} = (0)$.

Since $\mathbb{Q}[x]/(x-1) \cong \mathbb{Q}$ (via $\tilde{f}$), we see that $(x-1)$ is prime and maximal.

$\mathbb{Z}[x]$:



$f(p(x)) = p(1)$

Not too hard to show $\tilde{f}$ is 1–1 and onto. Since $\mathbb{Z}$ is a domain but not a field, $(x-1)$ is prime but not maximal in $\mathbb{Z}[x]$.

Let R be any ring. There is exactly one homomorphism $\phi\colon \mathbb{Z} \to R$, given by $\phi(n) = n$, called the characteristic homomorphism. Since $\ker \phi$ is an ideal of $\mathbb{Z}$, we have $\ker \phi = (n)$ for some $n \geq 0$. This n is called the characteristic of R, and is written $\operatorname{char} R$.

$\mathbb{Z}/n\mathbb{Z}$ has characteristic n.
$\operatorname{char} R$ = first positive integer n such that $n = 0$ in R
If none, then $\operatorname{char} R = 0$.

Example: $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{Z} = 0$.
Fact: R is a domain $\implies$ $\operatorname{char} R$ is 0 or prime.

PMATH 345 Lecture 9: May 21, 2010

Let R be a ring, $\phi\colon \mathbb{Z} \to R$ the characteristic homomorphism $\operatorname{char} R = n$, where $\ker \phi = (n)$. Every ring of characteristic $n > 0$ has a subring isomorphic to $\mathbb{Z}/n\mathbb{Z}$, namely, $\operatorname{im} \phi$.

Every ring of characteristic 0 has a subring isomorphic to $\mathbb{Z}$, namely $\operatorname{im} \phi$.

Theorem: Let D be a domain. Then $\operatorname{char} D = 0$ or $\operatorname{char} D$ is prime.
Proof: Say $\operatorname{char} D > 0$ and $\operatorname{char} D = ab$ for integers a, b. We want to show $a = 1$ or $b = 1$.

Well, $ab = 0$ in D. Since D is a domain, this means $a = 0$ or $b = 0$; without loss of generality, say $a = 0$. Then by definition of $\operatorname{char} D$, $a \geq ab$, so $b \leq 1$. Since $b \in \mathbb{Z}$, $b > 0$, we get $b = 1$. □

Fraction fields
Let D be a domain. We will construct a field that contains D.

Definition: Let D be a domain. Define the fraction field $K(D)$ by:

$$K(D) = \left\{ \frac{a}{b} : a, b \in D,\, b \neq 0 \right\} \Big/ \sim$$

where $\frac{a}{b} \sim \frac{c}{d}$ *iff* $ad = bc$, and:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Need to show:

(1) If $\frac{a}{b} \sim \frac{a'}{b'}$, then $\frac{a}{b} + \frac{c}{d} \sim \frac{a'}{b'} + \frac{c}{d}$ *and* $\frac{a'}{b'} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{c}{d}$

(2) $K(D)$ with all these operations is a field.

I do not deign to do so.

Note that there is a natural homomorphism $\phi\colon D \hookrightarrow K(D)$, $\phi(d) = \frac{d}{1}$. Typically, we identify D with $\phi(D)$, and say that $D \subset K(D)$.

Example: $K(\mathbb{Z}) = \mathbb{Q}$.
Example: $K(F[x]) = F(x)$ if F is a field

$$F(x) = \left\{ \frac{f(x)}{q(x)} : p, q \in F[x],\, q \neq 0 \right\}$$

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

$$K(\mathbb{Z}[i]) = \left\{ \frac{a + bi}{c + di} : a, b, c, d \in \mathbb{Z},\, c + di \neq 0 \right\}$$

$$\begin{aligned} \text{But} \qquad \frac{a + bi}{c + di} &= \frac{(a + bi)(c - di)}{c^2 + d^2} \\ &= \Big(\frac{ac + bd}{c^2 + d^2}\Big) + \Big(\frac{bc - ad}{c^2 + d^2}\Big) i \\ &\in \mathbb{Q}(i) = \{\, a + bi : a, b \in \mathbb{Q} \,\} \end{aligned}$$

So $K(\mathbb{Z}[i]) = \mathbb{Q}(i)$[7]

Theorem: (Universal Property of Fraction Fields) Let F be a field, and D a domain, $\phi\colon D \hookrightarrow F$ an injective homomorphism. Then ϕ extends to an injective homomorphism $\tilde{\phi}\colon K(D) \hookrightarrow F$.
Proof: Define $\tilde{\phi}(\frac{a}{b}) = \frac{\phi(a)}{\phi(b)}$. This is well defined because $\phi(b) \neq 0$ (since $b \neq 0$ and ϕ is 1–1). Checking that this is an injective homomorphism is straightforward. □

Theorem: Let $\phi\colon F \to E$ be a homomorphism of fields E and F. Then ϕ is 1–1.
Proof: Consider $\ker\phi$. It's an ideal of F, so $\ker\phi = (0)$ or (1). Since $\phi(1) = 1$, we get $\ker\phi = (0)$, and so ϕ is 1–1. □

PMATH 345 Lecture 10: May 26, 2010

`http://cumc.math.ca/`
July 6–July 10

Definition: Let D be a domain, $x \in D$ any element, $x \neq 0$, $x \notin D^*$. Recall: $D^* = \{\text{units of } D\}$. Then x is prime *iff* (x) is a prime ideal. Also, x is irreducible *iff* when $x = ab$ for $a, b \in D$, we have $a \in D^*$ or $b \in D^*$.

Example: Prime elements of $\mathbb{Z}$ are prime numbers. Irreducible elements of $\mathbb{Z}$ are prime numbers.

Example: $D = \mathbb{Z}[\sqrt{10}]$, $x = 2$. Showing that x is irreducible is not easy, but can be done.

But x is not prime. We will prove this by showing (2) is not a prime ideal, by showing that $\mathbb{Z}[\sqrt{10}]/(2)$ is not a domain.

Well, $\mathbb{Z}[\sqrt{10}] = \{\, a + b\sqrt{10} : a, b \in \mathbb{Z} \,\}$. $\mathbb{Z}[\sqrt{10}]/(2)$ has 4 elements, represented by 0, 1, $\sqrt{10}$, $1 + \sqrt{10}$. To prove this, note that those 4 elements are all different mod 2, and any $a + b\sqrt{10}$ is congruent to one of these 4 mod 2.

Notice that $\sqrt{10} \not\equiv 0 \bmod 2$, but $(\sqrt{10})^2 \equiv 0 \bmod 2$, so 2 is not prime.

Definition: A domain D is a Principal Ideal Domain (PID) *iff* every ideal of D is principal; *i.e.*, every ideal is of the form (x) for some $x \in D$.

Definition: A domain D is a Unique Factorization Domain (UFD) *iff* every $x \in D$, $x \neq 0$, can be factored into irreducible elements of $p_1, \ldots, p_n \in D$:

$$x = p_1 p_2 \cdots p_n$$

and this factorization is unique up to multiplication by units and reordering the p_is.

We will show that every PID is a UFD. However, $\mathbb{Q}[x, y]$ is a UFD, but not a PID because (x, y) is not principal.

Theorem: Every prime element of a domain D is irreducible.
Proof: Let $x \in D$ be prime, and assume $x = ab$, $a, b \in D$. We want to show either $a \in D^*$ or $b \in D^*$. Since x is prime, $ab \in (x) \implies a \in (x)$ or $b \in (x)$; without loss of generality $a \in (x)$.

So $a = xd$ for some $d \in D$:

$$x = xdb.$$

Since $x \neq 0$, we get $1 = db$, and so $b \in D^*$. □

Theorem: Let D be a PID. Then every irreducible element of D is prime.

Note: This theorem is not true if D is not a PID! (*E.g.*, $D = \mathbb{Z}[\sqrt{10}]$.)
Proof: Say $a \in D$, $a \neq 0$, $a \notin D^*$. Assume a is irreducible. Then (a) is a maximal ideal:

If $(a) \subset I$ for some ideal I, then $I = (x)$ for some $x \in D$. Then $a = xd$ for some $d \in D$. Since a is irreducible, we get $x \in D^*$ or $d \in D^*$. If $x \in D^*$ then $I = (1)$. If $d \in D^*$ then $I = (a)$. So (a) is a maximal ideal. Which means (a) is a prime ideal. So a is prime. □

[7] Aside: $\mathbb{Q}[i] = \{\, a + bi : a, b \in \mathbb{Q} \,\}$

Theorem: Let D be a PID, $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending chain of ideals I_n of D. Then for some m, $I_n = I_m$ for all $n \geq m$.
Proof: Consider $I = \bigcup_n I_n$. Then I is an ideal of D:

(1) $0 \in I_1 \subset I$

(2) If $a, b \in I$, then $a \in I_n$ and $b \in I_l$ for some n, l. Without loss of generality, $n \geq l$, in which case $I_l \subset I_n$ so $a, b \in I_n$. So $a - b \in I_n \subset I$. ✓

(3) Similarly, if $d \in D$, $a \in I$, then $a \in I_n \implies da \in I_n \subset I$ ✓

Since D is a PID, we get $I = (x)$ for some $x \in D$. But $x \in I_n$ for some n, so $I = (x) \subset I_n \subset I$, and so $I = I_n$. □

PMATH 345 Lecture 11: May 28, 2010

Theorem: Every PID is a UFD.
Proof: Recall from last time:
Theorem: Every irreducible element of a PID is prime.
Theorem: Let $I_1 \subset I_2 \subset \cdots$ be a chain of ideals in a PID. Then for some n, $I_m = I_n$ for all $m \geq n$.

Digression: Every irreducible element of a UFD is prime.
Proof: Say x is irreducible in a UFD D. We will show that (x) is a prime ideal, so x is prime.

So, assume $ab \in (x)$. Then $ab = xc$ for some $c \in D$. Factoring both sides into irreducibles gives:

$$\underbrace{(p_1 \cdots p_n)}_{a}\underbrace{(q_1 \cdots q_m)}_{b} = x\underbrace{(r_1 \cdots r_l)}_{c}$$

By uniqueness of factorization, we get $x = up_i$ or $x = uq_i$ for some $u \in D^*$ and index i.

So either $a \in (x)$ (if $x = up_i$) or $b \in (x)$ (if $x = uq_i$). Hence (x) is a prime ideal and x is prime, as desired. □

We will now show that if D is a PID, then D is a UFD. To do this, we will show that any element $a \in D$, $a \neq 0$, $a \notin D^*$, can be factored uniquely into a product of irreducibles.

Thus, choose any $a \in D$, $a \neq 0$, $a \notin D^*$. We want to find some irreducible element $p \in D$ such that $p \mid a$. Well, if a is irreducible, then we may choose $p = a$. If a is not irreducible, then we may write $a = bc$ for $b, c \in D$, $b, c \notin D^*$. If b or c are irreducible, we win. Otherwise, we get $(a) \subset (b)$ with $(b) \neq (1)$. Write $a_1 = b$.

Write $a_1 = a_2b_2$ for $a_2, b_2 \notin D^*$. Write $a_2 = a_3b_3$ for $a_3 \notin D^*$, and continue writing $a_n = a_{n+1}b_{n+1}$ with $a_{n+1} \notin D^*$, and $b_{n+1} \notin D^*$ whenever a_n is reducible. We have an ascending chain of ideals: $(a) \subset (a_1) \subset (a_2) \subset \cdots$. By ACC for PIDs, there is an n such that $(a_n) = (a_m)$ for all $m \geq n$. In particular, $(a_n) = (a_{n+1})$, where $a_n = a_{n+1}b_{n+1}$. This means $b_{n+1} \in D^*$, so a_n is irreducible, with $a_n \mid a$.

Now we'll show that a can be factored completely into irreducibles. Write $a = p_1a_1$ for irreducible $p_1 \in D$. Write $a = p_1p_2a_2$ for irreducible $p_2 \in D$ (unless $a_1 \in D^*$). Keep going until $a_n \in D^*$, at which point:

$$a = \underbrace{p_1p_2p_3 \cdots (a_np_n)}_{\text{all irreducible}}$$

To show that $a_n \in D^*$ for some n, note that $(a) \subset (a_1) \subset (a_2) \subset \cdots$ is an ascending chain of ideals. By ACC, this means $(a_n) = (a_{n+1})$ for some n, with $a_n = p_{n+1}a_{n+1}$; this is impossible! So a_n must have been a unit, and so a has been factored completely into irreducibles.

Finally, we show that this factorization is unique. Say

$$a = p_1 \cdots p_n = q_1 \cdots q_m \qquad (*)$$

for irreducibles $p_1, \ldots, p_n, q_1, \ldots, q_m \in D$. First, note that $p_1, \ldots, p_n, q_1, \ldots, q_m$ are all prime, so $p_1 \mid q_1 \cdots q_m \implies p_1 \mid q_i$ for some i. Then $q_i = p_1x$ for some $x \in D$ and $x \in D^*$ because $p_1 \notin D^*$ and q_i is irreducible. So we cancel p_1 from both sides of $(*)$:

$$p_2 \cdots p_n = q_1 \cdots \hat{q_i} \cdots q_m x$$

where the hat means q_i is not present. Keep doing this for each p_j in turn until either the p_is run out or the q_is do. If the two sets don't run out at the same step, then a nonempty product of primes would be a unit, which is impossible. So $n = m$, and so the two factorizations are the same up to permutation and multiplication by units. $\square$

PMATH 345 Lecture 12: May 31, 2010

Definition: Let D be a UFD, $p(x) \in D[x]$ any nonzero polynomial. The content of $p(x)$ is the greatest common factor of the coefficients of $p(x)$. A polynomial $p(x)$ is primitive *iff* its content is 1.

