25.1

Ring Theory.

Def. A *ring* is a set R with two operations $+$ and $\times$ (or $\cdot$) satisfying:

(1). $(R, +)$ is an abelian group. (write 0 for the identity.)

(2). Multiplication is associative:

$$a \times (b \times c) = (a \times b) \times c.$$

(c) Addition distributes over multiplication:

$$(a+b) \times c = (a \times c) + (b \times c)$$

$$a \times (b + c) = (a \times b) + (a \times c)$$

(d) There is a multiplicative identity 1 with

$1 \times a = a \times 1$ for all $a \in R$. (Assume $1 \neq 0$.)

[Not assumed in DF]

Multiplication might or might not be commutative. If it is, R is a *commutative ring*.

Examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$.

Polynomial rings $R[x]$ where R is a commutative ring and x is an indeterminate.

~~One power set~~

If X is a set and A is a ring, $\{\text{functions } X \to A\}$ is a ring. Ops inherited from A.

Matrix rings $M_{n \times n}(R)$.

Not commutative even if R is.

Hamiltonian quaternions

$\mathbb{H} := \{ a + bi + cj + dk : a,b,c,d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1,$
$ij = -ji = k,\ jk = -kj = i,$
$ki = -ik = j \}.$

We'll see more.

Def. (1) If every $x \in R - \{0\}$ has a multiplicative inverse (i.e. if $R - \{0\}$ is a group) then R is a <u>division ring</u>.

(2) If in addition ~~multip~~ R is commutative, it is a <u>field</u>.

(3) $x \in R$ is a <u>zero divisor</u> if $xr = 0$ or $rx = 0$ for some $r \in R$.

(4) $x \in R$ is a <u>unit</u> if $\exists\ y \in R$ with $xy = yx = 1$.
Write $R^\times$ for the group of units.

Trivial Properties. Let R be a ring.

(1) $0x = x0 = 0$ for all $x \in R$.

(2) $(-a)b = a(-b) = -ab$ where $-$ is the additive inverse.

(3) $(-a)(-b) = ab$.

(4) The mult. identity is unique and $-x = (-1)x$.

(5) A zero divisor can't be a unit.

More examples:

All continuous functions $[0,1] \longrightarrow \mathbb{R}$.

There are zero divisors.

Units: Functions that are nowhere zero.

Not a unit or a zero divisor: $x - \frac{1}{2}$.

not a perfect square

$\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$.

This is a field! Can you prove it?
(Can you find inverses)

$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$.

A ring but not a field.

If $D \equiv 1 \pmod 4$, then

$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] := \left\{a + b\left(\frac{1+\sqrt{D}}{2}\right) \cdot a, b \in \mathbb{Z}\right\}$

is a ring, but not if $D \equiv 2, 3 \pmod 4$.
This won't be closed under multiplication.

Can you find the units?

Group rings: If G is a group, consider the group ring

$\mathbb{Z}G := \sum_{g \in G} n_i g$, where: $n_i \in \mathbb{Z}$, is 0 for all but finitely many g.

i.e. formal sums and differences of elements of G.

Can replace $\mathbb{Z}$ w/ any commutative ring.

25.4 = 26.1

Direct products $R_1 \times R_2$

(r_1, r_2) w/ operations componentwise.

Identities are $(1,1)$ and $(0,0)$.

Always has zero divisors.

Subrings $S \subseteq R$: Demand S be a ring itself.

Enough if: * S is a subgroup of R

* S is closed under multiplication.

Def. A commutative ring w/ no zero divisors is called an integral domain. (or just a domain)

Prop. In any domain (in fact, more generally...),

$ab = ac \implies a = 0$ or $b = c$.

Proof. $a(b-c) = 0$.

Note that not true for non-domains.

e.g., in $\mathbb{Z}/10\mathbb{Z}$, $2 \cdot 2 = 2 \cdot 7$.

Prop. Any finite integral domain R is a field.

Proof. Let $0 \neq a \in R$.

The function $\begin{array}{l} R \longrightarrow R \\ x \longmapsto ax \end{array}$ is injective by above,

hence surjective. In particular $\exists\, x \in R$ with $ax = 1$.

25.5. = 26.2

<u>Homomorphisms</u>:

A ring map $\varphi: R \to S$ is a <u>homomorphism</u> if

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all a, b.

[equiv: homo. on the additive groups]

(2) $\varphi(ab) = \varphi(a)\varphi(b)$.

(3) $\varphi(1) = 1$.

Its <u>kernel</u> is $\ker(\varphi) = \{x \in R : \varphi(x) = 0\}$.

ex. Let $\varphi: \mathbb{Z} \to \mathbb{Z}/5$

$x \to x \pmod 5$.

Non-example: determinants.

This is a ring homomorphism.

Its kernel is $5\mathbb{Z}$. Does not contain 1.

Indeed: if $1 \in \ker(\varphi)$ then $\varphi = 0$.

So in general, kernels of ring homomorphisms are not subrings.

<u>Warning</u>. DF says they are, because it doesn't demand that rings contain 1.

<u>Prop</u>. Let $I = \ker(\varphi)$ for some $\varphi: R \to S$.

Then I is closed under:

(1) addition, i.e. $x \in I, y \in I \Rightarrow x + y \in I$

(2) multiplication by elements of R,

$x \in I, r \in R \Longrightarrow xr \in I$ and $rx \in I$.

Easily checked. Such an I is called a (two-sided) <u>ideal</u> of R.

Also, I is a <u>left ideal</u> if closed under addition and $RI \subseteq I$

<u>right ideal</u> if $IR \subseteq I$ instead of $RI \subseteq I$.

Note: As a special case, don't call R an ideal of itself.

Prop. If $\varphi : R \to S$ is a ring hom then $\varphi(R)$ is a subring of S and $\ker(\varphi)$ is an ideal of R.

<u>Quotient rings:</u>

Let R be a ring and I an ideal, then $R/I = \{ r + I : r \in R \}$ <u>forms a ring</u>, the quotient ring of R by I.

1: Mult. identity is $1 + I$.

(Note: if $1 \in I$, then $1 \cdot r = r \in I$ for all I, so $I = R$.
So 1 is never in any ideal.)

