27.24 Thm. If F is a field then $F[x]$ is a principal ideal domain (PID).

Proof: Let $I \subset F[x]$ be an ideal

if $I = \{0\}$. $I = (0)$ is principle

if $I \neq \{0\}$. then let $g(x) \in I$ be a elem with minimal degree.

If $g(x) \in F$, then $(g(x)) = F[x] \subset I$ and $I = F[x] = (1)$. is principal

For the remaining case $\deg g(x) \geq 1$. Let $f(x) \subset I$.

$$f(x) = q(x)\,g(x) + r(x).$$

for unique $q(x), r(x) \in F[x]$

s.t. $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Then $r(x) = \underbrace{f(x)}_{\in I} - q(x)\underbrace{g(x)}_{\in I}$

$\Rightarrow r(x) \in I$.

Since $g(x)$ is of minimal degree the case $\deg r(x) < \deg g(x)$ is impossible

$\Rightarrow r(x) = 0$.

$\Rightarrow f(x) = q(x)g(x) \Rightarrow (g(x)) \subset I \subset (g(x))$

$\Rightarrow I = (g(x))$ is principal.

So far, we have seen two PIDs:

① $R = \mathbb{Z}$.

② $R = F[x]$. F is a field.

27.25. Thm: The $p(x) \in F[x]$ be a nonzero polynomial

$(p(x))$ is a maximal ideal

$\Leftrightarrow$ $p(x)$ is irreducible over F.

Proof: "$\Rightarrow$" Assume $(p(x))$ is a maximal ideal

$(p(x))$ is maximal

$\Rightarrow F[x]/(p(x))$ is a field.

$\Rightarrow$ $F[x]/(p(x))$ has no zero divisors.

$\Rightarrow$ $p(x)$ is not of the form

$p(x) = a(x)\,b(x)$ for $\deg a(x) < \deg p(x)$ and $\deg b(x) < \deg p(x)$

$\Rightarrow$ $p(x)$ is irreducible.

Other proof: Using the def of maximal ideal.

if $p(x) = a(x)\,b(x)$.

then $(p(x)) \subset (a(x)) \subset F[x]$.

if $0 < \deg a(x) < \deg p(x)$.

then $(p(x)) \subsetneq (a(x)) \subsetneq F[x]$

and $p(x)$ is not maximal. $\Rightarrow \Leftarrow$.

"$\Leftarrow$" Assume $p(x)$ is irreducible and let $(p(x)) \subset I \subset F[x]$.

$F[x]$ is a PID $\Rightarrow$ I is of the form $I = (g(x))$.

$p(x) \in (g(x))$. $\Rightarrow$ $p(x) = q(x)\,g(x)$

Since $p(x)$ is irreducible

$\Rightarrow$ either $q(x) \in F$ or $g(x) \in F$.

If $q(x) \in F$, then $(p(x)) = (g(x)) = I$.

If $g(x) \in F$, then $I = (g(x)) = F$.

either or

$\Downarrow$

$p(x)$ is maximal.

Ex.: if p is a prime and $f(x) \in \mathbb{Z}_p[x]$ is an irreducible ploynomial, then $\mathbb{Z}_p[x]/(f(x))$ is a field.

the field is of size p^d. $d = \deg f(x)$.

Elements of the $\mathbb{Z}_p[x]/(f(x))$ are of the form

$a(x) + (f(x))$

$\nwarrow$ $a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}$

if $\deg f(x) = d$.

For given prime p, and degree d. is there an irreducible polynomial $f(x) \in F[x]$ of degree d?

Yes! for all p, d.

Thm: Every finite field is of size p^d, for some prime p. and some integer $d \geq 1$.
Any finite field of same size are isomorphic.
In particular, if $f_1(x), f_2(x) \in \mathbb{Z}_p[x]$ are different irreducible polynomials of the same degree. then $\mathbb{Z}_p/(f_1(x)) \simeq \mathbb{Z}_p/(f_2(x))$.

Ex: $p=3$ $d=2$. In $\mathbb{Z}_3[x]$,

a	a^2+1
0	1
1	2
2	2

$\Rightarrow$
$x^2+1 \in \mathbb{Z}_3[x]$ is irreducable

$\mathbb{Z}_3[x]/(x^2+1)$ is a field. of size 3^2.

For $a+bx$, $c+dx \in F$.
$(a+bx)+(c+dx) = (a+c)+(b+d)x$.

$(a+bx)(c+dx) = ac+(ad+bc)x+bdx^2$
$= (ac-bd)+(ad+bc)x$.

office. Tu 5-6 344 AH.

Th 7 p.m. DKH 114.