Theorem: (Gauss's Lemma)
The product of primitive polynomials is primitive. More precisely, let D be a UFD, $p(x)$, $q(x) \in D[x]$ primitive polynomials. Then $p(x)q(x)$ is primitive.
Proof: Assume $p(x)q(x)$ is not primitive. Then there is some prime l which divides all the coefficients of pq. Reducing mod l gives $p(x)q(x) \equiv 0 \bmod l$, so since l is prime, D/l is a domain, so $(D/l)[x]$ is a domain, so either $p(x) \equiv 0 \bmod l$ or $q(x) \equiv 0 \bmod l$. In other words, either l divides the content of p or l divides the content of q. Both are impossible by primitivity of $p(x)$ and $q(x)$. $\square$

Theorem: (Gauss's Lemma)
Let D be a UFD, $p(x) \in D[x]$ a nonzero polynomial. Then $p(x) = a(x)b(x)$ in $K(D)[x]$ *iff* $p(x) = A(x)B(x)$ in $D[x]$, where $A(x) = \alpha a(x)$ and $B(x) = \beta b(x)$ for some α, $\beta \in K(D)$. In particular, $p(x)$ is irreducible in $K(D)[x]$ *iff* it's irreducible in $D[x]$ (except possibly for constant factors).
Proof: Backwards is trivial.
Forwards: Say $p(x) = a(x)b(x)$ with a, $b \in K(D)[x]$. Write

$$\alpha\beta p(x) = [\alpha a(x)][\beta b(x)]$$

where αa, βb lie in $D[x]$. Factoring out the contents of αa and βb gives

$$c_3\alpha\beta p'(x) = c_1(\underbrace{\alpha' a'(x)}_{\text{primitive}})c_2(\underbrace{\beta' b'(x)}_{\text{primitive}})$$

Cancelling gives:

$$dp'(x) = [\alpha' a'(x)][\beta' b'(x)]$$

where $d \in D$ and p', $\alpha' a'$, and $\beta' b'$ are all primitive. By Gauss's Lemma, $dp'(x)$ is primitive, so $d \in D^*$ and so $p'(x) = [\alpha' d^{-1} a'(x)][\beta' b'(x)]$. Since $p(x) = c_3 p'(x)$, we get:

$$\begin{aligned} p(x) &= [c_3\alpha' d^{-1} a'(x)][\beta' b'(x)] \\ &= A(x)B(x) \end{aligned}$$

as desired. $\square$

Example: Consider $2x^2 - 5 \in (\mathbb{Z}[\sqrt{10}])[x]$. The polynomial is irreducible. However:

$$\begin{aligned} 2x^2 - 5 &= 2\big(x^2 - \tfrac{5}{2}\big) \\ &= 2\Big(x - \sqrt{\tfrac{5}{2}}\Big)\Big(x + \sqrt{\tfrac{5}{2}}\Big) \\ &= 2\big(x - \tfrac{\sqrt{10}}{2}\big)\big(x + \tfrac{\sqrt{10}}{2}\big) \end{aligned}$$

So Gauss's Lemma does *not* apply to $(\mathbb{Z}\sqrt{10})[x]$.

Example: Prove that $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.
Solution: Reducing mod 2 gives $x^2 + x + 1$, which has no roots: $0^2 + 0 + 1 \neq 0$, $1^2 + 1 + 1 \neq 0$
So $x^2 + x + 1$ can't factor in $\mathbb{Z}_2[x]$. If $x^2 + x + 1$ factored in $\mathbb{Z}[x]$, then the factorization could be reduced mod 2. So $x^2 + x + 1$ is irreducible in $\mathbb{Z}[x]$. By Gauss's Lemma, $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

PMATH 345 Lecture 13: June 2, 2010

Long division and Euclidean algorithm
Divide x^3-1 by x^2+2x-3 with remainder in $\mathbb{Z}_5$[8] $[x]$

$$
\begin{array}{r|l}
 & x-2 \\
\hline
x^2+2x-3 & x^3+0x^2+0x-1 \\
 & \underline{x^3+2x^2-3x} \\
 & -2x^2+3x-1 \\
 & \underline{-2x^2+\ \ x+1} \\
 & 2x-2
\end{array}
$$

Answer: $x^3-1=(x-2)(x^2+2x-3)+(2x-2)$

To find $\gcd(x^3-1, x^2+2x-3)$:

$$x^3-1=(x-2)(x^2+2x-3)+(2x-2)$$

$$
\begin{array}{r|l}
 & 3x-1 \\
\hline
2x-2 & x^2+2x-3 \\
 & \underline{x^2-\ \ x} \\
 & 3x-3 \\
 & \underline{3x-3} \\
 & 0
\end{array}
$$

$$x^2+2x-3=(2x-2)(3x-1)+0$$

So $\gcd(x^3-1, x^2+2x-3)=2x-2$ or $x-1$

Theorem: Let F be a field, $a(x)$, $b(x)\in F[x]$ with $b(x)\neq 0$. Then there are polynomials $q(x)$, $r(x)\in F[x]$ satisfying:

(1) $a(x)=q(x)b(x)+r(x)$

(2) $\deg(r(x))<\deg(b)$

(If $b(x)$ is constant, then (2) means $r(x)=0$.)
Proof: Not gonna do it. $\square$

Corollary: Let F be a field. Then $F[x]$ is a PID.
Proof: Let $I\subset F[x]$ be an ideal. If $I=(0)$, then it's principal. If not, then it contains a nonzero polynomial $p(x)$ of minimal degree. If $a(x)\in I$, then $a(x)=p(x)q(x)+r(x)$ where $\deg(r(x))<\deg(p(x))$. But $r(x)=a(x)-p(x)q(x)\in I$, so by minimality of $p(x)$, we get $r(x)=0$ and $a(x)\in(p(x))$. So $I\subset(p(x))$, and $p(x)\in I \implies (p(x))\subset I$, so $I=(p(x))$. $\square$

Corollary: Let F be a field, $a\in F$, $p(x)\in F[x]$ with $p(a)=0$. Then $x-a\mid p(x)$.
Proof: $p(x)=q(x)(x-a)+r(x)$ with $\deg r(x)<\deg(x-a)=1$. Plug in $x=a$ to deduce $r=0$. $\square$

Corollary: Let F be a field, $p(x)\in F[x]$ a nonzero polynomial of degree d. Then $p(x)$ has at most d roots.
Proof: Each root corresponds to a factor of $p(x)$, and $F[x]$ is a PID and hence a UFD. $\square$

If $p(x)$ has degree 3 or less, then $p(x)$ factors in $F[x]$ *iff* it has a root in F. The proof is easy.
Example: x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$ because its degree is $2\leq 3$, and $0^2+0+1\neq 0$ and $1^2+1+1\neq 0$.

Theorem: Let R be a ring, P a prime ideal of R, $p(x)\in R[x]$ a polynomial. If $p(x)$ is irreducible in $(R/P)[x]$ and if the leading coefficient of $p(x)$ doesn't lie in P, then $p(x)$ is irreducible in $R[x]$.
Proof: If $p(x)=a(x)b(x)$ in $R[x]$ with $\deg(a)$, $\deg(b)\geq 1$, then

$$p(x)\equiv a(x)b(x) \bmod P,$$

with $\deg(a)$, $\deg(b)\geq 1 \bmod P$ because $\deg(p(x))$ is the same over R/P as over R. By contrapositive, we're done. $\square$

[8] field

Example: $x^2 + x + 1$ is irreducible in $\mathbb{Z}[x]$ because it's irreducible mod 2.

Example: Is $x^3 - x + 1$ irreducible in $\mathbb{Q}[x]$?
Yes. Reducing mod 2 yields $x^3 + x + 1$, which has no roots, so $x^3 - x + 1$ is irreducible in $\mathbb{Z}_2[x]$ since deg ≤ 3, and so irreducible in $\mathbb{Z}[x]$, and by Gauss's Lemma irreducible in $\mathbb{Q}[x]$.

PMATH 345 Lecture 14: June 4, 2010

Theorem: Let D be a UFD, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$ any nonzero polynomial, $a_i \in D$. If $p(\frac{m}{l}) = 0$ for $l, m \in D$, then $l \mid a_n$ and $m \mid a_0$.

Example: Does $3x^3 + 1$ have any roots in $\mathbb{Q}$?
Answer: No. Any rational root $\frac{a}{b}$ satisfies $b \mid 3$ and $a \mid 1$, so $b \in \{\pm 1, \pm 3\}$ and $a \in \{\pm 1\}$. Without loss of generality, $b > 0$, so $b \in \{1, 3\}$. Now we check these roots:

$$3(1)^3 + 1 = 4 \neq 0$$
$$3(-1)^3 + 1 = -2 \neq 0$$
$$3(\tfrac{1}{3})^3 + 1 \neq 0$$
$$3(\tfrac{1}{3})^3 + 1 \neq 0$$

Therefore $3x^3 + 1$ has no roots in $\mathbb{Q}$. Since its degree is ≤ 3, this means it's irreducible over $\mathbb{Q}$.
Proof: Say $(\frac{m}{l}) = 0$. Then in $K(D)[x]$, we have $(x - \frac{m}{l}) \mid p(x)$, so $lx - m \mid p(x)$. By Gauss's Lemma, $p(x) = (lx - m)q(x)$ for some $q(x)$ in $D[x]$. If $q(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$, then $a_0 = -b_0 m$ and $a_n = l b_{n-1}$. □

Theorem: (Eisenstein's Criterion)
Let D be a domain, $P \subset D$ a prime ideal, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$ a nonzero polynomial satisfying:

(1) $a_i \in D$

(2) $a_i \in P$ if $i < n$

(3) $a_n \notin P$

(4) $a_0 \notin P^2$

[9]Then $f(x)$ has only constant factors in $D[x]$.

Example: Is $x^4 + 10x + 6$ irreducible over $\mathbb{Q}$?
Yes: Apply Eisenstein with $P = (2)$:

(2) 0, 0, 10, 6 all in (2)

(3) $1 \notin (2)$

(4) $6 \notin (4)$ ✓

Proof: Say $f(x) = a(x)b(x)$ in $D[x]$. Then $f(x) \equiv a(x)b(x)$ in $(D/P)[x]$.

$$\implies a(x)b(x) \equiv a_n x^n \bmod P$$

Since (D/P) is a domain, it has a fraction field K, and $K[x]$ is a UFD. So both $a(x)$ and $b(x)$ are both constant multiples of a power of x mod P.

If $a(x)$ and $b(x)$ are both not constant, then their constant coefficients are both 0 mod P. This would mean that both coefficients lie in P, so

$$a_0 = (\text{constant coefficient of } a(x)) \cdot (\text{constant coefficient of } b(x))$$

would lie in P^2. This is a contradiction, and so $f(x)$ has only constant factors, as desired. □

[9]Aside: $P = (x_1, \ldots, x_n) \implies P^2 = (x_i x_j)_{i,j \in \{1,\ldots,n\}}$ In particular $(x)^2 = (x^2)$

Corollary: If $f(x)$ satisfies the hypothesis of Eisenstein's Criterion and D is a UFD, then $f(x)$ is irreducible in $K(D)[x]$.
Proof: Gauss's Lemma. $\square$

Corollary: If $f(x)$ is monic (leading coefficient is one) and satisfies the hypotheses of Eisenstein's Criterion, then $f(x)$ is irreducible in $D[x]$.
Proof: Immediate. $\square$

Example: Is $x^3y + xy^3 - x + y - 1$ irreducible in $\mathbb{C}[x, y]$?
Yes: Apply Eisenstein's Criterion to $D = \mathbb{C}[y]$ and $P = (y - 1)$.
Write $x^3y + xy^3 - x + y - 1$
$= y^{10)}x^3 + (y^3 - 1)^{11)}x + (y - 1)^{12)}$

So, by Eisenstein's Criterion, $x^3y+xy^3-x+y-1$ has only constant factors; namely, factors lying in $D = \mathbb{C}[y]$. But y and $y - 1$ are both coefficients are relatively prime, so there are no nontrivial constant factors either.

PMATH 345 Lecture 15: June 7, 2010

Definition: A ring R is Noetharian *iff* every ideal of R is finitely generated. That is, R is Noetharian *iff* every ideal I of R can be written in the form $I = (r_1, \ldots, r_n)$ for some $r_1, \ldots, r_n \in R$.

Theorem: A ring R is Noetharian *iff* it satisfies the Ascending Chain Condition.
Proof: Forwards: Say R is Noetharian, and let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of ideals. We want to show that there is an index n such that $I_n = I_m$ for all $m \geq n$.

We've already seen that $I = \bigcup_k I_k$ is an ideal, so since R is Noetharian, $I = (r_1, \ldots, r_m)$ for some $r_1, \ldots, r_m \in R$. For each i, $r_i \in I$ implies $r_i \in I_m$, for some m_i.

If $n = \max\{m_i\}$, then $r_i \in I_n$ for all i. So $I = (r_1, \ldots, r_m) \subset I_n \subset I$, and therefore $I = I_n$ and $I_m = I_n$ for all $m \geq n$.

Backwards: We'll skip. $\square$

Theorem: (Hilbert Basis Theorem) Let R be a Noetharian ring. Then $R[x]$ is also Noetharian.
Remarks: Every field is Noetharian, as is every PID. By induction, HBT implies that $F[x_1, \ldots, x_n]$ is Noetharian for every field F.
Proof: Let $I \subset R[x]$ be any ideal. We want to find a finite set of elements $f_1, \ldots, f_n \in R[x]$ such that $I = (f_1, \ldots, f_n)$. Let $L =$ set of leading coefficients of elements of I (leading coefficient of 0 is 0).

Claim: L is an ideal of R.
Proof:

(1) $0 \in L$ ✓

(2) Say $l_1, l_2 \in L$. Let $f_1, f_2 \in I$ have leading coefficients l_1, l_2 respectively. If $\deg f_1 \geq \deg f_2$, then $f_1 - x^{\deg f_1 - \deg f_2} f_2$ is in I and has leading coefficient $l_1 - l_2$, so $l_1 - l_2 \in L$. Otherwise, $x^{\deg f_2 - \deg f_1} f_1 - f_2$ will do.

(3) Say $l \in L$, $r \in R$, $f \in I$ with leading coefficient l. Then rf has leading coefficient lr, so $lr \in L$. $\square$

Since R is Noetharian, we get $L = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in R$. Let $f_1, \ldots, f_n \in I$ have leading coefficients $a_1, \ldots, a_n$, respectively. For each integer $d \geq 0$, define

$$L_d = \{\text{set of leading cofficients of elements of } I \text{ of degree } d\} \cup \{0\}$$

It turns out (by a proof similar to Claim's) that L_d is an ideal of R, so we can write $L_d = (b_{d,1}, \ldots, b_{d,n_d})$ for some $b_{d,i} \in R$. Let $f_{d,i} \in I$ have leading coefficient $b_{d,i}$, with $\deg f_{d,i} = d$.
Let $N = \max\{\deg f_i\}$.