Addition:

$$(r + I) + (s + I) = r + s + I + I = (r + s) + I.$$

Note: $I + I \subseteq I$ because closed under addition

and $I + I = I$ because $I + I \supseteq 0 + I = I$.

Multiplication:

$$(r + I)(s + I) = rs + Is + rI + I^2$$

This might <u>not</u> be $rs + I$ as a set.

But it is <u>contained</u> in I, so we may <u>define</u> $(r + I)(s + I)$ and this will be WD.

26.4.

Theorem.

(1) If $I \trianglelefteq R$ (I is an ideal of R), then R/I is a ring as defined above, and the map

$$\begin{aligned} R &\xrightarrow{\pi} R/I \\ r &\longmapsto r+I \end{aligned}$$

is a surjective ring homomorphism with kernel I.

(2) (First Iso. Theorem)

If $\varphi : R \to S$ is a hom, then $\mathrm{Im}(\varphi)$ is a subring of S, $\mathrm{Ker}(\varphi)$ is an ideal of R, and

$R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.

Examples.

Ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ (including 0).

An ideal must be an additive subgroup of $\mathbb{Z}$, and we know what these are already.

Have the reduction by n map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Example. The equation $x^2+y^2-3z^2=0$ has no integer solutions other than $(0,0,0)$.

Proof. May divide any sol'n by any power of 2 dividing all of x,y,z, so WLOG not all of x,y,z are even.

Consider the image of x,y,z under $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Must have a nontrivial solution there. But now this is a finite computation: there isn't.

26.5.

Ex. Let $R = \mathbb{R}[x]$.

Then the map
$$\mathbb{R}[x] \longrightarrow \mathbb{R}$$
$$f \longrightarrow f(a)$$
is a ring homomorphism for each $a \in \mathbb{R}$.

Its kernel is the ideal
$$I = \{ f(x) \in \mathbb{R}[x] : f(a) = 0 \}.$$

Oops! wrong

Ex. Again let $R = \mathbb{R}[x]$.

Let $I = \{ f(x) \in \mathbb{R}[x] : \deg(f) \geq 2 \}$.

This is an ideal, R/I is the ring of polynomials modulo a weird equivalence.

This has zero divisors, e.g. $x \cdot x = 0$.

Ex. $R = \mathbb{R}[x]$ again.

Let I be the <u>principal ideal</u> (x^2+1).

(In a commutative ring R, a <u>principal ideal</u> (r) is $\{ ar : a \in R \}$, all multiples of r.
Can define them in noncommutative rings too but they're weird.)

Look at $\mathbb{R}[x] / (x^2+1)$.

Then: (1) Every element can be uniquely represented as $a + bx$.

(2) This is actually a field. Can you prove it?

(3) Do you recognize this ring?

27.2. More definitions.

If I and J are ideals, their sum is

$$I + J = \{a + b : a \in I,\ b \in J\}.$$

Their product IJ consists of finite sums of elts. $a \cdot b$ with $a \in I$ and $b \in J$.

Powers are a special case of this.

Example. In $\mathbb{Z}$, $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$.

$$(6\mathbb{Z})(10\mathbb{Z}) = 60\mathbb{Z}.$$

Example. Let $R = \mathbb{Z}[x]$,

$I = \{$polys whose constant term is even$\}$.

This is an ideal. Check directly, or use the fact that it's the kernel of

$$\mathbb{Z}[x] \xrightarrow{ev_0} \mathbb{Z} \longrightarrow \mathbb{Z}/2.$$

$$f \longmapsto f(0)$$

Then $x^2 + 4 \in I^2$, because $x^2 \in I^2$ and $4 \in I^2$.

Even though $x^2 + 4$ doesn't factor in $\mathbb{Z}[x]$.

Example. Let F be a field.

$M_n(F)$ has no nontrivial two-sided ideals. (Prove!)

It does have one-sided ideals.

e.g. $I = \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 0 \end{bmatrix}$ is a right ideal of $M_3(F)$.

Why? Let $W = \langle e_1, e_2 \rangle \subseteq \mathbb{R}^3$.

Then, ~~the set~~ I consists of LT's sending $V \to W$.

That is still true if you precompose w/ any elt of $\mathrm{End}(V)$.

To get left ideals, take transposes.

The remaining iso theorems:

(2) Let $A \subseteq R$ subring and $B \trianglelefteq R$.

Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of R, $A \cap B \trianglelefteq A$, and $(A+B)/B \cong A/(A \cap B)$.

(3) Let I, J ideals of R with $I \subseteq J$.

Then $J/I \trianglelefteq R/I$ and $(R/I)/(J/I) \cong R/J$.

(4) If $I \trianglelefteq R$, there is a correspondence

$$\begin{array}{ccc} \text{~~ideals of~~ subrings of } R \text{ containing } I & \longleftrightarrow & \text{subrings of } R/I. \\ S & \longrightarrow & S/I. \end{array}$$

Preserves containment.

27.3. More on ideals:

Def. Let $A \subseteq R$ any subset.

(1) The ideal generated by A, (A), is the smallest ideal of R containing A.

[Here we implicitly regard R as itself.]

We have $(A) = \bigcap_{\substack{I \triangleleft R \\ A \subseteq I}} I$.

Here arbitrary intersections of ideals are again ideals.

If A is finite, (A) is said to be finitely generated

If A is a singleton, (A) (or (x) with $A = \{x\}$) is principal.

This cleans up when R is commutative, in which case

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

(even when A is infinite, defined as finite sums.)

This is easy to prove. Check that:

* (A) is an ideal of R
* If I is any other ideal of R containing A, it must contain (a).

In particular, when R is commutative,

$(x) = \{ rx : r \in R \}$.

Even principal ideals are terrible when R is not commutative.

27.4.

Examples.

1. In $\mathbb{Z}$, every ideal is of the form $n\mathbb{Z} = (n)$ for some n.
   (Easy to prove: let n be the minimum nonzero element of an ideal I.)

   So $\mathbb{Z}$ is a principal ideal domain.

   Properties of ideals mimic those of integers:

   $(n)\cdot(m) = (nm)$.

   $(n)+(m) = (\gcd(n,m))$.

   $b \in (a) \iff (b) \subseteq (a) \iff a \mid b$.

