Rings and Modules.

1. Rings.

A ring R is a set equipped with operations: $+$ (addition), $-$ (negation), $\times$ (multiplication), and special elements 0 (zero) and 1 (one, unity, identity), with properties:

(A) $R, +, -, 0$ form an abelian group. Ie, $\forall\, x, y, z \in R$,
- (A0) closed: $x+y \in R$
- (A1) associative: $(x+y)+z = x+(y+z)$
- (A2) identity: $x+0 = 0+x = x$
- (A3) inverse: $x+(-x) = (-x)+x = 0$
- (A4) commutative: $x+y = y+x$

(B) $R, \times, 1$ form a monoid:
- (B0) closed: $xy \in R$
- (B1) associative: $x(yz) = (xy)z$
- (B2) identity: $x.1 = 1.x = x$
- (B3) commutative: $xy = yx$

(C) Multiplication distributes over addition, ie:
- (C1) $x(y+z) = xy + xz$
- (C2) $(y+z)x = yx + zx$.

Note: many books do not assume B2, B3 - speak of "commutative ring with a 1".

Examples: (i) The integers, $\mathbb{Z}$, form a ring under the usual rules.
(ii) The rationals, $\mathbb{Q}$.
(iii) The reals, $\mathbb{R}$.
(iv) The complexes, $\mathbb{C}$.
} Also "fields" - ie, division is possible.

(v) Recall that integers mod m are classes of integers under the relation $a \equiv b \bmod m$, ie $m \mid (a-b)$. We identify the classes with the representatives $0, 1, \ldots, m-1$. Let $[a]$ denote the class of integers congruent to $a \pmod m$. Define $+, -, \times$ on such classes by: $[a]+[b] = [a+b]$, $-[a] = [-a]$, $[a] \times [b] = [ab]$. Must check that this is well-defined: ie, if $[a]=[a']$, $[b]=[b']$, then $[a+b] = [a'+b']$, etc. Trivial proof. Now easy to check that classes $\{[a]\}$ form a ring called $\mathbb{Z}/m\mathbb{Z}$, with $[0]$ and $[1]$ as zero and one respectively - "residue class ring modulo m".

Constructions.

Let R, S be rings. The direct product or Cartesian product $R \times S = \{(r,s) : r \in R, s \in S\}$, with operations: $(r,s)+(r',s') = (r+r', s+s')$, $-(r,s) = (-r,-s)$, $(r,s) \times (r',s') = (rr', ss')$, and $(1_R, 1_S) = 1$, $(0_R, 0_S) = 0$

Example: $\mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/6$

Polynomial Rings.

Let R be a ring. Consider sequences of form $(c_0, c_1, c_2, \ldots)$ indexed by $\mathbb{N}_0$, with property that $c_n = 0$ $\forall n$ greater than some value (depending on sequence).
Add sequences by: $(c_n) + (d_n) = (c_n + d_n)$ - clearly of the same type.
Multiply sequences by: $(c \times d)_n = \sum_{k=0}^{n} c_k d_{n-k}$ - also of same type.
Suppose $c_i = 0$ $\forall i > N$, $d_i = 0$ $\forall i > M$. Then, if $n > M+N$, either $k > M$ or $n-k > N$, so $c_k = 0$ or $d_{n-k} = 0$, so $(c \times d)_n = \sum(\text{zero}) = 0$.
I identify sequences (c_n) with polynomial $\sum c_n X^n$.
Now, $[\sum c_n X^n][\sum d_n X^n] = \sum_n \sum_{k=0}^{n} c_k d_{n-k} X^n$ - usual rule for multiplication of polynomials.

X is simply a notational device. Sometimes call X an "indeterminate" or "transcendental" - implication always that a polynomial is not a formula in R or even a mapping - simply a sequence of coefficients.

Denote by $R[X]$ the set of all polynomials with coefficients in R, (X as notation).
Claim $R[X]$ is a ring with addition and multiplication as defined.
Define negation by: $f = \sum c_n X^n \Rightarrow -f = \sum (-c_n) X^n$. The zero element of $R[X]$ is the sequence $(0,0,0,\ldots) = 0 + 0X + 0X^2 + \ldots = 0$. The unity in $R[X]$ is the sequence $(1,0,0,\ldots) = 1 + 0X + \cdots = 1$. The constant term of a polynomial is the 0^{th} term, ie the coefficient of X^0.
We have to verify all axioms for a ring. Only axiom not entirely trivial is associativity of multiplication: $((c \times d) \times e)_n = \sum_{k=0}^{n} (c \times d)_k e_{n-k} = \sum_{k=0}^{n} \sum_{j=0}^{k} c_j d_{k-j} e_{n-k}$
$= \sum_{j=0}^{n} \sum_{k=j}^{n} c_j d_{k-j} e_{n-k} = \sum_{j=0}^{n} \sum_{m=0}^{n-j} c_j d_m e_{n-j-m} = \sum_{j=0}^{n} c_j (d \times e)_{n-j} = (c \times (d \times e))_n$.

The constant term, $(c_0 + d_0) = (c+d)_0$, $(c \times d)_0 = \sum_{j=0}^{0} c_j d_{0-j} = \text{constant}, c_0 d_0$.
So, polynomials $(x, 0, 0, \ldots)$ "look like" elements of R.

Subrings

A subring S of a ring R is a subset of R which is a ring wrt inherited operations from R. In particular, $0, 1 \in S$, and S has to be closed under addition, negation and multiplication. Associativity, commutativity and distributivity ~~are~~ follow from R. For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ of $\mathbb{R}$, $\mathbb{R}$ of $\mathbb{C}$.

We observed that constant polynomials in $R[X]$ form a subring isomorphic to R.
In particular, the additive group of S is a subgroup of additive group of R.
So apply any results about subgroups - eg Lagrange's Theorem, ie, if R is finite and S is a subring of R, then $|S| \mid |R|$.

Maps Between Rings.

A ring homomorphism (or morphism) from ring R to ring T is a map $\varphi: R \to T$ which preserves all algebraic operations. Ie, $x, y \in R$: $\varphi(x+y) = \varphi(x) + \varphi(y)$, $\varphi(-x) = -\varphi(x)$, $\varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(0) = 0$, $\varphi(1) = 1$.
In particular, φ preserves all additive structure, so φ is a homomorphism of groups, looking at additive groups in R and T.
Define the kernel of φ, $\ker \varphi := \{x \in R : \varphi(x) = 0\}$.
Define the congruence attached to φ as relation $x \equiv y \iff \varphi(x) = \varphi(y)$.

Example: $\varphi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$; $x \mapsto [x]$. We showed that φ is a ring homomorphism while showing $\mathbb{Z}/m\mathbb{Z}$ is a ring. $\ker = m\mathbb{Z}$, congruence attached is $x \equiv y \iff \varphi(x) = \varphi(y) \iff x \bmod m = y \bmod m \iff x \equiv y \bmod m$.

Proposition: $\equiv_\varphi$ is an equivalence relation.
Proof: We have to show: reflexive: $\varphi(x) = \varphi(x) \Rightarrow x \equiv x$.
symmetric: $\varphi(x) = \varphi(y) \Rightarrow \varphi(y) = \varphi(x)$, so $x \equiv y \Rightarrow y \equiv x$.
transitive: $\varphi(x) = \varphi(y)$, $\varphi(y) = \varphi(z) \Rightarrow \varphi(x) = \varphi(z)$.

Furthermore, definition of φ implies that if $\varphi(x) = \varphi(x')$ and $\varphi(y) = \varphi(y')$ then $\varphi(x) + \varphi(y) = \varphi(x') + \varphi(y')$, so $\varphi(x+y) = \varphi(x+y')$. So, $x \equiv x'$, $y \equiv y' \Rightarrow x + x' \equiv y + y'$.

Exercise: $\equiv_\varphi$ has properties: if $x \equiv x'$, $y \equiv y'$, then $x+y \equiv x'+y'$, $-x \equiv -x'$, $xy \equiv x'y'$

Definition: An (abstract) congruence on R is an equivalence relation $\equiv$ such that $x \equiv x'$ and $y \equiv y' \Rightarrow x+y \equiv x'+y'$, $-x \equiv -x'$, $xy \equiv x'y'$.

A congruence $\equiv$ partitions R into classes $[x] = \{y \in R : x \equiv y\}$. A special class is $[0]$.

Proposition: If $x, y \in [0]$, then $x+y \in [0]$, $-x \in [0]$, $xy \in [0]$.

Corollary: $[0]$ is an additive subgroup of R.

Proposition: Suppose $x \in [0]$ and r is any element of R. Then, $xr = rx \in [0]$.
Proof: $x \equiv 0$, $r \equiv r$, so $xr \equiv 0r \equiv 0$, so $xr \in [0]$.

In summary, $[0]$ is an additive subgroup of R which is closed under multiplication by the whole of R.
An ideal in R is a subset I of R such that (i) I is a subgroup under addition, (ii) I is closed under multiplication by anything in R. (ie, $x \in I$, $r \in R \Rightarrow xr \in I$).

So, the two previous propositions say that if $\equiv$ is an abstract congruence, then $[0]$ is an ideal.

Proposition: Let I be an ideal in R, and define a relation $\sim$ on R by $x \sim y \iff x-y \in I$. Then, $\sim$ is a congruence and $I = [0]$ for $\sim$.

Proof: We first have to show $\sim$ is an equivalence relation.

R: I is an additive subgroup, so $x-x \in I$, ie $x \sim x$.

S: I is closed under negation, so if $(x-y) \in I \Rightarrow -(x-y) = (y-x) \in I$.

T: I is closed under addition, so $x-y \in I$, $y-z \in I \Rightarrow (x-y)+(y-z) = x-z \in I$.

So $\sim$ is an equivalence relation.

Now we need to show it is a congruence, ie, if $x \sim x'$ and $y \sim y'$, then:

$x+y \sim x'+y'$: have $x-x' \in I$, $y-y' \in I$, so $(x-x')+(y-y') \in I$, so $x+x' \sim y+y'$.

$-x \sim -x'$: have $-(x-x') \in I$, so $-x-(-x') \in I$, so $-x \sim -x'$.

$xy \sim x'y'$: $x-x' \in I$, $y-y' \in I$, so $(x-x')y \in I$, $x'(y-y') \in I$, so $(x-x')y + x'(y-y') \in I$, so $xy - x'y' \in I$.

So $\sim$ is a congruence. Finally, $[0] = \{y : y \sim 0\} = \{y : y-0 \in I\} = \{y : y \in I\} = I$.

Examples of ideals: (i) Kernels of morphisms.

(ii) $\{0\}$ (often written 0) in any ring. R itself is an ideal in R. These are trivial ideals in R. Others, if any, are non-trivial, or proper, ideals.

(iii) Let $x \in R$. $\langle x \rangle = \{xr : r \in R\}$. This is the principal ideal on x (with generator x)

Check ideal: if xr and $xs \in \langle x \rangle$, $xr+xs = x(r+s) \in \langle x \rangle$, $-xs = x(-s) \in \langle x \rangle$, $x.0 = 0 \in \langle x \rangle$. If $t \in R$, $(xr)t = x(rt) \in \langle x \rangle$, so done.

Proposition: $\mathbb{Z}$ is a Principal Ideal Ring, ie, every ideal is principal.

Proof: Let I be an ideal of $\mathbb{Z}$. First, if $I = \{0\} = \langle 0 \rangle$. If not, $\exists$ non-zero elements in I, and since I is closed under negation, $\exists$ positive elements. Let S be a (non-empty) set of positive elements of I. By the well-ordering property, it has a least element g, say. Claim $I = \langle g \rangle$.

$g \in S$, and $S \subseteq I$, so $g \in I$, so $\langle g \rangle = \{gr : r \in \mathbb{Z}\} \subseteq I$. So suppose, if possible, that $I \neq \langle g \rangle$, so $\exists x \in I$ with $x \notin \langle g \rangle$, ie $x \in I$ and x not a multiple of g. Divide x by g to give $x = gq + r$ with $0 < r < g$. Now, x and $gq \in I$, so $r \in I$. But $r > 0$ and $r < g$ - $\not\!\!\!$. So $I = \langle g \rangle$, and $\mathbb{Z}$ is a PIR.

Let $\equiv$ be an abstract congruence, and I the associated ideal. Let R/I, or $R/\equiv$, denote the set of classes: $\{[x] : x \in R\}$ - quotient set.

Define operations: $[x]+[y] = [x+y]$, $-[x] = [-x]$, $[x].[y] = [xy]$.

Proposition: with operations just defined, and special elements $[0]$ and $[1]$ for zero and one, R/I is a ring.

Have map $q_I : R \to R/I$, $x \mapsto [x]$ - quotient map.

Proposition: quotient map is a ring morphism.

Proof: $q(x+y) = [x+y] = [x]+[y] = q(x) + q(y)$, etc.

Proposition: The congruence and ideal attached to the quotient morphism $q_I : R \to R/I$ are just the original $\equiv$ and I.

Proof: $\ker q_I = \{ y \in R : q_I(y) = 0_{R/I} \} = \{ y \in R : [y] = [0] \} = \{ y \equiv 0 \} = I$.

Theorem: Let $\varphi : R \to T$ be any morphism. Let $K = \ker \varphi$, $S = \varphi R$. Then K is an ideal in R; S is a subring of T. $S \cong R/K$.

Proof: Have already done "K is an ideal".
S is a subring: need to check $0, 1 \in S$, and S closed under $+, -, \times$.
$\varphi(0_R) = 0_T \in S$, $\varphi(1_R) = 1_T \in S$, $\varphi(x+y) = \varphi(x) + \varphi(y) \in S$, $-\varphi(x) = \varphi(-x) \in S$,
$\varphi(xy) = \varphi(x)\varphi(y) \in S$, so S is a subring.
Define $\bar{\varphi} : R/K \to S$; $[x] \mapsto \varphi(x)$. Clearly surjective.
$[x] = [x']$ iff $x \equiv x'$ iff $x - x' \in K$ iff $\varphi(x - x') = 0$ iff $\varphi(x) - \varphi(x') = 0$ iff $\varphi(x) = \varphi(x')$.

Note: as a matter of principle it is often easiest to prove some subset is an ideal by identifying a morphism for which it is a kernel. Similarly for a subring, to identify a morphism for which it is the image.

We observed that $\mathbb{Z}$ is a PIR, ie, any ideal in $\mathbb{Z}$ is principal, with generator least positive element. Note also that if $\varphi : \mathbb{Z} \to R$ is a morphism, then φ is completely determined, since $\varphi(1) = 1_R$ and $n = \begin{cases} 1 + \cdots + 1 \\ -(1 + \cdots + 1) \end{cases}$, $|n|$ times. So, $\varphi(n) = \begin{cases} \varphi(1) + \cdots + \varphi(1) \\ -(\varphi(1) + \cdots + \varphi(1)) \end{cases}$, $|n|$ times, and $\varphi(0) = 0$. This defines a unique morphism $\mathbb{Z} \to$ any given ring R.
So, given R, let φ be this unique morphism, $\varphi : \mathbb{Z} \to R$. $\ker \varphi$ = ideal of $\mathbb{Z}$ with some generator $c \geq 0$. We define the characteristic of R to be this generator.
We have $\underbrace{1_R + \cdots + 1_R}_{c \text{ times}} = 0_R$, and c is the least positive number with this property, or 0 if there is no such positive number.

Further, the image of morphism φ is a subring of R called the prime subring of R, and consists of all elements $0_R, \pm 1_R, \pm(1_R + 1_R), \cdots$ Now, $\operatorname{Im}\varphi \cong \mathbb{Z}/\langle c \rangle$, where c is the characteristic of R, $\langle c \rangle$ denotes principal ideal. Hence, prime subring $\cong \mathbb{Z}$ (if $c = 0$), and $\cong \mathbb{Z}/c\mathbb{Z}$ if $c \neq 0$.