10) not in $(y - 1)$
11) in $(y - 1)$
12) in $(y - 1)$ but not $(y - 1)^2$

Claim: I is generated by $f_1, \ldots, f_n$ and $f_{d,i}$ for $d_i \le N$.
Proof of claim: It's clear that every f_i and $f_{d,i}$ is contained in I, so it suffices to show that every element of I can be written in terms of f_i and $f_{d,i}$.

Assume $f \in I$ is the element of smallest degree that cannot be written as an $R[x]$-linear combination of the f_i and $f_{d,i}$. ($d = \deg f$)

Case I: $\deg f \ge N$. Let $a =$ leading coefficient of f. Since $a \in L$, we can write $a = r_1 a_1 + \cdots + r_n a_n$ for some $r_i \in R$. So $f - r_1 x^{d-\deg f_1} f_1 - \cdots - r_n x^{d - \deg f_n} f_n = g$ has degree less than d, and is nonzero by construction of f. This implies that g cannot be written as an $R[x]$-linear combination of f_i and $f_{d,i}$, which contradicts minimality of f.

Case II: $\deg f < N$. Then $a \in L_d$ for $\deg f = d < N$, so the Case I argument applies to L_d instead of L. By contradiction, we're done. $\square$

PMATH 345 Lecture 16: June 9, 2010

Office Hours
Thursday 1:30–3:30

Theorem: Let R be Noetharian, $I \subset R$ any ideal. Then R/I is Noetharian.
Proof: Let J be any ideal of R/I. We want to show that $J = (r_1, \ldots, r_n)$ for some elements $r_i \in R/I$. Let $q\colon R \to R/I$ be the quotient homomorphism, and let $A = q^{-1}(J) = \{ r \in R : r \in J \bmod I \}$. Then A is an ideal of R, which is a Noetharian ring, so $A = (r_1, \ldots, r_n)$ for some $r_1, \ldots, r_n \in R$.

Claim: $J = (\overline{r_1}, \ldots, \overline{r_n})$, where $\overline{r_i} = r_i \bmod I$.
Proof of claim: Say $a \in J$. Then there is some $r \in A$ such that $q(r) = a$. So we can write

$$r = \alpha_1 r_1 + \alpha_2 r_2 + \cdots + \alpha_n r_n$$

for some $\alpha_1, \ldots, \alpha_n \in R$, so:

$$\begin{aligned} a &= \overline{\alpha_1 r_1} + \cdots + \overline{\alpha_n r_n} \bmod I \\ &\in (\overline{r_1}, \ldots, \overline{r_n}) \quad \square \end{aligned}$$

Corollary: Let R be any Noetharian ring (e.g., a field, or $\mathbb{Z}$). Then for any ideal I of R, the ring

$$R[x_1, \ldots, x_n]/I$$

is Noetharian.

[13]**Definition:** A monomial ordering on the set of monomials $\{ x_1^{a_1} \cdots x_n^{a_n} : a_i \in \mathbb{Z}_{\ge 0} \}$ is a partial ordering $\le$ satisfying:

(1) It must be a total order: for any two monomials m_1 and m_2, either $m_1 \le m_2$ or $m_1 \ge m_2$. If both hold, then $m_1 = m_2$.

(2) It must be a well ordering: there are no infinite descending sequences of monomials.

(3) Given monomials m_1, m_2, m_3 with $m_1 \le m_2$, then $m_1 m_3 \le m_2 m_3$.

Example: Lexicographic order:

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} > x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$$

iff $a_1 > b_1$
or $a_1 = b_1$ and $a_2 > b_2$
or $a_1 = b_1$, $a_2 = b_2$, and $a_3 > b_3$

[13] Aside: Ideals, Varieties, and Algorithms: Cox, Little, O'Shea

$\vdots$
or $a_i = b_i \; \forall i < n$ and $a_n > b_n$

$$x_1^2 x_2 > x_1 x_2^2 \qquad x_1^2 x_2{}^{[14]} - x_2^2 x_1$$
$$x_1^2 x_2 < x_1^2 x_2^2$$
$$x_1 x_2^{7917} < x_1^2 x_2$$
$$a^2 > a$$

Definition: Let $p(x_1, \ldots, x_n)$ be a polynomial. The leading monomial of p is the "biggest" monomial with a nonzero coefficient. The leading coefficient is the coefficient of the leading monomial. The leading term is (leading coefficient)(leading monomial). The multidegree of a monomial $x_1^{a_1} \cdots a_n^{a_n}$ is $(a_1, \ldots, a_n)$. The multidegree of p is the multidegree of its leading monomial.

PMATH 345 Lecture 17: June 14, 2010

Long division helps with:
Telling if $p(x) \in (q(x))$.
Finding $\gcd(p(x), q(x))$.

In many variables:
Tell if $p(x_1, \ldots, x_n) \in (f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n))$
Find a "good" set of generators for $(f_1, \ldots, f_r)$.

Example: Divide $x^2y + xy^2 + y^2$ by $\{xy - 1, y^2 - 1\}$. (Use lex order with $x > y$.) long division

$$\begin{array}{rl} & x + y,\ 1 \\ xy-1,\ y^2-1 \,\big) & x^2y + xy^2 + y^2 \\ & \underline{x^2y - x} \\ & xy^2 + x + y^2 \\ & \underline{xy^2 - y} \\ & \not{x}\nearrow + y^2 + y \\ & \underline{y^2 - 1} \\ & \not{y}\nearrow + \not{1}\nearrow \end{array} \qquad \begin{array}{c} \underline{\text{Remainder}} \\ x \quad y \quad 1 \end{array}$$

$$\therefore\ x^2y + xy^2 + y^2 = (x+y)^{[15]}(xy-1) + (1)^{[16]}(y^2-1) + (x+y+1)^{[17]}$$

Example: Same as before:

$$\begin{array}{rl} & x + 1,\ x \\ y^2-1,\ xy-1 \,\big) & x^2y + xy^2 + y^2 \\ & \underline{x^2y - x} \\ & xy^2 + x + y^2 \\ & \underline{xy^2 - x} \\ & \not{2x}\nearrow + y^2 \\ & \underline{y^2 - 1} \\ & \not{1}\nearrow \end{array} \qquad \begin{array}{c} \underline{\text{Remainder}} \\ 2x \quad 1 \end{array}$$

$$x^2y + xy^2 + y^2 = (x+1)^{[18]}(y^2-1) + (x)^{[19]}(xy-1) + (2x+1)^{[20]}$$

Theorem: Let $f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$ where F is a field, $f_1, \ldots, f_s$ not all the zero polynomial. Then

[14] leading term
[15] coefficient of $xy - 1$
[16] coefficient of $y^2 - 1$
[17] remainder
[18] coefficient of $y^2 - 1$
[19] coefficient of $xy - 1$
[20] remainder

every $f \in F[x_1, \dots, x_n]$ can be written as:

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

where a_i, $r \in F[x_1, \dots, x_n]$, every term in r not divisible by *any* $\mathrm{LT}(f_i)$. If $a_i f_i \neq 0$, then $\mathrm{multideg}(a_i f_i) \leq \mathrm{multideg}(f)$.
Proof: In Papantonopoulou. □

Let I be an ideal of $F[x_1, \dots, x_n]$.
Define $\mathrm{LT}(I) =$ ideal generated by $\{\, \mathrm{LT}(f) : f \in I \,\}$.
Fact: If $I = (f_1, \dots, f_r)$, then

$$\mathrm{LT}(I) \neq (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_r))$$

unless the f_i are carefully chosen.

Definition: Let $I = (f_1, \dots, f_r)$ be an ideal of $F[x_1, \dots, x_n]$. Then $\{f_1, \dots, f_r\}$ is a Gröbner basis for I *iff* $\mathrm{LT}(I) = (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_r))$.

PMATH 345 Lecture 18: June 16, 2010

Definition: Let $f_1, \dots, f_r \in E[x_1, \dots, x_n]$ be any set of polynomials. Then $\{f_1, \dots, f_r\}$ is a Gröbner basis for $I = (f_1, \dots, f_r)$ *iff*

$$\mathrm{LT}(I) = (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_r)).$$

In other words, any monomial m that is divisible by $\mathrm{LT}(g)$ for some $g \in I$ is divisible by some $\mathrm{LT}(f_i)$.

Theorem: If $\mathrm{LT}(I) = (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_r))$ and $f_1, \dots, f_r \in I$, then $I = (f_1, \dots, f_r)$.
Proof: Since $f_1, \dots, f_r \in I$, it follows immediately that $(f_1, \dots, f_r) \subset I$. So it suffices to show $I \subset (f_1, \dots, f_r)$. Let $g \in I$, and divide g by $\{f_1, \dots, f_r\}$. By the Division Theorem, we get:

$$g = a_1 f_1 + \cdots + a_r f_r + t$$

where t is the remainder, whose terms are all *not* divisible by any $(\mathrm{LT}(f_i))$. But $t \in I$, so $\mathrm{LT}(t) \in \mathrm{LT}(I) = (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_r))$. This immediately implies $t = 0$ so $g \in (f_1, \dots, f_r)$. □

Do Gröbner bases exist? Yes!
Theorem: Let $I \subset F[x_1, \dots, x_n]$ be an ideal. Then there is a Gröbner basis for I.
Proof: Consider $\mathrm{LT}(I)$, which is generated by an infinite collection of monomials:

$$\mathcal{M} = \{\, \mathrm{LT}(f) : f \in I \,\}$$

Notice that $\mathrm{LT}(I)$ is also generated by the set of leading monomials of elements of I:

$$\mathcal{L} = \{\, \mathrm{LM}(f) : f \in I \,\}$$

The set $\mathcal{L}$ is countably infinite, since each monomial $x_1^{a_1} \cdots x_n^{a_n}$ corresponding uniquely to $(a_1, \dots, a_n) \in \mathbb{Z}^n$. Therefore, we can enumerate the monomials in $\mathcal{L}$:

$$m_1, m_2, m_3, \dots$$

Define $I_j = (m_1, \dots, m_j)$

$$I_1 \subset I_2 \subset I_3 \subset I_4 \subset \cdots$$

So by ACC, this chain stabilizes at some finite step v, so:

$$\begin{aligned} \mathrm{LT}(I) &= \bigcup_{j=1}^{\infty} I_j = I_v \\ &= (m_1, \dots, m_v) \\ &= (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_v)) \end{aligned}$$

for some $f_1, \ldots, f_v \in I$. $\square$

Theorem: Let $\{f_1, \ldots, f_t\}$ be a Gröbner basis (for $I = (f_1, \ldots, f_t) \neq (0)$), $f \in F[x_1, \ldots, x_n]$. Then there exists a unique $r \in F[x_1, \ldots, x_n]$ such that

$$f = a_1 f_1 + \cdots + a_t f_t + r$$

for some $a_1, \ldots, a_t \in F[x_1, \ldots, x_n]$, and no term of r is divisible by any $\mathrm{LT}(f_i)$.
Proof: Say:

$$a_1 f_1 + \cdots + a_t f_t + r = a_1' f_1 + \cdots + a_t' f_t + r'$$

Then:

$$(a_1 - a_1')f_1 + \cdots + (a_t - a_t')f_t = r' - r$$

So $\mathrm{LT}(r' - r) \in \mathrm{LT}(I) = (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t))$. But r' and r aren't allowed to have any terms divisible by any $\mathrm{LT}(f_i)$, so $r' - r$ has no terms and is therefore 0. So $r' = r$. $\square$
Corollary: Let $f \in F[x_1, \ldots, x_n]$ be any polynomial, I any nonzero ideal, $f_1, \ldots, f_t$ a Gröbner basis for I. Then $f \in I$ *iff* f divided by $\{f_1, \ldots, f_t\}$ gives zero remainder.
Proof: Immediate. $\square$

Definition: Let $f, g \in F[x_1, \ldots, x_n]$ be any nonzero polynomials. Then

$$S(f, g) = \Big(\frac{\mathrm{LCM}}{\mathrm{LT}(f)}\Big) f - \Big(\frac{\mathrm{LCM}}{\mathrm{LT}(g)}\Big) g$$

where $\mathrm{LCM} = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$.

$$\begin{aligned} f &= 3x^2 - 2 & g &= -xy + 1 \\ \mathrm{LT}(f) &= 3x^2 & \mathrm{LT}(g) &= -xy \\ \mathrm{LM}(f) &= x^2 & \mathrm{LM}(g) &= xy \end{aligned}$$

$$\mathrm{LCM} = x^2 y$$

$$\begin{aligned} \implies S(f, g) &= \frac{x^2 y}{3x^2}(3x^2 - 2) - \frac{x^2 y}{-xy}(-xy + 1) \\ &= \tfrac{1}{3} y(3x^2 - 2) - (-x)(-xy + 1) \\ &= (x^2 y - \tfrac{2}{3} y) - (x^2 y - x) \\ &= x - \tfrac{2}{3} y \end{aligned}$$

PMATH 345 Lecture 19: June 18, 2010

How can one tell if $\{g_1, \ldots, g_r\}$ is a Gröbner basis?
Definition: Let $f, g \in F[x_1, \ldots, x_n]$ be two nonzero polynomials. Then:

$$S(f, g) = \Big(\frac{\mathrm{LCM}}{\mathrm{LT}(f)}\Big) f - \Big(\frac{\mathrm{LCM}}{\mathrm{LT}(g)}\Big) g$$

where $\mathrm{LCM} = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$.

Theorem: (Buchberger's Criterion) Say $I = (f_1, \ldots, f_r)$ is an ideal of $F[x_1, \ldots, x_n]$. Then $\{f_1, \ldots, f_r\}$ is a Gröbner basis for I *iff* for all i, j, $S(f_i, f_j)$ gives zero remainder upon division by $\{f_1, \ldots, f_r\}$.
Proof: Forwards is trivial. Backwards is too hard. $\square$

Example: Is $\{xy - 1, y^2 - 1\}$ a Gröbner basis? By Buchberger's Criterion:

$$\begin{aligned} S(xy - 1, y^2 - 1) &= y(xy - 1) - x(y^2 - 1) \\ &= xy^2 - y - xy^2 + x \\ &= x - y \end{aligned}$$

Clearly, a long division of $x - y$ by $\{xy - 1, y^2 - 1\}$ yields a remainder of $x - y$. Since this is nonzero, we conclude that $\{xy - 1, y^2 - 1\}$ is not a Gröbner basis.

