can find a lin ind one

1. Let V be a 5-dimensional vector space over $\mathbb{C}$ and let $T : V \to V$ be a linear transformation. Assume that there is $v \in V$ such that $\{v, Tv, T^2v, T^3v, T^4v\}$ spans V. Assume that the set of eigenvalues of T is precisely equal to $\{1, 2\}$. On the basis of this information, how many possible Jordan canonical forms are there for T, and what are they? Justify your answer.

are lin ind.

$\boxed{714}$

Kaylee's sol.

JCF is unique.
Find it...

$\{v, Tv, T^2v, T^3v, T^4v\}$ pick so spans + is lin ind.

corresponding matrices I, T, T^2, T^3, T^4 are lin ind
$\Rightarrow$ min poly of T has deg @ least 5

deg ≥ 5

Given: $\dim(V) = 5$ $\Rightarrow$ deg min poly ≤ 5 $\Rightarrow$ $\boxed{\deg = 5}$

char poly of deg 5 LT is 5
min poly divides char poly
$\Rightarrow$ Both have deg 5 + one divides the other
Thus $c_T(x) = m_T(x)$

(*) ✓ (this is an =, BTW)

The JCF of A has one block for every λ Given $\lambda = 1, 2$
Partition 5 into 2 (2 eigenvals)
Block sizes: $\{1,4\}, \{2,3\}, \{3,2\}, \{4,1\}$ for $\{\overset{\lambda_1}{1}, \overset{\lambda_2}{2}\}$

(write out what they look like)

2. Let $G = G_1 \times G_2$ where $G_1 \cong G_2 \cong S_4$, the symmetric group on four letters. Suppose that H is any subgroup of G such that $H \cong S_4$. Show that either $H \cap G_1 = 1$ or $H \cap G_2 = 1$.

Credit: AJ

$G = G_1 \times G_2$
$\quad\;\; \underset{S_4}{\cong} \quad \underset{S_4}{\cong}$

let $H_1 = H \cap G_1$
$H_2 = H \cap G_2$

WTS: (one of H_1 or $H_2 = 1$)

$G_1 \cap G_2 = 1$, so
$H_1 \cap H_2 = (H \cap G_1) \cap (H \cap G_2)$
$= H \cap G_1 \cap G_2 = 1$

Note $H_1, H_2 \trianglelefteq G$

$G_1, G_2 \trianglelefteq G$
by def of direct product

$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$
$G_1 = \{(g_1, 1_{G_2})\}$
$G_2 = \{(1_{G_1}, g_2)\}$
Then
$G_1 \cap G_2 = (1_{G_1}, 1_{G_2})$
$= 1_G$

when projected onto G
↳ like taking the intersection in $\underline{G} = G_1 \times G_2$

* For any $N \trianglelefteq G$, $H \leq G$, $N \cap H \trianglelefteq H$
$\Rightarrow G_1 \cap H = H_1 \trianglelefteq G$
$\Rightarrow G_2 \cap H = H_2 \trianglelefteq G$
$\Rightarrow H_1 \times H_2 \cong H_1 H_2$
since both $\trianglelefteq$ + $\cap = 1$

note: $H_1 H_2 \leq H$

For any $x \in H$, $xH_1H_2x^{-1}$
$= \underbrace{xH_1x^{-1}}_{H_1} \underbrace{xH_2x^{-1}}_{H_2}$ since both $\trianglelefteq$
$= H_1H_2$
Since $xH_1H_2x^{-1} = H_1H_2$ $\forall x \in H$, $H_1H_2 \trianglelefteq H$

$H_1, H_2, H_1H_2 \trianglelefteq H \cong S_4$
Examine normal subgps of S_4
1, S_4, A_4 $V_4 = C_2 \times C_2$
$|S_4| = 24$, $|A_4| = 12$

For $n \geq 5$
only ones are $1, A_n, S_n$

Since $H_1 \cap H_2 = 1$, $|H_1H_2| = |H_1| \cdot |H_2|$
The only option is $24 = 1 \cdot 24$ or $4 = 1 \cdot 4$ or $12 = 1 \cdot 12$
Then one of $H_1, H_2 = 1$ + the other $= S_4$

3. Let S be an integral domain and let $a \in S$. Let R be a subring of S such that $S = R[a]$. Prove or disprove the following:

poly ring in disguise

(a) If R is a principal ideal domain, then S is a principal ideal domain.

