# GRM

## 1 Groups

*Lemma* 1.1 (Subgroup correspondence). Let $H \trianglelefteq G$ then subgroups of $G/H$ is in bijective correspondence with subgroups of $G$ containing $H$. This specializes to a bijection between normal subgroups.

**Theorem 1.2** (Isomorphism theorems). *1. $f : G \to H$ homomorphism, $\operatorname{im}(f) \cong G/\ker(f)$*

*2. $H \leq G$, $K$ normal subgroup of $G$, Then $HK \leq G$, $H \cap K$ normal subgrp of $G$ and $HK/K \cong H/(H \cap K)$*

*3. $K \leq L \leq G$, $K, L$ normal subgrps of $G$. $(G/K)/(L/K) \cong G/L$*

*Proof.* First isomorphism (well-definedness, bijectivity) Second isomorphism (first show that $HK$ is a subgroup, then consider $\phi : H \to G/K, h \mapsto hK$. Image is $HK/K$ kernel is $H \cap K$). Third iso Third isomorphism theorem (define $\phi : G/K \to G/L, gK \mapsto gL$) □

**Theorem 1.3.** *$A_n$ is simple for $n \geq 5$.*

*Proof.* Step 1: $A_n$ is generated by 3-cycles. Write $(ab)(bc) = (abc)$ and $(ab)(cd) = (acb)(acd)$

Step 2: If $H \trianglelefteq A_n$ and $H$ contains a 3-cycle, then $H = G$. Conjugate by $\sigma \in S_n$ to move that to (123) (WLOG), If $\sigma \in A_n$, then (123) is in $A_n$. If odd, then replace $\sigma$ by $\sigma \cdot (45)$ ($n \geq 5$) and use commutativity of $(45), (123)$. Can do the same for any other 3-cycle.

Step 3: If $H \trianglelefteq A_n$ and $H \neq \{e\}$ then $H$ contains a 3-cycle.

- In disjoint cycle notation, $(123 \ldots r)\tau$ (WLOG)
- $(123)(456)\tau$
- $(123)\tau$, where$\tau$ is a product of disjoint transposition.
- $(12)(34)\tau$, where $\tau$ is a product of disjoint transpositions.

□

**Theorem 1.4.** *$G$ finite group. $H \leq G$ of index $n$, then there exists a normal subgroup $K \trianglelefteq G$ s.t. $K \leq H$ and $|G/K| \mid n!$ and $|G : K| \geq n$.*

*Proof.* Let $G$ act on $[G : H]$ by left mult. This gives a hom $\phi : G \to S_n$. $\ker \phi = \cap_{g \in G} gHg^{-1}$, which is a normal subgroup of $G$ contained in $H$. $|G/K| \mid n!$ by 1st iso and Lagrange. $|G : K| \geq n$ as $K \leq H$. □

**Corollary 1.5.** *If $G$ is a non-abelian finite simple group, and $H \leq G$ is a subgroup of index $n > 1$, then $G$ is isomorphic to a subgroup of $A_n$, where $n \geq 5$.*

*Proof.* Left coset action is non-trivial, so $\ker \phi = \{e\}$ by simplicity, so $G$ embeds in $S_n$, Compose with the sign hom, deduce that $G$ embeds in $A_n$ (o/w get an index two subgrp). $n \geq 5$ because $S_1, S_2, S_3, S_4$ have no non-abelian simple subgroups. □

**Proposition 1.6.** *Let $G$ be a finite $p$-group (of order $p^a$), then $G$ has subgroups of order $p^b$ for all $0 \leq b \leq a$.*

*Proof.* Proceed by induction. Trivial if $a = 1$. Suppose true for all $a < k$. Note that by considering conjugation action of $G$ on itself, we see that $Z(G)$ is non-trivial, so it contains an element $g$ of order $p$ by Cauchy, so $G$ has a (normal) subgroup of order $p$. Taking quotient, get a group of order $p^{k-1}$. Induction hypothesis says that $G/\langle g \rangle$ contains subgroups of order $p^b$ for all $0 \leq b \leq k - 1$. By subgroup correspondence, each subgroup $K$ corresponds to some subgroup of $H \leq G$ s.t. $H/\langle g \rangle = K$, so true for $a = k$. Hence true for all $a$ by strong induction. □