Theorem: (Buchberger's Algorithm) One can compute a Gröbner basis for $I = (f_1, \dots, f_r)$ by the following method:

(1) Compute $S(f_i, f_j)$ and divide it by $\{f_1, \dots, f_r\}$ for each i, j

(2) If all remainders are zero, STOP; you have a Gröbner basis.

(3) Otherwise, enlarge the set $\{f_1, \dots, f_r\}$ by the nonzero remainders, and return to step (1).

Proof: This algorithm terminates because the ideal generated by $\{\mathrm{LT}(f_i)\}$ strictly increases at each iteration, so by the ACC, the set of nonzero remainders must eventually be empty. When this happens, Buchberger's Criterion implies that $\{f_i\}$ is a Gröbner basis. $\square$

Example: Find a Gröbner basis of $(xy - 1, y^2 - 1)$.

$$S(xy - 1, y^2 - 1) = x - y$$

This gives remainder $x - y$, so:

$$\begin{aligned} &\{xy - 1, y^2 - 1, x - y\} \\ S(xy - 1, x - y) &= 1(xy - 1) - y(x - y) \\ &= xy - 1 - xy + y^2 \\ &= y^2 - 1 \end{aligned}$$

This clearly gives remainder 0, so we just need to check:

$$\begin{aligned} S(y^2 - 1, x - y) &= x(y^2 - 1) - y^2(x - y) \\ &= xy^2 - x - xy^2 + y^3 \\ &= -x + y^3 \end{aligned}$$

Long divide:

$$\begin{array}{r@{}l} & \;\;0,\ y,\ -1 \\ \cline{2-2} xy - 1,\ y^2 - 1,\ x - y \big) & -x + y^3 \\ & \underline{-x + \ \ y} \\ & \qquad y^3 - y \\ & \qquad \underline{y^3 - y} \\ & \qquad\qquad 0 \end{array}$$

Zero remainder of all S-polynomials implies (by Buchberger) that $\{xy - 1, y^2 - 1, x - y\}$ is a Gröbner basis.

Notice that $\mathrm{LT}(x - y) \mid \mathrm{LT}(xy - 1)$ so:

$$(\mathrm{LT}(xy - 1), \mathrm{LT}(y^2 - 1), \mathrm{LT}(x - y)) = (\mathrm{LT}(y^2 - 1), \mathrm{LT}(x - y)) = \mathrm{LT}(xy - 1, y^2 - 1)$$

Therefore, *since* $\{xy - 1, y^2 - 1, x - y\}$ *is a Gröbner basis*, we see that $\{x - y, y^2 - 1\}$ is also a Gröbner basis.

Any subset of I that contains a Gröbner basis for I is itself a Gröbner basis for I.

Definition: Let $I \subset F[x_1, \dots, x_n]$ be a nonzero ideal. Then $\{f_1, \dots, f_r\}$ is a minimal Gröbner basis for I *iff*

(1) $\{f_1, \dots, f_r\}$ is a Gröbner basis for I

(2) $\mathrm{LC}(f_i) = 1$ for all i

(3) $\mathrm{LT}(f_i) \nmid \mathrm{LT}(f_j)$ for $i \neq j$
$\iff$ $\mathrm{LT}(f_i) \notin (\mathrm{LT}(f_j))_{j \neq i}$

Example: $\{xy-1, y^2-1, x-y\}$ is not minimal, because $\mathrm{LT}(x-y) \mid \mathrm{LT}(xy-1)$. By deleting f_i whose leading terms are redundant (*i.e.,* divisible by some other leading term), we can always construct a minimal Gröbner basis from an arbitrary one. Since Gröbner bases always exist, therefore, so do minimal Gröbner bases.

Example: $\{y^2-1, x-y\}$ is a minimal Gröbner basis. So is $\{y^2-1, x-y+\frac{1}{17}(y^2-1)\}$.

PMATH 345 Lecture 20: June 21, 2010

Definition: A set $\{f_1, \ldots, f_r\} \subset F[x_1, \ldots, x_n]$ is a Gröbner basis *iff*

$$\mathrm{LT}(f_1, \ldots, f_r) = (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r))$$

Definition: A Gröbner basis $\{f_1, \ldots, f_r\}$ is minimal *iff* every f_i has leading coefficient 1 and $\mathrm{LT}(f_i) \nmid \mathrm{LT}(f_j)$ if $i \neq j$.

Theorem: Any two minimal Gröbner bases for the same ideal have the same number of elements.
Proof: Let $\{f_1, \ldots, f_r\}$ and $\{g_1, \ldots, g_t\}$ be two minimal Gröbner bases for the ideal $I = (f_1, \ldots, f_r) = (g_1, \ldots, g_t)$. We want to show $r = t$. Let $f_i \in \{f_1, \ldots, f_r\}$ be any element. Then there is some g_j such that $\mathrm{LT}(g_j) \mid \mathrm{LT}(f_i)$, since $\mathrm{LT}(f_i)$ is not in the (zero) remainder left upon division of f_i by $\{g_1, \ldots, g_t\}$. Similarly, some f_k satisfies $\mathrm{LT}(f_k) \mid \mathrm{LT}(g_j)$. So $\mathrm{LT}(f_k) \mid \mathrm{LT}(f_i)$. Then minimality of $\{f_1, \ldots, f_r\}$ implies $i = k$, and so $\mathrm{LT}(f_i) = \mathrm{LT}(g_j)$. Since all the leading terms of the f_is are different, and similarly for the g_js, we've just built a bijection between the f_is and g_js. $\square$

Definition: A Gröbner basis $\{f_1, \ldots, f_r\}$ is reduced *iff* it is minimal and no term of any f_i is divisible by $\mathrm{LT}(f_j)$ for $i \neq j$.

Example: $\{x-y, y^2-1\}$ is reduced.
$\{x-y^2-y+1, y^2-1\}$ is not reduced.

To find a reduced Gröbner basis, first find a minimal one $\{f_1, \ldots, f_r\}$. For each i, replace f_i by its remainder upon division by $\{f_1, \ldots, \hat{f}_i, \ldots, f_r\}$.

Theorem: Any nonzero ideal $I \subset F[x_1, \ldots, x_n]$ has a unique reduced Gröbner basis.
Proof: Say $\{g_1, \ldots, g_r\}$ and $\{g'_1, \ldots, g'_r\}$ are reduced Gröbner bases for $I = (g_1, \ldots, g_r) = (g'_1, \ldots, g'_r)$. For any g_i, let g'_j be the element such that $\mathrm{LT}(g_i) = \mathrm{LT}(g'_j)$.

The element $g_i - g'_j$ has no terms divisible by *any* $\mathrm{LT}(g_k)$ (because $\mathrm{LT}(g_i)$ is cancelled by $\mathrm{LT}(g'_j)$). But $g_i - g'_j \in I$, so $g_i - g'_j = 0$, and so $g_i = g'_j$. $\square$

Let F be a field, $F[x]$ the polynomial ring in one variable. Then F has two ideals: (0) and (1), and every nonzero element of F is a unit.

Fact: Let R be a nonzero ring. F a field. Then every homomorphism from $F \to R$ is 1–1.

$F[x]$ is a PID, so it's also a UFD. Every ideal of $F[x]$ is of the form $I = (p(x))$ for some $p(x) \in F[x]$. The ideal $(p(x))$ is maximal *iff* $p(x)$ is irreducible, and prime *iff* $p(x)$ is irreducible or zero.

What does $F[x]/(p(x))$ look like?

Theorem: (Chinese Remainder) Let $p(x)$, $q(x) \in F[x]$ be coprime polynomials. Then:

$$\phi\colon F[x]/(pq) \to F[x]/(p) \oplus F[x]/(q)$$

given by $\phi(a(x) \bmod pq) = (a(x) \bmod p, a(x) \bmod q)$ is an isomorphism.
Proof: ϕ is clearly a homomorphism.
1–1: Say $a(x) \equiv b(x) \bmod p$ and $a(x) \equiv b(x) \bmod q$. We want to show

$$a(x) \equiv b(x) \bmod pq.$$

Since $p \mid a-b$ and $q \mid a-b$, the fact that p, q are coprime and $F[x]$ is a UFD $\implies pq \mid a-b$, so

$$a(x) \equiv b(x) \bmod pq.$$

Onto: Say $f(x)$, $g(x)$ are any elements of $F[x]$. We want to find a single $h(x) \in F[x]$ satisfying $\phi(h(x) \bmod pq) = (f(x) \bmod p, g(x) \bmod q)$:

$$h(x) \equiv f(x) \bmod p$$
$$h(x) \equiv g(x) \bmod q$$

Since p, q coprime, there are $a(x)$, $b(x) \in F[x]$ such that:

$$a(x)p(x) + b(x)q(x) = 1.$$

PMATH 345 Lecture 21: June 23, 2010

Theorem: (Chinese Remainder) Let F be a field, $p(x)$, $q(x) \in F[x]$ coprime polynomials. Then the function:

$$\phi\colon F[x]/(pq) \to F[x]/(p) \oplus F[x]/(q)$$

given by

$$(a(x) \bmod pq) \mapsto (a(x) \bmod p, a(x) \bmod q)$$

is an isomorphism.
Proof: (Continued) To show that ϕ is onto, we first note that since $F[x]$ is a PID, and since p, q are coprime, we get $(p(x), q(x)) = (1)$. In other words, there are $a(x)$, $b(x) \in F[x]$ such that

$$a(x)p(x) + b(x)q(x) = 1.$$

Now let $f(x)$, $g(x) \in F[x]$ be any polynomials. We want to find $h(x) \in F[x]$ such that

$$h(x) \equiv f(x) \bmod p$$
$$h(x) \equiv g(x) \bmod q$$

Let $h(x) = f(x)b(x)q(x) + g(x)a(x)p(x)$. Then

$$h(x) \equiv f(x) \bmod p$$
$$\text{and} \qquad h(x) \equiv g(x) \bmod q$$

So $\phi(h(x) \bmod pq) = (f(x) \bmod p, g(x) \bmod q)$, as desired. □

In light of the CRT, to understand $F[x]/(f(x))$, it suffices to understand

$$F[x]/(p(x)^a)$$

for irreducible polynomials $p(x)$. We will study $F[x]/(p(x))$ for irreducible $p(x)$. Note that $F[x]/(p(x))$ is a field *iff* $p(x)$ is irreducible in $F[x]$.

Linear Algebra over general fields.
Non-definition: A vector space over a field F is a set V of "vectors" that you can add, subtract, and multiply by scalars in a sensible way.

Spanning, linear independence, basis, dimension, linear transformation, kernel, range, eigenstuff… they all have the same definitions and properties over a general field as they do over, say, $\mathbb{R}$.

Note that if F is a field and R is any ring with $F \subset R$, then R is an F-vector space.

In particular, $F[x]/(p(x))$ is an F-vector space.

$$F \hookrightarrow F[x]/(p)$$
$$\alpha \mapsto (\alpha \bmod p)$$

Theorem: Let F be a field, $p(x) \in F[x]$ any polynomial. If $p(x) = 0$, then $\dim_F F[x]/(p(x)) = \infty$. Otherwise, $\dim_F F[x]/(p(x)) = \deg(p(x))$.

Proof: If $p(x) = 0$, then $F[x]/(0) = F[x]$, which contains the infinite linearly independent set $\{1, x, x^2, x^3, \ldots\}$. Now assume $p(x) \neq 0$. Then by the Division Theorem, for any $f(x) \in F[x]$, we can write:

$$f(x) = q(x)p(x) + r(x)$$

where $q(x)$, $r(x) \in F[x]$, and $\deg(r(x)) < \deg(p(x))$. Better yet, $r(x)$ is unique!

So $F[x]/(p(x))$ is in 1–1 correspondence with $\{\, r(x) : \deg(r) < \deg(p) \,\}$. Furthermore, this correspondence respects addition and scalar multiplication, but not multiplication (unless you reduce the result mod $p(x)$ again).

In particular, $F[x]/(p(x))$ is isomorphic as an F-vector space to:

$$V = \{\, r(x) : \deg(r(x)) < \deg(p(x)) \,\}$$

A basis for V is

$$\{1, x, x^2, \ldots, x^{\deg p - 1}\}$$

so $\dim_F F[x]/(p(x)) = \deg(p(x))$ as desired. □

Example: $\dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^2 - 1) = 2$

$$(a + bx)(c + dx) = (ac + bd) + (ad + bc)x$$

Basis: $\{1, x\}$

Example: $\dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^2 - 2) = 2$

$$(a + bx)(c + dx) = (ac + 2bd) + (ad + bc)x$$

Basis: $\{1, x\}$.

These two rings are *not* isomorphic, but the two $\mathbb{Q}$-vector spaces are.

PMATH 345 Lecture 22: June 25, 2010

Say R is a ring, contained in another ring T. Let $\alpha \in T$. Then:

$$R[\alpha] = \{\, f(\alpha) : f(x) \in R[x] \,\}^{21)}$$

Example:

$$\begin{aligned} \mathbb{Z}[\sqrt{2}] &= \{\, f(\sqrt{2}) : f(x) \in \mathbb{Z}[x] \,\} \\ &= \{\, a + b\sqrt{2} : a, b \in \mathbb{Z} \,\} \end{aligned}$$

Say F is a field, contained in some other field E. Let $\alpha \in E$. Then:

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[x],\ g(\alpha) \neq 0 \right\}$$

Example:

$$\begin{aligned} \mathbb{Q}(\sqrt{2}) &= \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} : f, g \in \mathbb{Q}[x],\ g(\sqrt{2}) \neq 0 \right\} \\ &= \left\{ \frac{a + b\sqrt{2}}{c + d\sqrt{2}} : c + d\sqrt{2} \neq 0,\ a, b, c, d \in \mathbb{Q} \right\} \\ &= \left\{ \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} : a, b, c, d \in \mathbb{Q},\ c + d\sqrt{2} \neq 0 \right\} \\ &= \left\{ \begin{pmatrix} \text{Messy} \\ \text{rational} \\ \text{number} \end{pmatrix} + \begin{pmatrix} \text{Other messy} \\ \text{rational} \\ \text{number} \end{pmatrix} \sqrt{2} \right\} \end{aligned}$$

21) ring

so $\mathbb{Q}(\sqrt{2}) \subset \{ A + B\sqrt{2} : A, B \in \mathbb{Q} \}$. It's clear that $A + B\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ for all A, $B \in \mathbb{Q}$, so:

$$\begin{aligned}\mathbb{Q}(\sqrt{2}) &= \{ A + B\sqrt{2} : A, B \in \mathbb{Q} \} \\ &= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}\} \\ \mathbb{Q}[\sqrt{2}] &= \{ f(\sqrt{2}) : f(x) \in \mathbb{Q}[x] \} \\ &= \{ A + B\sqrt{2} : A, B \in \mathbb{Q} \} \\ &= \mathbb{Q}(\sqrt{2})\end{aligned}$$

Definition: A field extension E/F is a pair of fields E, F with $F \subset E$. If $\alpha \in E$, then α is algebraic over F *iff* there is some nonzero $p(x) \in F[x]$ such that $p(\alpha) = 0$. Otherwise, α is called transcendental over F.