(b) If R is noetherian, then S is noetherian.

You may use major theorems in your justification as long as they are specifically mentioned.

$R \subset S$
$\quad \overset{\shortparallel}{R[a]}$

I is an ideal $\Rightarrow a \in I$, $r \in R$ then $ar \in I$

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

a.) R PID $\Rightarrow$ S PID

PID is NOT preserved by poly ring

Let I_R be an ideal of R s.t. $I = (r)$

But note that $I_S = (I_R, a)$ is an ideal of S which is not principal (it has two generators and cannot be written w/ only 1 generator as $a \notin R$)

b.) R Noetherian $\Rightarrow$ S Noetherian

By Hilbert Basis Thm, if R is Noetherian, then so is $R[a] = S$

4. Let $V = \mathbb{R}^2$. Show that the forms x_1x_2 and $2x_1^2 - 2x_2^2$ on V are equivalent.

$\Psi(x_1, x_2) = 2x_1^2 - 2x_2^2$
$\Phi(x_1, x_2) = x_1x_2$

Equivalent Forms:

Ψ & Φ equiv $\iff \exists M \in GL_2(\mathbb{R})$ s.t. $\Psi(x_1, x_2) = \Phi(M\begin{bmatrix} x_1 \\ x_2 \end{bmatrix})$

Find a matrix where it multiplies properly

$$\begin{aligned}
\Psi(x_1, x_2) &= 2x_1^2 - 2x_2^2 && \text{by def.} \\
&= 2(x_1 - x_2)(x_1 + x_2) && \text{factor} \\
&= \Phi(2x_1 - 2x_2, x_1 + x_2) && \text{think} \\
&= \Phi(\underbrace{\begin{bmatrix} 2 & -2 \\ 1 & 1 \end{bmatrix}}_{\in GL_2(\mathbb{R})} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}) && \checkmark
\end{aligned}$$

5. Let R be a commutative ring with 1. Let I and J be ideals in R such that for every $x \in R$ there is $y \in I$ such that $x \equiv y \pmod{J}$. Show that for every $x \in R$ there is $z \in I$ such that $x \equiv z \pmod{J^2}$. (Here J^2 is the ideal generated by all products rs, $r \in J$, $s \in J$.)

AJ'S SOLUTION

Given: $\forall x \in R$, $\exists$ $y \in I$ s.t. $x \equiv y \bmod J$

$\Rightarrow x = y + J$

$\Rightarrow x - y \in J$

$1 \in R$ (duh), so $1 - y \in J$

$x \in R$, so $x - v \in J$ some v (may be not $= y$)

Let $s, t \in J$

$1 - y \in J \Rightarrow 1 - y = s$

$\Rightarrow 1 = y + s$

$x - v \in J \Rightarrow x - v = t$

$\Rightarrow x = v + t$

$$\begin{aligned}
x &= 1 \cdot x \\
&= (y+s)(v+t) \\
&= \underbrace{yv + yt + sv}_{\text{call it } z} + \underbrace{st}_{\in J^2\text{, woohoo!}}
\end{aligned}$$

$z \in I$ since $y, v \in I$ (initial def.)

$= z + st$

$x \equiv z + J^2$ $\checkmark$

1. Prove that the group $\mathbb{Q}$ of rationals under addition is a torsion free abelian group, but is not a free abelian group.

S15

Torsion free ~~gp~~ module = no (nontriv) torsion eles.
Torsion ele = $m \in M$ s.t. $rm = 0$ for $r \neq 0 \in R$ (pg. 344)

Torsion free gp = no nontriv. ele has finite order
Duh! Take $q \in \mathbb{Q}$. $q^n = q + q + \ldots + q = n(q)$
For any n, $nq = 0$ only if n or $q = 0$ (no zero divisors)
$nq \to \pm\infty$ as $n \to \infty$ (further from 0)

NOT free abelian
If gen set S exists, eles must be lin ind (basis)
But lcm always exists

2. Let $\mathbb{Z}[x]$ denote the polynomial ring in the variable x with coefficients in $\mathbb{Z}$.

(a) Let $I \subset \mathbb{Z}[x]$ be the the ideal consisting of all elements whose constant term is 0. Prove that I is a prime ideal of $\mathbb{Z}[x]$ but is not a maximal ideal.