Caution: c is not necessarily a prime number.

An important example of a morphism arises from polynomial rings. Let $R[X]$ be the ring of polynomials over ring R. For any $a \in R$, let η_a be the map $\eta_a : f(X) \to f(a)$; $\sum c_i X^i \mapsto \sum c_i a^i$.
So, $\eta_a : R[X] \to R$. The definition makes sense as only finitely many c_i are non-zero, so $\sum c_i a^i$ is a finite expression in R and so can be evaluated. Clear that η_a is a morphism.

Proposition (Factor and Remainder Theorem): $\ker \varphi$ is $\langle X - a \rangle$, principal ideal. Indeed, $f(X) = (X-a)q(X) + f(a)$, for some $q(X) \in R[X]$.

Proof: we aim to prove $f(X) \equiv f(a) \bmod \langle X - a \rangle$. First we observe $X^r \equiv a^r \bmod \langle X - a \rangle$, since $X^r - a^r = (X-a)(X^{r-1} + aX^{r-2} + \cdots + a^{r-1})$. So, $\sum c_r X^r \equiv \sum c_r a^r \bmod \langle X - a \rangle$, ie $f(X) \equiv f(a) \bmod \langle X - a \rangle$, ie $f(X) = (X-a)q(X) + f(a)$.

Example: $\mathbb{Z}[x]$ does not have the P.I. property. Consider $\mathbb{Z}[x] \xrightarrow{\eta_0} \mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z}$.
$f(x) \longmapsto f(0) \longmapsto f(0) \bmod 2$.

Lemma: If $R \xrightarrow{\varphi} S \xrightarrow{\psi} T$, then the composite $\psi\varphi : R \to T$ is also a morphism.
Proof: Easy exercise.

So consider $\alpha : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$; $f(x) \mapsto f(0) \bmod 2$ - a morphism.
$K := \ker \alpha = \{f(x) \in \mathbb{Z}[x] : f(0) \text{ is even}\}$ is an ideal. Claim K is not principal.
We see that $\ker(\eta_0) = \langle x \rangle$, so $\eta_0(x) = 0$, so $\alpha(x) = 0 \bmod 2 = 0$, so $x \in K$.
Similarly, polynomial $2 \bmod 2 = 0$, so $2 \in K$. Now suppose if possible that $K = \langle k(x) \rangle$. Then x is a multiple of k and 2 is a multiple of k, so $k(x) = 1$. But $K = \langle 1 \rangle \Rightarrow K = \mathbb{Z}[x]$. But then everything in $\mathbb{Z}[x]$ would go to 0 under α, but $\alpha(1) = 1 \neq 0 \bmod 2$. ⁂.
So K cannot be principal, so $\mathbb{Z}[x]$ is not a PIR.

Define an element $x \in R$ to be invertible if $\exists\, x^{-1} \in R$ such that $x.x^{-1} = x^{-1}.x = 1_R$.
For example, invertible elements of: $\mathbb{Z}$ are ± 1.
$\mathbb{Z}/6\mathbb{Z}$ are $\{1, 5 \bmod 6\}$
$\mathbb{Q}$ are non-zero elements.
$\mathbb{Z}/5\mathbb{Z}$ are $\{1, 2, 3, 4 \bmod 5\}$ - ie, the non-zero elements.
Clearly, 0 is never invertible (except when $0 = 1$, in ring $R = \{0\}$).

Proposition: The invertible elements of R form a group R^* or $U(R)$, the unit group of R, under multiplication.
Proof: Associative - ✓. $1 \in R^*$. Inverses - ✓ ($(x^{-1})^{-1} = x$). Closure: if x, y are invertible with inverses x^{-1}, y^{-1} respectively, then xy has inverse $y^{-1}x^{-1}$.

Note - the group is commutative.

Definition: A field F is a ring in which all non-zero elements are invertible.
Ie. $U(F) = F \setminus \{0\}$.

Note: $\{0\}$ is not a field.

Proposition: Ideals of field F are just trivial ones, ie $\{0\} = \langle 0 \rangle$, $\{1\} = \langle 1 \rangle$.
Proof: Let I be an ideal. If $I \neq \langle 0 \rangle$, then $\exists\, x \in I$, $x \neq 0$. So x invertible, so $xx^{-1} \in I$, ie $1_F \in I$. Now if f is any element of F, then $1.f = f \in I$, so $I = F$.

Hence a ring morphism $\varphi : F \to T$ (T a ring) is either zero map $f \mapsto 0_T$ with kernel F, or has kernel $\{0\}$ and is an injection. Now if φ is the zero map, then $\varphi(1) = 0$, but $\varphi(1) = 1$, so $T = \{0 = 1\}$ is zero ring. A morphism of fields is a ring morphism which is not the zero map. So a morphism of fields is an injection and image is a field isomorphic to F. Denote by $F \xhookrightarrow{\varphi} T$. - monomorphism

Examples of fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Claim that $\mathbb{Z}/p\mathbb{Z}$ is a field for p prime.

Proposition: Let $R = \mathbb{Z}/m\mathbb{Z}$. Then $U(R) = \{a \bmod m : (a,m) = 1\}$.

Corollary: If p is prime, $U(\mathbb{Z}/p\mathbb{Z}) = \{a \bmod p : a \neq 0 \bmod p\}$, so $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof: If $d|a$ and $d|m$, $d>1$, then $a \bmod m$ cannot be invertible. Because, $ab \equiv 1 \bmod m \Rightarrow ab = 1 + mx$, but $d|a, d|m \Rightarrow d|1$ - ⁂. Conversely, suppose $(a,m) = 1$. By Euclid's Algorithm, we can construct x, y such that $mx + ay = 1$, and they $ay \equiv 1 \bmod m$. So $y \bmod m$ is an inverse for $a \bmod m$.

Now we consider the characteristic of a field F. If not zero, suppose it is c, ie, $\mathbb{Z} \to F; 1 \mapsto 1_F$ has kernel $\langle c \rangle$, and $\mathbb{Z}/c\mathbb{Z}$ is image of map. So a field of characteristic c contains a copy of $\mathbb{Z}/c\mathbb{Z}$.

Proposition: The characteristic $c(F)$ is 0 or a prime.

Proof: Claim c is composite $\Rightarrow$ $\mathbb{Z}/c\mathbb{Z}$ is not isomorphic to a subring of any field. Indeed, if $c = de$ with $d, e > 1$, so $d\,(= 1 + \cdots + 1)$ and $e\,(= 1 + \cdots + 1)$ are not zero, then $de \equiv 0 \bmod c$, ie, d, e are zero divisors. And a field cannot contain zero divisors: for, if $xy = 0$ with x, y both non-zero, then $1 = xyy^{-1}x^{-1} = 0\,y^{-1}x^{-1} = 0$ ⁂, as $1 \neq 0$ in a field. We showed a field has no zero divisors.

We call a ring an Integral Domain (ID) if there are no zero-divisors.

Examples: Any field.
$\mathbb{Z}$ is an ID (but not a field)
$\mathbb{Z}/m\mathbb{Z}$ is an ID $\Leftrightarrow$ m is prime.
A subring of a field is an ID.

Theorem: If D is an ID, then there is a field F containing a subring $\bar{D}$ isomorphic to D, and such that every element of F is of form $d_1 d_2^{-1}$, where $d_1, d_2 \in D$.

Let S = non-zero elements in domain D. By definition, if $s_1, s_2 \in S$, then $s_1 s_2 \in D$. Consider product set $D \times S = \{(d,s) : d \in D, s \in S\}$. Set up relation $\sim$ on $D \times S$: $(d,s) \sim (d',s') \Leftrightarrow ds' = d's$.
Claim $\sim$ is an equivalence relation.
R: $ds = ds$, so $(d,s) \sim (d,s)$. S: $(d,s) \sim (d',s') \Rightarrow (d',s') = (d,s)$.
T: $ds' = d's$ and $ds'' = d''s$, so $ds's'' = d'ss''$ and $d's''s = d''s's$.
Hence, $ds's'' = d''s's$, so $(ds'' - d''s)s' = 0 \Rightarrow ds'' - d''s = 0$, ie, $ds'' = d''s$.
Let d/s denote the $\sim$ class of (d,s), ie $d/s = d'/s' \Leftrightarrow ds' = d's$.
We will proceed to define ring operations on these classes: $\frac{d}{s} + \frac{d'}{s'} = \frac{ds' + d's}{ss'}$, $-\frac{d}{s} = \frac{(-d)}{s}$, $\frac{d}{s} \cdot \frac{d'}{s'} = \frac{dd'}{ss'}$. We will check that this makes sense.

Checking well-defined:

(i) Suppose $\frac{d}{s} = \frac{d'}{s'}$, ie, $ds' = d's$. So $\frac{d}{s} + \frac{e}{t} = \frac{dt+es}{st}$, $\frac{d'}{s'} + \frac{e}{t} = \frac{dt+es'}{s't}$ - must show equal.

Must show: $(dt+es)s't = (d't+es')st \iff dts't + ess't = d'tst + es'st \iff ds't^2 = d's t^2$

$\iff (ds'-d's)t^2 = 0$. $(t \in S$, so $t \neq 0) \iff ds'-d's = 0 \iff ds' = d's$.

(ii) Suppose $\frac{d}{s} = \frac{d'}{s'}$, ie $ds' = d's \Rightarrow -ds' = -d's \Rightarrow \frac{-d}{s} = \frac{-d'}{s'} \Rightarrow -(\frac{d}{s}) = -(\frac{d'}{s'})$

(iii) Finally, if $\frac{d}{s} = \frac{d'}{s'}$, ie, $ds' = d's$, so $\frac{de}{st} = \frac{d'e}{s't}$ and similarly $\frac{e}{t} = \frac{e'}{t'} \Rightarrow \frac{de}{st} = \frac{de'}{st'}$.

Hence, $+, -, \times$ all make sense.

Further, $\frac{0}{1} + \frac{d}{s} = \frac{0s+1d}{1s} = \frac{d}{s}$, so $\frac{0}{1}$ is a zero element for $F(D)$, and $(\frac{1}{1})\cdot(\frac{d}{s}) = \frac{1\cdot d}{1\cdot s} = \frac{d}{s}$, so $\frac{1}{1}$ is one element for $F(D)$

Now have to verify ring axioms.

A1: $(\frac{d}{s} + \frac{e}{t}) + \frac{f}{u} = \frac{dt+es}{st} + \frac{f}{u} = \frac{(dt+es)u + f(st)}{(st)u} = \frac{d(tu) + s(eu+ft)}{s(tu)} = \frac{d}{s} + \frac{eu+ft}{tu} = \frac{d}{s} + (\frac{e}{t} + \frac{f}{u})$

A2: $\frac{0}{1}$ is zero.

A3: $\frac{d}{s} + \frac{-d}{s} = \frac{ds+(-d)s}{s^2} = \frac{(d-d)s}{s^2} = \frac{0}{s^2} = \frac{0}{1}$ since $0.1 = 0.s^2$.

A4: $\frac{d}{s} + \frac{e}{t} = \frac{e}{t} + \frac{d}{s}$

B1: $\frac{d}{s} \times (\frac{e}{t} \times \frac{f}{u}) = \frac{d}{s}(\frac{ef}{tu}) = \frac{def}{stu} = (\frac{de}{st})\frac{f}{u}$.

B2: $\frac{1}{1}$ is one.

B3: $\times$ is commutative.

So $F(D)$ is a ring. Now check it is a field.

$\frac{0}{1} \neq \frac{1}{1}$? Well, $\frac{0}{1} = \frac{1}{1} \iff 0.1 = 1.1 \iff 0 = 1$ in D.

To be a field, consider invertible elements. We claim $\frac{d}{s} \neq \frac{0}{1} \iff d \neq 0$. Indeed, $\frac{d}{s} = \frac{0}{1} \iff d.1 = s.0 = 0 \iff d = 0$. If $\frac{d}{s} \neq \frac{0}{1}$, then $d \neq 0$, so $d \in S$ so $\frac{s}{d} \in F(D)$.

Now, $\frac{d}{s} \times \frac{s}{d} = \frac{ds}{sd} = \frac{1}{1}$, since $1ds = 1sd$.

So every non-zero element of $F(D)$ is invertible, and $F(D)$ is a field.

Consider $\varepsilon : D \to F(D)$, $x \mapsto \frac{x}{1}$. Claim ε is a ring morphism.

$\varepsilon(x) + \varepsilon(y) = \frac{x}{1} + \frac{y}{1} = \frac{x.1 + y.1}{1.1} = \frac{x+y}{1} = \varepsilon(x+y)$.

$\varepsilon(-x) = \frac{-x}{1} = -\frac{x}{1} = -\varepsilon(x)$.

$\varepsilon(xy) = \frac{xy}{1} = \frac{x}{1}\cdot\frac{y}{1} = \varepsilon(x)\varepsilon(y)$.

$\varepsilon(0) = \frac{0}{1}$ = zero of $F(D)$, $\varepsilon(1) = \frac{1}{1}$ = one of $F(D)$.

What is $\ker \varepsilon$? $\ker \varepsilon = \{x : \varepsilon(x) = 0 \in F(D)\} = \{x : \frac{x}{1} = \frac{0}{1}\} = \{0\}$, so ε is injective.

So $\operatorname{im}\varepsilon$ is a subring of $F(D)$, and it is isomorphic to D as $\varepsilon : D \to \operatorname{im}\varepsilon$ is a bijection. So $F(D)$ is a field with a subring isomorphic to D, as claimed.

So a ring is an integral domain $\iff$ it is isomorphic to a subring of some field.

Example: $\mathbb{Z}$ is an integral domain, and $\mathbb{Q}$ is the field of fractions $F(\mathbb{Z})$.

Proposition: Let D be an integral domain. Then $D[X]$ is also an integral domain.

Proof: Let $f = f_0 + f_1 X + \cdots + f_d X^d$ and $g = g_0 + g_1 X + \cdots + g_e X^e$. Wlog, $f_d, g_e \neq 0$.

Then, $fxg = f_0 g_0 + \cdots + f_d g_e X^{d+e}$. f_d, g_e non-zero elements of D (a domain), so $f_d g_e \neq 0$, so $fxg \neq 0$.

Special case: If K is a field, then K is certainly an I.D. So $K[x]$ is an I.D.

Field of fractions of $K[x] := \{ \frac{f(x)}{g(x)} : f, g \in K[x], g \neq 0 \} =: K(x)$. - field of rational functions on K.

Interlude: Factorisation in $\mathbb{Z}$. A (positive) integer p is "prime" if p has no non-trivial factors. (ie, not $1, p$). If p prime, then $p|ab \Rightarrow p|a$ or $p|b$. Use to prove fundamental theorem of arithmetic: if $n \in \mathbb{Z}$, then $n = \pm 1 . \prod_i^t p_i^{r_i}$, where p_i are primes and the expression is unique (up to order). (Existence and uniqueness are descent/induction arguments, cf, Euclid's Algorithm).

2. Factorisation.

Unless stated, all rings here are integral domains.

If $a, b \in R$, we say a divides b if $\exists x \in R$ such that $ax = b$. Write $a|b$. b is a multiple of a. Equivalently, $b \in \langle a \rangle$, or $\langle b \rangle \subseteq \langle a \rangle$.
Trivial cases: • 1 divides any element of R,
• any element divides 0.
• only multiple of 0 is 0.
• divisors of 1 are the invertible elements, units, ie, $U(R)$.
Clearly, $a|a$, as $a = 1.a$, and $a|b, b|c \Rightarrow a|c$.
If $a|b$ and $b|a$ we say a and b are associates.