**Theorem 1.7** (Sylow's theorem)**.** *Let $G$ be a finite group and $p$ prime. Suppose $p^a m = |G|$ and $p \nmid m$.*

1. *There exists a Sylow $p$-subgroup of $G$, i.e., $Syl_p(G) \neq \varnothing$;*
2. *All Sylow $p$-subgroups of $G$ are conjugate to each other. (In fact all $p$-subgroups can be conjugated into a Sylow $p$-subgroup);*
3. *Let $n_p$ be the number of Sylow $p$-subgroups of $G$, then $n_p \equiv 1 \pmod p$ and $n_p \mid |G|$ (so $n_p \mid m$)*

*Proof.* Let $G$ act on the set of size $p^a$ subsets of $G$ pointwise. Pick an orbit $\Sigma$, then $|Sigma| \geq |G|/p^a = m$ (for all $g \in G$ there exists $X \in \Sigma$ s.t. $g \in X$) If $|\Sigma| = m$, then its stabilizer is a Sylow $p$-subgroup. If all orbits have size $> m$, then use Orbit-stabilizer to deduce that

$$p \mid \binom{|G|}{p^a} = \prod_{j=0}^{p^a-1} \frac{p^a m - j}{p^a - j}$$

Note that each factor on RHS is not divisible by $p$, so contradiction. So there must be an orbit of size $m$.

Pick a $p$-subgroup $Q \leq G$, and let $Q$ acts on the set of left cosets of a Sylow $p$-subgroup $P$. At least one orbit has size 1 otherwise $p$ divides $|G : P| = m$. so consider this orbit $gP$, then $qgP = gP$ for all $q \in Q$, this implies that $qQg^{-1} \leq P$.

Sylow II says that the conjugation action of $G$ on $Syl_p(G)$ is transitive so $n_p \mid |G|$ by orbit-stabilizer. Let $P \in Syl_p(G)$, let $P$ act on $Syl_p(G)$ by conjugation. $P$ has orbit size 1. If $Q$ also has orbit size 1, then $P \leq N_G(Q)$, so $P$ and $Q$ are both Sylow $p$-subgroups of $N_G(Q)$, then Sylow II says $P$ and $Q$ are conjugate, so $P = Q$. This means that precisely one orbit has size 1, so $n_p \equiv 1 \pmod p$ as other orbits must have size divisible by $p$ by orbit-stabilizer. □

**Corollary 1.8.** *If $n_p = 1$ for some $p$, then the unique Sylow $p$-subgroup is normal.*

**Corollary 1.9.** *If $G$ is a non-abelian simple group, then for all prime $p \mid |G|$, $G$ embeds as a subgroup of $A_{n_p}$ ($|G| \mid \frac{n_p!}{2}$), and $n_p \geq 5$ as $A_2, A_3, A_4$ don't contain non-abelian simple subgroups.*

*Proof.* $G$ acts on $Syl_p(G)$ by conjugation. Embeds in $S_{n_p}$. Compose with sgn to show that the image lies in $A_{n_p}$. □

**Proposition 1.10** (Frattini argument)**.** *$K \trianglelefteq G$, $P$ is a Sylow $p$-subgroup of $K$. Then $G = N_G(P)K$.*

*Proof.* For all $g \in G$, $g^{-1}Pg$ is another Sylow $p$-subgroup of $K$ (since $K$ is normal). Sylow II implies that $k^{-1}g^{-1}Pgk = P$ for some $k \in K$, so $gk = n \in N_G(P)$, so $g = nk^{-1} \in N_G(P)K$. Hence $G = N_G(P)K$. □

# 2 Rings

**Proposition 2.1** (Subring/Ideal correspondence)**.** *Let $I \trianglelefteq R$, then there is a a bijective correspondence between subrings of $R/I$ and subrings of $R$ contianing $I$. This specializes to a bijection between ideals.*

**Theorem 2.2** (Isomorphism theorems)**.**

1. *$\phi : R \to S$ ring hom, then $\operatorname{im}(\phi) \cong R/\ker\phi$.*
2. *$R \leq S$, $J \trianglelefteq R$, then $(R + J)/J \cong R/(R \cap J)$*
3. *$I, J \trianglelefteq R$, $I \subseteq J$, then $(R/I)/(J/I) \cong R/J$.*

**Theorem 2.3** (Characterization of prime ideal and maximal ideal)**.** *$I \trianglelefteq R$ is maximal (resp. prime) if $R/I$ is a field (resp. ID).*