   $(b) \subseteq (a) \iff \exists$ an ideal (c) with $(b)=(c)(a)$.

2. Let F be a field. Then $F[x]$ is also a PID.
   Turns out to be the same proof as for $\mathbb{Z}$:
   can do division with remainder.
   (a Euclidean algorithm exists)

3. $\mathbb{Z}[x]$ is not a PID. $(2, x)$ is not principal.
   This is our ideal from before,

   $\ker(\mathbb{Z}[x] \xrightarrow{ev_0} \mathbb{Z} \longrightarrow \mathbb{Z}/2)$.

   Think your way through a proof.

4. Let R be functions $\mathbb{R} \to \mathbb{R}$.
   Let $I = \ker(ev_0)$.
   Then I is principal. A generator is

$$f(x) = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

27.5. = 28.1

If R is the ring of continuous functions, no longer true.

Prop. Let I be an ideal of R.

(1) I can't contain any units of R, unless $I = R$.

~~(or else $I = R \Rightarrow$ we exclude)~~

(2) If R is commutative,

R is a field $\Longleftrightarrow$ only ideals are 0 and R.

Proof.

(1) If $u \in I$, then $\exists\, x \in R$ with $xu = 1$, so $1 \in R$ and $1r \in I$ for all r

(2) $\Rightarrow$ Every elt of $R - \{0\}$ is a unit

$\Leftarrow$ For each $x \in R - \{0\}$, $(x) = R$ (since it's not 0.)

So x has a multiplicative inverse.

Cor. If R is a field, any nonzero ring hom from R is an injection.

Maximal and prime ideals.

Def. An ideal $I \trianglelefteq R$ is maximal if $I \neq R$ and the only ideals containing I are I and R.

[Assume R is commutative.]

Def. An ideal $I \trianglelefteq R$ is prime if $I \neq R$ and, for $a, b \in R$,

$ab \in P \Longrightarrow a \in P$ or $b \in P$.

28.2.

Example. In $\mathbb{Z}$, the maximal ideals are (p) where p is a prime number.

Recall that $(n) \subseteq (m) \iff m \mid n$, so this says the only divisors of p are 1 and p.

The prime ideals are (p) for p prime, and (0).

Example. In $\mathbb{C}[x]$, the maximal ideals are $(x-a)$ for $a \in \mathbb{C}$.

The prime ideals are these, and (0).

Example. In $\mathbb{C}[x,y]$, the maximal ideals are of the form $(x-a, y-b)$ for $a, b \in \mathbb{C}$.

(Can you prove this? maybe slightly messy...)

The prime ideals are:

* Those above (indeed: every max'l ideal is prime)
* 0 (always prime in an integral domain)
* (f), where $f \in \mathbb{C}[x,y]$ is any polynomial that doesn't factor.

We want to be able to prove this easily.

Regard these as corresponding to:

* Points in $\mathbb{C}^2$ ("closed points in $\mathbb{A}^2(\mathbb{C})$")
* All of $\mathbb{C}^2$ (the "generic point")
* Irreducible curves in $\mathbb{C}^2$.

28.3.

Write $\mathbb{A}^2_{\mathbb{C}}$ for the set of all such prime ideals (= "Spec $\mathbb{C}[x,y]$") w/ the correspondences above.

This turns out to be a nice thing to do.

Indeed, if R is <u>any</u> commutative ring, can make a nice space ("affine scheme") out of its prime ideals.

<u>Question.</u> Is $(y^2 - x^3 - 7)$ prime in $\mathbb{C}[x,y]$? How can we tell?

<u>Theorem.</u> Let R be commutative and $I \trianglelefteq R$. Then

(1) I is maximal $\longleftrightarrow$ R/I is a field.

(2) I is prime $\longleftrightarrow$ R/I is an integral domain.

<u>Cor.</u> Maximal ideals are prime.

<u>Proof.</u> (1) By the correspondence thm,

Ideals $I \subseteq J \subseteq R \longleftrightarrow$ Ideals $0 \subseteq J/I \subseteq R/I$.

(2) $ab \in P \Rightarrow a \in P$ or $b \in P$ in R

$\Updownarrow$

$ab = 0 \Rightarrow a = 0$ or $b = 0$ in R/P.

28.4.

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

This is a PID and all nonzero prime ideals are maximal.

Classify prime ideals $P \triangleleft \mathbb{Z}[i]$ by looking at $P \cap \mathbb{Z}$.

Note that $P \cap \mathbb{Z} = (p)$ for a prime integer p.

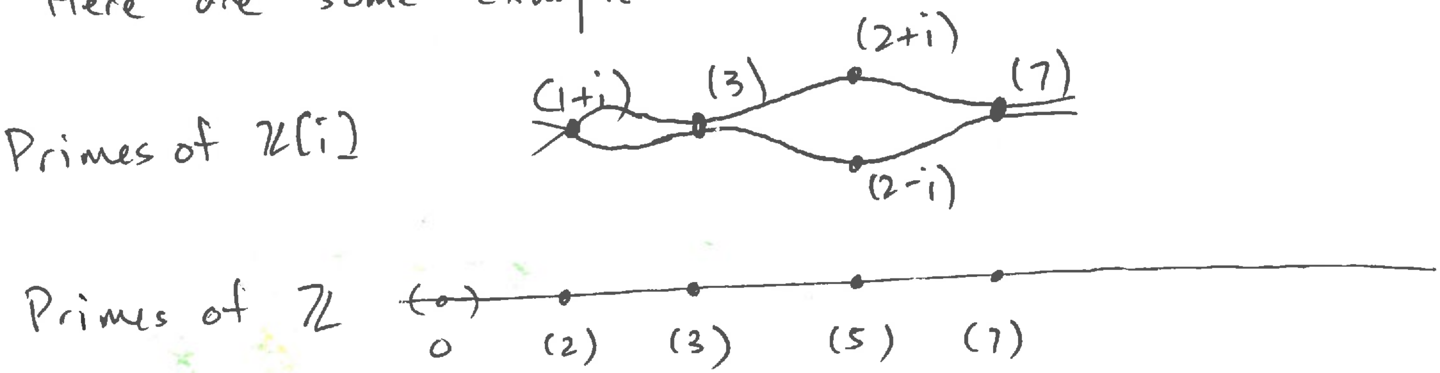
(1) $P \cap \mathbb{Z}$ contains a nonzero integer:

Let $0 \neq a+bi \in \mathbb{Z}[i]$, then $a^2+b^2 \in P$.