Proposition: a, b are associates $\Leftrightarrow$ $b = a.u$ with u a unit.
Proof: ($\Leftarrow$). $b = au$, so $a|b$. $b = au \Rightarrow bu^{-1} = auu^{-1} = a$, so $b|a$.
($\Rightarrow$) If $a|b$ and $b|a$, then $a = by$, $b = ax$, so $b = bxy$, so $b(1-xy) = 0$.
ID $\Rightarrow$ either $b = 0$ (whence $a = 0$, $a = 1.b$), or $xy = 1$, ie x, y are units.

If $a|b$ and a is not an associate of b or a unit, then a is a non-trivial divisor of b.
Note - likely, the units ~~divide~~ divide every element of R.
An element of R which is not a unit (not invertible) and has no non-trivial divisors is called irreducible.
We call an ID a unique factorisation domain (UFD) if every element can be uniquely factored into irreducible elements up to order of factors and multiplication by units.
We call $p \in R$ a prime element if $p|ab \Rightarrow p|a$ or $p|b$.

Lemma: prime $\Rightarrow$ irreducible in R.
Proof: Suppose p is prime but not irreducible, ie, $p = ab$ with neither a or b units.
$p = ab \Rightarrow p|ab$. By assumption p is prime, so (wlog) $p|a$. We know $a|p$, so a is an associate of p - a trivial factor, #.

However, as we will show, the converse is false. Let $d \in \mathbb{Z}$, not square. Consider $\mathbb{Z}[\sqrt{d}]$ - subring of a field, so an integral domain. Define <u>norm</u> map $N: \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ by $N: a+b\sqrt{d} \mapsto a^2 - b^2 d$

<u>Proposition</u>: Fix d. If $\alpha \in \mathbb{Z}[\sqrt{d}]$, then α is a unit $\Leftrightarrow N(\alpha) = \pm 1$.

<u>Proof</u>: ($\Rightarrow$) α a unit $\Rightarrow \alpha\alpha^{-1} = 1$, so $N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}) = N(1) = 1$.
So $N(\alpha) \mid 1$ and $\in \mathbb{Z}$, so $N(\alpha) = \pm 1$.

($\Leftarrow$) If $N(\alpha) = \pm 1$, then if $\alpha = a+b\sqrt{d}$, we have $N(\alpha) = a^2 - b^2 d = (a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$.
So, $(a+b\sqrt{d})(\pm(a-b\sqrt{d})) = 1$, ie $\alpha \times$ "α^{-1}" $= 1$.

<u>Examples</u>:
- $\mathbb{Z}[i]$ - Gaussian integers. $N(a+bi) = a^2+b^2 = \pm 1$, whence units are $\pm 1, \pm i$. So $U(\mathbb{Z}[i])$ is of order 4.
- $\mathbb{Z}[\sqrt{5}]$. $N(a+b\sqrt{5}) = a^2 - 5b^2$. If $a=2, b=1$, $\varepsilon = 2+\sqrt{5}$ is a unit with $N(\varepsilon) = -1$. Indeed, all powers of ε are units, and $U(\mathbb{Z}[\sqrt{5}])$ is infinite.
- $\mathbb{Z}[\sqrt{-6}]$. Claim 2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$.
If not, $2 = \alpha\beta$ (α, β not units). So, $N(2) = N(\alpha)N(\beta) = 4$, so, since $N(\alpha), N(\beta) \neq \pm 1$, have $N(\alpha) = \pm 2$. But, if $\alpha = a + b\sqrt{-6}$, then $N(\alpha) = a^2 + 6b^2 = \pm 2$ - $\not\!\!\!$.
But, $2.3 = \sqrt{-6}(-\sqrt{-6})$, so $2 \mid (\sqrt{-6})^2$, but $2 \nmid \sqrt{-6}$, as $\frac{1}{2}\sqrt{-6} \notin \mathbb{Z}[\sqrt{-6}]$.
So 2 is not prime.
Indeed, $2, 3, \sqrt{-6}$ are all irreducible, and $-6 = 2.(-3) = (\sqrt{-6})^2$, so -6 has two essentially different irreducible factorisations. Hence $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.

<u>Proposition</u>: In a UFD, the irreducibles are all prime.

<u>Proof</u>: Suppose R a UFD and p irreducible, suppose $p \mid ab$, ie $ab = px$, some x. Now, ab has a unique factorisation into irreducibles, and x is also a product of irreducibles; $x = \prod q_i^{e_i} u$, u a unit, $e_i \geq 0$. So, $ab = p\prod q_i^{e_i} u$.
Now consider the irreducible factors of a and b, and the product of these factors is the unique factorisation of ab, ie, $p\prod q_i^{e_i} u$. So p is one of the irreducible factors of a or of b, ie, $p \mid a$ or $p \mid b$.

<u>Proposition</u>: If R satisfies: (i) every irreducible is prime, (ii) every element is a product of irreducibles, then R is a UFD.

<u>Proof</u>: Existence of factorisation guaranteed by assumption (ii).
Suppose $\prod p_i^{f_i} v = \prod q_j^{e_j} u$ are two essentially different factorisations of some element. Ie, p_1, say, $\neq$ any q_j (or a unit multiple of any q_j). But p_1 is irreducible, hence by (i) p_1 is prime, so $p_1 \mid$ LHS $\Rightarrow p_1 \mid$ RHS $\Rightarrow p_1 \mid \prod q_j^{e_j}$, so $p_1 \mid q_j$, some j. But q_j irreducible, so $q_j = p_1 x$, but p_1 is not a unit, so x is a unit, ie $p_1 = q_j \times$ unit - $\not\!\!\!$. So factorisation into irreducibles is unique, and R is a UFD.

We usually prove that a ring is a UFD by proving stronger properties, such as ED $\Rightarrow$ PID $\Rightarrow$ UFD. An exception is a result to be proved later.

Proposition: If R is a UFD, then so is $R[X]$.

A PID is an ID which also a PIR. Aim is to prove PID $\Rightarrow$ UFD. Eg: $\mathbb{Z}$ is a PID.

We need to prove: (i) every irreducible is prime, (ii) every element factors into irreducibles.

Notation: Let G be a subset of R. Write $\langle G\rangle = \{ r_1 g_1 + \cdots + r_k g_k : k \geq 1,\ r_i \in R,\ g_i \in G\}$. - any finite number of terms. In particular, if $G = \{g\}$, then $\langle G\rangle = \langle g\rangle$.

Proposition: $\langle G\rangle$ is an ideal of R.

Proof: Need to show an additive subgroup closed under multiplication by R.
Clearly, sum of two finite expressions of this form is again of this form.
Similarly for negation. $0g = 0$. So we have an additive subgroup.
Further, $r(r_1 g_1 + \cdots + r_k g_k) = (rr_1)g_1 + \cdots + (rr_k)g_k \in \langle G\rangle$. So $\langle G\rangle$ is an ideal.

Notation: $\langle g\rangle = \langle\{g\}\rangle$, $\langle g_1, g_2\rangle = \langle\{g_1, g_2\}\rangle$, etc. We call $\langle G\rangle$ the ideal generated by the set G.

In a PID, every ideal is principal. Ie, given $a, b \in R$, $\langle a, b\rangle = \langle h\rangle$, some $h \in R$.
Ie, $\langle h\rangle = \{xa + yb : x, y \in R\}$. We certainly have $a, b \in \langle h\rangle$, since $a = 1\cdot a + 0\cdot b$, $b = 0\cdot a + 1\cdot b$, so $a, b \in \langle h\rangle$, ie, $h \mid a$, $h \mid b$, so h is a common factor of a, b. Furthermore, suppose $c \mid a$, $c \mid b$. Then $c \mid (xa + yb)$ $\forall x, y$. So c divides every element of $\langle a, b\rangle$. In particular, $c \mid h$.

Definition: If $a, b \in R$ and h has the properties: (i) $h \mid a$, $h \mid b$, (ii) $c \mid a$, $c \mid b \Rightarrow c \mid h$, then h is a highest common factor of a, b, written $\mathrm{hcf}(a, b) = \gcd(a, b) = (a, b)$.

Proposition: The hcfs of a, b are all associates. Ie if h, h' are hcfs of a, b, then $h = h' \times$ unit.
Proof: By definition, $h \mid h'$ and $h' \mid h$, so $h = h' \times$ unit.

Proposition: If R is a PID, then elements $a, b \in R$ have a hcf h such that $\langle h\rangle = \langle a, b\rangle$ and $\exists\ x, y \in R$ such that $ax + by = h$.

Note: the last point ("$\exists x, y \ldots$") is special to PIDs, and is not part of the definition of the hcf.

Proposition: If R has the property that any two elements have a hcf, then every irreducible in R is prime.

Proposition: R a PID $\Rightarrow$ every irreducible is prime.
Proof: Let p be irreducible in R, suppose $p \mid ab$, $p \nmid a$, $p \nmid b$. Consider $\mathrm{hcf}(p, a) =: h$. We have $h \mid p$, so $h = p$ or 1 (up to units). If $h = p$, then $h \mid a \Rightarrow p \mid a$. So $h = 1$; have $\mathrm{hcf}(p, b) = 1$ similarly.
So we have $1 = px + ay$, $1 = pu + bv$. So $ay = 1 - px$, $bv = 1 - pu$. So $abyv = 1 + p(xup - u - x)$.
But $p \mid ab \Rightarrow p \mid abyv \Rightarrow p \mid 1$ ✱. So $p \mid a$ or $p \mid b \Rightarrow p$ is prime.

Proposition: R a PID $\Rightarrow$ every element of R is a product of irreducibles.

Proof: Suppose not. Suppose x is not a product of irreducibles. In particular, x is not an irreducible. So $x = x_1 y_1$, with neither x_1, y_1 units. Further, x_1 (say), is not a product of irreducibles. We have $x_1 | x$ but $x \nmid x_1$, so x is not an associate of x_1. We will continue to produce sequence x_n with $x_n | x_{n-1}$, x_n not an associate of x_{n-1}. So the principal ideals $\langle x \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \cdots$

Let $I = \bigcup_n \langle x_n \rangle$. Claim I is an ideal.

Let $a, b \in I$. So $a \in \langle x_i \rangle$, $b \in \langle x_j \rangle$, wlog, some $i \geq j$. So $b \in \langle x_i \rangle$ also.

So $a + b \in \langle x_i \rangle \Rightarrow a + b \in I$. If $a \in \langle x_i \rangle$, $r \in R$, then $ra \in \langle x_i \rangle$, so $ra \in I$.

$0 \in \langle x_i \rangle \; \forall i$. Hence I is an ideal. Let $I = \langle z \rangle$, i.e $\langle x \rangle \subset \langle x_1 \rangle \subset \cdots \subset \langle z \rangle$.

But $z \in I$, so $z \in \langle x_i \rangle$, some i, so $\langle x_i \rangle \supseteq \langle z \rangle$.

Hence, $\langle x_i \rangle \subsetneq \langle x_{i+1} \rangle \subsetneq \cdots \subsetneq \langle z \rangle \subseteq \langle x_i \rangle$ - ⁂.

So supposition that x has no factorisation fails.

Theorem: R a PID $\Rightarrow$ R a UFD.

In the course of the proof we showed that R a PID $\Rightarrow$ cannot have an ascending sequence $X_1 \subsetneq X_2 \subsetneq \cdots$ of ideals in R. This is the **Noetherian Property.**

Let R be an ID. Define a **Euclidean Function** φ on R as a map $\varphi : R \to \mathbb{N}$ such that:

(E1): $\varphi(0) = 0$, $\varphi(1) = 1$

(E2): $\varphi(ab) = \varphi(a)\varphi(b)$

(E3): if $a, b \in R$, $b \neq 0$, $\exists\, q, r \in R$ such that $a = bq + r$ and $\varphi(r) < \varphi(b)$.

An ID with Euclidean Function is called a **Euclidean Domain** (ED).

Example: $\mathbb{Z}$ with $\varphi(n) = |n|$.

Theorem: R an ED $\Rightarrow$ R a PID.

Proof: Let I be an ideal of R. If $I = \{0\}$ then $I = \langle 0 \rangle$. If not, consider the set of values $\{\varphi(i) : i \in I, i \neq 0\}$. This is a non-empty subset of $\mathbb{N}$, so let $\varphi(g)$ be a minimal element for some $g \in I$. Claim $I = \langle g \rangle$.

Certainly, $g \in I \Rightarrow \langle g \rangle \subseteq I$.

If $\langle g \rangle \neq I$, then let $f \in I \setminus \langle g \rangle$. $g \neq 0$, so divide f by g to give $f = gq + r$, $\varphi(r) < \varphi(g)$. But $f, gq \in I \Rightarrow r \in I$, but $\varphi(r) < \varphi(g)$ - ⁂.

So, $I = \langle g \rangle$ is principal.

So $\mathbb{Z}$ is an ED $\Rightarrow$ PID $\Rightarrow$ UFD. (We have proved the fundamental theorem of arithmetic!)

Let F be a field. Aim to show $F[x]$ is an ED.

Further examples: $\mathbb{Z}[\sqrt{d}]$. Show, eg, $\mathbb{Z}[\sqrt{-1}]$ is an ED with $\varphi(x + y\sqrt{-1}) = x^2 + y^2$

$\mathbb{Z}[\sqrt{-2}]$ with $\varphi(x + y\sqrt{-2}) = x^2 + 2y^2$

$\mathbb{Z}[\sqrt{2}]$ with $\varphi(x + y\sqrt{2}) = x^2 - 2y^2$.

Let degree of $f(x) = \sum c_n X^n \in F[X]$ be d where c_d is non-zero coefficient of highest subscript. Write as ∂f. Clearly, $\partial(\text{constant}) = 0$, $\partial(0) = -\infty$, $\partial(fg) = \partial(f) + \partial(g)$.
Let $\varphi(f) = 2^{\partial f}$. So, $\varphi(0) = 0$, $\varphi(\text{const.}) = 1$, $\varphi(fg) = \varphi(f)\varphi(g)$.
Claim φ is a Euclidean Function. To show (E3), sufficient to show: given $b \neq 0$, $\forall\, X^n \exists\, r_n$ such that $X^n - r_n$ is a multiple of b, and $\partial r_n < \partial b$. — ⊛
Proof: If b is constant, $r_n = 0$ $\forall n$.
If not, $X^0 \equiv r_0 = 1 \mod \langle b \rangle$. $X^{n+1} = X r_n$, either r_{n+1} already, or $\partial(X r_n) = \partial(b)$, and subtract multiples of b.

Consider $\mathbb{Z}[i]$. $N(x+iy) = x^2+y^2 = |x+iy|^2$ in $\mathbb{C}$.
We showed $N(\alpha)N(\beta) = N(\alpha\beta)$. Clearly $N(0) = 0$, $N(1) = 1 \neq 0$.
Look at (E3): $\alpha \in \mathbb{Z}[i]$, $\beta \neq 0$ in $\mathbb{Z}[i]$. $\alpha = u+iv$, $\beta = x+iy$. Now, in $\mathbb{C}$,

$$\frac{\alpha}{\beta} = \frac{u+iv}{x+iy} = \frac{(u+iv)(x-iy)}{x^2+y^2} = \frac{r+is}{N(\beta)} = p+iq + \frac{c+id}{N(\beta)} \qquad \left(-\frac{N(\beta)}{2} \leq c,d \leq \frac{N(\beta)}{2}\right)$$

$\alpha = \beta(p+iq) + \beta\left(\frac{c}{N(\beta)} + i\frac{d}{N(\beta)}\right)$ — $R \in \mathbb{Z}[i]$. what is $N(R)$?