(b) Prove that $\mathbb{Z}[x]$ is not a principal ideal domain.

a.) Prime: $\forall ab \in I$, either a or $b \in I$
Say $p(x) \cdot q(x) \in I$. The multiple $p(x)q(x)$ has no const term (is in I to begin with)
AFSOC neither $p(x), q(x) \in I$. Then both have const terms
$p(x) = a_n x^n + \ldots + a_1 x + a_0$
$q(x) = b_m x^m + \ldots + b_1 x + b_0$
but then $p(x)q(x) = a_n b_m x^{n+m} + \ldots + \underbrace{a_0 b_0}_{\text{const term}}$
so $p(x)q(x) \notin I$ ↯

Not maximal ... find one bigger!
$I \subset (I, 2) \subset \mathbb{Z}[x]$
↳ cont. polys w/o const terms
AND polys w/ const term $a_0 = 2$
clearly $(I, 2) \supset I$
But $(I, 2) \subset \mathbb{Z}[x]$ proper
(e.g. $(x+3) \notin (I, 2)$)

b.) Not PID, find an ideal that is not principal
Ex: $(2, x)$

*Note to self: when you append an ele to R, use that ele in your PID counterexample

3. Prove that a finite group G is the internal direct product of its Sylow subgroups if and only if every Sylow subgroup is normal in G.

Both normal & comaximal

Internal = HK } for $H, K \trianglelefteq G$
External = $H \times K$

($\Leftarrow$) Every Sylow subgp is normal.
Then each is unique ($n_p = 1$)
Then $P_1 \cap P_2 \cap \ldots \cap P_n = 1$.
Recognition Thm: inductively $P_1 P_2 \ldots P_n \cong P_1 \times P_2 \times \ldots \times P_n$ (WTS: $\cong G$)
$|P_1| = p_1^{\alpha_1}$ for some α, then use a counting argument
$|P_1 P_2 \ldots P_n| = |P_1| \cdot |P_2| \cdot \ldots \cdot |P_n| = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = |G|$
Obviously $P_i \subseteq G$ $\forall i \in [1, n]$, so $P_1 \ldots P_n \cong P_1 \times \ldots \times P_n \subseteq G$
Since order equiv, concluding $P_1 \times \ldots \times P_n \cong G$ ✓
($\Rightarrow$) Assume $G \cong P_1 P_2 \ldots P_n$
WTS: all P_i normal by kernel of homo
Try $\phi : G/P_i \ldots$
Internal direct product $\Rightarrow$ trivial intersection

(would make more sense for the problem to ask about external direct products, although that version is still somewhat trivial in one direction)

Internal direct product $\Rightarrow$ each P_i must be normal, else the internal direct product isn't defined $\Rightarrow$ Hence each $P_i \trianglelefteq G$ $\forall i \in [1, n]$

4. Recall that the group $GL_2(\mathbb{R})$ acts on $\mathbb{R}^2$ by the usual matrix-vector multiplication $A \cdot v = Av$, where $A \in GL_2(\mathbb{R})$ and v is a column vector in $\mathbb{R}^2$.
(a) Determine the number of orbits for this action, and describe each orbit.
(b) Find the pointwise stabilizer of the set $\{(x, y) \in \mathbb{R}^2 \mid y = x,\ x \neq 0\}$.