*Proof.* If $I$ is a maximal ideal then $R/I$ has only two ideals $(0), R/I$ by ideal correspondence, so $R/I$ is a field. Conversely if $R/I$ is a field, it has two ideals, and by ideal correspondence $I$ is maximal. If $I$ is a prime ideal, If $ab \in I$, then $ab + I = 0 + I$ in $R/I$, then $a + I = 0 + I$ or $b + I = 0 + I$, so $a \in I$ or $b \in I$. □

**Proposition 2.4.** *Let $R$ be an ID. A principal ideal $(p)$ is a prime ideal iff $p$ is $0$ or prime.*

**Proposition 2.5.** *In ID, prime $\implies$ irreducible.*

*Proof.* Let $p$ be prime. Suppose $p = ab$ for some $a, b \in R$. then $p \mid ab$, so $p \mid a$ WLOG. so $a = pr$ some $r \in R$, so $p = prb$, so $p(1 - rb) = 0$, so $1 - rb = 0$ as $p = 0$ and $R$ is ID, so $r, b$ are units. So $p$ is irreducible. □

**Proposition 2.6.** *In PID, irreducible $\implies$ prime. (This is crucial in the proof of PID $\implies$ UFD)*

*Proof.* Let $p$ be irreducible and suppose $p \mid ab$ but $p \nmid a$. Then consider $(p, a) = (m) \trianglelefteq R$, so $a = rm$, $p = sm$. Either $s$ or $m$ is a unit. If $s$ is a unit , then $m = s^{-1}p$, then $p \mid a$ (contradiction), so $m$ must be a unit, so $(m) = R$, so $1 = ak + pl$, so $b = abk + pbl$ and $p$ divides RHS, so $p \mid b$. □

**Proposition 2.7.** *In UFD, irreducible $\implies$ prime.*

*Proof.* Let $r$ be irreducible in some UFD $R$. Suppose $r \mid ab$, then $sr = ab$ for some $s \in R$. Replace $s, a, b$ with their unique factorizations into irreducibles, then up to units $r$ must appear as one of the factors on RHS, so $r$ is either a irreducible factor of $a$ or $b$ up to associates, so $r \mid a$ or $r \mid b$. □

**Theorem 2.8.** *ED $\implies$ PID, and PID $\implies$ UFD.*

*Proof.* ED $\implies$ PID. Let $I \trianglelefteq R$ be an ideal. Pick an element $r \in I$ with minimal non-zero euclidean function value (by WOP). Apply division algorithm to show that everything in $I$ is divisible by this element. so $I$ is principal.

PID $\implies$ UFD. If $R$ is a PID, then it is Noetherian. Given $r \in R$, if $r$ cannot be factorized as products of irreducibles then can write $r = r_1 s_1$ with $r_1, s_1$ both non-units and $r_1$ cannot be factorized into irreducibles. Keep going. Write $r_1 = r_2 s_2$ with $r_2, s_2$ non-unit and $r_2$ not irreducible. Get an increasing chain of ideals

$$(r_1) \subseteq (r_2) \subseteq \dots$$

By Noetherian property, for all sufficiently large $n$, $(r_n) = (r_{n+1})$, so $r_n$ and $r_{n+1}$ are associates, meaning that $r_n$ must be irreducible.

To see uniqueness, suppose have two factorizations into irreducibles, then each irreducible is prime so must divide something in the other factorization. Deduce uniqueness up to associates. □

**Theorem 2.9.** *In PID, TFAE*

- *$p$ is prime*
- *$p$ is irreducible*
- *$(p)$ is maximal*
- *$R/(p)$ is a field*
- *$R/(p)$ is an ID*

## 2.1 Polynomials

**Proposition 2.10.** *If $R$ is UFD, $f, g$ primitive in $R[X]$, then $fg$ is primitive.*

*Proof.* Suppose not. Take content and let $p$ be a prime (irreducible) dividing $c(fg)$. Write $f = a_0 + a_1X + ... + a_nX^n$, $g = b_0 + b_1X + ... + b_mX^m$. Then $\exists k \geq 0$ s.t. $p \mid a_0, ..., a_{k-1}$ but $p \nmid a_k$ and $\exists l \geq 0$ s.t. $p \mid b_0, ..., b_{l-1}$ but $p \nmid b_l$. Check the coeff of $X^{k+l}$, which is $a_0b^{k+l} + ... + a_{k-1}b_{l+1} + a_kb_l + a_{k+1}b_{l-1} + ... + a^{k+l}b_0$. Note that $p$ divides this coeff and all terms except $a_kb_l$. Contradiction. □