(2) Now if $P \cap \mathbb{Z} = (de)$ then $de \in P \Rightarrow d \in P$ or $e \in P$.

So one of them is ± 1.

Here are some examples:



The classification is:

If $p \equiv 3 \pmod 4$, (p) is still prime (it is inert)

So, e.g., $\mathbb{Z}[i]/(3)$ is a field of order 9.

If $p \equiv 1 \pmod 4$, $(p) = PP'$ for a prime ideal P of $\mathbb{Z}[i]$ with conjugate P' (p is split)

If $p = 2$, $(2) = (1+i)^2$.

This is called ramification.

So: Theorem. A prime p is the sum of two integer squares iff it is 2 or $\equiv 1 \pmod 4$.

Want to learn more? TAKE MATT'S ALGEBRAIC NUMBER THEORY CLASS!

28.5.

In general, all prime ideals are contained in a maximal ideal.

This uses the axiom of choice, or equivalently Zorn's lemma

Theorem. The following are equivalent, and independent of the usual set theory axioms.

1. Zorn's Lemma: Given a set A with a partial order $\leq$ satisfying

   (a) $x \leq x$ for all A

   (b) $x \leq y,\ y \leq z \Rightarrow x \leq z$

   (c) $x \leq y,\ y \leq x \Rightarrow x = y$

   (but you can't necessarily compare any two elements)

   Definition: B is a chain of A if $x \leq y$ or $y \leq x$ when $x, y \in B$.

   Assume that every chain B of A has an upper bound, i.e. $\exists\ u \in A$ with $b \leq u$ for all $b \in B$.

   Then A contains a maximal element m, satisfying

   $$m \leq x \Rightarrow m = x.$$

   [Does not say $n \leq m$ for all n. Can have multiple maximal elements!]

2. The axiom of choice.

   The Cartesian product of a nonempty collection of nonempty sets is empty.

   e.g. if S is any nonempty set and A_α is a nonempty set for each $\alpha \in S$, there exists a function

   $$S \longrightarrow \bigcup_{\alpha \in S} A_\alpha.$$

25.6.

3. ~~Ex~~ The well ordering principle. Given any set S, there exists a total ordering on S s.t. every nonempty $A \subseteq S$ has a smallest element.

"The axiom of choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?"
— Jerry Bona.

Proof that every proper ideal I is contained in a maximal ideal.

Let $S = \{$proper ideals of R containing $I\}$

Then containment is a partial order.

Let C be a chain : a collection of proper ideals so that $J, J' \in C \longrightarrow J \subseteq J'$ or $J' \subseteq J$.

Then $K = \bigcup_{J \in C} J$ is an ideal :

If $x \in K$ then $x \in J$ for some J, so $xr \in J$.

If $x, x' \in K$, both are contained in J, so their sum is also.

It is proper because $1 \notin J$ for each $J \in C$.

So every chain in C has an upper bound in S.

Dig out Zorn's Hammer.

28.7. (≥30,1) Fractions and localization:

Let R be a commutative ring containing 1,
D = any nonempty subset of R, not containing zero or any zero divisors, and closed under multiplication.

Then, we can form a ring of fractions RD^{-1}

The elements are symbols $\frac{r}{d}$ with $r \in R$, $d \in D$

with $\frac{r}{d} = \frac{r'}{d'}$ if $rd' - r'd = 0$.

If R is a domain and $D = R - \{0\}$, then RD^{-1} is a field, the field of fractions of R.

Theorem.

(0) All of this is WD and actually gives you a ring.
(1) R embeds as a subring of RD^{-1}
(2) RD^{-1} is the "smallest ring in which all elts of D become units":

Given $R \overset{\varphi}{\hookrightarrow} S$ s.t. $\varphi(D) \subseteq$ units of S.

Then, we get a commutative diagram

$$\begin{tikzcd}
R \arrow[r, hook, "\varphi"] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & S \\
RD^{-1} \arrow[ur, dashed, "\exists!"'] &
\end{tikzcd}$$

So S must contain a copy of RD^{-1}.

This is an example of a universal property.

28.9.

Example. Let $R = \mathbb{C}[x]$.

Its field of fractions, $\mathbb{C}(x)$, consists of rational functions.

Now let $P = (x-a)$ for some $a \in \mathbb{C}$.

Then $R_P = \{ \text{rational functions } \frac{f}{g} : g(a) \neq 0 \}$.

So R_P contains functions defined in a neighborhood of a.

Example. Let $R = \{ \text{holomorphic functions } \mathbb{C} \longrightarrow \mathbb{C} \}$.

The fraction field of R consists of meromorphic functions (poles are isolated).

Consider the maximal ideal (it's prime of course)

$(x) \subseteq R = \operatorname{Ker}(ev_0)$.

It has residue field $R/(x) \cong \mathbb{C}$

and localization $R_{(x)} = \{ \text{mero fns. holo in a nbd of } 0 \}$.

This is also a local ring. Max ideal: functions that vanish at 0.

Many of these local rings are discrete valuation rings.

(DVR's are local PID's that are not fields)

Indeed (see 15.4) you can avoid assuming that D contains no zero divisors.

$$\frac{r}{d} = \frac{r'}{d'} \quad \text{if} \quad rd' - dr' \text{ is a zero divisor.}$$

But then the map $R \longrightarrow RD^{-1}$ might not be an injection.

If $0 \in D$ then $RD^{-1} = 0$.

Examples. $R = \mathbb{Z}$, $D = \mathbb{Z} - \{0\}$. Then $RD^{-1} = \mathbb{Q}$.

~~Examples~~ $R = \mathbb{Z}$, $D = \{p^c : c \geq 0\}$ for a prime p.

Then RD^{-1} consists of fractions with only p's in the denominator.

Localization at a prime. Let P be a prime ideal, $D = R - P$.

Then, because $xy \in P \Rightarrow x \in P$ or $y \in P$, we have $x \in D$ and $y \in D \Rightarrow xy \in D$.