Burnside's Lemma:
$\# \text{orb of } G = \frac{1}{|G|} \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}|$ ↳ finite
Keep in mind, but not for this problem

$A \in GL_2(\mathbb{R})$, $A \cdot v = Av$
a.) $\text{Orb}(v) = \{A \cdot v = Av \mid A \in GL_2(\mathbb{R})\}$
Orb-Stab Thm: $|\text{Orb}(x)| = [G : \text{Stab}(x)] = \frac{|G|}{|\text{Stab}(x)|}$ $\Rightarrow$ $|\text{Orb}(x)| \cdot |\text{Stab}(x)| = |G|$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$

Hypothesis: 2 orbits
$\{\begin{bmatrix} 0 \\ 0 \end{bmatrix}\}$ + $\{\begin{bmatrix} x \\ y \end{bmatrix} \mid \text{at least 1 of } x \text{ or } y \neq 0\}$
$A_1 \cdot v_1 = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$
$A_2 \cdot v_2 = \begin{bmatrix} ex + fy \\ gx + hy \end{bmatrix}$ } could be equivalent
But also, any $A \cdot \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$
and $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ ✓ } another orbit

and in fact you can get from $\begin{bmatrix} x \\ y \end{bmatrix}$ to any $\begin{bmatrix} u \\ v \end{bmatrix} \in \mathbb{R}^2$
$\begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} \overset{?}{=} \begin{bmatrix} u \\ v \end{bmatrix}$
$x, y \neq 0$, let $a = \frac{u}{x}$, $b = 0$, $c = 0$, $d = \frac{v}{y}$
WLOG $x = 0$, then $b = \frac{u}{y}$, $d = \frac{v}{y}$ etc.

b.) $\{(x, y) \mid y = x,\ x \neq 0\} = \{\begin{bmatrix} x \\ x \end{bmatrix} \mid x \neq 0\}$
$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ x \end{bmatrix} = \begin{bmatrix} (a+b)x \\ (c+d)x \end{bmatrix}$ when is this $= \begin{bmatrix} x \\ x \end{bmatrix}$?
when $a + b = c + d = 1$
So $\text{Stab} = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a + b = c + d = 1\}$ ✓

5. Let $\rho : G \to GL_3(\mathbb{C})$ be a homomorphism, where G is the cyclic group of order 3. Show that with respect to some basis of $\mathbb{C}^3$, every element of $\rho(G)$ is a diagonal matrix having cube roots of unity on its diagonal.

clearly matrices of this form have order 3, so check that all matrices of order 3 look like this

G is cyclic of order 3, so any $x \in G$ has $x^3 = 1$
Since ρ is homo, $\rho(x)$ also has order 3 $\rho(x)^3 = 1$

$\rho(x) = A \Rightarrow A^3 = 1 \Rightarrow A^3 - 1 = 0$ $\omega = \zeta_3$
$(x - \omega^0)(x - \omega^1)(x - \omega^2)$ 3rd roots
$(x - 1)(x - \omega)(x - \omega^2)$

RECALL $m(x) = C(x)$ MIGHT HAPPEN

$J = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$ $J^3 = \begin{bmatrix} 1^3 & 0 & 0 \\ 0 & \omega^3 & 0 \\ 0 & 0 & \omega^6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$ ✓
$A = PJP^{-1}$
$A^3 = P^3 J^3 (P^{-1})^3 = P^3 (I) (P^{-1})^3 = (PP^{-1})^3 = I$ ✓

Great! all matrices of order 3 look like this, so double contain. is satisfied!

1. Let $\mathbb{F}$ be a finite field of order q, with q odd. Show that the following are equivalent:

(a) the equation $x^2 = -1$ has a solution in $\mathbb{F}$

(b) $q \equiv 1 \pmod 4$.

Hint: work with the multiplicative group $\mathbb{F}^\times$ of nonzero elements in $\mathbb{F}$.

715

technically, $q = p^k$
only works for q prime

$q=5$ $x^2 = 9 = -1 \bmod 5$
$q=9$ $x^2 = \quad = -1 \bmod 9$
8 17 26 35 44 53 62 71

(a) ⇒ (b) $x^2 = -1$ for some $x \in \mathbb{F}$
$|\mathbb{F}| = q \Rightarrow q = 0 \Rightarrow q-1 = -1$
Then $x^2 = q-1$ $\quad$ q odd
x odd $\Rightarrow x^2$ odd $\quad$ $x^2+1 = q$
odd + odd = odd? X

x even $\Rightarrow x^2$ even $\quad$ $x^2+1 = q$
$x = 2n$ $\quad$ $(2n)^2+1 = q$
$n \in \mathbb{Z}$ $\quad$ $4n^2+1 = q$ $\quad$ $(4n^2+1) \bmod 4 = 1$
$\Rightarrow q \equiv 1 \bmod 4$

NOT on the syllabus!