**Corollary 2.11.** *Content is multiplicative up to associates.*

**Theorem 2.12** (Gauss's lemma)**.** *Let $R$ be a UFD, $F$ its field of fractions. Let $f \in R[X]$ be a primitive polynomial. $f$ is reducible in $R[X]$ iff $f$ is reducible in $F[X]$.*

*Proof.* If reducible in $R[X]$, then obviously reducible in $F[X]$. Conversely if $f = gh$ in $F[X]$, then can clear denominators by multipying $a$ and $b$ to get $abf = (ag)(bh)$, $ag \in R[X]$, $bh \in R[X]$. Have $ag = c(ag)g_1$ for some primitive $g_1 \in R[X]$ (similarly for $bh$). Take content,

$$ab = c(abf) = uc(ag)c(bh)$$

where $u$ is a unit, so $c(ag)c(bh) = u^{-1}ab$, so $abf = u^{-1}abg_1h_1$, where $g_1, h_1$ are primitive. $R$ is an ID, so may cancel $a, b$ and get $f = u^{-1}g_1h_1$ which is a factorization over $R$. □

**Proposition 2.13.** *Let $R$ be a UFD, $F$ its field of fractions. Let $g \in R[X]$ be primitive. If $J = (g) \trianglelefteq R[x]$ and $I = (g) \trianglelefteq F[X]$. Then $I \cap R[X] = J$. Equivalently. If $g$ divides $f \in R[X]$ in $F[X]$, then $g$ divides $f$ in $R[X]$.*

*Proof.* Let $f \in J$. Write $f = gh$ for some $h \in F[X]$. Clearing denominators, get $bf = g(bh)$ where $bh \in R[X]$. Taking contents, get $c(bf) = uc(bh)$. Have $c(bf) = bc(f)$. Write $bh = c(bh)h_1$, where $h_1$ is primitive, then $bc(f) = uc(bh)$, so $c(bh) = u^{-1}bc(f)$, so $bf = u^{-1}bc(f)gh_1$ where $h_1$ are primitive. Cancel $b$ as we're in ID. $f = g(u^{-1}c(f)h_1)$, so $g$ divides $f$ in $R[X]$. □

**Theorem 2.14.** *$R$ is a UFD $\implies$ $R[X]$ is a UFD. (The converse is also true)*

*Proof.* By taking contents, it suffices to consider primitive polynomials since $c(f)$ is a product of unique irreducibles by unique factorization property in $R$. Take $f \in R[X]$ primitive. If $f$ is irreducible then we are done. If not, then $f = f_1 f_2$, where both factors are non-unit, hence non-constant. Hence we strictly reduces degree. Repeat factorization for $f_1$ and $f_2$. This process eventually terminate as each factorization strictly reduces degree. Hence eventually we must end up getting a product of irreducibles.

Uniqueness. Note that $c(f)$ has unique factorization, so it suffices to deal with primitive polynomials. Suppose $f = p_1 ... p_n = q_n .... q_n$ are two factorizations in $R[X]$. Consider these factorizations in $F[X]$ (ED hence PID hence UFD), so up to reordering, $p_i = u_i q_i$ for some unit $u_i \in F[X]$ ($u_i \in F$). (Apply the preceding proposition, we are done.) Clearing denominators, $a_i p_i = b_i q_i$ for some $a_i, b_i \in R$. Taking contents, we see that $a_i = v_i b_i$ for some unit $v_i \in R$ (as $p_i, q_i$ are irreducible hence primitive). $v_i b_i p_i = b_i q_i \implies v_i p_i = q_i$, i.e., unique up to associates. □

**Theorem 2.15.** *If $R[X]$ is a PID, then $R$ is a field. In general, if $R$ is a PID, $S$ is an ID, and $\phi : R \to S$ is a surjective ring hom, then $\phi$ is either an iso or $S$ is a field.*

*Proof.* If $R[X]$ is a PID, then $R \leq R[X]$ is an ID. Consider $\phi : R[X] \to R, f(X) \mapsto f(0)$. This is a surjective ring hom, then $R \cong R[X]/\ker\phi$ is an ID, so $\ker\phi$ is a prime ideal, hence maximal (in a PID), so $R$ is a field. □

**Theorem 2.16** (Eisenstein's criterion)**.** *Let $R$ be a UFD and $f = a_0 + a_1 X + \ldots + a_n X^n \in R[X]$ be primitive. Let $p$ be an irreducible (hence prime) s.t.*

- $p \nmid a_n$
- $p \mid a_i$ *for* $0 \leq i \leq n-1$
- $p^2 \nmid a_0$.