Also, D contains 1 (because P can't).

We write $R_P = R(R-P)^{-1}$, the localization at P.

Examples. $\mathbb{Z}_{(5)} = \{\frac{a}{b} \in \mathbb{Q} :$ ~~[illegible]~~ b is coprime to $5\}$.

This is a ring (not $\mathbb{Z}_5$ or $\mathbb{Z}/5$), not a field, and a local ring: it has a unique maximal ideal.

30.4 (28.10)

Here a discrete valuation is a function

$R \xrightarrow{v} \mathbb{Z}$ where $v(x) = i$

local ring with maximal ideal M with $x \in M^i$ and $x \notin M^{i+1}$.

Example (1) In $\mathbb{Z}_{(5)}$, this is the p-adic valuation, v_5:

$v_5(5^k \cdot \frac{a}{b}) = k$ if a and b are coprime to 5.

(2) with R the ring of holo functions, the discrete valuation associated to (x) and $R_{(x)}$ is the order of vanishing at 0.

$v(x^k \cdot f) = k$ if f is a meromorphic function defined and nonvanishing at 0.

You also get an absolute value $|r| = e^{-v(r)}$ which defines a metric.

(Alternatively, if $v = v_p$, you can use base p.)

You get completions (power series, p-adic integers) which (at least in this case) coincide with inverse limits.

30.5.

Chinese remainder theorem:

R = comm. ring

Let $I_1, \dots, I_k$ be comaximal ideals ($I_i + I_j = R$ if $i \neq j$).

Consider the ring homomorphism

$$R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_k$$
$$r \longmapsto (r, r, \dots, r),$$

whose kernel is exactly $I_1 \cap \cdots \cap I_k$. Then, the map is surjective and $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$.

Example. In $\mathbb{Z}$, $I_1 = (a)$ and $I_2 = (b)$ are comaximal iff a and b don't have a common factor.

Then, if they are
$$\mathbb{Z}/(ab) \xrightarrow{\sim} \mathbb{Z}/(a) \times \mathbb{Z}/(b)$$
and similarly for bigger products.

Example. (Partial fractions)

Let $g(x) = (x-a_1)\cdots(x-a_r)$ where the a_i distinct.

$f(x) \in \mathbb{C}[x]$ of degree $< r$.

Then $$\frac{f(x)}{g(x)} = \frac{b_1}{x-a_1} + \cdots + \frac{b_r}{x-a_r}$$ for some b_i.

Same if you replace $\mathbb{C}$ by any field.

Proof. $$\mathbb{C}[x]/((x-a_1)\cdots(x-a_r)) \xrightarrow{\sim} \mathbb{C}[x]/(x-a_1) \times \cdots \times \mathbb{C}[x]/(x-a_r).$$

Apply this to f and chase down the consequences.

31.1. Proof.

Induction on k.

If $k=2$, look at

$$R \xrightarrow{\varphi} R/I_1 \times R/I_2$$
$$r \xmapsto{\varphi} (r \bmod I_1,\ r \bmod I_2).$$

Will argue $(1,0)$ and $(0,1)$ in the image.

Since $I_1 + I_2 = R$, can solve $x_1 + x_2 = 1$, $x_i \in I_i$.

Then $\varphi(x_1) = (x_1, 1 - x_2) = (0,1)$

$\varphi(x_2) = (1 - x_1, x_2) = (1,0)$.

So surjective.

Why $I_1 \cap I_2 = I_1 I_2$? Certainly $I_1 I_2 \subseteq I_1 \cap I_2$.

Conversely, if $z \in I_1 \cap I_2$, $z = z(x_1 + x_2)$

$$= z x_1 + z x_2$$
$$\in I_2 I_1 + I_1 I_2 = I_1 I_2.$$

If $k \geq 2$, follows by induction (with I_1, $I_2 \cdots I_k$) if these two ideals are comaximal.

For each $i \geq 2$, write $1 = x_i + y_i$, now with $x_i \in I_1$, $y_i \in I_i$.

Then $1 = (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k)$

$$= \underbrace{y_2 y_3 \cdots y_k}_{\in I_2 \cdots I_k} + \underbrace{(\text{terms with at least one } x_i)}_{\in I_1}.$$

So done.

31.2.

Notice that the groups of units on both sides are thus proved to be isomorphic. So, if $(m,n)=1$,

$$(\mathbb{Z}/mn)^\times \cong (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times .$$

In particular, if $n = p_1^{a_1} \cdots p_k^{a_k}$ (prime factorization)

then
$$(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{a_1})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k})^\times .$$

Writing $\varphi(n) = \#(\mathbb{Z}/n)^\times = \#$ residue classes mod n,

we have $\varphi(n)$ is <u>multiplicative</u>:

$$\varphi(nm) = \varphi(n)\varphi(m) \quad \text{if } \gcd(n,m)=1.$$

Can also compute: $\varphi(p^a) = p^{a-1}\cdot(p-1)$.

//

<u>Euclidean rings</u>.

If R is an integral domain, a <u>norm</u> on R is any function

$N: R \to \{0,1,2,\dots\}$ with $N(0)=0$.

The norm is <u>positive</u> if $N(a)>0$ for $a \neq 0$.

<u>Def.</u> R is a <u>Euclidean domain</u> if it has a norm N s.t.:

Given $a,b \in R$ with $b \neq 0$, there exist $q,r \in R$ with

$$a = qb + r$$
$$r = 0 \text{ or } N(r) < N(b).$$

31.3.

The point: can run the Euclidean algorithm.

Examples.

$\mathbb{Z}$, $N(a) = |a|$.

$F[x]$ (F a field), $N(f) = \deg(f)$.

Polynomial long division is a thing.

$\mathbb{Z}[x]$ is <u>not</u>.

You can't write $x^2 = q \cdot (2x) + r$

for any q and r with $\deg(r) < 2$.

$\mathbb{Z}[i]$, $N(x + yi) = x^2 + y^2$.

Solve $a = qb + r$ again.