I guess you can use Fermat?
$a^{q-1} \equiv 1 \bmod q$ $\quad$ q prime, $\forall a \in \mathbb{F}_q^\times$
$q = 4n+1$
$a^{4n} \equiv 1 \bmod q$
$a^{4n} = 1$
$(a^{2n})^2 = 1 \Rightarrow a^{2n} = \pm 1$
$\Rightarrow (a^n)^2 = -1$

(b) ⇒ (a) $q \equiv 1 \bmod 4 \Rightarrow q = 4n+1$
$-1 = q-1$ $\quad$ n fixed, m flexible
$= (4n+1)-1$
$= 4n$ $\quad$ requires n perfect square
luckily $\underbrace{4n+1}_{4m^2+1}$ is odd + prime

$x = 2\sqrt{n}$ works

2. Recall that the *algebraic multiplicity* of an eigenvalue of a square matrix is defined as its multiplicity as a root of the characteristic polynomial of that matrix. If A is a square matrix with complex entries, let $\exp(A)$ denote the exponential of A, defined as the power series

$$\exp(A) = \sum_{n=0}^{\infty} \frac{1}{n!} A^n = I + A + \frac{1}{2}A^2 + \cdots .$$

Assume all eigenvalues of A are real. If λ is an eigenvalue for A with algebraic multiplicity μ, show that e^λ is an eigenvalue for $\exp(A)$, and has the same algebraic multiplicity μ.

$C_A(x) = (x-\lambda)^\mu \times \ldots$ other linear factors
$C_A(A) = 0$
Eigenvalue: $A\vec{v} = \lambda\vec{v}$ $\quad$ eigenvector $\vec{v}$
To show e^λ is eigenvalue of $\exp(A)$, $\exp(A)\vec{u} = e^\lambda\vec{u}$ for some $\vec{u}$
$\exp(A)\vec{v} = \sum_{n=0}^{\infty} \frac{1}{n!} A^n \vec{v}$ $\quad$ choose same $\vec{v}$
$= \sum_{n=0}^{\infty} \frac{1}{n!} A^{n-1}(\lambda\vec{v})$
$\vdots$
$= \sum_{n=0}^{\infty} \frac{1}{n!} \lambda^n \vec{v}$
$= \exp(\lambda)\vec{v}$
$\exp(A)\vec{v} = e^\lambda\vec{v}$ ✓ $\quad$ e^λ is eigenvalue ✓

$A = PJP^{-1}$ + the eigenvalues generate Jordan blocks (w/ multiplicity!)
Then J_A has μ blocks w/ λ $\quad$ WTS: same for $J_{\exp(A)}$
$A \sim J$ (similar iff same JCF) (trivial)
J is upper tri + λ on diagonals
$\exp(J) = \sum_{n=0}^{\infty} \frac{1}{n!} J^n$ $\quad$ still upper Δ, + diags are $\lambda^n = e^\lambda$
$\exp(J) = \begin{bmatrix} e^\lambda & & \\ & \ddots & \\ & & e^\lambda \end{bmatrix}$ mult of λ is preserved by J^n
so e^λ has same mult
+ since $A \sim J$, same is true for $\exp(A)$

3. Let G be the group $\mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}$ and $\mathbb{Z}$ are viewed as groups under addition. Prove the following.

(a) Every element of G has finite order.

(b) Every finitely generated subgroup of G is cyclic. → $H \leq G$ w/ gen set S $(|S| = n)$
$\exists h_0 \in H$ s.t. $h = h_0^k \ \forall h \in H$
$= k \cdot h_0$

$G = \mathbb{Q}/\mathbb{Z} = \{ p/q \mid p \in \mathbb{Z}, q \neq 1, np \text{ for } n \in \mathbb{Z} \}$
every $z \in \mathbb{Z} = 0$
Then $(p/q)^q = p/q + p/q + \ldots + p/q = q(p/q) = \underbrace{p}_{\in \mathbb{Z}} = 0$
So $p/q \in \mathbb{Q}/\mathbb{Z}$ has order $\underbrace{q}_{< \infty}$, otherwise $p/\infty = 0$, which has order 0