*Then $f$ is irreducible in $R[X]$ (hence in $F[X]$ by Gauss).*

*Proof.* Suppose we have a factorization $f = gh$ in $R[X]$, Write

$$g(X) = r_0 + r_1 X + \ldots + r_k X^k, \ h(X) = s_0 + s_1 X + \ldots + s_l X^l$$

where $r_k, s_k \neq 0$. $p \nmid a_n$ implies $p \nmid r_k$ and $p \nmid s_l$. $p \mid a_0$ but $p^2 \nmid a_0$ implies that we may assume WLOG $p \mid r_0$ and $p \nmid s_0$. Suppose $p \mid r_0, \ldots, p \mid r_{j-1}$ and $p \nmid r_j$ for some $1 \leq j \leq n$. Then

$$a_j = \sum_{i=0}^{j} r_i s_{j-i} = r_0 s_j + ... + r_{j-1} s_1 + r_j s_0$$

Note that $p$ divides everything on RHS except $r_j s_0$, so $p \nmid a_j$, so $j = n$, so $h$ is a constant polynomial. $f$ is primitive, so $h$ is a unit, so $f$ is irreducible. □

**Proposition 2.17.** *Let $\alpha$ be an algebraic integer. Consider $\phi : \mathbb{Z}[X] \to \mathbb{C}$ $f \mapsto f(\alpha)$, then $\ker(\phi)$ is principal and is generated by the minimal polynomial which is monic and irreducible.*

*Proof.* Since $\alpha$ is an algebraic integer, the kernel is non-trivial and there exists a monic polynomial that annihilates $\alpha$. Choose a $f_\alpha \in \ker\phi$ of minimal positive degree. $f_\alpha$ is primitive. Work over the field of fraction $\mathbb{Q}$. Let $h \in \ker\phi$. By division algorithm, can find $q, r \in \mathbb{Q}[X]$ s.t. $h = qf_\alpha + r$, where $r = 0$ or $\deg(r) < \deg(f_\alpha)$. Clear denominators, $ah = (aq)f_\alpha + ar$. See that $ar \in \ker\phi$ and $\deg r < \deg f_\alpha$, so $r = 0$, so $ah = f_\alpha(aq)$. Taking content, $c(ah) = ac(h) = uc(aq)$. So $c(aq) = u^{-1}ac(h)$, so $ah = f_\alpha u^{-1} ac(h) q_1$, where $aq = c(aq)q_1$, $q_1$ primitive. Cancelling $a$ have $f_\alpha u^{-1} c(h) q_1 = h$, so $h \in (f_\alpha)$. $\ker\phi = (f_\alpha)$ is a prime ideal as the image is an ID, so $f_\alpha$ is prime hence irreducible. □

## 2.2 Noetherian stuff

**Proposition 2.18.** *$R$ is Noetherian $\Leftrightarrow$ every ideal is finitely generated.*

*Proof.* $\Leftarrow$: Given an ascending chain of ideals, their union is an ideal, finitely generated, so the chain eventually stabilizes.
$\Rightarrow$: Suppose $I$ is not finitely generated. Construct an ascending chain. Pick $a_1 \in I$ and then $a_2 \in I \setminus (a_1)$ and so on. Get an ascending chain which does not stabilize. □

**Theorem 2.19** (Hilbert's basis theorem). *$R$ is Noetherian $\implies$ $R[X]$ is Noetherian.*

*Proof.* Let $J \trianglelefteq R[X]$. Construct an ascending chain of ideals as in the proof of the preceding theorem (BUT each time choose polynomial of minimal degree). If this process terminates then $J$ is finitely generated. Suppose this doesn't terminate, then get an ascending chain of ideals

$$(f_1) \subseteq (f_1, f_2) \subseteq (f_1, f_2, f_3) \subseteq \dots$$

Consider the leading coefficients $a_i$ of $f_i$. The chain $(a_1) \subseteq (a_1, a_2) \subseteq \dots$ eventually stabilizes by ACC, so $(a_1, a_2, a_3, \dots) = (a_1, a_2, \dots, a_m)$. In particular, $a_{m+1} = \sum_{i=1}^{m} a_i b_i$, $b_i \in R$. Now consider a polynomial $g \in J$ defined as follows.