$\cancel{(a+bi) = q(c+di) + r}$

Let $a = a_1 + a_2 i$ $(a_1, a_2 \in \mathbb{Z})$

$b = b_1 + b_2 i$

Then, $$\frac{a}{b} = \frac{(a_1 + a_2 i)(b_1 - b_2 i)}{b_1^2 + b_2^2}$$

$\cancel{= a_1 + b_1}$

$$= \frac{a_1 b_1 + a_2 b_2}{b_1^2 + b_2^2} + \frac{a_2 b_1 - a_1 b_2}{b_1^2 + b_2^2}\, i.$$

Write $c + di$ for the <u>closest</u> elt. of $\mathbb{Z}[i]$,

so that $$\frac{a}{b} = (c + di) + \frac{r}{b}.$$

31.4.

Now, $\left|\operatorname{Re}\left(\frac{r}{b}\right)\right| \le \frac{1}{2}$ and $\left|\operatorname{Im}\left(\frac{r}{b}\right)\right| \le \frac{1}{2}$

so that $\frac{N(r)}{N(b)} = N\left(\frac{r}{b}\right) \le \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right) < 1.$

This bears checking!

Note. This works for $\mathbb{Z}[\sqrt{D}]$ when $D = -2, -3, -7, -11$.
It eventually stops working.

Here's the point.

Theorem. Any Euclidean domain is a PID.

Proof. Given $I \trianglelefteq R$ in a Euclidean domain w/ norm N.
Choose $d \in I$ nonzero of minimum norm.
Clearly $(d) \subseteq I$. If there exists $x \in I \setminus (d)$,
write $x = qd + r$
with $N(r) < N(d)$ (note: r can't be 0).
But $r \in I$, contradiction.

Note that gcd's exist in Euclidean domains.

Also, in a ring R, $b \mid a \Longleftrightarrow a \in (b)$

$\Updownarrow$ $\Updownarrow$

$a = bx$ for $x \in R$ (by def.) $(a) \subseteq (b)$.

Translating the definitions,
in a PID, $(a) + (b) = (\gcd(a, b))$.
So $(a, b) = ((a, b))$. Ha!

31.5 = 32.1

They'll be unique up to units:

Prop. Let R be an integral domain and suppose $(d) = (d')$ for some d, d'. Then $d' = ud$ for some $u \in R^\times$.

Proof. Assume nonzero. $d' = xd$ and $d = yd'$ for some $x, y \in R$. So $d = xyd$, so $xy = 1$ (R a domain!) So x and y are units.

Note also that you can write

$$\gcd(a,b) = ax + by \quad \text{for some } d \in R$$

(just as in NT).

Prop. Every nonzero prime ideal in a PID is maximal.

Proof. Given $(p) \subsetneq (m)$, $p = mx$ for some $x \in R$,

So $x \in (p)$ because m isn't.

But then $p = myp$ for some $y \in P$.

So m is a unit and $(m) = R$.

31.6. = 32.2

Unique factorization:

Let R be an integral domain.

Def. (1) If $r \in R$ (nonzero, not a unit), r is irreducible if, whenever $r = ab$ in R, a or b is a unit.

(2) $p \in R$ is prime if (p) is,

Equivalently, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Prop. In an integral domain, prime $\Rightarrow$ irreducible.

Proof. Given $p = ab$. Then $p \mid a$ or $p \mid b$.

WLOG $p \mid a$, so $a = px$

and once again $p = pxb$,

b is a unit.

The converse is NOT true.

Example. $\mathbb{Z}[\sqrt{-5}]$. Check: 3 is irreducible:

Suppose $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. ~~$\Rightarrow bc = ad$~~

~~$= (ac + 5bd) + \sqrt{-5}(bc$~~ $\Rightarrow$

$= (ac + 5bd) + \sqrt{-5}\,(\underbrace{bc + ad}_{\text{uggh}\ldots\ldots})$] Solve this?

Sensible way to think: Take the field norm.

$$9 = (a^2 + 5b^2)(c^2 + 5d^2).$$

There's no way to get 3, and $a^2 + 5b^2 = 1$

$\Rightarrow$ $a + b\sqrt{5} = \pm 1$

a unit.

31.7 = 32.3

But 3 is not prime, because:

$$9 = (2+\sqrt{-5})(2-\sqrt{5})$$

$3 \mid 9$, but $3 \nmid 2 \pm \sqrt{-5}$.

But:

Prop. In a PID, irreducible $\Rightarrow$ prime.

Proof. Given x irreducible.
will show (x) maximal, therefore prime, therefore x prime.

So suppose $(x) \subseteq (y)$.
Then $x = yz$ for some $z \in R$.
Either y is a unit (so $(y) = R$)
or z is a unit (so $(y) = (x)$)
and so (x) is maximal.

Def. An integral domain R is a UFD (unique factorization domain) if every nonzero nonunit $r \in R$ satisfies:

(1) r can be written as a finite product of irreducibles;

(2) Unique up to units.
If $r = p_1 p_2 \cdots p_n = q_1 \cdots q_m$
then $n = m$ and after a reordering, $q_i = u_i p_i$ for units u_i.

32.4.

Examples.

Fields (vacuously)

$\mathbb{Z}$.

$R[x]$, whenever R is. (To be proved)

$\mathbb{Z}[\sqrt{-5}]$ is not.

$\mathbb{Z}[2i]$ is not, $4 = 2 \cdot 2 = (-2i) \cdot 2i$ and 2 and $\pm 2i$ do not differ by a unit of this ring.

Prop. In a UFD, prime $\longleftrightarrow$ irreducible.

Proof. $\longrightarrow$ already done.

Assume x irreducible and $x \mid ab$.

So $xy = ab$ for some $y \in R$.

Factor into irreducibles!

x has to occur as a factor dividing a or b.

Have the usual gcd formula

$$\gcd(\underbrace{u p_1^{e_1} \cdots p_n^{e_n}, v}_{\text{units}} p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}) = p_1^{\min(e_1,f_1)} \cdots p_n^{\min(e_n,f_n)}.$$

[Note: we assume the e_i and f_i are ≥ 0, so we can write the same prime factors for both.]

32.5.

Goal. Every PID (hence every Euclidean domain) is a UFD.

We need more structure theory first.

Def. A ring R is Noetherian if it satisfies the ascending chain condition wrt ideals: given a chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$, it must eventually stabilize, i.e. $I_i = I_j$ for $i, j \geq k$ (for some k).

Prop. Any PID is Noetherian.