An extension E/F is called algebraic *iff* every element $\alpha \in E$ is algebraic over F. Otherwise, E/F is called transcendental.

If E/F is an extension of fields, then E is an F-vector space. The dimension of E over F is called the *degree* of E/F.

$$[E : F] = \dim_F E = \text{dimension of } E \text{ as an } F\text{-vector space}$$

Example: $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, basis $\{1, \sqrt{2}\}$
$[\mathbb{C} : \mathbb{R}] = 2$
$[\mathbb{R} : \mathbb{Q}] = \infty$
The degree of α over F is the degree of $F(\alpha)$ over F.

Theorem: Let E/F be a field extension, $\alpha \in E$ algebraic over F. Then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that

$$F(\alpha) \cong F[x]/(p(x))$$

where the isomorphism is given by

$$(f(x) \bmod p(x)) \mapsto f(\alpha)$$

Proof: Define $\phi\colon F[x] \to E$ by $\phi(f(x)) = f(\alpha)$. The kernel of ϕ is an ideal of $F[x]$, which is a PID, so we can write $\ker\phi = (p(x))$ for some polynomial $p(x) \in F[x]$. Since α is algebraic over F, $\ker\phi \neq (0)$, so $p(x) \neq 0$. There is a unique monic $p(x)$ that generates $\ker\phi$; choose that one.

Now, E is a domain, so $\operatorname{im}\phi$ is a domain, so $F[x]/\ker\phi \cong \operatorname{im}\phi$ is a domain, so $\ker\phi = (p(x))$ is a prime ideal. Since $\ker\phi \neq (0)$ and $F[x]$ is a PID, we know that $(p(x))$ is a maximal ideal, so $p(x)$ is irreducible in $F[x]$.

It remains only to show that $F(\alpha) = \operatorname{im}\phi$. First, note that $\operatorname{im}\phi$ is a field that contains α, so $F(\alpha) \subset \operatorname{im}\phi$, because $\operatorname{im}\phi$ is closed under $+$, $-$, $\cdot$, and $\div$. The definitions of $F(\alpha)$ and ϕ immediately imply that $\operatorname{im}\phi \subset F(\alpha)$, so $\operatorname{im}\phi = F(\alpha)$, as desired. $\square$

PMATH 345 Lecture 23: June 28, 2010

Let E/F be a field extension, $\alpha \in E$, α algebraic over F. Then $F(\alpha) \cong F[x]/(p(x))$, where $p(x)$ is a unique, monic, irreducible polynomial in $F[x]$. The polynomial $p(x)$ is called the minimal polynomial for α over F.

Note that this fact immediately implies that:

$$[F(\alpha) : F] = \deg_F F(\alpha) = \deg(p),$$

and that a basis for $F(\alpha)/F$ is $\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(p)-1}\}$.

Theorem: Let α be algebraic over F, $p(x) \in F[x]$ the minimal polynomial for α/F. If $q(x) \in F[x]$ satisfies $q(\alpha) = 0$, then $p(x) \mid q(x)$. In particular, if $q(\alpha) = 0$, $q(x) \in F[x]$, $q(x)$ monic and irreducible, then $q(x) = p(x)$.
Proof: We may write $q(x) = a(x)p(x) + r(x)$ where $\deg(r(x)) < \deg(p(x))$. Then:

$$r(\alpha) = q(\alpha) - a(\alpha)p(\alpha) = 0$$

so $r(x) \in$ kernel of "plug in α" homomorphism. This kernel is, by definition of the minimal polynomial, just $(p(x))$. Since $\deg(r) < \deg(p)$, this means that $r(x) = 0$, and $p(x) \mid q(x)$. $\square$

Theorem: Let α be algebraic over F, $p(x)$ the polynomial for α/F. Then $p(x)$ is the monic, nonzero polynomial in $F[x]$ of smallest degree such that $p(\alpha) = 0$.
Proof: By definition, $(p(x)) = \ker(\text{plug-in-}\alpha)$. Since $p(x)$ is the monic polynomial in $(p(x))$ of smallest degree, it is immediately also the monic, nonzero polynomial of smallest degree in $\ker(\text{plug-in-}\alpha)$

$$= \{ q(x) \in F[x] : q(\alpha) = 0 \}. \quad \square$$

Example: Find the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$.
Answer: $x^2 - 2$, because $(\sqrt{2})^2 - 2 = 0$ and $x^2 - 2$ is monic and irreducible (by Eisenstein on (2)).
Example: Find the minimal polynomial for $e^{2\pi i/5}$ over $\mathbb{Q}$.

$x^5 - 1$ has $e^{2\pi i/5}$ as a root, but is not irreducible:

$$x^5 - 1 = (x-1)(\underbrace{x^4 + x^3 + x^2 + x + 1}_{\text{Is this it?}})$$

Reduce mod 2: $x^4 + x^3 + x^2 + x + 1$ has no roots, so it's either irreducible or factors into 2 quadratics:

$$\cancel{x^2}, \cancel{x^2+1}, \cancel{x^2+x}, x^2 + x + 1$$

Since $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x^3 + x^2 + x + 1$, our polynomial doesn't factor into two quadratics, so $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, and hence, also irreducible over $\mathbb{Z}$ and $\mathbb{Q}$.

$$x^3 + x \neq 0 \text{ in } \mathbb{Z}_2[x].$$
$$(\sqrt{2})^5 - (\sqrt{2}) = 4\sqrt{2} - \sqrt{2} = 3\sqrt{2} \neq 0$$

so $x^5 - x \neq 0$ in $\mathbb{Z}_5[x]$.

Example: Find the minimal polynomial for $3 + 2i$ over $\mathbb{Q}$.
Answer: If $a_0 + a_1 x + \cdots + a_n x^{n-1} + x^n$ is the minimal polynomial, then:

$$a_0 + a_1(3 + 2i) + \cdots + (3 + 2i)^n = 0$$

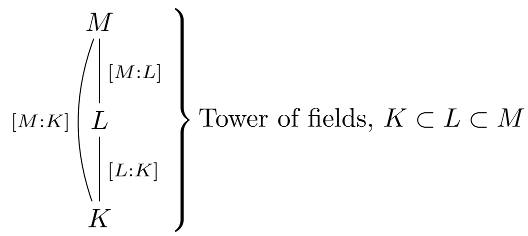
$n = 0$: Obvious non-starter.
$n = 1$: $a_0 + a_1(3 + 2i) = 0$
$\implies (a_0 + 3a_1) + (2a_1)i = 0$
Since $\{1, i\}$ are linearly independent over $\mathbb{Q}$, we get:

$$\begin{cases} a_0 + 3a_1 = 0 \\ 2a_1 = 0 \end{cases}$$

$\implies a_0 = a_1 = 0$. So no good.
$n = 2$: $a_0 + a_1(3 + 2i) + a_2(3 + 2i)^2 = 0$
$\implies (a_0 + 3a_1 + 5a_2) + (2a_1 + 12a_2)i = 0$
$\begin{cases} a_0 + 3a_1 + 5a_2 = 0 \\ 2a_1 + 12a_2 = 0 \end{cases}$
$a_2 = 1 \implies \begin{cases} a_0 + 3a_1 = -5 \\ 2a_1 = -12 \end{cases}$
$\implies a_1 = -6$, $a_0 = 13$
Therefore $x^2 - 6x + 13$ is the minimal polynomial
Check for irreducibility: $x = \frac{6 \pm \sqrt{36-52}}{2} = \frac{6 \pm \sqrt{-16}}{2} = 3 \pm 2i$
Roots are not in $\mathbb{Q}$, so irreducible.

PMATH 345 Lecture 24: June 30, 2010

Fact: If F is a field, α an element of some ring R containing F, then any field E that contains F and α must contain $F(\alpha)$.



Theorem: (KLM) Say $K \subset L \subset M$ is a tower of fields. Then:

$$[M : K] = [M : L][L : K]$$

where $[M : K] = \infty$ *iff* either $[M : L] = \infty$ or $[L : K] = \infty$.
Proof: Let $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l\}$ be a basis for L/K, and let $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ be a basis of M/L.
Claim: $\{\boldsymbol{u}_i\boldsymbol{v}_j\}_{\substack{i\in\{1,\ldots,l\}\\ j\in\{1,\ldots,m\}}}$ is a basis of M/K.
Note that the claim immediately implies the theorem.
Proof of claim: Spanning: Let $\boldsymbol{x} \in M$ be any element. We want to find $a_{ij} \in K$ such that $\boldsymbol{x} = \sum_{i,j} a_{ij}\boldsymbol{u}_i\boldsymbol{v}_j$. Since $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ is a basis of M/L, we can find $b_1, \ldots, b_m \in L$ such that:

$$\boldsymbol{x} = b_1\boldsymbol{v}_1 + \cdots + b_m\boldsymbol{v}_m$$

for each j, write:

$$b_j = a_{1j}\boldsymbol{u}_1 + a_{2j}\boldsymbol{u}_2 + \cdots + a_{lj}\boldsymbol{u}_l$$

for $a_{ij} \in K$. Then:

$$\begin{aligned}\boldsymbol{x} &= \Big(\sum_i a_{i1}\boldsymbol{u}_i\Big)\boldsymbol{v}_1 + \cdots + \Big(\sum_i a_{im}\boldsymbol{u}_i\Big)\boldsymbol{v}_m \\ &= \sum_{i,j} a_{ij}\boldsymbol{u}_i\boldsymbol{v}_j\end{aligned}$$

where $a_{ij} \in K$, as desired.

Linear independence: Set $\sum_{i,j} a_{ij}\boldsymbol{u}_i\boldsymbol{v}_j = 0$. We want to show that if $a_{ij} \in K$, then $a_{ij} = 0$ for all i, j. Rewrite:

$$\Big(\sum_i a_{i1}\boldsymbol{u}_i\Big)\boldsymbol{v}_1 + \cdots + \Big(\sum_i a_{im}\boldsymbol{u}_i\Big)\boldsymbol{v}_m = 0$$

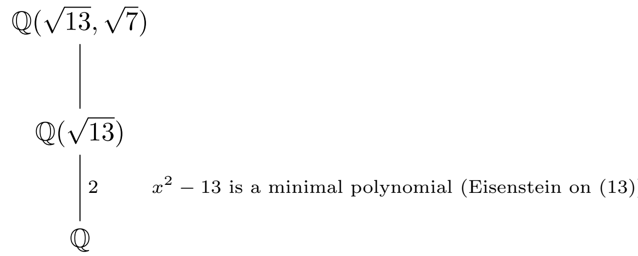
The coefficient of each $\boldsymbol{v}_j$ lies in L, since $a_{ij} \in K \subset L$ and $\boldsymbol{u}_1 \in L$. So:

$$\text{Since } \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\} \text{ is linear independent over } L \begin{cases} a_{11}\boldsymbol{u}_1 + a_{21}\boldsymbol{u}_2 + \cdots + a_{l1}\boldsymbol{u}_l = 0 \\ \vdots \\ a_{1m}\boldsymbol{u}_1 + a_{2m}\boldsymbol{u}_2 + \cdots + a_{lm}\boldsymbol{u}_l = 0 \end{cases}$$

Since $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l\}$ is linearly independent over K, we conclude $a_{ij} = 0$ for all i, j, as desired. □ (claim)
If $[M : L]$ or $[L : K]$ is infinite, then it is clear that $[M : K] = \infty$ because any infinite linearly independent subset of M/L or L/K is also linearly independent in M/K.

Otherwise, if $[M : L]$ and $[L : K]$ are both finite, we've already shown that $[M : K]$ is also finite. □

Example: Compute $[\mathbb{Q}(\sqrt{13}, \sqrt{7}) : \mathbb{Q}]$. Find a basis for $\mathbb{Q}(\sqrt{13}, \sqrt{7})/\mathbb{Q}$.



Claim: $x^2 - 7$ is irreducible over $\mathbb{Q}(\sqrt{13})$.
Proof of claim: Look for roots:

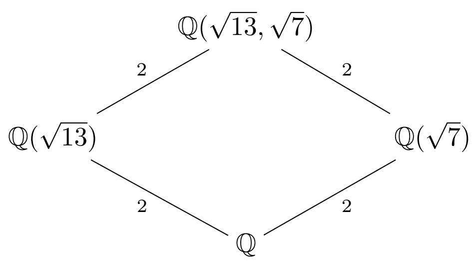
$$\begin{aligned} (a + b\sqrt{13})^2 - 7 &= a^2 + 13b^2 + 2ab\sqrt{13} - 7 \\ &= 0 \\ \implies (a^2 + 13b^2 - 7) + (2ab)\sqrt{13} &= 0 \end{aligned}$$

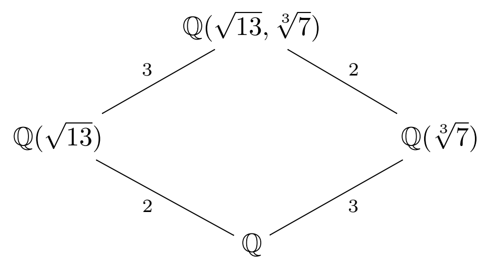
Since $\{1, \sqrt{13}\}$ is linearly independent over $\mathbb{Q}$:

$$\begin{cases} a^2 + 13b^2 - 7 = 0 \\ 2ab = 0 \end{cases}$$

It is easy to see that there are no a, $b \in \mathbb{Q}$ satisfying both equations, so $x^2 - 7$ has no roots in $\mathbb{Q}(\sqrt{13})$, and so $x^2 - 7$ is irreducible over $\mathbb{Q}(\sqrt{13})$. □ (claim)
So $[\mathbb{Q}(\sqrt{13}, \sqrt{7}) : \mathbb{Q}] = 4$ by KLM. A basis for $\mathbb{Q}(\sqrt{13}, \sqrt{7})/\mathbb{Q}$ is $\{1, \sqrt{13}, \sqrt{7}, \sqrt{91}\}$.