Fact: There are rings $\mathbb{Z}[\sqrt{d}]$ which are PIDs but not EDs. Eg, $\mathbb{Z}[\sqrt{-19}]$.
(Hard - have to show no Euclidean Function exists).

Better proof of ⊛ (above): Going to divide g by f, $f \neq 0$.
If f is constant then f is a unit, so: $g = (gf^{-1})f + 0$, and $\varphi(0) = 0 < \varphi(f) = 1$.
If not, suppose f of degree d, $f = a_d X^d + \cdots + a_0$, $a_d \neq 0$. We claim $\forall n$, $\exists$ polynomial r_n with $\partial r_n < d$ such that $X^n \equiv r_n \mod \langle f \rangle$.
If so, then $g = \sum b_i X^i$, so $g \equiv \sum b_i r_i \mod \langle f \rangle$. Call $\sum b_i r_i =: R$, so $\partial R < d$.
So $g - R =$ multiple of $\langle f \rangle = fQ$, say. So $g = fQ + R$ with $\partial R < \partial f$, ie $\varphi(R) < \varphi(f)$.
Now establish claim (by induction).
$n = 0$, $X^0 \equiv 1 = r_0 \mod \langle f \rangle$, and $\partial 1 = 0 < d$.
Assume true for n. $X^n \equiv r_n \mod \langle f \rangle$. So $X^{n+1} \equiv X r_n \mod \langle f \rangle$.
If $X r_n$ is still of degree $< d$, put $r_{n+1} = X r_n$ - done.
If not, $X r_n$ is of degree d, so $X r_n = cX^d + \{\text{lower degrees}\}$
So, $X r_n - \left(\frac{c}{a_d}\right) f = (cX^d + \cdots) - (cX^d + \cdots)$, and let r_{n+1} be $X r_n - \left(\frac{c}{a_d}\right) f$.

Long Division of Polynomials.

Example:

$$\begin{array}{r} X^2 - X - 1 \\ X^2 + X + 1 \;\overline{)\; X^4 + 0X^3 + -X^2 - 2X + 1} \\ \underline{X^4 + X^3 + X^2} \\ -X^3 - 2X^2 - 2X \\ \underline{-X^3 - X^2 - X} \\ -X^2 - X + 1 \\ \underline{-X^2 - X - 1} \\ \text{remainder} \rightarrow \quad 0X + 2 \end{array} \quad \leftarrow \text{quotient}$$

ie, $X^4 - X^2 - 2X + 1 = (X^2 - X - 1)(X^2 + X + 1) + 2$

Let D be any UFD. $D[X]$ is not in general an ED. For example, $\mathbb{Z}[X]$ is not even a PID, as we showed that $\langle 2, x\rangle$ non-principal in $\mathbb{Z}[X]$.
But $\mathbb{Q}[X]$ is an ED.
So aim to relate factorisation in $D[X]$ to factorisation in $F[X]$, where $F = F(D)$
In $D[X]$ we find (at least) two sorts of irreducible:

- if π is irreducible in D, it is still irreducible in $D[X]$. (Only possible factors of constants are constants).
- if $f(X)$ is a polynomial in $D[X]$ which is irreducible in $F[X]$, it must also be irreducible in $D[X]$.

It will turn out that these are the only sort of irreducibles.

Let π be irreducible in D. D is a UFD, so π is a prime element.

Proposition (Gauss' Lemma): π is prime in $D[X]$.

Lemma: Let R be an ID. p is a prime element of R iff $R/\langle p\rangle$ is an ID.
Proof: $R/\langle p\rangle$ is an ID iff $xy \equiv 0 \mod \langle p\rangle \Rightarrow x \equiv 0$ or $y \equiv 0 \mod \langle p\rangle$
iff $p \mid xy \Rightarrow p \mid x$ or $p \mid y$
iff p a prime element.

Proof of Gauss' Lemma: π is prime in $D[X]$ iff $D[X]/\langle\pi\rangle$ is an ID.
But $D[X]/\langle\pi\rangle \cong (D/\langle\pi\rangle)[X]$, and p prime in $D \Rightarrow D/\langle\pi\rangle$ is an ID, and ring of polynomials over an ID is again an ID.
So $(D/\langle\pi\rangle)[X]$ is an ID, so π is prime in $D[X]$.

Corollary: Suppose coefficients of $f(X)$ have hcf 1, as do those of $g(X)$. Then the same is true of $f(X)g(X)$.

Let $c(f)$, the content of f, denote the hcf of the coefficients. Then, the corollary states that $c(fg) = c(f)c(g)$.
Proof: Induction on the number of irreducible factors of $c(fg)$.

Proposition: Let $f \in D[X]$ have degree ≥ 1. Then, $f(x)$ irreducible in $D[X] \Leftrightarrow$ irreducible in $F[X]$.
Proof: ($\Leftarrow$) Irreducible in $F[X] \Rightarrow$ irreducible in subring $D[X]$.
($\Rightarrow$) Suppose $f(x)$ irreducible in $D[X]$, but reducible in $F[X]$, ie $f(X) = g(X)h(X)$, $g, h \in F[X]$.
Coefficients of g, h are in F, so $\exists\, k \in D$ such that $kg, kh \in D[X]$.
Now, $k^2 f = (kg)(kh)$ is a factorisation of $k^2 f$ in $D[X]$.
Let π be an irreducible factor of k^2 (in D). $\pi \mid (kg)(kh)$.
By Gauss' Lemma, $\pi \mid (kg)$ or $\pi \mid (kh)$ in $D[X]$. Say $(k^2/\pi) f(X) = (\frac{k}{\pi} g)(kh)$, wlog.
Repeat, ie: $Af = (Bg)(Ch)$, let $\pi \mid A$, $(A/\pi) f = (\cdots)(\cdots)$
Finally, get $f =$ product of polynomials in $D[X]$, so f reducible in $D[X]$ - $\ast$.

Proposition: If $f(x)$ is irreducible in $D[X]$ then $f(x)$ is prime in $D[X]$.

Proof: Let $f \mid gh$ in $D[X]$, then $f \mid gh$ in $F[X]$. By previous result, f irreducible in $F[X]$, hence f prime in $F[X]$. So, $f \mid gh \Rightarrow f \mid g$ (say) in $F[X]$.
So, $g(x) = f(x)\,l(x)$ in $F(x)$, so $l(x) \in F(x)$.
Aim to show $f \mid g$ in $D[X]$, ie, need to show $l(x) \in D[X]$.
So let $kl \in D[x]$, ie $kg = f(kl)$ for some $k \in D$. As before, we can remove irreducible factors $\pi \mid k$ from product. We cannot have $\pi \mid f$ as f is irreducible.
So each π is removed from $kl(x)$. So $g = fL$ and $L \in D[X]$, so $f \mid g$ in $D[X]$.

Theorem: Let D be a UFD. $D[X]$ is also a UFD, and the irreducibles are:
(i) irreducibles of D.
(ii) polynomials of degree ≥ 1 irreducible over F.

Proof: We proved: constant irreducible in $D \Rightarrow$ irreducible and prime in $D[X]$.
Non-constant which is irreducible in F is irreducible in D and prime.

Examples: $\mathbb{Z}[X]$ is a UFD.

Definition: A prime ideal P in R is an ideal with the further property that if $ab \in P$ then $a \in P$ or $b \in P$.

If P is prime and principal, $P = \langle \pi \rangle$. $ab \in \langle \pi \rangle \Leftrightarrow \pi \mid ab$, and a or $b \in \langle \pi \rangle \Leftrightarrow \pi \mid a$ or $\pi \mid b$.
So, $\langle \pi \rangle$ is a prime ideal $\Leftrightarrow$ π is a prime element of R.

Proposition: Let P be an ideal of R.
Proof: R/P an ID $\Leftrightarrow (a \bmod P)(b \bmod P) = 0 \Rightarrow \{a \bmod P = 0$ or $b \bmod P = 0$
$\Leftrightarrow ab \in P \Rightarrow a \in P$ or $b \in P$
$\Leftrightarrow P$ a prime ideal.

In particular, π a prime element $\Leftrightarrow R/\langle \pi \rangle$ an ID.

Lemma (Eisenstein's Criterion): Let D be a UFD, and $f \in D[X]$. Suppose $\exists$ an irreducible π such that $f(X) = a_d X^d + \cdots + a_0$, $\pi \nmid a_d$, $\pi \mid a_{d-1}, \ldots, \pi \mid a_0$, $\pi^2 \nmid a_0$. Then f is irreducible.

Proof: Suppose $f(x) = g(x)\,h(x)$. Let $g(x)$ have coefficients $b_0, b_1, \ldots$; let $h(x)$ have $c_0, c_1, \ldots$
Now, $a_0 = b_0 c_0$. So, $\pi \mid a_0 \Rightarrow \pi \mid b_0$ or $\pi \mid c_0$, and $\pi^2 \nmid a_0$, so (wlog) $\pi \mid b_0$, $\pi \nmid c_0$.
Let $A = D/\langle \pi \rangle$. π an irreducible in a UFD $\Rightarrow$ π prime $\Rightarrow$ A an I.D.
Now, in $A[X]$, $f \equiv a_d X^d$, $g \equiv b_m X^m + \cdots + b_1 X$, $h \equiv c_n X^n + \cdots + c_0$, and $f = gh$.
So, term of lowest degree in $gh \bmod \langle \pi \rangle$ is $c_0 \neq 0 \bmod \langle \pi \rangle$.
So if $b_r X^r$ is term of lowest degree in $g \bmod \langle \pi \rangle$, then $c_0 b_r X^r = a_d X^d$.
So the term of lowest degree in $g \bmod \langle \pi \rangle$ is of degree d. Hence, degree of g is $\geq d$. But $g \mid f$ in $D[X]$, so degree of $g = d$, and h is a constant. Hence f is irreducible.

Examples: (i) $X^3 + 6X^2 + 12X + 6 \in \mathbb{Z}[X]$ - satisfies Eisenstein for $p = 2, 3$.
Hence irreducible.

(ii) $2X^2 + 2X + 1$. Not Eisenstein, but consider $X^2 f(\frac{1}{X})$ - it is irreducible.

Let p be a prime. Then $(X^p - 1) = (X-1)(X^{p-1} + \cdots + 1)$.
Claim $\Phi_p(X) := X^{p-1} + \cdots + 1$ is irreducible in $\mathbb{Z}[X]$
Consider $Y := X - 1$. Then, $\Phi_p(X) = \Phi_p(Y+1) = \frac{(Y+1)^p - 1}{(Y+1) - 1} = \frac{(Y+1)^p - 1}{Y}$

$$= Y^{p-1} + \binom{p}{p-1} Y^{p-2} + \cdots + \binom{p}{1}$$

Now claim that all $\binom{p}{r}$, $1 \le r \le p-1$, are divisible by p.
$\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{r!}$, and top term has factor p not cancelled by any factor in $r!$
So $\Phi_p(X)$ is Eisenstein wrt p.

Euclid's Algorithm.

Recall that if R is a PID then $\langle a, b \rangle = \langle h \rangle$, where $h = \text{hcf}(a,b)$, and $h = ax + by$ for some $x, y \in R$. In a Euclidean Domain, we can use Euclid's Algorithm to compute h, x, y. This is as follows:
Given $a, b \in E$ (an ED) with $\varphi : E \to \mathbb{N}$, the Euclidean function.
If $a = 0$ or $b = 0$, then hcf is b or a respectively.
Otherwise, divide: $b = aq_1 + r_1$, $\varphi(r_1) < \varphi(a)$, by (E3)
Continue in this way: $a = r_1 q_2 + r_2$, $\varphi(r_2) < \varphi(r_1)$

$$r_1 = r_2 q_3 + r_3, \quad \varphi(r_3) < \varphi(r_2)$$
$$\vdots$$
$$r_{n-1} = r_n q_{n+1} + 0.$$

It must terminate as $\varphi(r_n)$ is a decreasing sequence of natural numbers.
Claim: (i) $r_n = \text{hcf}(a,b)$
(ii) $r_n = ax + by$, some $x, y \in E$

Proof: (i) If $c \mid a$, $c \mid b$, a common factor, then $c \mid b - aq_1 = r_1$, so $c \mid a - q_2 r_1 = r_2$, ...,
so $c \mid r_n$. Also, $r_n \mid r_{n-1}$, so $r_n \mid q_n r_{n-1} + r_n = r_{n-2}$, ..., so $r_n \mid a$, $r_n \mid b$.
Thus, r_n is a common factor divisible by every common factor, so is an hcf.

(ii) Letting $r_0 = a$, $r_{-1} = b$, we claim that $r_i = ax_i + by_i$, some $x_i, y_i \in E$, each i.
Now, $r_{-1} = b = a \cdot 0 + b \cdot 1$

$$r_0 = a = a \cdot 1 + b \cdot 0$$
$$r_1 = b - aq_1 = a(-q_1) + b(1)$$
$$\vdots$$
$$r_{i+1} = r_{i-1} - r_i q_{i+1} = ax_{i-1} + by_{i-1} - q_{i+1}(ax_i + by_i) = a(x_{i-1} - q_{i+1}x_i) + b(y_{i-1} - q_{i+1}y_i)$$

So, $x_{i+1} = x_{i-1} + q_{i+1}x_i$, $y_{i+1} = y_{i-1} + q_{i+1}y_i$
In particular, $r_n = ax_n + by_n$

Let π be an irreducible element of E. Consider $E/\langle \pi \rangle$. We saw that this is an ID as $\langle \pi \rangle$ is prime. If α is prime to π, then $\text{hcf}(\alpha, \pi) = 1$ and $\alpha x + \pi y = 1$. So, $(\alpha \bmod \pi)(x \bmod \pi) = 1 \bmod \pi$ - ie α is invertible in $E/\langle \pi \rangle$.
Ie, α prime to π iff $\alpha \bmod \pi \neq 0 \Rightarrow \alpha \bmod \pi$ invertible.

Proposition: $E/\langle\pi\rangle$ is a field.

Example: $\mathbb{Z}/p\mathbb{Z}$ is a field if p is a prime number.

Define ideal M in a ring R to be **maximal** if there is no proper ideal I with $M \subsetneq I \subsetneq R$.

Proposition: If M is a maximal ideal of R, then R/M is a field.
Proof: Suppose $x \bmod M \neq 0$, ie $x \notin M$. Then, $I = \langle M \cup \{x\}\rangle$ is an ideal, $I \supsetneq M$.
So, I an ideal, $\neq M$, so $I = R$ by maximality of M.
So $1 \in I$, that is, $1 = m + xy$, $m \in M$, $y \in R$. So $(x \bmod M)(y \bmod M) = 1 \bmod M$.
Ie, $x \bmod M \neq 0 \Rightarrow$ invertible. Hence R/M is a field.

In a PID, $\langle\alpha\rangle$ is maximal iff $\langle\alpha\rangle \subseteq \langle\beta\rangle \subseteq R = \langle 1\rangle \Rightarrow \langle\alpha\rangle = \langle\beta\rangle$ or $\langle\beta\rangle = \langle 1\rangle$.
Ie, $\langle\alpha\rangle$ maximal iff $\beta \mid \alpha$ ($\Rightarrow \beta$ an associate of α) or β is a unit. - ie, α is an irreducible.
So, in a PID, $\langle\alpha\rangle$ maximal $\Leftrightarrow \alpha$ irreducible.
Hence, if π is an irreducible element in a PID R, then $R/\langle\pi\rangle$ is a field.