Proof. Given an increasing chain of ideals
$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$
here $(x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \dots$

Their union is also an ideal, hence (x) for some $x \in R$.

Must have $x \in (x_i)$ for some i, hence $(x) \subseteq (x_i)$ hence $(x) = (x_i)$.

[33.1] —

Thm. Every PID is a UFD.

Part 1. Existence of factorization into irreducibles.

Given x.

Irreducible? $\xrightarrow{\text{Yes}}$ Done.

$\downarrow$ No

$x = x_1 x_2$.

Are both x_1 and x_2 irreducible?

Yes $\rightarrow$ done.

No $\rightarrow$ factor one of them.

32.6. = 33.2.

The claim is that the process must terminate:

We get a sequence of elements

$x_1 \mid x$ and $(x) \subseteq (x_1)$, with $(x) \neq (x_1)$

because x_2 is not a unit.

and $(x_1) \neq R$

because x_1 not a unit.

Similarly $(x) \subsetneq (x_2)$.

If the process doesn't terminate, would similarly get

$(x_1) \subsetneq (x_3)$ or $(x_2) \subsetneq (x_3)$, and so on.

But R was proved Noetherian.

Uniqueness. Given

$r = p_1 \cdots p_n = q_1 \cdots q_m$, induct on n.

(factored into irreducibles)

Since irred $\Longrightarrow$ prime in a PID,

$p_1 \mid q_i$ for some i. WLOG $p_1 \mid q_1$.

But q_1 is irreducible so $q_1 = u p_1$ for some $u \in R^\times$.

Get $r = p_1 \cdots p_n = u p_1 q_2 \cdots q_m$

$= p_1 \cdots p_n = p_1 (u q_2) \cdots q_m$.

Now cancel p_1 and use induction.

33.3.

Note. See Ch. 8.3 (or Boylan's class) for prime factorization in $\mathbb{Z}[i]$.

Summary.

Fields $\subseteq$ Euclidean domains $\subseteq$ PIDs $\subseteq$ UFD's $\subseteq$ Integral domains.

examples.

$\mathbb{Q}$ $\qquad \mathbb{Z}[i] \qquad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \qquad \mathbb{Z}[x] \qquad \mathbb{Z}[\sqrt{-5}]$.

Polynomial rings.

Let R be a commutative ring.

The polynomial ring $R[x]$ consists of formal sums $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$.

A polynomial is monic if $a_n = 1$.

The degree of the above is n.

Addition and multiplication as usual.

Have an injection $R \longrightarrow R[x]$.

Prop. (easy) If R is a domain, then $R[x]$ is, and

(1) $\deg pq = \deg p + \deg q$ (if $pq \neq 0$)

(2) $R[x]^\times = R^\times$.

33.4.

Can also define polynomial rings in multiple variables

$$R[x_1, x_2, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$$

by induction. Can do infinitely many variables too.

Terminology:

A monic term $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ is a <u>monomial</u> is the <u>monomial part</u> of $a x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$.

Any elt. of a polynomial ring is a finite sum of these.

The term has degree <u>d_i in x_i for each i</u>

$d = d_1 + \cdots + d_n$ (total degree).

f is <u>homogeneous</u> if all terms have the same degree.

Prop. Let R be a comm. ring, $I \trianglelefteq R$.

Write (I) = ideal generated by I in $R[x]$.

(1) I is the set of polynomials with coeffs in I.

[Do by pure thought.]

(2) $R[x]/(I) \cong (R/I)[x]$.

(So, for example, $\mathbb{Z}[x]/p\mathbb{Z}[x] = \mathbb{F}_p[x]$.

(3) If I is a prime ideal of R, (I) is prime in $R[x]$.

Proof of (2). Define

$$R[x] \xrightarrow{\varphi} (R/I)[x]$$

Immediate to check: - is a homomorphism

- kernel is polynomials w/ coeffs in I.

This is exactly (I).

---

(3) I prime $\Leftrightarrow$ R/I domain $\longleftrightarrow$ $(R/I)[x]$ domain $\Leftrightarrow$ $R[x]/(I)$ domain $\Leftrightarrow$ (I) prime in $R[x]$.

33.5 = 34.1

Prop. If F is a field, then $F[x]$ is Euclidean:

Given $f, g \in F[x]$ with $g \neq 0$, $\exists!\ q, r \in F[x]$ with

$$f = qg + r, \qquad r = 0 \text{ or } \deg(r) < \deg(g).$$

(Proof omitted. Do long division.)

Cor. $F[x]$ is a PID and a UFD.

Start here. (Dummit-Foote Ch. 9.3)

Gauss's Lemma. Let R be a UFD w/ fraction field F.

Given p ~~...~~ $\in R[x]$.

Then, p reducible in $F[x] \Longrightarrow p$ reducible in $R[x]$.

In other words: If we can write $p = fg$ for nonconstant polynomials f, g in $F[x]$, we can do so in $R[x]$.

Proof. Given a factorization $p = fg$ in $F[x]$,
Clear denominators to write $dp = f'g'$ in $R[x]$ for some f', g'. (Note: dashes don't denote derivatives here.)
Here $d \in R$.

If d is a unit we're done with $p = (d^{-1}f')g'$.
Otherwise, factor into irreducibles $d = d_1 d_2 \cdots d_k$.
Look at $dp = f'g'$ in the ring $(R/d_1)[x]$:

d_1 irreducible in $R \longrightarrow d_1$ and (d_1) prime in R
$\longrightarrow (d_1)$ prime in $R[x]$
$\longrightarrow (R/d_1)[x]$ is an integral domain.

In $(R/d_1)[x]$, have $0 = dp = d_1 \cdots d_k p = f'g'$.
But $(R/d_1)[x]$ is a domain.
Conclusion: d_1 divides f' or g'.
So cancel it from ~~the~~ both sides, and move through the rest of the d_i's.

Corollary. Let R = UFD w/ fraction field F, $p \in R[x]$.
~~Then~~ Suppose further gcd(coeffs of p) = 1.
(i.e., true if p is monic.)
Then, $p(x)$ irreducible in $R[x] \Longleftrightarrow$ irred in $F[x]$.