Say L/K is a field extension of degree n. If $K \subset F \subset L$ with F a field, then n is a multiple of $[F : K]$ and $[L : F]$.





PMATH 345 Lecture 25: July 5, 2010

Definition: Let F be a field, $p(x) \in F[x]$ any nonconstant polynomial. A splitting field for $p(x)$ over F is a field E such that:

(1) $p(x) = c(x - a_1) \cdots (x - a_n)$ for c, a_1, …, $a_n \in E$

(2) $E = F(a_1, \ldots, a_n)$.

Example: A splitting field for $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, since $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$.
Example: A splitting field for $x^2 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}$.
Example: A splitting field for $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, \frac{-1+\sqrt{-3}}{2})$
Proof: Let $\gamma = e^{2\pi i/3}$ be a primitive cube root of unity. Then:

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \gamma\sqrt[3]{2})(x - \gamma^2\sqrt[3]{2})$$

So a splitting field is:

$$\mathbb{Q}(\sqrt[3]{2}, \gamma\sqrt[3]{2}, \gamma^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \gamma)$$

Definition: An extension E/F is finite *iff* $[E:F] < \infty$.
Theorem: Let E/F be a finite extension. Then E/F is algebraic.
Proof: Let $\alpha \in E$, $[E:F] = n$. Then $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is linearly dependent over F:

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$$

for $a_0, \dots, a_n \in F$, not all zero. Then α is a root of $a_0 + \cdots + a_n x^n \in F[x]$, so α is algebraic over F. $\square$

This means that for any E/F, the set of elements of E that are algebraic over F is a field:

$$E^{\text{alg}} = \{\, \alpha \in E : \alpha \text{ is algebraic over } F \,\}$$

because if α, $\beta \in E^{\text{alg}}$, then $F(\alpha)/F$ and $F(\beta)/F$ are both finite extensions:

$$\left.\begin{array}{c} F(\alpha,\beta) \\ {\scriptstyle\text{finite}}\big| \\ F(\alpha) \\ {\scriptstyle\text{finite}}\big| \\ F \end{array}\right\} \text{finite, by KLM}$$

So $F(\alpha, \beta)$ is finite over F, and $F(\alpha, \beta)$ contains $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$, α/β. These four are all algebraic over F, by the theorem, so E^{alg} is closed under $+$, $-$, $\cdot$, $\div$.

For any field F, there is a field $\overline{F}$ that is algebraic over F, and every non-constant polynomial $p(x) \in F[x]$ factors into linear factors in $\overline{F}[x]$. $\overline{F}$ is called an algebraic closure of F.

Definition: Let F be a field, $p(x) \in F[x]$ a nonconstant polynomial. Then $p(x)$ is separable *iff* $\gcd(p(x), p'(x)) = 1$, where $p'(x)$ is the derivative of $p(x)$.

Definition: Let F be a field. Then the derivative of $a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ is $a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in F[x]$.
Clearly $(cf(x))' = cf'(x)$ and $(f+g)' = f' + g'$.
Theorem: (Product Rule)

$$(fg)' = f'g + g'f$$

where f, $g \in F[x]$, F a field.
Proof: By additivity and linearity, we may reduce to the case $f = x^n$, $g = x^m$. Then:

$$\begin{aligned} (fg)' &= (x^{n+m})' = (n+m)x^{n+m-1} \\ \text{and } f'g + g'f &= n(x^{n-1})x^m + m(x^n)x^{m-1} \\ &= (n+m)x^{n+m-1} \quad \square \end{aligned}$$

Theorem: Let F be a field, $p(x) \in F[x]$ non-constant, $\overline{F}$ an algebraic closure of F. Then $p(x)$ is separable *iff* $p(x)$ has no multiple roots in $\overline{F}$.
Proof: Forwards: If $p(x) = (x-a)^2 q(x)$, then $p'(x) = (x-a)^2 q'(x) + 2(x-a)q(x) \implies p'(a) = 0$ and $x - a \mid \gcd(p(x), p'(x))$, so $p(x)$ is not separable.

PMATH 345 Lecture 26: July 7, 2010

Theorem: Let F be a field, $p(x) \in F[x]$ a non-constant polynomial, $\overline{F}$ an algebraic closure of F. Then $p(x)$ is separable *iff* $p(x)$ has no multiple roots in $\overline{F}$.
Proof: Forwards: If $p(x)$ has a multiple root $a \in \overline{F}$, then $(x-a)^2 \mid p(x)$, so by Product Rule $x - a \mid p'(x)$ so $x - a \mid \gcd(p, p')$ in $\overline{F}[x]$. Since a is algebraic over F, it has a minimal polynomial $q(x)$ in $F[x]$, and $q(x) \mid \gcd(p, p')$ in $F[x]$.

Backwards: Say $g(x) = \gcd(p, p')$, and assume $g \neq 1$. Then $g(x)$ has a root $a \in \overline{F}$. So $p(a) = p'(a) = 0$. Then $p(x) = (x-a)q(x)$ for some $q(x) \in \overline{F}[x]$, so

$$\begin{aligned} &p'(x) = q(x) + (x-a)q'(x) \\ \implies &q(a) = 0. \end{aligned}$$

This means $x - a \mid q(x) \implies (x-a)^2 \mid p(x)$. ☐

Theorem: Let F be a field, $p(x) \in F[x]$ an irreducible polynomial. Then $p(x)$ is separable, unless $p'(x) = 0$.

Proof: Well, $p'(x) \in F[x]$, and has smaller degree than $p(x)$. In particular, $p(x) \nmid p'(x)$ unless $p'(x) = 0$. So $\gcd(p(x), p'(x)) = 1$. ☐

Corollary: If $\operatorname{char} F = 0$, then every irreducible polynomial in $F[x]$ is separable.

Example: $x^3 - 1 \in \mathbb{Z}_3$. Then:

$$(x^3-1)' = 3x^2 = 0$$

Example: $F = \mathbb{Z}_3(T)$

Consider $x^3 - T \in F[x]$[22]. Then $(x^3 - T)' = 3x^2 = 0$ but $x^3 - T$ has no roots in F, because $\sqrt[3]{T}$ is not a rational function.

Definition: A field is perfect *iff* every irreducible polynomial in $F[x]$ is separable.

Note: Every field of characteristic 0 is perfect.

Fact: Every finite field is perfect.

Definition: Let E/F be a field extension, $\alpha \in E$ any element. Then α is separable over F *iff* α is algebraic over F and its minimal polynomial is separable. E/F is separable *iff* every $\alpha \in E$ is separable over F.

Note: F is perfect *iff* every extension of F of finite degree is separable. Say $f(x) = a_0 + \cdots + a_n x^n$ satisfies $f'(x) = 0$. Assume $\operatorname{char} F = p > 0$.

Then $f'(x) = a_1 + 2a_2 + \cdots + n a_n x^{n-1} = 0$ so for all i, $i a_i = 0$. This means:

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{kp} x^{kp}$$

Theorem: If $\operatorname{char} R = p$ is prime, then for all $a, b \in R$, $(a+b)^p = a^p + b^p$.

Proof:

$$\begin{aligned} (a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \\ &= a^p + b^p \end{aligned}$$

because $p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$ for $i \in \{1, \ldots, p-1\}$. ☐

Definition: Let R be a ring of characteristic p for p prime. Then the function

$$\Phi_p(a) = a^p$$

is a homomorphism, called the Frobenius homomorphism. It's often written Frob_p.

Theorem: Let F be a field of characteristic p. Then F is perfect *iff* $\mathrm{Frob}_p \colon F \to F$ is onto.

Proof: Forwards: Say F is perfect, and let $a \in F$ be any element. We want to show $a = b^p$ for some $b \in F$. Consider $x^p - a \in F[x]$. Its derivative is 0, so $x^p - a$ is reducible in $F[x]$. However, if $\overline{F}$ is an algebraic closure of F, and $b \in \overline{F}$ is a root of $x^p - a$, we get,

$$(x-b)^p = x^p - a.$$

Comparing constant terms gives $b^p = a$. Write $x^p - a = f(x)g(x)$ for f, $g \in F[x]$. Then $f(x) = (x-b)^k$ for some $k \in \{1, \ldots, p-1\}$. The coefficient of x^{k-1} in $f(x)$ is $-kb \in F$. Since $k \in \{1, \ldots, p-1\}$, this means $k \neq 0$, so $b \in F$.

Backwards: Say $f(x) = a_0 + \cdots + a_n x^n$ is irreducible. If $f'(x) \neq 0$, then $f(x)$ is separable, so assume $f'(x) = 0$.

$$\begin{aligned} \text{Then } f(x) &= a_0 + a_p x^p + \cdots + a_{pk} x^{pk} \\ &= b_0^p + b_1^p x^p + \cdots + b_k^p x^{pk} \end{aligned}$$

[22] imperfect

for some $b_i \in F$.

$$\begin{aligned} &= \Phi_p(b_0) + \Phi_p(b_1 x) + \cdots + \Phi_p(b_k x^k) \\ &= \Phi_p(b_0 + b_1 x + \cdots + b_k x^k) \\ &= (b_0 + b_1 x + \cdots + b_k x^k)^p \end{aligned}$$

so $f(x)$ factors, a contradiction. So $f'(x) \neq 0$, and $f(x)$ is separable. □

Theorem: Let F be a finite field. Then F is perfect.
Proof: The Frobenius homomorphism from F to F is 1–1, so since F is finite, Frobenius is also onto. So F is perfect. □

PMATH 345 Lecture 27: July 9, 2010

Splitting fields
Definition: Let F be a field, $p(x) \in F[x]$ a nonconstant polynomial. A splitting field for $p(x)$ over F is a field E containing F such that

(1) $p(x) = c(x - a_1) \cdots (x - a_n)$ for $c, a_1, \ldots, a_n \in E$

and (2) $E = F(a_1, \ldots, a_n)$.

If $p(x)$ is constant, then we say F is a splitting field for $p(x)$ over F.

Theorem: Let F be a field, $p(x) \in F[x]$ any polynomial. Then there is a splitting field for $p(x)$ over F, and any two splitting fields for $p(x)$ over F are isomorphic.
Proof: Existence. We prove this by induction on $\deg(p(x))$.
Base case: $\deg(p(x)) = 0 \implies$ splitting field is F.
Inductive Hypothesis: for any field F, and any $p(x) \in F[x]$ of degree $< n$, there exists a splitting field for $p(x)$ over F.

Let $p(x) \in F[x]$ have degree n. Write:

$$p(x) = p_1(x) \cdots p_k(x)$$

for irreducible $p_1(x), \ldots, p_k(x) \in F[x]$. Consider $E = F[a]/(p_1(a))$. Then E is a field (because $p_1(x)$ is irreducible), and it contains a root (namely a) of $p(x)$. Then, in $E[x]$, we have:

$$p(x) = (x - a)q(x)$$

for some $q(x) \in E[x]$. Since $\deg(q(x)) < n$, by induction, there exists a splitting field E' of $q(x)$ over E. Then, in $E'[x]$, we have:

$$p(x) = c(x - a)(x - a_2) \cdots (x - a_n)$$

for $c, a_1, \ldots, a_n \in E'$, and

$$\begin{aligned} E' &= E(a_2, \ldots, a_n) \\ &= F(a)(a_2, \ldots, a_n) \\ &= F(a, a_2, \ldots, a_n) \end{aligned}$$

so E' is a splitting field for $p(x)$ over F, as desired.

Uniqueness: We will induce on $\deg(p(x))$, over all fields simultaneously. The base case is trivial, so assume the inductive hypothesis for polynomials of degree $< n$, and let $\deg(p(x)) = n$. Let E_1 and E_2 be splitting fields for $p(x)$ over F.

Write $p(x) = c(x - a_1) \cdots (x - a_n) \in E_1[x]$ and $p(x) = c(x - b_1) \cdots (x - b_n) \in E_2[x]$.
Lemma: Let L/K be a field extension, $p(x) \in K[x]$ irreducible, $\alpha, \beta \in L$ such that $p(\alpha) = p(\beta) = 0$. Then $K(\alpha) \cong K(\beta)$ and the isomorphism maps α to β.
Proof of lemma: We already know $K(\alpha) \cong K[x]/(p(x)) \cong K(\beta)$. □ lemma

Without loss of generality, assume that a_1 and b_1 are roots of the same irreducible factor of $p(x)$. Then by the lemma, $F(a_1) \cong F(b_1)$, and:

$$p(x) = (x - a_1)q_1(x) \text{ in } F(a_1)[x]$$
$$\text{and } p(x) = (x - b_1)q_2(x) \text{ in } F(b_1)[x]$$

We identify a_1 and b_1 via the isomorphism $F(a_1) \cong F(b_1)$. This identifies $q_1(x) = \frac{p(x)}{x-a_1}$ with $q_2(x) = \frac{p(x)}{x-b_1}$, so by induction, any splitting field for q_1 over $F(a_1)$ is isomorphic to any splitting field for q_2 over $F(b_1) \cong F(a_1)$. These two fields are exactly E_1 and E_2 which are therefore isomorphic. □

PMATH 345 Lecture 28: July 12, 2010

Finite Fields, *F*

Example: $\mathbb{Z}_p$ residues mod p, p prime.

Every field contains one of $\mathbb{Q}$ or $\mathbb{Z}_p$.
Since F is finite, $F \supseteq \mathbb{Z}_p$ for some prime p.

F is a vector space over $\mathbb{Z}_p$ with basis $v_1, \ldots, v_n$.
Every v in F looks like

$$v = a_1 v_1 + \cdots + a_n v_n \text{ where } a_j \in \mathbb{Z}_p$$

There are p possibilities for each a_j and a change in any a_j makes a fresh v.
So there are p^n vs in all

$$\text{i.e., } \#F = p^n.$$

Proposition: Let A be a commutative ring and G the set of units in A. If $\#G = \text{finite} = m$, say, then for any u in G, $u^m = 1$.
Proof: Let $v_1, v_2, \ldots, v_m$ be the full list of G.
Put $v = v_1 v_2 \cdots v_m$.
Take any u in G. Look at list

$$uv_1, uv_2, \ldots, uv_m \text{ inside } G.$$

This list has no duplicates. Indeed if $uv_j = uv_i$, cancel u and get $v_j = v_i$.
So our list exhausts G.

$$\begin{aligned} \text{Hence } 1 \cdot v &= (uv_1)(uv_2)\cdots(uv_m) \\ &= u^m (v_1 v_2 \cdots v_m) \\ &= u^m v \end{aligned}$$

Cancel v and get $u^m = 1$.