Note: not true for UFDs which are not PIDs. **Eg:** in $\mathbb{Z}[x]$, the element x is irreducible, but $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$ - not a field.
Non-principal ideal: $\langle 2, x\rangle$. $\langle x\rangle \subsetneq \langle 2, x\rangle \subsetneq \mathbb{Z}[x]$.

3. Fields.

An important aim of this section is to classify finite fields completely.

Theorem: There is exactly one finite field of each prime power order (and no others).

N.B: The other finite fields are not $\mathbb{Z}/p^n\mathbb{Z}$ $(n>1)$, which are not even IDs.

Example: Naively construct a field of order 4. ID $\Rightarrow$ characteristic is prime $\Rightarrow$ must be 2.
So, we have 0, 1 and $1+1=0$. Let α be another element, so $\alpha+1$ is the fourth.
So field must be $\{0, 1, \alpha, \alpha+1\}$. Characteristic $2 \Rightarrow \alpha + \alpha = 0$.
What is α^2?: $\alpha^2 = 0 \Rightarrow \alpha \cdot \alpha = 0 \Rightarrow \alpha$ a zero-divisor - ✱
$\alpha^2 = 1 \Rightarrow (\alpha+1)(\alpha-1) = 0 \Rightarrow \alpha = \pm 1$ - ✱
$\alpha^2 = \alpha \Rightarrow 0^2 = 0,\ 1^2 = 1$, so $x^2 = x$ has 3 roots - ✱
} So $\alpha^2 = \alpha + 1$.

$F = \{0, 1, \alpha, \alpha+1\}$:

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

×	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

F - field of order 4.

Multiplication: F^* is cyclic of order 3.

Every field F has a prime subring: Image of $\mathbb{Z} \to F$, $1 \mapsto 1$.
Kernel of map is $\langle c \rangle$, where $c = \text{char } F$. F a field $\Rightarrow$ $c = 0$, or $c = p$, prime.
Since F contains $\mathbb{Z}/\langle c \rangle$ as subring ("prime subring"), we have $\mathbb{Z}/\langle c \rangle$ an ID.
If F has characteristic 0, then F contains a copy of $\mathbb{Z}$ itself, so F contains a copy of $\mathbb{Q}$. If $\text{char } F = p \neq 0$, then F contains a copy of $\mathbb{Z}/\langle p \rangle$, already a field.

We call $\mathbb{Q}$, respectively $\mathbb{Z}/\langle p \rangle$ the prime subfield of F.
Denote $\mathbb{Z}/\langle p \rangle$ by $\mathbb{F}_p$ or $GF(p)$ - the field of p elements.

In our example, $\text{char } F = 2$, and $\{0, 1\}$ is a prime subfield $\mathbb{F}_2$.

Let K be a field containing a copy of a field F. (Special case: $F \subseteq K$)
Generally, $\varphi: F \to K$ is a field morphism (automatically injective).
Call K an extension of F, and write K/F. (This is not a quotient!)
Examples: $F/\mathbb{F}_2$, $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, etc...
Every field is an extension of a prime subfield.

Go back to $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ with $\alpha^2 = \alpha + 1$.
Every element of $\mathbb{F}_4$ is a polynomial in α (subject to condition $\alpha^2 = \alpha + 1$)
In other words, $\mathbb{F}_4 = \mathbb{F}_2[X]/\langle x^2 - (x+1) \rangle$.
We take map: $\mathbb{F}_2[X] \to \mathbb{F}_4$; $X \mapsto \alpha$. This has kernel $\langle X^2 - X - 1 \rangle$.
$f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$ is irreducible: reducible and quadratic $\Rightarrow$ linear factors, but $f(0) = f(1) = 1$, in $\mathbb{F}_2$. So f has no roots in $\mathbb{F}_2$, hence no linear factors, hence irreducible.
So, $\mathbb{F}_2[X]/\langle x^2 + X + 1 \rangle$ is a field as $\langle f(X) \rangle$ is maximal.

So, recipe for constructing finite fields of characteristic p is to find an irreducible polynomial $f \in \mathbb{F}_p[X]$ and form quotient $\mathbb{F}_p[X]/\langle f(X) \rangle$.

Digression: There are infinitely many irreducible polynomials in $\mathbb{F}_p[X]$.
Proof: If not, multiply all together and add 1.

Suppose now K/F extension. K,+ is an additive group, can multiply elements of K by elements of F, and distributive - ie, claim K is a vector space over F.

Example: $\mathbb{C}/\mathbb{R}$: $\mathbb{C}$ forms a vector space over $\mathbb{R}$, and has basis $\{1, i\}$.

In general, if K is finite dimensional as an F-vector space, we call this dimension the degree or index, written $[K:F]$.

Examples: $[\mathbb{C}:\mathbb{R}] = 2$, and $[\mathbb{F}_4 : \mathbb{F}_2] = 2$, with basis $\{1, \alpha\}$

Note: Not always finite, eg $[\mathbb{R}:\mathbb{Q}] = \infty$.

If $[K:F] = d$, then $K \cong F^d$ as vector spaces.

Note: Only as vector spaces, not as rings.

So if F is finite with order q, then the order of K must be q^d.

Theorem: A finite field has order which is a prime power.
Proof: K finite, $\mathbb{F}_p$ the prime subfield, then $[K:\mathbb{F}_p] = d$, so $|K| = p^d$.

Splitting Fields.

Idea: Given an irreducible polynomial $f \in F[X]$, to find an extension field K/F such that K contains all roots of f. Ie, f = product of linear factors in $K[X]$.

Easy shortcut when $F = \mathbb{Q}$: take $K = \mathbb{C}$. Every polynomial in $\mathbb{Q}[X]$ splits completely in $\mathbb{C}[X]$. We cannot do this when $F = \mathbb{F}_p$, so we need a new approach.

Let $f(X) \in F[X]$, wlog f irreducible. Consider $F[X]/\langle f \rangle$. f irreducible $\Rightarrow \langle f \rangle$ maximal $\Rightarrow F[X]/\langle f \rangle$ is a field. Further, $F \to F[X] \to F[X]/\langle f \rangle$ is a morphism, so we have an extension of F. Now let $\alpha = X \bmod \langle f \rangle$. $f(\alpha) \equiv f(X) \equiv 0 \bmod \langle f \rangle$, so α is a root of f in the extension.

Examples: (i) $X^2 - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein with $p = 2$).
So, $\mathbb{Q}[X]/\langle f(X) \rangle = \mathbb{Q}(\sqrt{2})$ where $X \bmod X^2 - 2 = \sqrt{2}$.
Now, $f(X) = (X - \sqrt{2})(X + \sqrt{2})$ splits completely over $\mathbb{Q}(\sqrt{2})$.

(ii) $X^2 + 1$ irreducible over $\mathbb{R}$. $\mathbb{R}[X]/\langle x^2+1 \rangle = \mathbb{R}(i)$, where $X \bmod X^2 + 1 = i$.
We call this extension $\mathbb{C}$.

(iii) $f(X) = X^3 + 2X + 2 \in \mathbb{Q}[X]$, irreducible by Eisenstein with $p = 2$.
Let $\alpha = X \bmod f(X)$ in $\mathbb{Q}[X]/\langle f \rangle$. $f(X) = (X - \alpha) \cdot g(X) \in \mathbb{Q}(\alpha)[X]$.
Claim g remains irreducible.
Let α_0 be a real root of $f \in \mathbb{R}[X]$ (regarded as a real polynomial).
Then, map $\mathbb{Q}[X]/\langle f \rangle \to \mathbb{R}$; $\alpha = X \bmod \langle f \rangle \mapsto \alpha_0$.
Then, $f(X) = (X - \alpha_0) g(X) \in \mathbb{R}[X]$, and $g(X)$ is irreducible in $\mathbb{R}[X]$ as f has only 1 real root. So $g(X)$ is irreducible in $\mathbb{Q}(\alpha)[X]$.

(iv) $f = X^3 + X^2 - 2X - 1$. If α is a root, so is $\alpha^2 - 2$, so f splits completely over $\mathbb{Q}(\alpha)$. $f = (X - \alpha)[X - (\alpha^2 - 2)][X - ((\alpha^2 - 2)^2 - 2)]$.
Exercise: verify that the roots of f in $\mathbb{C}$ are: $2\cos\frac{2\pi}{7}$, $2\cos\frac{4\pi}{7}$, $2\cos\frac{8\pi}{7}$.

Definition: A splitting field for $f(x) \in F[X]$ is an extension K/F with the properties:
(i) $f(x)$ splits completely over K - ie, $f(x)$ is a product of linear factors in $K[X]$ - ie, K contains all roots of f.
(ii) if M is another field with property (i), then $\exists$ morphism $K \to M$, ie, M/K.

Theorem: A splitting field exists and is unique (up to isomorphism).

Proposition: If splitting field K exists then it has finite degree over F, ie, K is finite dimensional as a vector space over F.

Proof: Let f have degree d, and $\alpha_1, \ldots, \alpha_d$ the roots of f in K. Then K is generated, as a vector space, by $1, \alpha_1, \ldots, \alpha_1^d, \alpha_1\alpha_2, \ldots, \alpha_1 \cdots \alpha_d$, since K can only contain polynomials in roots of f. Hence, $\dim \leq d^d$.

Note: The degree of K is actually $\leq d!$

Proposition: If splitting field exists it is unique (up to isomorphism). - ie, any splitting fields for $f \in F[X]$ are isomorphic.

Proof: Let K, K' both be splitting fields for $f \in F[X]$. By property (ii) we have a morphism $K \to K'$. So K' contains a field $K'' \cong K$, and $[K':F] \geq [K'':F] = [K:F]$.
By the same argument, $[K:F] \geq [K':F]$. So, $[K:F] = [K':F] = [K'':F]$.
But $K'' \subseteq K'$ and so degree equation $\Rightarrow K'' = K'$. But $K \cong K'' \Rightarrow K \cong K'$.

Proposition: A splitting field exists for $f \in F[X]$.

Proof: Proceed by induction on ∂f. Assume splitting fields exist $\forall$ polynomials of degree $< d$. By previous result it is unique, each d.
Let $f(X) \in F[X]$ be a polynomial of degree d. Let $p(x)$ be an irreducible factor of $f(X)$ in $F[X]$. If f is already split completely, we are done, and F is the splitting field.
Otherwise, $F[X]/\langle p(x) \rangle = L$ is a field containing a root of f.
So write $f(x) = (x-\alpha) f_1(X)$ in $L[X]$.
The degree of f_1 is $d-1$, so by induction $\exists$ a splitting field K_1 for f_1 over L.
So K_1 contains all roots of f_1 and contains L, so contains α.
So K_1 contains all the roots of f, f_0, and let K be the subfield of K_1 containing all the roots of f. Ie, it is the finite-dimensional extension spanned as a vector space by all products of roots α.
This K is a splitting field for f, so such do exist.

We have thus proved the theorem.

Application to Finite Fields

We want to construct a field of order p^n, characteristic p, an extension of $\mathbb{F}_p$.
Call this field K. If K exists, K^* has order $p^n - 1$, so $x^{p^n-1} = 1 \quad \forall x \in K, x \neq 0$.

So, $x^{p^n} = x \quad \forall x \in K$. So every element of K is a root of $X^{p^n} - X$, and indeed K consists of roots of this polynomial.
Let S be the splitting field of $X^{p^n} - X$ in $\mathbb{F}_p[X]$. Claim S is of order p^n.
We know S is a finite field. Consider sets of roots of $X^{p^n} - X$ in S.
If x, y are roots of $X^{p^n} - X$ in S then $x^{p^n} = x$, $y^{p^n} = y$. So, $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$, so xy is a root.
Also, $0, 1$ are roots.
Now, $(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + y^p = x^p + y^p$ in characteristic p.
So, $(x+y)^{p^n} = (x+y)^{p.p.\cdots} = (x^p + y^p)^{p.\cdots} = \cdots = x^{p^n} + y^{p^n} = x + y$, so $x+y$ is a root.

Hence, set of roots is a field and of order p^n, since $X^{p^n} - X$ splits completely in S and has no repeated roots (as it has no factor in common with its derivative, which is $p^n X^{p^n - 1} - 1$, ie -1). But splitting field is smallest possible, hence S is this subfield of order p^n. Hence a field of order p^n exists and is unique.
The unique field is denoted by $\mathbb{F}_{p^n}$ (or $GF(p^n)$).

We constructed $\mathbb{F}_{p^n}$ as splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. Roots of polynomial are precisely elements of field

Example: $\mathbb{F}_4$, splitting field of $X^4 - X$ over $\mathbb{F}_2$. $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1 = \alpha^2\}$.
$X^4 - X = (X-0)(X-1)(X-\alpha)(X-\alpha^2)$ over $\mathbb{F}_4$
$= (X-0)(X-1)(X^2+X+1)$ over $\mathbb{F}_2$, where X^2+X+1 is irreducible over $\mathbb{F}_2$.
$\mathbb{F}_4 \cong \mathbb{F}_2[X] / \langle X^2+X+1 \rangle$

Example: $\mathbb{F}_8$ = splitting field of $X^8 - X$ over $\mathbb{F}_2$. $X^8 - X = (X)(X-1)(X^3+X^2+1)(X^3+X+1)$ over $\mathbb{F}_2$.
$\mathbb{F}_8 \cong \mathbb{F}_2[X] / \langle X^3+X^2+1 \rangle \cong \mathbb{F}_2[X] / \langle X^3+X+1 \rangle$. These are the same field, for if α is a root of X^3+X^2+1, then $1/\alpha$ is a root of X^3+X+1.
$\mathbb{F}_8 = \{0, 1, \underbrace{\alpha, \alpha^2, \alpha^4}_{\text{roots of } X^3+X^2+1}, \underbrace{\alpha^{-1} = \alpha^6, \alpha^{-2} = \alpha^5, \alpha^{-4} = \alpha^3}_{\text{roots of } X^3+X+1}\}$

Fix an extension K/F of finite degree. Let $\alpha \in K$, with $\{1, \alpha, \alpha^2, \ldots\}$ not an L.I. set. So, there is a linear relation of the form $\alpha^n =$ combination of lower powers.
Ie, α satisfies a polynomial in $F[X]$. Such an α is algebraic over F
Let $I_\alpha = \{f \in F[X] : f(\alpha) = 0\}$. $0 \in I_\alpha$, not only element. I_α is an ideal of $F[X]$:
If $f(\alpha) = 0$, $g(\alpha) = 0$, $h \in F[X]$, then $(f+g)(\alpha) = 0$ and $h(\alpha) f(\alpha) = 0$.
Since I_α is an ideal, have $I_\alpha = \langle m_\alpha(x) \rangle$ for some $m_\alpha \in F[X]$.
Fix m_α to be monic (ie, leading coefficient $= 1$) The m_α is the minimal polynomial of α and: (i) monic polynomial of least degree with α as root,
(ii) divides any other $f \in F[X]$ with α as root.

Example: In $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, $m_0 = X$, $m_1 = X-1$, $m_\alpha = m_{\alpha+1} = X^2 + X + 1$.

Proposition: m_α is irreducible in $F[X]$.

Proof: $m_\alpha = fg$ in $F[X]$, so $m_\alpha(\alpha) = 0 = f(\alpha)g(\alpha)$, so (wlog) $f(\alpha) = 0$.
By property (ii), $m_\alpha | f$, and $f | m_\alpha$, so m_α is irreducible.