$$g(X) = \sum_{i=1}^{m} b_i f_i X^{\deg f_{m+1} - \deg f_i}$$

(Note that by construction $f_i$ is a polynomial of minimal degree in $J \setminus (a_1, \dots, a_{i-1})$, so $g$ is indeed a polynomial) Then $f_{m+1} - g$ has degree strictly smaller than $\deg f_{m+1}$, and $f_{m+1} - g \notin (f_1, \dots, f_m)$, but $f_{m+1}$ has minimal degree in $J \setminus (a_1, \dots, a_m)$. Contradiction. So the chain must eventually terminate/stabilize. □

**Proposition 2.20.** *Quotient ring of Noetherian ring is Noetherian.*

*Proof.* Let $R$ be Noetherian and $I \trianglelefteq R$, Let $J \trianglelefteq R/I$. By ideal correspondence, $J$ corresponds to some ideal $I \subseteq J' \trianglelefteq R$. $J'$ is finitely generated, so $J$ is finitely generated in $R/I$. □

# 3 Modules

**Proposition 3.1** (Submodule correspondence). *Let $N \leq M$ be a submodule. Then submodules of $M/N$ are in bijective correspondence with submodules of $M$ containing $N$.*

**Theorem 3.2** (Isomorphism theorems).

1. *$f : M \to N$ $R$-mod hom then* $\operatorname{im} f = M/\ker f$.
2. *$A, B \leq M$ then $A + B$ is a submodule of $M$ and $(A + B)/B \cong A/(A \cap B)$.*
3. *$N \leq L \leq M$, then $(M/N)/(L/N) \cong M/L$.*

**Proposition 3.3.** *An $R$-mod $M$ is finitely generated iff there is a epimorphism $R^k \to M$ for some $k$.*

**Definition 3.4** (Free generation). A subset $S \subseteq M$ is said to freely generate $M$ if

- $S$ generates $M$
- Any (set-theoretic) function $\psi : S \to N$ to an $R$-mod $N$ uniquely extends to an $R$-mod hom $\tilde{\psi} : M \to N$

**Proposition 3.5** (Equivalent definitions of free generation). *Let $M$ be an $R$-mod and $S = \{m_1, m_2, \dots, m_k\} \subseteq M$. TFAE.*

- *$S$ freely generates $M$;*
- *$S$ generates $M$ and $S$ is independent.*
- *Every element of $M$ is uniquely expressible as an $R$-linear combination of things in $S$.*

**Proposition 3.6** (Invariance of dimension/rank). *$R$ non-zero ring. $R^n \cong R^m$ iff $n = m$.*

*Proof.* Choose a maximal ideal $I \trianglelefteq R^n$, then $R^n/IR^n \cong (R/I)^n$ is a $R/I$-vector space, so the given $R$-mod iso induces an vector space iso $(R/I)^n \cong (R/I)^m$. Apply stuff from LA. □

**Proposition 3.7.** *Let $M$ be an $R$-module. If $N \leq M$ and both $N, M/N$ are f.g., then $M$ is f.g. The converse is true if $R$ is Noetherian.*

**Proposition 3.8.** *Let $M$ be an $R$-mod. If $N \leq M$ and $M/N$ is free, then $M \cong N \oplus M/N$.*

*Proof.* Split SES $N \hookrightarrow M \to M/N$. □

**Theorem 3.9** (Smith normal form)**.** *Let $R$ be an ED. Every matrix with coeff in $R$ is equivalent to a* $\operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)$ *s.t.* $d_1 \mid d_2 \mid \dots \mid d_r$ *(and all non-zero).*

*Proof.* If the matrix is 0 then done. Otherwise there is a non-zero entry. Apply row/col operation to move that to $(1, 1)$ position. Look at stuff in the first row if there is anything not divisible by 11 entry then apply euclidean algorithm to reduce the euclidean func and move that remainder to 11 entry. This eventually terminates so we can then clear out the first row. Similarly, can clear out the first column. Then will get a submatrix $C$. If there is any entry in $C$ that's not divisible by 11 entry, apply euclidean algo and move that to 11 entry. This messes up the first row and column, so repeat the preceding steps. Each step strictly reduces the norm of the 11 entry, so this process eventually stops. Apply this process recursively to submatrices. Eventually will get a matrix in SNF. □

*Lemma* 3.10. $R$ PID. Any submodule of $R^m$ is generated by at most $m$ elements.