When we apply this to the set of non-zero elements of our finite field F (where $\#p^n$) we get $u^{p^n-1} = 1$ for all u in F where $u \neq 0$.

Refresh on splitting fields
Let K be any field and $p(x)$[23] $\in K[x]$ (monic, say, $\deg p(x) = n$). A splitting field for $p(x)$ is a field L such that

(1) $K \subseteq L$

(2) $p(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$ where $a_j \in L$.

(3) If M is a field such that $K \subseteq M \subsetneq L$ then some $a_j \notin M$ *OR* if $K \subseteq M \subseteq L$ and all $a_j \in M$ then $M = L$.

Every $p(x)$ has a splitting field and if L_1, L_2 are splitting fields of $p(x)$ then there is an isomorphism $\phi\colon L_1 \to L_2$ such that $\phi(a) = a$ for each a in K.

Proposition: If F is finite field and $\#F = p^n$ then F is *the* splitting field of $x^{p^n} - x$ as a polynomial in $\mathbb{Z}_p[x]$.
Proof:

[23] $\neq 0$

1) $\mathbb{Z}_p \subseteq F$

2) $u^{p^n-1} = 1$, for all $u \neq 0$ in F
multiply by u, get $u^{p^n} - u = 0$, also holds for $u = 0$

3) Since *every* element of F is a root of $x^{p^n} - x$, then any *proper* subfield $M \subsetneq F$ would not have at least one of these roots.

Proposition: If p is any prime and n a positive integer and $F =$ the splitting of $x^{p^n} - x$ in $\mathbb{Z}_p[x]$, then $\#F = p^n$.

PMATH 345 Lecture 29: July 14, 2010

Every finite field F has p^n elements for some prime p and some positive integer n.
Every such F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.
Any two fields of cardinality p^n are isomorphic.

Proposition: If p is a prime and n a positive integer and $F =$ splitting field of $x^{p^n} - x$, then $\#F = p^n$.
Lemma: If $\phi\colon K \to K$ is a field homomorphism, then $M = \{ a \in K : \phi(a) = a \}$ is a subfield of K.
Proof: Let $a, b \in M$, i.e., $\phi(a) = a$, $\phi(b) = b$.
Then $\phi(a \pm b) = \phi(a) \pm \phi(b) = a \pm b$,
and if $a \neq 0$, we also get $\phi(a^{-1}) = \phi(a)^{-1} = a^{-1}$.
Proof of proposition: Have F: splitting field of $x^{p^n} - x$.
Take Frobenius automorphism:

$$\left.\begin{aligned} \phi\colon F &\to F \\ a &\mapsto a^p \end{aligned}\right\} \text{(use } (a \pm b)^p = a^p \pm b^p \text{ to show this is a field homomorphism)}$$

Then $\phi^n = \phi \circ \phi \circ \cdots \circ \phi$, n-times is also a field homomorphism, whose set of fixed elements is $M = \{ a \in F : a^{p^n} = a \}$, which is a field inside F, by the lemma.

We see that $M =$ set of roots of $x^{p^n} - x$. So F is a subfield of F, which was the splitting field of $x^{p^n} - x$.
Since $F =$ smallest field containing roots of $x^{p^n} - x$, we get $M = F$.
Finally, note that $x^{p^n} - x$ has no repeated roots, because its derivative

$$(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1 \text{ in } \mathbb{Z}_p[x]$$

is coprime with $x^{p^n} - x$. So $\#F = p^n$. $\square$

Primitive generators
Let $F =$ finite field and $F^* = F \setminus \{0\}$.
Let $q = p^n - 1 = \#F^*$.
We saw that for every a in F^*, $a^q = 1$.

Theorem: There is some $a \in F^*$ such that the list $1, a^1, a^2, \ldots, a^{q-1}$ picks up all of F^*.

Definition: If $a \in F^*$ its *order* is the least integer $k \geq 1$ such that $a^k = 1$. Write $k = \operatorname{ord}(a)$.

Proposition 1: If $k = \operatorname{ord}(a)$ and $a^m = 1$, then $k \mid m$.
Proof: Write $m = ks + r$, where $0 \leq r < k$. Then

$$1 = a^m = a^{ks+r} = (a^k)^s a^r = 1^s a^r = a^r.$$

By the minimality of k get $r = 0$. So $m = ks$. $\square$

Proposition 2: If $a \in F^*$ and $\operatorname{ord}(a) = k \geq 1$, then $1, a, a^2, \ldots, a^{k-1}$ is the complete non-repeating list of all b in F^* such that $b^k = 1$.
Proof:

i) If a^j is in the list, we see that $(a^j)^k = (a^k)^j = 1^j = 1$.

ii) No repeats: Say $a^i = a^j$, where $0 \leq i \leq j \leq k - 1$.
Thus $a^{j-i} = 1$, and since $0 \leq j - i < k$, the minimality of k gives $j = i$.

iii) Let $b \in F^*$ where $b^k = 1$. Then b is a root of $x^k - 1 \in \mathbb{Z}_p[x]$. This polynomial has at most k roots. But the list is made up of such roots, and the list has k elements. So b is in the list. $\square$

PMATH 345 Lecture 30: July 16, 2010

We had finite field F, $\#F = p^n$, $F^* = F \setminus \{0\}$.
$q = p^n - 1$.
If $a \in F^*$, $\operatorname{ord}(a)$ = least $k \geq 1$ such that $a^k = 1$. (Recall $a^q = 1$).

Proposition 1: If $k = \operatorname{ord}(a)$ and $a^m = 1$, then $k \mid m$. So $\operatorname{ord}(a) \mid q$.

Proposition 2: If $k = \operatorname{ord}(a)$, then the list $1, a, a^2, \ldots, a^{k-1}$ does not repeat and includes *all* b in F^* that satisfy $b^k = 1$.

Proposition 3: If $\operatorname{ord}(a) = k$ and $\operatorname{ord}(b) = l$, and k, l are coprime, then $\operatorname{ord}(ab) = kl$.
Proof: Let $m = \operatorname{ord}(ab)$.
Since $(ab)^{kl} = a^{kl}b^{kl} = (a^k)^l(b^l)^k = (1)^l(1)^k = 1$.
Thus $m \mid kl$.
Now check $kl \mid m$. Since k, l are coprime, enough to check $k \mid m$ and $l \mid m$.
Aside: If $c \in F^*$ then $\operatorname{ord}(c) = \operatorname{ord}(c^{-1})$: $c^k = 1 \iff (c^{-1})^k = 1$
Now we have $1 = (ab)^m = a^m b^m$.
Let $j = \operatorname{ord}(a^m) = \operatorname{ord}(b^m)$.
Now $(a^m)^k = (a^k)^m = 1^m = 1$.
$\implies j \mid k$
and likewise $j \mid l$.
Since k, l are coprime, we get $j = 1$.
So $a^m = 1 = b^m$
Then $k \mid m$ and $l \mid m$. $\square$

Theorem: In F^* there is some a such that $1, a, a^2, \ldots, a^{q-1}$ picks up all of F^*.
Proof: Just check F^* has an element of order q.
Pick any a in F^* and put $k = \operatorname{ord}(a)$.
If $k = q$, done.
If $k < q$, the list $1, a, \ldots, a^{k-1}$ does not cover all of F^*. Pick b not in list. Let $l = \operatorname{ord}(b)$.
Note: $b^k \neq 1$, by Proposition 2.
Hence $l \nmid k$. Indeed, if $k = lr$ we would get

$$b^k = (b^l)^r = 1^r = 1.$$

So some prime p (not original "p") divides l more often than it divides k. Write $k = p^i k_1$ and $l = p^j l_1$ where $0 \leq i < j$ and k_1, l_1 have no p in them.
Put $c = a^{p^i}$, $\operatorname{ord} c = k_1$
$d = b^{l_1}$, $\operatorname{ord} d = p^j$[24)]
Thus $\operatorname{ord}(cd) = p^j k_1 > p^i k_1 = k$.
We found an element, namely cd, whose order is bigger than $\operatorname{ord} a$.
Keep doing this until an element in F^* of order q is found. $\square$

Example: The polynomial $x^2 - 2$ is irreducible in $\mathbb{Z}_5[x]$. Hence $F = \mathbb{Z}_5[x]/\langle p(x)\rangle$ is a field and $\#F = 25$, $\#F^* = 24$. Have $\underset{f(x)\mapsto f(x)+\langle p(x)\rangle}{\phi\colon \mathbb{Z}_5[x]\to F}$ and *if* $\alpha = x + \langle p(x)\rangle$ we *know* that $1, \alpha$, is basis for F over $\mathbb{Z}_5$.
Every element in F looks like $a + b\alpha$ where $a, b \in \mathbb{Z}_5$.
Know $\alpha^2 - 2 = 0$, $\alpha^2 = 2$.
Find primitive generator of F.
Start with α.
Take powers

$$1,\ \alpha,\ \alpha^2 = 2,\ \alpha^3 = 2\alpha,\ \alpha^4 = 4,\ \alpha^5 = 4\alpha,\ \alpha^6 = 3,\ \alpha^7 = 3\alpha,\ \alpha^8 = 6 = 1$$

too short. Pick β not in list. Say $\beta = \alpha + 1$.

[24)] k_1, p^j coprime

Powers of β.

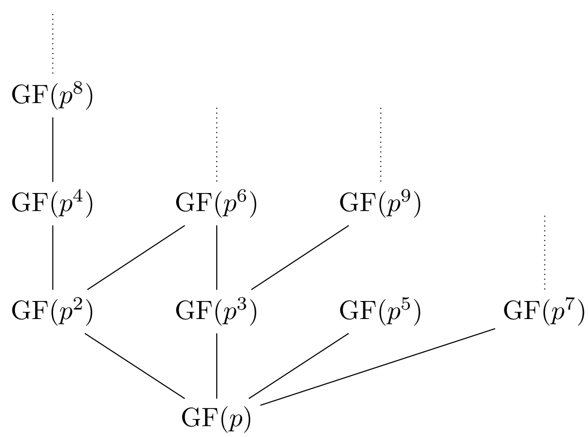
$$\begin{aligned}
&1\\
&\beta\\
&\beta^2 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha + 3\\
&\beta^3 = 2\\
&\beta^4 = 2\alpha + 2\\
&\beta^5 = 4\alpha + 1\\
&\beta^6 = 4 = -1\\
&\quad\vdots\\
&\beta^{12} = 1
\end{aligned}$$

So $\operatorname{ord}\beta = 12$.
So $\operatorname{ord}\alpha = 3^0 \cdot 2^3$, $\operatorname{ord}\beta = 3^1 \cdot 2^2$
Put $\gamma = \alpha^{3^0} = \alpha$, $\operatorname{ord}\gamma = 8$
$\delta = \beta^4 = 2\alpha + 2$, $\operatorname{ord}\delta = 3$[25]
So $\operatorname{ord}(\gamma\delta) = 8 \cdot 3 = 24$

PMATH 345 Lecture 31: July 19, 2010

$\mathrm{GF}(p^n)$ = Field with p^n elements
GF[26]$(p) = \mathbb{Z}_p$ = integers mod p
$\mathrm{GF}(p^n) \not\cong \mathbb{Z}_{p^n}$ if $n \geq 2$
Fix a prime p.

$$\overline{\mathbb{F}_p} = \overline{\mathrm{GF}(p)} = \text{algebraic closure of } \mathrm{GF}(p)$$



Theorem: Let p be prime, $n, m \in \mathbb{Z}_{\geq 1}$. Then $\mathrm{GF}(p^n) \subset \mathrm{GF}(p^m)$ *iff* $n \mid m$. Moreover, if $n \mid m$, then there is a unique subfield of $\mathrm{GF}(p^m)$ with p^n elements.
Proof: If $\mathrm{GF}(p^n) \subset \mathrm{GF}(p^m)$, then $\mathrm{GF}(p^m)$ is a vector space over $\mathrm{GF}(p^n)$, with finite dimension k. Then $\mathrm{GF}(p^m)$ has $(p^n)^k$ elements (p^n scalars, k coefficients in basis), so $p^m = p^{nk}$ and so $n \mid m$.

Now assume $n \mid m$. Then $x^{p^n} - x$ divides $x^{p^m} - x$, because $x^{p^n-1} - 1$ divides $x^{p^m-1} - 1$, because $p^n - 1$ divides $p^m - 1$, because n divides m.

Every element of $\mathrm{GF}(p^n)$ is a root of $x^{p^n} - x$, and so is a root of $x^{p^m} - x$, and so is an element of $\mathrm{GF}(p^m)$.

Finally, any subfield of $\mathrm{GF}(p^m)$ with p^n elements must be exactly the set of roots of $x^{p^n} - x$. $\square$

[25] $\operatorname{ord}\delta$, $\operatorname{ord}\gamma$ coprime
[26] "Galois Field"

Example: $\mathbb{Z}[\sqrt{10}]$, $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$
2, 5, $\sqrt{10}$ are all irreducible in $\mathbb{Z}[\sqrt{10}]$
But: $(10) = (2, \sqrt{10})^2 \cdot (5, \sqrt{10})^2$
Check: $(2, \sqrt{10})(5, \sqrt{10}) = (10, 5\sqrt{10}, 2\sqrt{10}, 10) = (\sqrt{10})$

PMATH 345 Lecture 32: July 21, 2010

Definition: Let D be a domain, $K = K(D)$ its field of fractions. A fractional ideal (same as "fractionary ideal") of D is a subset I of K satisfying:

(1) $0 \in I$

(2) If a, $b \in I$, then $a - b \in I$

(3) If $a \in I$, $r \in D$, then $ra \in I$

(4) There is some $d \in D$, $d \neq 0$, such that $dI \subset D$.

Note: The set dI is an (integral) ideal of D, so $I = \frac{1}{d}(dI)$ is just some integral ideal of D divided by a nonzero element of D.