Example: $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[X]/\langle x^2 - 2\rangle$. Check that equation $X^2 = 3$ insoluble over $\mathbb{Q}(\sqrt{2})$
So, $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is of degree > 2 over $\mathbb{Q}$.
Let $\gamma = \sqrt{2} + \sqrt{3}$, so $\gamma^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 5 + 2\sqrt{6} \Rightarrow (\gamma^2 - 5)^2 = (2\sqrt{6})^2 = 24$
So $\gamma^4 - 10\gamma^2 + 1 = 0$. Hence γ satisfies $X^4 - 10x^2 + 1$
Now, $\gamma \notin \mathbb{Q}(\sqrt{2})$, else $\sqrt{3} = \gamma - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$. So $\mathbb{Q}(\gamma) \supsetneq \mathbb{Q}(\sqrt{2})$
So, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$. Hence $1, \gamma, \gamma^2, \gamma^3$ are linearly independent.
Thus, $X^4 - 10X^2 + 1$ is minimal polynomial.

A **simple extension** of F is an extension $K = F(\alpha)$.

Facts: Every extension in characteristic 0 is simple.
Every extension ~~in~~ which is a finite field is simple.

Theorem A: A finite subgroup of the multiplicative group of a field is cyclic.

Corollary: Multiplicative group $\mathbb{F}_{p^n}^*$ is cyclic (of order $p^n - 1$)

A **primitive element** of $\mathbb{F}_{p^n}$ is a generator of $\mathbb{F}_p^*$.

Proposition (a): If A is an abelian group, and $\alpha, \beta \in A$ with orders m, n respectively, (m, n coprime), then there is an element of order mn in A.

Proposition (b): If G is a finite subgroup of F^* and $|G| = N = \pi p_1^{e_1} \cdots p_r^{e_r}$, then there is an element of order $p_i^{e_i}$ in G $\forall$ $p_i^{e_i} | N$.

Proof of Theorem A: Let x_1 be element of G of order $p_1^{e_1}$, x_2 with order $p_1^{e_1} p_2^{e_2}$, and so on, to x_r with order $p_1^{e_1} \cdots p_r^{e_r} = N$.
Now G is cyclic with generator x_r.

Proof of Proposition (a): Let α have order m, β order n, and $mu + nv = 1 = hcf(m,n)$.
Let $\gamma = \alpha^v \beta^u \Rightarrow \gamma^m = \alpha^{mv} \beta^{mu} = 1 \cdot \beta^{1-nv} = \beta$, and $\gamma^n = \alpha^{nv} \beta^{mu} = \alpha^{1-mu} \cdot 1 = \alpha$.
So the group generated by γ has elements of orders m and n.
So if r = order of γ = order of $\langle\gamma\rangle$, then $m | r, n | r \Rightarrow mn | r$ (as $(m,n) = 1$)
But $\gamma^{mn} = 1$, so order of $\gamma = mn$.

Proof of Proposition (b): If $p^e | N$ = order of G, then $\exists$ element of order p^e
Consider map: $\lambda : G \to G$; $x \mapsto x^{N/p}$ - a group homomorphism, so image, kernel are subgroups of G. Can $\ker \lambda = G$? If so, then N elements of G - all roots of $x^{N/p} = 1$ ~~*~~
So, $\exists\, x \in G$ such that $\lambda(x) \neq 1$, ~~but~~ $\lambda(x^p) = x^N = 1$. Let $y = x^{N/p^e}$. So, $y^{p^{e-1}} = x^{N/p} \neq 1$,
but $y^{p^e} = x^N = 1$, so y has order p^e, as required.

4. Modules.

Fix a ring R. An **R-module** M is a set with operations $+, -$, and element 0, and operations of R on M (ie, $r \in R$, $m \in M \Rightarrow rm \in M$) such that M is an abelian group w.r.t $+, 0$.

Ie, (A1): $m_1 + (m_2 + m_3) = (m_1 + m_2) + m_3$

(A2): $m + 0 = 0 + m = m$

(A3): $m + (-m) = -m + m = 0$

(A4): $m_1 + m_2 = m_2 + m_1$

(C1): $(r+s)m = rm + sm$

(C2): $r(m+n) = rm + rn$

(C3): $(rs)m = r(sm)$

(C4): $1 \cdot m = m$

Examples: If R is a field, an R-module is exactly a vector space over R.

If A is any abelian group then A has a natural (unique) structure as a $\mathbb{Z}$-module: if $n > 0$ then $n = 1 + \cdots + 1$, hence $na = (1 + \cdots + 1)a = 1a + \cdots + 1a = a + \cdots + a$

if $n < 0$ then $(-n)a = a + \cdots + a \Rightarrow na = (-a) + \cdots + (-a)$.

- check that these obey C1, C2, C3. Hence A has unique structure as a $\mathbb{Z}$-module.

Let V be a vector space over field F - so V is an F-module. Let α be an endomorphism of V. Then α makes V into an $F[x]$-module as follows:

If $c \in F$, then cv = scalar multiple, and $xv = \alpha(v)$. So $f(x) = \sum c_i x^i$ acts as $v \mapsto \sum c_i \alpha^i(v)$.

So we say V becomes an $F[x]$-module via α.

Example: R is an R-module by using ring multiplication as our scalar multiplication.

Let X be any set. Define $R^X = \{ f : X \to R \}$. This has pointwise operations.

(ie, $f+g : x \mapsto f(x) + g(x)$, $-f : x \mapsto -f(x)$, $0 : x \mapsto 0$)

So, R^X is an abelian group. Claim R^X is an R-module by $r \cdot f : x \mapsto r \cdot f(x)$.

Special case: $X = \{1, \ldots, n\}$. Any function is described by values $f = (f(1), \ldots, f(n))$

Ie, $f + g = (f(1) + g(1), \ldots, f(n) + g(n))$, etc.

R^X - denote $R^n = \{ (r_1, \ldots, r_n) : r_i \in R \}$, with component-wise operations.

We call R^n a **free module** over R (or any module isomorphic to R^n)

Let S be a subset of module M. Define $\langle S \rangle = \{ r_1 s_1 + \cdots + r_n s_n : s_1, \ldots, s_n \in S, n < \infty \}$

If $\langle S \rangle = M$, say that S **generates** (or **spans**) M.

If M has a finite set of generators, we call M **finitely generated** (FG), or **finite dimensional**.

If S has property that $r_1 s_1 + \cdots + r_n s_n = 0 \Rightarrow$ all $r_i = 0$ then S is **linearly independent** (LI)

If S is LI and generates M, then S is a **basis** for M.

If M is FG with a basis $\{x_1, \dots, x_n\}$ then every element of M is uniquely expressible as $m = r_1 x_1 + \dots + r_n x_n$ with co-ordinates r_i, and $m \leftrightarrow (r_1, \dots, r_n)$.
Then $M \leftrightarrow R^n$ - free module. Ie, FG-module with basis $\Rightarrow$ free module.

Note: Not every module is free.

If N is a subset of R-module M which is also an R-module wit the inherited operations, then N is a submodule of M.
N a submodule $\Leftrightarrow$ closed under addition, and multiplication by elements of R.
Trivial submodules: $0 = \{0\}$ and M itself.

Have R an R-module. What are submodules? - a subgroup of $(R,+)$ which is closed under multiplication by whole of R. Ie, submodules are ideals.
When is ideal I free? We need a single element x such that $I = \langle \{x\} \rangle$ is an R-module. Hence $I = Rx \Rightarrow I$ is a principal ideal.
Thus, non-principal ideal is not free.

Example: $(\mathbb{Z}/6\mathbb{Z}, +)$ is an abelian group, hence a $\mathbb{Z}$-module. It is generated by $\{1 \bmod 6\}$. But the set is not LI, since $6.(1 \bmod 6) = 0$ is a non-trivial linear relation.

A map $\varphi: M \to N$ between R-modules is an R-module homomorphism if it preserves all R-module structure.
Ie, $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$
$\varphi(-m) = -\varphi(m)$
$\varphi(0_M) = 0_N$
$\varphi(rm) = r\varphi(m)$
} φ is a homomorphism of groups.

- generalisation of linear maps.

Given $\varphi: M \to N$, homomorphism, define $\ker(\varphi) = \{m \in M : \varphi(m) = 0_N\}$, $\operatorname{im}(\varphi) = \{\varphi(m) : m \in M\}$.
Define relation $\equiv_\varphi$ on M by: $x \equiv y \Leftrightarrow \varphi(x) = \varphi(y)$. Clearly $\equiv$ is an equivalence relation.
So: $x \equiv x'$, $y \equiv y' \Rightarrow \varphi(x) = \varphi(x')$, $\varphi(y) = \varphi(y') \Rightarrow \varphi(x+y) = \varphi(x'+y') \Rightarrow x+y \equiv x'+y'$.
and, $\varphi(rx) = r\varphi(x) = r\varphi(x') = \varphi(rx')$, so $rx \equiv rx'$ $\forall r \in R$.

Define an abstract congruence on M, an equivalence relation $\equiv$ such that if $x \equiv x'$, $y \equiv y'$ then $x+y \equiv x'+y'$ and $rx \equiv rx'$ $\forall r \in R$.
Let $[x]_\equiv$ denote the equivalence class of x under $\equiv$.
Consider $[0]$. Claim that $[0]$ is a submodule of M.
If $x, y \in [0]$ then $x \equiv 0$, $y \equiv 0$, so $x+y \equiv 0+0 = 0$, ie $x+y \in [0]$ - closed under addition.
Also, $rx \equiv r.0 = 0$, so $rx \in [0]$, so closed under scalar multiplication.
So $[0]$ is a submodule.

Given N a submodule of M, let $x \sim y$ if $x - y \in N$. Claim $\sim$ is a congruence.
Reflexive: $x \sim x$ iff $x - x \in N$. $0 \in N$ ✓.
Symmetric: $x \sim y \Rightarrow y \sim x$ iff $x - y \in N \Rightarrow y - x \in N$ ✓
Transitive: $x \sim y$, $y \sim z \Rightarrow x \sim z$ iff $x - y$, $y - z \in N \Rightarrow x - z \in N$ ✓
So $\sim$ is an equivalence relation. Need to show congruence.

$x \sim x'$, $y \sim y' \Rightarrow x - x'$, $y - y' \in N \Rightarrow (x+y) - (x'+y') \in N \Rightarrow x+y \sim x'+y'$.
Finally, $r(x - x') \in N \Rightarrow rx - rx' \in N \Rightarrow rx \sim rx'$.

So, abstract congruences $\leftrightarrow$ submodules.
$\equiv \quad \rightarrow \quad [0]$
$\sim \quad \leftarrow \quad N$.

Also showed morphism φ defined on M gives rise to $\equiv_\varphi$, $\varphi(x) = \varphi(y)$.
Submodule attached is $[0] = \{m : \varphi(m) = \varphi(0)\} = \{m : \varphi(m) = 0\} = \ker \varphi$.

Construct quotient module M/N or $M/\sim$ where $\sim \leftrightarrow N$. Elements of M/N are classes $[x]$. Operations: $[x] + [y] = [x+y]$, $-[x] = [-x]$, $[0] = 0$, $r[x] = [rx]$.
Need to check that these make sense, ie, $[x] = [x']$, $[y] = [y'] \Rightarrow$ $[x+y] = [x'+y']$ ✓, $-[x] = -[x']$, $[rx] = [rx']$

$x \sim x'$, $y \sim y'$, so $x+y \sim x'+y'$ and $rx \sim rx'$ as $\sim$ is a congruence. So operations well-defined.
Need to check that M/N is a module wrt these operations.
Eg: (A1): $([x] + [y]) + [z] = [x+y] + [z] = [(x+y)+z] = [x+(y+z)] = [x] + [y+z] = [x] + ([y] + [z])$
(e3): $r(s[x]) = r[sx] = [r(sx)] = [(rs)x] = (rs)[x]$. - etc.
Hence M/N is a module.

Define $q : x \mapsto [x]$, the quotient map. (Obviously a morphism).

Isomorphism Theorem For Modules: Let $\varphi : M \to L$ be a morphism of R-modules. Then, $\ker \varphi$ is a submodule of M, $\operatorname{im} \varphi$ is a submodule of L, and $M/N \cong \operatorname{im} \varphi$, where $N = \ker \varphi$.
Proof: N is a submodule of M as N is $[0]_\equiv$, where $\equiv$ is the congruence for φ.
Define $\bar{\varphi} : M/N \to L$ by $\bar{\varphi} : [x] \mapsto \varphi(x) \in L$. Claim $\bar{\varphi}$ is a well-defined bijective morphism. Note: $\operatorname{im} \bar{\varphi} = \operatorname{im} \varphi$. Prove well-defined and injective thus:
$[x] = [x'] \Leftrightarrow x \equiv x' \Leftrightarrow \varphi(x) = \varphi(x') \Leftrightarrow \bar{\varphi}([x]) = \bar{\varphi}([x'])$.
It is clearly surjective, so we must show only that it is a morphism.
$\bar{\varphi}([x]+[y]) = \bar{\varphi}([x+y]) = \varphi(x+y) = \varphi(x) + \varphi(y) = \bar{\varphi}([x]) + \bar{\varphi}([y])$. Similarly, $\bar{\varphi}(r[x]) = r\bar{\varphi}([x])$.

Quotients, Kernels and Subobjects.

	Subobjects	Kernels	
Groups	Subgroups.	Normal subgroups	- subset
Vector Spaces	Subspaces.	Subspaces	- same
Rings	Subrings.	Ideals	- different
Modules	Submodules.	Submodules	- same.

Any submodule is the kernel of some morphism, ie, quotient $M \to M/N$.
In particular, any subspace of a vector space is the kernel of a linear map.

Example: A - an abelian group regarded as a $\mathbb{Z}$-module. Submodules of A are subgroups.
Every subgroup of an abelian group is normal, hence kernel of some group morphism,
and every group morphism on A is a $\mathbb{Z}$-module morphism.

Let A, B be submodules of M. Define $A+B = \{a+b : a \in A, b \in B\}$ - clearly a submodule of M.
If, in addition, $A \cap B = \{0\}$, we write $A \oplus B$ - (internal) direct sum.
$A \cap B = \{0\} \iff$ every element of $A+B$ is uniquely expressible as $a+b$ with $a \in A$, $b \in B$.

Corollary (2nd Isomorphism Theorem): $(A+B)/B \cong A/(A \cap B)$
Proof: Let $q_B : M \to M/B$ be the quotient map. Let $X = \{x \in M : q_B(x) \in q_B[A]\}$
Claim that $X = A+B$. For: $x \in X \iff q_B(x) = q_B(a)$, some $a \in A \iff q_B(x-a) = q_B(0)$
$\iff x-a \in B \iff x = a+b$, some $b \in B$.
Now consider the restriction of q_B to A, ie, $q_B|_A : A \to q_B[A]$
So, by isomorphism theorem, image of restriction, $q_B[A] \cong A/\ker(q_B|A)$
So, $q_B[A] \cong A/(A \cap B)$. So we have: $X/B \cong q_B(A) \cong A/(A \cap B)$, ie, $(A+B)/B \cong A/(A \cap B)$

Let M be an R-module. The annihilator of M is $\operatorname{ann}(M) = \{r \in R : rm = 0 \ \forall m \in M\}$.
In the case where $R = \mathbb{Z}$ and M an abelian group, this is also called the exponent
of the group.
Claim that $\operatorname{ann}(M)$ is an ideal of R.
If $rm = 0 \ \forall m \in M$, $sm = 0 \ \forall m \in M$, then $(r+s)m = 0 \ \forall m \in M$, and if $t \in R$, then $(tr)m = t(rm) = t.0 = 0$.

For example, $M = \mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}$-module, annihilator $= \langle n \rangle$, exponent $= n$.

A finite abelian group is annihilated by its order N (say) - Lagrange's Theorem.
So any finite abelian group A has non-trivial annihilator $\operatorname{ann}(A) \supseteq \langle N \rangle$, (but necessarily $=$).