Proof. ~~___~~ $\Longrightarrow$ is Gauss' Lemma.
$\Longleftarrow$: Suppose p is reducible in $R[x]$.
Then $p = fg$ in $R[x]$, but neither f nor
with f, g nonunits. g can be a constant.
(Because no nonunit divides all the coeffs of p by hypothesis.)
So this is a factorization in $F[x]$.

Note. Why the condition on the gcd of the coeffs of p?
Consider $R = \mathbb{Z}$, $F = \mathbb{Q}$, $p(x) = 5x + 5$.
Then p is reducible in $\mathbb{Z}[x]$, $5x + 5 = 5(x+1)$ is a nontrivial factorization in $\mathbb{Z}[x]$.
Neither 5 nor $x+1$ is a unit in this ring.
We still have $5x + 5 = 5(x+1)$ in $\mathbb{Q}[x]$, but now 5 is a unit, so this factorization "doesn't count".

34.3.

Thm. If R is a UFD, so is $R[x]$.

Note. $R[x]$ UFD $\longrightarrow$ R is.

why? Factorizations of elements of R are the same in R and in $R[x]$. So are the units.

Proof. Existence of a factorization into irreducibles:

~~If f is irreducible in R, done.~~
~~Otherwise, factor $f = f_1 f_2$ in $F[x]$~~
~~(where F = fraction field)~~

First step.

Write $f = d \cdot f'$, where $d = (\gcd$ of coeffs of $f)$.

Such a factorization exists and is unique.

R is a UFD part, so handle d.

Also assume $\deg(f') > 0$. (otherwise, take $f' = 1$.)

So: Reduced to the case where $d = 1$, $\gcd(\text{coeffs of } f') = 1$.

Now, factor f' in $F[x]$, where F = fraction field of R.

Since $\gcd(\text{coeffs of } f') = 1$,

reducible in $R[x]$ $\longleftrightarrow$ reducible in $F[x]$.

Moreover, looking at the proof of Gauss's Lemma,

I don't think we need this.

If we factor $f' = gh$ in $F[x]$,

then our factorization in $R[x]$ looks like

$f' = (cg)(c^{-1}h)$ for some $c \in H$.

So keep factoring in R.

Note that, in $R[x]$, if we write $g = h_1 h_2$

for $g, h_1, h_2 \in R[x]$ and $\gcd(\text{coeffs of } g) = 1$,

then we must also have

$\gcd(\text{coeffs of } h_1) = \gcd(\text{coeffs of } h_2)$ divide $\gcd(\text{coeffs of } g) = 1$. Hence 1.

34.4.

This means we can apply the corollary at every stage. Eventually we get a factorization in $R[x]$, which exactly follows that in $F[x]$.

Uniqueness.

Suppose that

$$f' = g_1 \cdots g_r = h_1 \cdots h_s \text{ in } R[x].$$

(As before, each g_i, h_j must have the gcd of its coeffs $=1$.)

Then, by unique factorization in $F[x]$, $r=s$ and after reordering $g_i = c_i h_i$ for some unit $c_i \in F[x]^\times$, i.e. for some $c_i \in F$.

Write $c_i = \frac{x}{y}$ with x, y coprime and in R,

Then $g_i = c_i h_i \Rightarrow y g_i = x h_i$ in R.

Choose any prime factor p of y.

Then $p \mid x h_i$, so $p \mid x$ or $p \mid h_i$.

But $p \nmid x$ by hypothesis that x, y coprime

$p \nmid h_i$ because gcd (coeffs of h_i) $= 1$.

So ~~ϕ~~ y can't have any prime factors

Hence $y \in R^\times$ and similarly $x \in R^\times$ and $c_i \in R^\times$.

This means $g_i = c_i h_i$ where c_i lives in $R^\times$.

.... and we're done.

34.5 .

Cor. If R is a UFD, so is $R[x_1, \ldots, x_n]$.

Proof. Use above + induct on n.

Irreducibility criteria.

When can we tell if a polynomial is irreducible?

Example. x^2+1. Is it irreducible?

Depends. Is irreducible over $\mathbb{R}$

not over $\mathbb{C}$.

It is not irreducible over $\mathbb{Z}/2$: $(x^2+1) = (x+1)^2$.

141 students:
We're trained professionals.
Don't try this at home.

For odd primes p,

x^2+1 irreducible over $p \Longleftrightarrow p \equiv 3 \pmod 4$.

Sketch proof.
Look at the group $(\mathbb{Z}/p)^\times$ of order $p-1$.
It's cyclic (take this for granted).
The map $x \longrightarrow x^2$ has kernel of size 2
(we know because the group is cyclic)
and image of size $\frac{p-1}{2}$.

The image is the set

$\{a \in \mathbb{F}_p^\times : a = y^2 \text{ for some } y \in \mathbb{F}_p\}$

$= \{a \in \mathbb{F}_p^\times : y^2 - a = 0 \text{ has a solution } y \in \mathbb{F}_p\}$

$= \{a \in \mathbb{F}_p^\times : y^2 - a \text{ factors (i.e. is reducible) in } \mathbb{F}_p\}$.

34.6.

If we write x for a generator of $\mathbb{F}_p^\times$,

$$-1 = x^{\frac{p-1}{2}} \text{ in } \mathbb{F}_p.$$

(It's the unique element whose square is $x^{p-1} = 1$.)

If $p \equiv 1 \pmod 4$, then

$$-1 = \left(x^{\frac{p-1}{4}}\right)^2,$$ so can factor x^2+1.

If $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd

and the squares in $\mathbb{F}_p$ are exactly

$\{x^b : 0 \le b \le p-2 : b \text{ even}\}$.

This question is also interesting over prime powers.

Interesting Exercise. If $p \equiv 1 \pmod 4$ is prime, and $a \ge 1$ is any integer, then x^2+1 is reducible in $\mathbb{Z}/p^a$.

Proof sketch. Induction on a. Above is a base case.

Prove reducible in $\mathbb{Z}/p^a \longrightarrow$ reducible in $\mathbb{Z}/p^{a+1}$.

This is actually fairly easy.

It's the first case of "Hensel's Lemma"

The argument also establishes that x^2+1 is reducible over the p-adic integers $\mathbb{Z}_p$

(basically all $\mathbb{Z}/p^a$ mashed together).