*Proof.* Let $N \leq R^m$. Consider the ideal

$$I = \{r \in R : \exists r_2, \dots, r_m \in R, (r, r_2, r_3, \dots, r_m) \in N\}$$

This is generated by some element $a \in R$ (PID) and $(a, a_2, \dots, a_m) \in N$. Pick an arbitrary $(r_1, \dots, r_m) \in N$, then $r_1 = ra$, so subtracting gives $(r_1, r_2, \dots, r_m) - r(a, a_2, \dots, a_m) = (0, r_2 - ra_2, \dots, r_m - ra_m) \in N \cap (\{0\} \times R^{m-1}) \leq N$. Apply induction. Base case is trivial. $R$ is a PID, so any submodule of $R$ (ideals) are generated by a single element. □

**Proposition 3.11.** *Let $R$ be an ED and $N \leq R^m$. Then there exists a basis $v_1, \dots, v_m$ of $R^m$ s.t. $N$ is generated by $d_1 v_1, \dots, d_r v_r$ for some $r \leq m$ and $d_1 \mid d_2 \mid \dots \mid d_r$*

*Proof.* Pick a generating set of $N$ given by $u_1, \dots, u_n$, $n \leq m$. Write down the matrix $A = (u_1 \; u_2 \; \dots \; u_n)$ each $u_i$ is a column vector. Put it in SNF. Column operations change basis for $N$. Row operations change basis for $R^m$. So the resulting invariant factors give the new coordinates of generators of $N$ in the new basis of $R^m$. □

**Theorem 3.12** (Classification of finitely generated modules over ED)**.** *Let $R$ be an ED. Let $M$ be a finitely generated $R$-module. Then*

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \dots \oplus R/(d_r) \oplus R \oplus R \oplus \dots \oplus R$$

*where $d_1 \mid d_2 \mid d_3 \mid \dots \mid d_r$.*

*Proof.* $M$ is f.g., so there is a surjective hom $\phi : R^n \to M$, so $M \cong R^n / \ker \phi$. $\ker \phi$ is a submodule of $M$, so by preceding proposition, can find a basis of $M$ such that $d_1 v_2, \dots d_r v_r$ is a basis for $\ker \phi$. Then $M \cong R^n / \langle d_1 v_1, d_2 v_2, \dots, d_r v_r \rangle \cong R/(d_1) \oplus \dots \oplus R/(d_r) \oplus R^m$. □

**Theorem 3.13** (Primary decomposition theorem)**.** *Let $R$ be an ED. Suppose $M$ is a f.g. $R$-mod, then*

$$M \cong N_1 \oplus N_2 \oplus \dots \oplus N_k$$

*where $N_i \cong R$ or $N_i \cong R/(p^n)$ for some prime $p \in R$ and $n \geq 1$.*

*Proof.* Apply CRT to the classification theorem □

## 3.1 Matrices

Let $V$ be an $\mathbb{F}$-vector space, then can make $V$ an $\mathbb{F}[X]$-mod $V_\alpha$ by using the action $f(x) \cdot v = f(\alpha)(v)$, where $\alpha \in L(V, V)$.

**Theorem 3.14** (Rational canonical form). *Let $\alpha : V \to V$ be an endomorphism of a finite dim $\mathbb{F}$-vector space. Then as an $\mathbb{F}[X]$-module, we have*

$$V_\alpha \cong \frac{\mathbb{F}[X]}{(f_1)} \oplus \ldots \oplus \frac{\mathbb{F}[X]}{(f_r)}$$

*such that $f_1 \mid f_2 \mid \ldots \mid f_r$. Thus there exists a basis such that $\alpha$ is block-diagonal, and each block is the companion matrix for $f_i$.*

*Proof.* Apply classification theorem for finitely generated $\mathbb{F}[X]$-modules. Note that $V$ is finite dim, so we can't have free factors. □

**Theorem 3.15** (Jordan normal form). *Let $V$ be a finite dimensional $\mathbb{C}$-vector space and $\alpha \in L(V, V)$. Then the associated $\mathbb{C}[X]$-module has the form*

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X - \lambda_1)^{n_1})} \oplus \ldots \oplus \frac{\mathbb{C}[X]}{((X - \lambda_k)^{n_k})}$$

*Thus there is a basis of $V$ in which $\alpha$ is in JNF.*

*Proof.* Apply primary decomposition theorem, noting that the only primes in $\mathbb{C}[X]$ are linear polynomials. □