Example: $V = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \{1, (12)(34), (13)(24), (14)(23)\}$
Every element of V is annihilated by 2, so $\operatorname{ann}(V) = \langle 2 \rangle$, but order of $V = 4$.

Annihilator of an element $m \in M$ is: $\operatorname{ann}(m) = \{r \in R : rm = 0\}$ - again an ideal of R.
$\operatorname{ann}(M) = \bigcap_{m \in M} \operatorname{ann}(m)$.

Example: M cyclic group of order 6, say $\mathbb{Z}/6\mathbb{Z}$ as $\mathbb{Z}$-module.

m	0	1	2	3	4	5
$\operatorname{ann}(m)$	$\langle 1 \rangle$	$\langle 6 \rangle$	$\langle 3 \rangle$	$\langle 2 \rangle$	$\langle 3 \rangle$	$\langle 6 \rangle$

So, $\operatorname{ann}(M) = \langle 6 \rangle$

Let V be a finite-dimensional vector space over $\mathbb{C}$, α an endomorphism of V, and
make V a $\mathbb{C}[X]$-module via α. Ie, $f(X)$ acts on $v \in V$ by $f(\alpha)$. $\operatorname{ann}(V) = \{f \in \mathbb{C}[X] : f(\alpha)v = 0\}$
Now, $\mathbb{C}[X]$ is an ED, hence a PID, so $\operatorname{ann}(V) = \langle \mu_\alpha(X) \rangle$, where $\mu_\alpha(X)$ is a polynomial

which is of lowest degree such that $\mu(\alpha) = 0$ acting on V.
Fix μ by further condition that μ be monic - ie, leading coefficient 1.
Then this specifies μ_α completely, and μ_α is the minimal polynomial for α.

Fact: $\text{ann}(V) = \langle \mu_\alpha \rangle$ states that any polynomial annihilating α (ie, $f(\alpha) = 0$) is a multiple of μ_α.

Cayley-Hamilton Theorem: Let $\chi_\alpha(x) = \det(\alpha - X.1)$ be the characteristic polynomial.
Then $\chi_\alpha(\alpha) = 0$, $\deg \chi_\alpha = n$.

So, $\mu_\alpha(x)$ divides $\chi_\alpha(x)$. In fact:

Proposition: χ_α, μ_α have the same roots.
Proof: $\chi_\alpha(\lambda) = 0 \iff \det(\alpha - \lambda I) = 0 \iff \alpha - \lambda I$ is singular $\iff \ker(\alpha - \lambda I)$ non-trivial
$\iff \exists\, x \neq 0$ such that $\alpha x = \lambda x \iff \lambda$ is an eigenvalue.
Suppose λ is not a root of μ_α, ie $(x-\lambda) \nmid \mu_\alpha(x)$. Now, $x - \lambda$ is irreducible (degree 1), so coprime to $\mu_\alpha(x)$. So, $\exists\, u(x), v(x) \in \mathbb{C}[x]$ such that $(x-\lambda)u(x) - \mu_\alpha(x)v(x) = 1$.
Substitute $X = \alpha$ and obtain: $u(\alpha)(\alpha - \lambda) - 0 = 1$, identity.
So, $u(\alpha)(\alpha - \lambda)(x) = 1 \cdot x = x$. But LHS $= u(\alpha)(0) = 0$ as x an eigenvector $-$ $\lightning$.
So μ_α has λ as a root.
Conversely, since $\mu \mid \chi$, roots of μ are also roots of χ.

If $\text{ann}(m) \neq \langle 0 \rangle$, ie $\exists\, r \neq 0$ such that $rm = 0$, then we say that m is a torsion element of M.
[In abelian groups of finite order, $\text{ann}(m) = \langle o \rangle$, where o is element of order n].
A module is torsion-free if the only torsion element is $0 \in M$.

5. Structure Theory.

From now on, R is an ED, and we shall be interested in finitely-generated modules.

Structure theory is particularly simple.
We shall find that $M \cong R^n \oplus T$, where R^n is free module and T consists of torsion elements of M. Rank n is well-defined, and T has unique structure,
$T \cong R/\langle p_1^{e_1} \rangle \oplus \cdots \oplus R/\langle p_r^{e_r} \rangle$, with p_i irreducible.

Theorem (Structure Theorem, Invariant Factors): Let R be an ED, and M a finitely-generated R-module. Then, $M = M_1 \oplus \cdots \oplus M_t$, where each M_i is cyclic, and $\text{ann}(M_1) \supseteq \cdots \supseteq \text{ann}(M_t)$

The generators a_i for $\text{ann}(M_i)$ are invariant factors of M - essentially unique. Ie, t and ideals $\langle a_i \rangle$ are determined by M. Note that $a_1 \mid a_2 \mid \cdots \mid a_t$.

Corollary [Structure Theorem, Elementary Divisor]: R, M as before. Then $M \cong R^n \oplus T$, where R^n is free and T is torsion (ie, $\text{ann}(T) \neq \langle 0 \rangle$), $T \cong M_1 \oplus \cdots \oplus M_s$, with M_i cyclic and $\text{ann}(M_i)$ a power of a prime element of R, say $p_i^{e_i}$.

The $p_i^{e_i}$ are **elementary divisors** of M, n is the **free-rank** of M, and both are determined uniquely by M.

Note: we shall not be proving uniqueness, but will give algorithm for finding invariant factors and deducing free rank and elementary divisors.

Consequences of Structure Theorem.

FG abelian groups, $\mathbb{Z}$ is an ED, so an FG abelian group is an FG $\mathbb{Z}$-module. So any FG abelian group A is of form: $\mathbb{Z}^n \oplus \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{e_s}\mathbb{Z}$, where $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ is a cyclic group of order $p_i^{e_i}$ and thus is unique.

If A is finite, then free-rank must be zero, hence A is a product of cyclic groups of prime power order. Hence we can list all abelian groups of given order $|A| = \pi\, |\mathbb{Z}/p_i^{e_i}\mathbb{Z}| = \pi\, p_i^{e_i}$ by factorising the order $|A|$.

Examples:

$\|A\| =$		
4	$\mathbb{Z}/4\mathbb{Z}$,	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$	
6	$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$	(and 1 non-abelian).
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.	(2 non-abelian also)

Look at invariant factor form. Abelian group $A \cong A_1 \oplus \cdots \oplus A_t$, with A_i cyclic, where $\text{ann}(A_i) = a_i$. Ie, $A \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_t\mathbb{Z}$, where $a_1 | a_2 | \cdots | a_t$.

So we have:

$\mathbb{Z}/4\mathbb{Z}$	4
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	2|2
$\mathbb{Z}/6\mathbb{Z}$	6
$\mathbb{Z}/8\mathbb{Z}$	8
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	2|4
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	2|2|2

(*) Recall the situation of finite subgroup G of multiplicative group of a field F. Let $|G| = n$, let exponent of G be a. By proposition, G has an element of order a. But $x^a = 1$ $\forall x \in G$, - equation with n roots in F $\Rightarrow$ degree $\geq n$, so $a \geq n$. But $x^n = 1$ (Lagrange), so $a \leq n$. Hence $a = n$. Hence G has order n, ie, G is cyclic.
So we have another proof that G is cyclic (*).

So if a group has prime power order (primary, or p-group), form is same as ED form. For invariant factors, let $a_t = a$ - the largest or last a_i. Then, a annihilates every element of group. So, $\text{ann}(A) = \langle a \rangle$. Ie, a is exponent of group.

Observe that A contains an element of order a, since $\mathbb{Z}/a\mathbb{Z}$ is a constituent direct summand of A.

Let V be a vector space over a field F of dimension n, and let α be an endomorphism of V. Make V an $F[X]$-module via α. Ie, $f(x): v \mapsto f(\alpha)(v)$.
V is FG over F, hence over $F[X]$. We know V is a torsion module, as $\operatorname{ann}(V) = \langle \mu_\alpha \rangle$, where μ_α is the minimal polynomial for α α and μ_α divides characteristic polynomial $\chi_\alpha = \det(\alpha - x.1)$, and has same roots.
So free-rank of V over $F[X]$ is zero.
By structure theorem, $V = M_1 \oplus \cdots$, where each M_i is a cyclic $F[X]$-module with $\operatorname{ann}(M_i) = \langle a_i(x) \rangle$.

Need to understand "a cyclic $F[X]$-module with annihilator $a(x)$".
Cyclic-generated over $F[X]$ by one element v, say.
Ie, $M = \{ f(X)v : f(X) \in F[X] \} = \{ f(\alpha)v : f(X) \in F[X] \} = \{ f_0 v + f_1 \alpha(v) + \cdots + f_d \alpha^d(v) : f_i \in F, d < \infty \}$.
So M is spanned over F by $v, \alpha(v), \alpha^2(v), \ldots$

But M has annihilator $\langle a(x) \rangle$, where $a(x) = a_d X^d + \cdots + a_0$ $(a_d \neq 0)$, so
$\alpha^d = -\frac{a_{d-1}\alpha^{d-1}}{a_d} - \cdots - \frac{a_0}{a_d}$ - acting on M.
So $\alpha^d(v)$ = linear combination of $\alpha^{d-1}(v), \ldots, \alpha(v), v$, and for any $r \geq d$, $\alpha^r(v)$ has has a similar linear combination
So, M is spanned over F by $v, \alpha(v), \ldots, \alpha^{d-1}(v)$

We claim that $\{ v, \alpha(v), \ldots, \alpha^{d-1}(v) \}$ is a basis (over F) for M.
We need to show that they are L.I. If not, suppose $b_0 v + b_1 \alpha v + \cdots + b_{d-1}\alpha^{d-1} v = 0$, ie, $b(\alpha)v = 0$, some b of degree $< d$.
Then, $b(x)f(x)v = f(x)b(x)v = f(\alpha)b(\alpha)v = f(\alpha)0 = 0$, so $b(x)$ annihilates M.
But $\deg b < \deg a$ and $\langle a \rangle = \operatorname{ann} M$ - $\ast\ast$.
So M has basis $\{ v, \alpha v, \ldots, \alpha^{d-1} v \}$. So $\dim M$ (as an F-vector space) $= \deg(\alpha(x))$.

Action of α on basis:
$$v \mapsto \alpha v$$
$$\alpha v \mapsto \alpha^2 v$$
$$\vdots \quad \vdots$$
$$\alpha^{d-1} v \mapsto \alpha^d v = \left(-\frac{a_{d-1}}{a_d}\alpha^{d-1} - \cdots - \frac{a_0}{a_d} \right)(v).$$

So, matrix of α is companion matrix of $a(x)$: $\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0/a_d \\ 1 & 0 & \cdots & 0 & -a_1/a_d \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1}/a_d \end{pmatrix}$

- where $a_d X^d + \cdots + a_0 = a(x)$ is the annihilator of M.

Now, by the structure theorem, $V = M_1 \oplus \cdots \oplus M_t$, of cyclic submodules, with annihilators $a_1 | a_2 | \cdots | a_t$. Choosing cyclic vector for each M_i, we see that we have a basis for V wrt which α has matrix: $\begin{pmatrix} C(a_1) & & 0 \\ & \ddots & \\ 0 & & C(a_t) \end{pmatrix}$, where $C(a_i)$ is the companion matrix of polynomial $a_i(x)$.

This is the <u>rational canonical (normal) form</u>.

The annihilator of V is final $a_t(x)$, the minimal polynomial of α.
It is an elementary exercise to show that a companion matrix $C(a)$ has minimal polynomial $a(x)$ and characteristic polynomial also $a(x)$ (up to constant factors).
Hence characteristic polynomial of α is $a_1(x) \cdots a_t(x)$, and the minimal polynomial is seen to be $a_t(x)$. So, minimal polynomial divides characteristic polynomial.
Hence deduce Cayley-Hamilton Theorem.

Rational canonical form works over any field F.
We can also obtain a version with elementary factors, but we need to know what prime elements are in $F[X]$. So we specialise to $F = \mathbb{C}$, as the prime elements of $\mathbb{C}[X]$ are just linear polynomials $X-\lambda$, for $\lambda \in \mathbb{C}$.
So, elementary divisor form of Structure Theorem says $V = M_1 \oplus \cdots \oplus M_k$, where $\text{ann}(M_i) = \langle p_i^{e_i} \rangle$ with p_i a prime element of $\mathbb{C}[X]$. Ie, $p_i = X - \lambda_i$, $\lambda_i \in \mathbb{C}$.
So each cyclic submodule M has an annihilator of the form $(X-\lambda)^e$, some $\lambda \in \mathbb{C}$, and $e \geq 1$.

We have that $\alpha - \lambda.1$ acts on M as a nilpotent endomorphism (ie, some power acts as 0), so has companion matrix $\begin{pmatrix} 0 & & 0 \\ 1 & \ddots & \\ 0 & 1 & 0 \end{pmatrix}$, as minimal polynomial of $\alpha - \lambda 1$ is $X^e - 0$.
So α has matrix formed by above + λI, ie: $\begin{pmatrix} \lambda & & 0 \\ 1 & \ddots & \\ 0 & 1 & \lambda \end{pmatrix} =: J_e(\lambda)$

- called Jordan Block Form.

So V has basis wrt which matrix of α is: $\begin{pmatrix} J_{e_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{e_t}(\lambda_t) \end{pmatrix}$

- called Jordan Normal (Canonical) Form. (JNF)

JNF is (lower) triangular, so diagonal entries are eigenvalues. Indeed, characteristic polynomial of α is: $\pm \prod (x-\lambda_i)^{e_i}$, as a Jordan block $J_e(\lambda)$ has $\pm(X-\lambda)^e$ as a characteristic minimal polynomial.
Minimal polynomial of α is least common multiple of $(\lambda - \lambda_i)^{e_i}$, ie $\prod_{\lambda, \text{distinct}} (X-\lambda)^f$, where f = maximum number of e's attached to λ.

So as a consequence of general theory, we obtain:
(i) minimal polynomial | characteristic polynomial (ie, Cayley-Hamiltonian Theorem).
(ii) minimal and characteristic polynomials have same roots (ie, eigenvalues!).

Look at Jordan block $J_e(\lambda) = \begin{pmatrix} \lambda & & 0 \\ 1 & \ddots & \\ 0 & 1 & \lambda \end{pmatrix}$. Clear that last basis vector is an eigenvector.
Are there any others?
$J_e(\lambda) - \lambda I = \begin{pmatrix} 0 & & 0 \\ 1 & \ddots & \\ 0 & 1 & 0 \end{pmatrix}$, and has rank $e-1$, so nullity $= 1$.
So $\ker(J - \lambda I) = \langle \text{last basis vector} \rangle$
Hence, number of L.I. eigenvectors of α = number of Jordan blocks.

So, a matrix or endomorphism is diagonalisable $\Leftrightarrow$ $\exists$ basis of eigenvectors
$\Leftrightarrow$ $\exists$ n L.I. eigenvectors $\Leftrightarrow$ all Jordan blocks have size 1 $\Leftrightarrow$ $e_i = 1$ $\forall i$
$\Leftrightarrow$ minimal polynomial has distinct linear factors $\Leftrightarrow$ minimal polynomial has distinct roots.

We can view this another way: If a matrix is in JNF with all blocks of size 1 and JNF is unique by (improved part of) Structure Theorem. This is diagonal.

Example: $n=2$. (i) Characteristic polynomial has distinct roots λ, μ. We have at least one block for each, so must have $J_1(\lambda) \oplus J_1(\mu)$, ie: $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$.
(ii) If characteristic polynomial has repeated root λ we have either
$J_1(\lambda) \oplus J_1(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, or $J_2(\lambda) = \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}$
The first is diagonalisable; the second is not, as number of L.I. eigenvectors = number of blocks = 1, so no basis of eigenvectors.