Example: The fractional ideals of $\mathbb{Z}$ are $\frac{1}{m}(n\mathbb{Z}) = \frac{n}{m}\mathbb{Z}$ for integers n, $m \in \mathbb{Z}$ with $m \neq 0$.

$$\tfrac{3}{2}\mathbb{Z} = \{\, \tfrac{3n}{2} : n \in \mathbb{Z} \,\} = \{\ldots, -3, -\tfrac{3}{2}, 0, \tfrac{3}{2}, 3, 4\tfrac{1}{2}, 6, \ldots\}$$

Example: $D = \mathbb{Z}[\sqrt{10}]$, $I = \sqrt{10}D + 3D = (\sqrt{10}, 3)D$ or

$$\begin{aligned} I &= \tfrac{\sqrt{10}}{2}D + D \neq 0 \\ &= \{\, (a + b\sqrt{10})\tfrac{\sqrt{10}}{2} + (c + d\sqrt{10}) : a, b, c, d \in \mathbb{Z} \,\} \end{aligned}$$

One can add and multiply fractional ideals simply:

$$(a_1D + \cdots + a_nD) + (b_1D + \cdots + b_mD) = a_1D + \cdots + a_nD + b_1D + \cdots + b_mD$$
$$(a_1D + \cdots + a_nD)(b_1D + \cdots + b_mD) = \sum_{i,j} a_ib_jD$$

Example: $(aD + bD)(cD + dD) = acD + bcD + adD + bdD$
Example: $D = \mathbb{Z}[\sqrt{10}]$:

$$\big(\tfrac{\sqrt{10}}{2}D + D\big)\big(\sqrt{10}D + \tfrac{1}{2}D\big) = \cancel{5D + \sqrt{10}D} + \tfrac{\sqrt{10}}{4}D + \tfrac{1}{2}D$$

$5D \subset \frac{1}{2}D$ and $\sqrt{10}D \subset \frac{\sqrt{10}}{4}D$ so product is $\frac{\sqrt{10}}{4}D + \frac{1}{2}D$

Definition: A fractional ideal is invertible *iff* there is a fractional ideal J such that $IJ = D$.

Say I, J fractional ideals of D, $J \neq (0)$. Then $I/J = \{\, x \in K(D) : xJ \subset I \,\}$. I/J is a fractional ideal because

(1) $0 \in I/J$

(2) If $xJ \subset I$ and $yJ \subset I$ then $(x - y)J \subset$[27)] $xJ - yJ \subset I$

(3) If $xJ \subset I$ and $r \in D$, then $rxJ \subset xJ \subset I$, so $rx \in I/J$.

(4) Need $b \in D$, $b \neq 0$ such that $b(I/J) \subset D$. Let $a \in D$, $a \neq 0$ satisfy $aI \subset D$ and choose $x \in J \cap D$, $x \neq 0$. Then $b = ax$ works:

If $y \in I/J$, then
$$axy = a(xy) \in aI \subset D$$
so $ax(I/J) \subset D$.

[27)] NOT the same!

Example:

$$\begin{aligned}(n\mathbb{Z})/(m\mathbb{Z}) &= \left\{ \tfrac{a}{b} \in \mathbb{Q} : \tfrac{a}{b}(mk) \in n\mathbb{Z} \text{ for all } k \in \mathbb{Z} \right\} \\ &= \left\{ \tfrac{a}{b} \in \mathbb{Q} : \tfrac{amk}{b} \in n\mathbb{Z} \text{ for all } k \in \mathbb{Z} \right\} \\ &= \left\{ \tfrac{a}{b} \in \mathbb{Q} : \tfrac{am}{b} \in n\mathbb{Z} \right\} \\ &= \left\{ \tfrac{a}{b} \in \mathbb{Q} : \tfrac{a}{b} \in \tfrac{n}{m}\mathbb{Z} \right\} \\ &= \tfrac{n}{m}\mathbb{Z}.\end{aligned}$$

In general, if a, $b \in D$, then $aD/bD = \frac{a}{b}D$ if $b \neq 0$. In particular, every principal fractional ideal (nonzero) is invertible: $aD/aD = D$.
Example: Compute a, b such that $D/(\sqrt{10}D + 5D) = aD + bD$ for $D = \mathbb{Z}[\sqrt{10}]$.

Let $I = D/(\sqrt{10}D + 5D)$. Then:

$$\begin{aligned} I &= \Big\{ \underset{a,b\in\mathbb{Q}}{a + b\sqrt{10}} : (a + b\sqrt{10})x \in \mathbb{Z}[\sqrt{10}] \text{ for all } x \in \sqrt{10}D + 5D \Big\} \\ &= \Big\{ \underset{a,b\in\mathbb{Q}}{a + b\sqrt{10}} : (a + b\sqrt{10}) \in \mathbb{Z}[\sqrt{10}] \text{ and } (a + b\sqrt{10})5 \in \mathbb{Z}[\sqrt{10}] \Big\} \end{aligned}$$

$$10b + \sqrt{10}a \in \mathbb{Z}[\sqrt{10}] \implies a \in \mathbb{Z},\ b \in \tfrac{1}{10}\mathbb{Z}$$
$$(5\sqrt{10})b + 5a \in \mathbb{Z}[\sqrt{10}] \implies b \in \tfrac{1}{5}\mathbb{Z}$$

Therefore guess: $I = \frac{\sqrt{10}}{5}D + D$
$(a + b\sqrt{10} = (\text{integer}) + (\text{integer})\frac{\sqrt{10}}{5})$
Check: $(\frac{\sqrt{10}}{5}D + D)(\sqrt{10}D + 5D) = 2D + \sqrt{10}D + \sqrt{10}D + 5D = D$

PMATH 345 Lecture 33: July 23, 2010

Definition: A fractional ideal I of a domain D is invertible *iff* there is a fractional ideal J such that $IJ = D$.

Definition: A Dedekind domain is a domain is a domain in which every nonzero fractional ideal is invertible.
Example: Every PID is Dedekind.
Theorem: Let D be a Dedekind domain, P a nonzero prime ideal. Then P is maximal.
Proof: Assume that there is some ideal $I \subset D$ with $P \subset I$. We want to show either $P = I$ or $I = D$.

The fractional ideal PI^{-1} is a subset of $II^{-1} = D$, so PI^{-1} is an integral ideal of D. Now:

$$(PI^{-1})I = P$$

so since P is prime, either $PI^{-1} \subset P$ or $I \subset P$. If $PI^{-1} \subset P$, then $I^{-1} \subset D$ so $II^{-1} \subset I$ so $I = D$ because $D = II^{-1}$.

If $I \subset P$, then $P \subset I \implies P = I$. □

Theorem: Let D be a Dedekind domain, $I \subset D$ any nonzero ideal. Then I can be factored as a product of prime ideals:

$$I = P_1 \cdots P_n$$

and this factorization is unique up to permutation of the P_i.
Proof: Existence: If I is maximal, then it's prime and $I = I$ will do.

If I is not maximal, then there is an ideal J with $I \subsetneq J \subsetneq D$. Then $I = J(J^{-1}I)$, where $J^{-1}I \subset J^{-1}J = D$, so $J^{-1}I$ is an integral ideal. If J and $J^{-1}I$ are both prime, then we're done. If not, then keep factoring the non-prime factors of I until all the factors are prime.

If this process never stops, then we have constructed an infinite ascending chain of ideals:

$$I \subsetneq I_1{}^{28)} \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

28) "J"

Lemma: Every invertible ideal is finitely generated.
Proof of lemma: Let I be an invertible ideal of a domain D. Then $II^{-1} = D$, so $1 = a_1a_1' + \cdots + a_na_n'$ for $a_i \in I$, $a_i' \in I^{-1}$. Clearly $(a_1, \ldots, a_n) \subset I$, so let $x \in I$. Then $x = (xa_1')a_1 + \cdots + (xa_n')a_n$.

Since $x \in I$, $a_i' \in I^{-1}$, we get $xa_i' \in D$ so $x \in (a_1, \ldots, a_n)$. Therefore, $I = (a_1, \ldots, a_n)$ is finitely generated.
□ lemma

Corollary: Every Dedekind domain is Noetherian.
Proof: Immediate. □
By the Corollary, D is Noetherian, so it obeys the ACC, and we obtain a contradiction.
Uniqueness: Say $I = P_1 \cdots P_n = Q_1 \cdots Q_m$ for P_i, Q_j prime. We want to show that these two factorizations are the same up to permutation.

Since $P_1 \cdots P_n \subset Q_1 \cdots Q_m \subset Q_1$, we get $P_i \subset Q_1$ for some i. But D is Dedekind, so P_i is maximal and so $P_i = Q_1$. Multiplying both sides by Q_1^{-1}, we obtain $P_1 \cdots \hat{P_i} \cdots P_n = Q_2 \cdots Q_m$. Continuing in this manner, we eventually obtain either a product of some P_is equals D, or some Q_js equals D.

This is only possible if the product of P_is or Q_js is empty, so our repeated cancellation process constructed a bijection between the Q_js and P_is, as desired. □

Definition: Let D be a domain, I, J two nonzero ideals of D. Then I and J are in the same ideal class *iff* there is some $a \in K(D)$ such that $I = aJ$. This is an equivalence relation, and the equivalence classes are called ideal classes.

Note that D is a PID *iff* it has only one ideal class.

Definition: The class number of D is the number of ideal classes of D.

PMATH 345 Lecture 34: July 26, 2010

Recall:

$$A/B = \{\, x \in K(D) : xB \subset A \,\}$$

Is this the same as AB^{-1}?
Answer: No, because B might not be invertible.

Theorem: Let D be a domain, $K(D)$ its fraction field, A, B two fractional ideals of D, with B invertible. Then

$$A/B = AB^{-1}$$

Proof: Clearly $B(A/B) \subset A$, so $A/B \subset AB^{-1}$.

Conversely, say $x \in AB^{-1}$. We want to show $x \in A/B$. Well, $x \in AB^{-1} \implies xB \subset A$, so $x \in A/B$. □
Corollary: Let I be an invertible ideal of a domain D. Then $I^{-1} = D/I$.

Warning: If B is not invertible, then $(A/B)B \neq A$, necessarily.

Example: Compute $(2, \sqrt{-5}+1)^{-1}$ in $\mathbb{Z}[\sqrt{-5}] = D$.
Solution: Let $J = (2, 1+\sqrt{-5})$. If $a + b\sqrt{-5} \in J^{-1}$, then

$$2(a + b\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}] \quad (1)$$
$$\textit{and } (1+\sqrt{-5})(a+b\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}] \quad (2)$$

$$(1) \implies a, b \in \tfrac{1}{2}\mathbb{Z}$$
$$(2) \implies \begin{cases} a - 5b \in \mathbb{Z} \\ a + b \in \mathbb{Z} \end{cases}$$

Write $a = \frac{c}{2}$, $b = \frac{d}{2}$. Then $c - 5d$ and $c + d$ are even. This is equivalent to $c \equiv d \bmod 2$:

$$\begin{aligned} a + b\sqrt{-5} &= \frac{c + (c+2k)\sqrt{-5}}{2} \qquad k \in \mathbb{Z} \\ &= c\left(\frac{1+\sqrt{-5}}{2}\right) + k\sqrt{-5} \end{aligned}$$

So guess: $J^{-1} = (\frac{1+\sqrt{-5}}{2})D + (\sqrt{-5})D = I$
Check: $((\frac{1+\sqrt{-5}}{2})D + \sqrt{-5}D)(2D + (1+\sqrt{-5})D) = (1+\sqrt{-5})D + (-2+\sqrt{-5})D + (2\sqrt{-5})D + (-5+\sqrt{-5})D$

$$\begin{aligned} 3 &= (1+\sqrt{-5}) - (-2+\sqrt{-5}) \in IJ \\ -4 &= (1+\sqrt{-5}) - (2\sqrt{-5}) + (-5+\sqrt{-5}) \in IJ \\ &-(3+(-4)) \in IJ \\ &\implies D \subset IJ \end{aligned}$$

Since $IJ \subset D$, we get $IJ = D \implies I = J^{-1}$.

Example: Factor (6) in $\mathbb{Z}[\sqrt{7}]$.
Solution: $(6) = (2)(3)$.
Is (2) prime? Compute $\mathbb{Z}[\sqrt{7}]/(2)$: $\{0, 1, \sqrt{7}, 1+\sqrt{7}\}$

$$\begin{aligned} (\sqrt{7})^2 &= 7 \neq 0 \\ \sqrt{7}(1+\sqrt{7}) &= 7 + \sqrt{7} = 1 + \sqrt{7} \neq 0 \\ (1+\sqrt{7})^2 &= 1 + 2\sqrt{7} + 7 = 0! \end{aligned}$$

Consider $(2, 1+\sqrt{7})$. Since $(1+\sqrt{7})^2 \equiv 0 \bmod (2)$, we're guessing that $(2) = (2, 1+\sqrt{7})^2$:

$$\begin{aligned} (2, 1+\sqrt{7})^2 &= (4, 2+2\sqrt{7}, 8+2\sqrt{7}) \\ &= (4, 6, 2+2\sqrt{7}, 8+2\sqrt{7}) \\ &= (2) \end{aligned}$$

Is $(2, 1+\sqrt{7})$ prime? Yes, because $\mathbb{Z}[\sqrt{7}]/(2, 1+\sqrt{7}) \cong \mathbb{Z}/2\mathbb{Z}$ via $a + b\sqrt{7} \mapsto a + b \pmod 2$. So $(6) = (2, 1+\sqrt{7})^2(3)$
Is (3) prime?

$$\begin{aligned} \mathbb{Z}[\sqrt{7}]/(3) &\cong \mathbb{Z}[x]/(x^2 - 7, 3) \\ &\cong \mathbb{Z}_3[x]/(x^2 - 7) \\ &\cong \mathbb{Z}_3[x]/(x^2 - 1) \end{aligned}$$

This is not a domain, since $x^2 - 1$ is reducible. $1 \pm \sqrt{7}$ are zero divisors mod 3:

$$(1+\sqrt{7})(1-\sqrt{7}) = -6 \equiv 0 \bmod 3.$$

Compute $(3, 1+\sqrt{7})(3, 1-\sqrt{7}) = (9, 3+3\sqrt{7}, 3-3\sqrt{7}, -6) = (3)$
$(3, 1 \pm \sqrt{7})$ is prime, because:
$\mathbb{Z}[\sqrt{7}]/(3, 1\pm\sqrt{7}) \cong \mathbb{Z}_3$ via

$$a + b\sqrt{7} \mapsto a \mp b \bmod 3$$

So $(6) = (2, 1+\sqrt{7})^2(3, 1+\sqrt{7})(3, 1-\sqrt{7})$.