**Proposition 3.16.** *Two endomorphisms $\alpha \in L(V, V)$ $\beta \in L(W, W)$. $V_\alpha \cong W_\beta$ as $F[X]$-modules if and only if there exists a linear isomorphism $\gamma : V \to W$ s.t. $\gamma^{-1}\beta\gamma = \alpha$.*

*Proof.* Let $\phi$ be the module iso and $\gamma$ its underlying linear iso. Look at the action of $X$.

$$\phi(\alpha(v)) = \phi(Xv) = X\phi(v) = \beta(\phi(v))$$

i.e., $\gamma\alpha = \beta\gamma$. Conversely, if such $\gamma$ exists, then after making things into $F[X]$-mod, it becomes a module iso. □

## 3.2 Noetherian stuff

An $R$-module $M$ is Noetherian iff every ascending chain of submodules eventually stabilizes (equivalently every submodule is finitely generated).

**Proposition 3.17.** *If $R$ is a Noetherian ring, then $R^n$ is Noetherian as an $R$-module.*

*Proof.* $R$ is Noetherian as a ring so it is also Noetherian as an $R$-module. Proceed by induction. Define an ideal

$$I = \{r \in R : \exists r_2, \ldots, r_n, (r, r_2, ..., r_n) \in N\}$$

Then since $R$ is Noetherian, $I$ is finitely generated, say $I = (a_1, a_2, ..., a_k)$. Then can find $a_{2j}, \ldots, a_{nj}$ s.t. $(a_j, a_{2j}, ..., a_{nj}) \in N$. Consider an arbitrary element $x = (r_1, \ldots, r_n) \in N$, then $r_1 \in I$, so can be written as an $R$-linear combination of $a_j$, so there exists an element in $m \in I$ s.t. $x - m \in N' = N \cap (\{0\} \times R^{n-1})$. $N'$ is a submodule of $R^{n-1}$ so must be finitely generated by induction hypothesis. This implies (direct sum) that $N$ is finitely generated. □

**Proposition 3.18.** *Quotient of Noetherian module is Noetherian*

*Proof.* $M$ is Noetherian and $N \leq M$, then By correspondence, submodules of $M/N$ are in bijective correspondence with submodules of $M$ containing $N$, so if $N' \leq M/N$, then $N'$ corresponds to $\tilde{N} \leq M$ containing $N$, so is generated by finitely many things, then since the quotient map is surjective, $N'$ is generated by finitely many cosets. □

**Proposition 3.19.** *If $R$ is a Noetherian ring, then any finitely generated $R$-module $M$ is Noetherian.*

*Proof.* There is a surjective homomorphism $R^n \to M$, and the result follows from preceding propositions and first isomorphism theorem. □

## 4 Counterexamples

$$F \subsetneq ED \subsetneq PID \subsetneq UFD \subsetneq ID$$

$$PID \implies \text{Noetherian}$$

**Example 1** (ID but not UFD)**.** $\mathbb{Z}[\sqrt{-5}]$. *2 is irreducible but not prime, so "irreducible" does NOT imply "prime", hence* $\mathbb{Z}[\sqrt{-5}]$ *is not a UFD.*

**Example 2** (UFD but not PID)**.** $\mathbb{Z}[X]$. $\mathbb{Z}$ *is UFD so* $\mathbb{Z}[X]$ *is UFD.* $(2, X)$ *is not principal.*

**Example 3** (PID but not ED)**.** *Probably not in the course?? Some ring of integers of field extension should work.*

**Example 4** (ED but not field)**.** $\mathbb{Z}$

**Example 5** (UFD but not Noetherian)**.** *Let $F$ be a field, then $F[X_1, X_2, \ldots]$ is UFD because any polynomial lies in the subring $F[X_{i_1}, \ldots, X_{i_k}]$ and observe that any factorization of $f$ must happen in this subring which is an ED. Not Noetherian because $(X_1, \ldots)$ is not finitely generated.*

**Example 6** (Noetherian but not PID)**.** $\mathbb{Z}[\sqrt{-5}]$. *Not UFD.* $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/(X^2+5)$ *is a quotient ring of a Noetherian ring so* $\mathbb{Z}[\sqrt{-5}]$ *is Noetherian.*

**Example 7.** *$R = \mathbb{Z}$, then $R$ is a PID, but $R[X]$ is not a PID.*

**Example 8.** *Subring of ED/PID/UFD need not be ED/PID/UFD, but subring of ID is ID.*