JNF contains data for: (i) eigenvalues
(ii) characteristic polynomial
(iii) minimal polynomial
(iv) number of eigenvalues.

Uniqueness finally answers question - what is 'standard' form of an endomorphism / matrix?

Proposition: $n \times n$ matrices A, B over $\mathbb{C}$ are conjugate (ie $\exists$ invertible P such that $P^{-1}AP = B$) iff A and B have the same JNF.

We have to prove structure theorem, at least as far as existence. We do this via invariant factors. We need some technical results. Remember that R is always an ED, and finitely generated modules only.

Proposition 1: Let $\varphi : M \to R^n$ be a surjective R-module homomorphism. Then $M \cong R^n \oplus K$, where $K = \ker \varphi$ - "rank-nullity".

Proof: Let $x_1, \dots, x_n \in M$ have property $\varphi(x_i) = e_i$, where $e_1, \dots, e_n$ is standard basis for R^n. Let $X = \langle x_1, \dots, x_n \rangle$. We claim that $M \cong X \oplus K$ and $X \cong R^n$.
$X \cap K = \{0\}$, since $\sum r_i x_i \in K \Rightarrow \varphi(\sum r_i x_i) = 0 \Rightarrow \sum r_i \varphi(x_i) = 0 \Rightarrow \sum r_i e_i = 0 \Rightarrow$ all $r_i = 0$ as R^n Free.
Further, $\sum r_i e_i = \varphi(\sum r_i x_i)$, so $\varphi : X \to R^n$ is an isomorphism.
Finally, $X + K = M$, since if $m \in M$ then $\varphi(m) = \sum r_i e_i$, some r_i. So $m' = m - \sum r_i x_i$ satisfies $\varphi(m') = \varphi(m) - \sum r_i e_i = 0$, ie, $m' \in K$. So done.

Proposition 2: A submodule of a free module $M \leq R^n$ is again free and of rank $\leq n$.
Ie, $M \cong R^m$, some $m \leq n$.

Corollary: The free-rank of a free module is uniquely determined.
Proof: If $R^m \cong R^n$, then $n \leq m$ and $m \leq n$ by proposition 2, so $m = n$.

Proof of proposition 2: Suppose $e_1, \cdots, e_n$ is a basis of R^n, and M is a submodule of R^n. Let $G = \langle e_1, \cdots, e_{n-1} \rangle$. Then by induction on n, $M \cap G$ is a submodule of $G \cong R^{n-1}$. Hence $M \cap G \cong R^L$, some $L \leq n-1$.

Now, $R^n/G \cong R^1$, and $M \to M/(G \cap M)$ is injective (image of $R^n \to R^n/G$)

So $M \to$ submodule of R^1. But R is an ED, hence PID, so any submodule of R^1 is an ideal of R, and is principal, say $= \langle g \rangle$. Hence it is free. $\langle g \rangle \cong Rg$. So $M \to R^1$ surjective. Hence $M \cong R^1 \oplus (G \cap M)$.

Now, $G \cap M$ is a free module of rank $L \leq n-1$. So $M \cong R^{L+1} = R^m$ with $m \leq n$.

For $n=1$: have already seen that every submodule of R^1 is an ideal, hence principal, hence free.

Proposition 3: R an ED. A finitely-generated torsion-free R-module M is free.

Note: free $\Rightarrow$ torsion-free, trivially.

Proof: Proceed by induction on number n of generators in a generating set for M.

$n=0$: $M = (0) \cong e^0$

$n=1$: $M = Rg_1 \cong R^1$, as g_1 is torsion-free.

So, assume $n>1$ and that the results holds for $n-1$.

Suppose $g_1, \cdots, g_n$ generate M. Either: (a) $\langle g_1 \rangle \cap \langle g_2, \cdots, g_n \rangle = \{0\}$

or: (b) $\langle g_1 \rangle \cap \langle g_2, \cdots, g_n \rangle \neq \{0\}$.

In case (a), we have $\langle g_1 \rangle \cong R^1$ (as g_1 is torsion-free), and by induction $\langle g_2, \cdots, g_n \rangle \cong R^m$, some m, so $M = \langle g_1 \rangle \oplus \langle g_2, \cdots, g_n \rangle \cong R^1 \oplus R^m \cong R^{m+1}$.

In case (b), we have $rg_1 \in \langle g_2, \cdots, g_n \rangle$, some $r \neq 0$. Now, map $\mu: M \to M;\ m \mapsto rm$ is a module homomorphism with image $\mu(M) \leq \langle g_2, \cdots, g_m \rangle$, and $\langle g_2, \cdots, g_m \rangle$ is free by induction. So, $\mu(M)$ is a submodule of a free module, and so is free by proposition 2. So, $\mu(M)$ is free, say $\mu(M) \cong R^m$.

So $M \cong R^m \oplus \ker \mu$, by proposition 1.

But, $\ker \mu = \{ m \in M : rm = 0 \} = \{0\}$, as M is torsion-free.

So $M = R^m \oplus \{0\} \cong R^m$ is free.

Proposition: Let M be FG over R, an ED. Then $M \cong T \oplus R^n$, some n, where T = torsion module (unique).

Proof: Let T = set of torsion elements in M. Let $t_1, t_2 \in T$ and $r_1 t_1 = r_2 t_2 = 0$, with $r_1, r_2 \in R$, non-zero. Then $r_1 r_2 \neq 0$, and $r_1 r_2 (t_1 + t_2) = r_2 r_1 t_1 + r_1 r_2 t_2 = 0 + 0 = 0$.

Also, if $r \in R$ then $r_1 (r t_1) = r r_1 t_1 = 0$. So T is a submodule of M.

Claim that M/T is torsion-free.

Suppose $[m] \in M/T$ with $r[m] = [0]$ in M/T, $(r \neq 0)$. Then $[rm] = [0]$, ie $rm \in T$, ie rm is torsion. So $(xr)m = 0$, some $x \neq 0$. But $xr \neq 0$, ie $m \in T$, ie $[m] = 0$.

So M/T is torsion-free.

M is generated by, say, $g_1, \cdots, g_s$, hence M/T is generated by $[g_1], \cdots, [g_s]$.

So M/T is FG torsion-free, and hence free by proposition 3. So $M/T \cong R^n$, some n.

Hence $M \cong R^n \oplus T$, by proposition 1.

We could now proceed to prove Elementary Divisor form of Structure Theorem by showing $T \cong R/\langle p_1^{e_1}\rangle \oplus \cdots$, but instead we'll prove Invariant Factor form.

Suppose M is FG over R with generators $\{g_1, \cdots, g_n\}$. Let R^n be free with $e_1, \cdots, e_n$ as a free basis, and consider map $\gamma : R^n \to M$; $e_i \mapsto g_i$.
Let $K = \ker \gamma$, a submodule of R^n. By proposition 2, K is free of rank $\leq n$.
Now, K could have rank $= n$.

Example: $R = \mathbb{Z}$ and $K = \langle 2e_1, \cdots, 2e_n\rangle$. $\mathbb{Z}^n/K \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$ (n times).

Theorem: R an ED, K a submodule of R^n, then there is a free basis for K of the form $\{r_1 e_1, \cdots, r_k e_k\}$, $k \leq n$, where $\{e_1, \cdots, e_k\}$ extends to a free basis of R^n, and $r_i \in R$ with $r_1 | r_2 | \cdots | r_k$.

Corollary: If M is a finitely generated R-module (with n generators), then $M \cong R^n/K \cong R/\langle r_1\rangle \oplus \cdots \oplus R/\langle r_k\rangle \oplus R^{n-k}$, with $r_1 | r_2 | \cdots | r_k$.
I.e., $M = M_1 \oplus \cdots \oplus M_i$, with M_i cyclic and $\operatorname{ann}(M_1) \supseteq \cdots \supseteq \operatorname{ann}(M_n)$

This corollary is the invariant factor form of the structure theorem.

We prove the theorem by giving an algorithm for construction of such a basis, which we express in matrix form.
Regard R^n as a module of row vectors of size n over R and a basis for K of size k as a set of k such vectors in a $k \times n$ matrix G.
Assertion of theorem is change in basis in R^n and in K such that G has form: $\left(\begin{array}{ccc|c} r_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & r_k & \end{array}\right)$ - Smith Normal Form. (SNF).

I.e., we can apply invertible column operations (changing basis in R^n) and invertible row operations (changing basis in K) to achieve this SNF.

Theorem: If $N \leq R^n$ then N is free with basis $\{r_1 e_1, \cdots, r_k e_k\}$, where $\{e_1, \cdots, e_n\}$ is some basis for R^n.

Express generators of N as rows of a $k \times n$ matrix, A, of row vectors.
Claim: $\exists$ invertible matrices U, V, where U is $k \times k$, V is $n \times n$, such that entries U, U^{-1}, V, V^{-1} are all in R and $UAV = \left(\begin{array}{ccc|c} r_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & r_k & \end{array}\right)$ with $r_i \in R$ and $r_1 | r_2 | \cdots | r_k$.

Matrices A and B such that $B = UAV$ in this way are called equivalent.

Proposition: Equivalence is an equivalence relation.
Proof: R: $A = I_k A I_n$. S: $B = UAV$ then $A = U^{-1} B V^{-1}$.
T: $C = U_1 B V_1$, then $C = U_1 U A V V_1$ and $U_1 U$, $V V_1$ and inverses $U^{-1}U_1^{-1}$, $V_1^{-1}V^{-1}$ all have entries in R.

Theorem: Any matrix over R is equivalent to exactly one in SNF.

Algorithm for reduction to SNF.

Define **height** of A to be $h(A) = \sum \varphi(A_{ij}) - \varphi$, the Euclidean function for R.
Algorithm will reduce $h(A)$ which is a positive integer, hence bound to terminate.
Suppose A is ~~SNF~~ not in SNF. Two possible reasons: (i) off-diagonal entry.
(ii) it is diagonal, but $r_i \nmid r_{i+1}$.

Case (i): Swap rows or columns to ensure non-zero entry on diagonal.
Ie, $\begin{pmatrix} \cdot & \cdot \\ \cdot & 0 \end{pmatrix}$ or $\begin{pmatrix} \cdot & 0 \\ \cdot & \cdot \end{pmatrix}$.

Corresponding U or V are of form: $\begin{pmatrix} \ddots & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix}$
Consider case $\begin{pmatrix} a & \\ b & \ddots \end{pmatrix}$ - ie, below diagonal.

Let $h = hcf(a,b)$. $h = a.x + b.y$, so $1 = \left(\frac{a}{h}\right)x + \left(\frac{b}{h}\right)y$.
So, matrix $\begin{pmatrix} x & y \\ -b/h & a/h \end{pmatrix}$ has entries in R and determinant 1, so inverse $= \begin{pmatrix} a/h & -y \\ b/h & x \end{pmatrix}$
also has entries in R. So, $U = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & x & y \\ & & -b/h & a/h \end{pmatrix}$ has these properties.

Now, $UA = \begin{pmatrix} ax+by & \\ \frac{-ab}{h} + \frac{ab}{h} & \ddots \end{pmatrix} = \begin{pmatrix} h & \\ 0 & \ddots \end{pmatrix}$ - so cleared entries below a in matrix.

Similarly, multiplication on right by such a matrix clears entries to right of a in matrix, and result is equivalent to the original. So we have increased the number of zeroes in A and we end up with a diagonal matrix.

Case (ii): Have $\begin{pmatrix} d_i & & \\ & \ddots & \\ & & d_j \end{pmatrix}$ with $d_i \nmid d_j$.

So apply row operation to add j^{th} row to i^{th}: $\begin{pmatrix} d_i & & \\ & \ddots & \\ d_j & & \end{pmatrix}$

Now clear to the right of d_i by case (i). Get: $\begin{pmatrix} h & & \\ & \ddots & \\ & & d_j \end{pmatrix}$ where $h \mid d_j$.

Now, $h \mid d_i$, and h not associate to d_i as $h \mid d_j$ and $d_i \nmid d_j$.
So $\varphi(h) < \varphi(d_i)$, so we have reduced $h(A)$ by this step.
Continue until $d_i \mid d_j$ $\forall i<j$. We get SNF.

⊛ **Proof of uniqueness:** If SNF is $\begin{pmatrix} r_1 & & \\ & \ddots & \\ & & r_k \end{pmatrix}$, then
(i) $\langle r_k \rangle$ = ideal generated by all determinants of $k \times k$ submatrices, $=: E_k$.
(ii) E_k is unaffected by steps in algorithm.

Examples: (i) $\begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$ $\xrightarrow{\text{swap}}$ $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ $\xrightarrow[\text{operations}]{\text{ordinary row}}$ $\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}$ -- (ordinary col. ops.)

$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}$ $\xrightarrow{\text{row ops.}}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}$ $\xrightarrow{\text{col. ops.}}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ - SNF.

Here, "special" row/column operations are just the ordinary ones.

(ii) $A = \begin{pmatrix} 2 & 1 \\ 3 & -7 \end{pmatrix}$, $\text{hcf}(2,3) = 1$, $2x + 3y = 1$ with $(x, y) = (-1, 1)$

$U = \begin{pmatrix} x & y \\ -b/h & a/h \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix}$, $UA = \begin{pmatrix} 1 & -8 \\ 0 & -17 \end{pmatrix}$ $\xrightarrow{\text{ordinary col. ops.}}$ $\begin{pmatrix} 1 & 0 \\ 0 & -17 \end{pmatrix}$

(iii) Rational canonical form of $M = \begin{pmatrix} 2 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$ over $\mathbb{Q}$ acting on V.

Kernel of map: $\mathbb{Q}[X]^4 \to V = \mathbb{Q}^4$, generated, by rows of $XI - M$, as a $\mathbb{Q}$-space. Ie: $\begin{pmatrix} x-2 & 0 & 0 & 0 \\ 1 & x-1 & 0 & 0 \\ 0 & 1 & x & 1 \\ -1 & -1 & -1 & x-2 \end{pmatrix}$

Reduce to SNF: swap rows: $\begin{pmatrix} 1 & x-1 & 0 & 0 \\ x-2 & 0 & 0 & 0 \\ 0 & 1 & x & 1 \\ -1 & -1 & -1 & x-2 \end{pmatrix}$

ordinary row ops: $\begin{pmatrix} 1 & x-1 & 0 & 0 \\ 0 & -(x-1)(x-2) & 0 & 0 \\ 0 & 1 & x & 1 \\ 0 & x-2 & -1 & x-2 \end{pmatrix}$

col. op: $\left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & -(x-1)(x-2) & 0 & 0 \\ 0 & 1 & x & 1 \\ 0 & x-2 & -1 & x-2 \end{array}\right)$

swap: $\begin{pmatrix} 1 & x & 1 \\ -(x-1)(x-2) & 0 & 0 \\ x-2 & -1 & x-2 \end{pmatrix}$

(continue) $\to \left(\begin{array}{c|cc} 1 & x & 1 \\ \hline 0 & x(x-1)(x-2) & (x-1)(x-2) \\ 0 & -(x-1)^2 & 0 \end{array}\right)$ $\to \begin{pmatrix} (x-1)(x-2) & 0 \\ 0 & -(x-1)^2 \end{pmatrix}$ --

$\to \begin{pmatrix} x-1 & 0 \\ 0 & (x-1)^2(x-2) \end{pmatrix}$.

So, invariant factors are: $1, 1, x-1, (x-1)^2(x-2)$.

So RCF $= C(x-1) \oplus C((x-1)^2(x-2)) = \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & -5 \\ 0 & 0 & 0 & 4 \end{array}\right)$