Exercise. $\mathbb{Q}[x]/(x^2-6x+6)$ a field?

Prove x^2-6x+6 is irreducible.

Assume that $x^2-6x+6=(ax+b)(cx+d)$

Divide both sides by $ac=1$ — Assume $a, b \in \mathbb{Z}$, $\gcd(a,b)=1$.

$$x^2-6x+6=(x+\frac{b}{a})(x+\frac{d}{c})$$

if it is reducible, it has a zero $x=-\frac{b}{a}\in\mathbb{Q}$

$$\frac{b^2}{a^2}+6\frac{b}{a}+6=0.$$

$$b^2+6ab+6a^2=0.$$

$$b^2=-6a(b+a)$$

$\Rightarrow$ $\underline{2\,|\,b}$, say $b=2c$. $\Rightarrow$ $4c^2+12ac+6a^2=0$.

$$3a^2=-2c(c+3a).$$

$$2\nmid 3.$$

$\Rightarrow 2\,|\,a^2 \Rightarrow \underline{2\,|\,a}$.

contradicts to $\gcd(a,b)=1$.

The general method is applying lemma.

(23.15) Thm

(23.16) Example.

§23.

$\underline{23.1\ \text{Thm}}$ Let $f(x)=a_n x^n+\cdots+a_0$.

$g(x)=b_m x^m+\cdots+b_0$

be two polyn over a field F. $m>0$. $a_n, b_m\neq 0$.

There exist unique polyn-s $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ s.t.

$f(x) = q(x)g(x) + r(x)$.

and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

(§3.3) Cor A polynomial $f(x) \in F[x]$ has a zero in $x=a$ $\iff (x-a) \mid f(x)$

Proof: "$\Leftarrow$": Let $(x-a) \mid f(x)$,

$f(x) = q(x)(x-a) = 0$

"$\Rightarrow$" Apply quotient reminder theorem with $f(x)$ and $g(x) = (x-a)$

$f(x) = q(x)(x-a) + \underline{r(x)}$

degree $= 0$.

$\Rightarrow r(x) = c \in \mathbb{F}$.

$\underbrace{f(a) = 0}_{a \text{ is zero}} = q(a) \cdot 0 + \underbrace{r(a)}_{=0}$.

$\Rightarrow r(x) = 0$.

and $(x-a) \mid f(x)$.

Pf 2.: $\phi_a : F[x] \to F$

$f(x) \mapsto f(a)$ is surjective ring homomorphism with kernel $\ker \phi_a$.

By defin of kernel

$f(a) = 0 \iff \cancel{a}\, f(x) \in \ker \phi_a$.

We have $\underbrace{(x-a)}_{\text{All multipler of } (x-a)} \subseteq \ker \phi_a \subsetneq F[x]$.

$(x-a)$ is a maximal ideal.

$\Rightarrow \ker \phi_a = (x-a)$.

Thus $f(a) = 0$.

$\iff f(x) \in \ker \phi_a$

$\iff f(x) \in (x-a)$

$\iff (x-a) \mid f(x)$.

Ex: Let F be the field of 9 elements
(e.g. $F = \mathbb{Z}_3[x]/(x^2+1)$)
let $F^* = F \setminus 0$ be the subset of all units in F.
F^* is abelian group under multiplication
F^* is abelian group of size 8.
$F^* \simeq \mathbb{Z}_8$.
$F^* \simeq \cancel{\mathbb{Z}_4 \times \mathbb{Z}_2}$ impossible
if $a \in F^*$ has order 2.
(only three elements)

(23.6) Thm Let F be a field
Let $F^* = F \setminus 0$, be gp of units
And let $G \leq F^*$ be a finite subgroup.
Then G is cyclic.

Pf: As a finite abelian group $G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \mathbb{Z}_{d_r}$
for integers $d_1, d_2, \cdots d_r$

Let $\gcd(d_1, d_2) > 1$.
if $d \mid d_1$, $d \mid d_2$ then G contains at least d^2 element. with $x^d = 1$.
And $x^d - 1$ would have at least d^2 zeros in F.
This implies $\gcd(d_1, d_2) = 1$.
Apply the same argument to each pair d_i, d_j. $i \neq j$.
shows that $d_1, d_2, \cdots, d_r$ are pairwise relatively prime
By the CRT $G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} - \times \mathbb{Z}_{d_r}$.
$\simeq \mathbb{Z}_{d_1 d_2 - d_r}$ is cyclic.

Let F be a finite field of size p^d.
The nonzero elements in F form a cyclic gp of order p^d-1. The nonzero elements in F are precisely the roots of x^N-1, $N=p^d-1$.
Fermat's theorem is a special case of $d=1$.