Let S be the finite generating set of $H \leq G$ $\qquad H = \langle S \rangle$
$S = \{ p_1/q_1, p_2/q_2, \ldots, p_n/q_n \}$
any $h \in H$ takes the form $c_1 \frac{p_1}{q_1} + c_2 \frac{p_2}{q_2} + \ldots + c_n \frac{p_n}{q_n}$ w/ $c_i \in \mathbb{N} \ \forall i \in [1, n]$
$h = c_1 \frac{p_1}{q_1} + \ldots + c_n \frac{p_n}{q_n}$
$h(q_1 \cdot \ldots \cdot q_n) = c_1 p_1 (q_2 \ldots q_n) + \ldots + c_n p_n (p_1 \cdot \ldots p_{n-1})$
$h = \underbrace{\frac{1}{(q_1 \cdot \ldots \cdot q_n)}}_{= h_0} \cdot \underbrace{\left[\sum_{i=1}^{n} c_i p_i \prod_{j \neq i} q_j \right]}_{\in \mathbb{Z} \text{ since } c_i, p_i, q_j \in \mathbb{Z}}$
$h = h_0 \cdot \underbrace{n}_{\in \mathbb{Z}}$
So $H = \langle h_0 \rangle$ as any $h \in H$ can be written as $n \cdot h_0$ for a fixed ele h_0
Note: h_0 is det by S (fixed for H)

4. Let G be a group of order $2015 = 5 \cdot 13 \cdot 31$.

(a) Prove the existence of normal subgroups of G of orders 13, 31, and 155.
Hint: establish the existence of those subgroups in that order.

(b) Show that G is isomorphic to the direct product of a group of order 13 with a group of order 155. $\qquad 31 \times 5 = 155$

By Sylow Thms, $Syl_5, Syl_{13}, Syl_{31} \neq \emptyset$
When there is a unique Sylow p-subgp, it is normal in G

~~$\exists P_5 \in Syl_5$ $\quad n_5 \equiv 1 \bmod 5$ & $n_5 \mid 13 \times 31 \Rightarrow n_5 = 1$ or 31~~
~~$1, 6, 11, 16, \ldots, 31$ $\quad 403$~~

$\exists P_{13} \in Syl_{13}$ $\quad n_{13} \equiv 1 \bmod 13$ & $n_{13} \mid \underbrace{5 \times 31}_{155} \Rightarrow n_{13} = 1$ $\quad$ unique $\Rightarrow$ normal
$1, 14, 27, 40, 53, \ldots$
not 5 or 31, which are the only #s that divide 155 since both are prime

$\exists P_{31} \in Syl_{31}$ $\quad n_{31} \equiv 1 \bmod 31$ & $n_{31} \mid \underbrace{5 \times 13}_{65} \Rightarrow n_{31} = 1$ $\quad$ unique $\Rightarrow$ normal
$1, 32, 63, \ldots$
not 5 or 13, //

$\exists P_5 \in Syl_5$ by Sylow.
$P_5 P_{31}$ has order $5 \cdot 31 = 155$ $\qquad P_5 P_{31} = H$
Thus $\exists$ subgp of order 155
Since $P_{13} \trianglelefteq G$, $P_{13}(P_5 P_{31})$ has order $13 \cdot 5 \cdot 31 = 2015$ so $G = P_{13}(P_5 P_{31})$
$P_{13} = N \trianglelefteq G$, $P_5 P_{31} = H \leq G$
Then $G = N \rtimes_\varphi H = P_{13} \rtimes_\varphi P_5 P_{31}$
$\varphi : H \to \mathrm{Aut}(N)$
$P_5 P_{31} \to \mathrm{Aut}(P_{13})$
↳ permute 12 nontrivial eles of P_{13}
$|P_5 P_{31}| = 155 = 5 \cdot 31$
$|\mathrm{Aut}(P_{13})| = 12$ $\quad$ rel. prime, so φ must be trivial homo.
↳ $= 2 \cdot 2 \cdot 3$ $\qquad$ Then $N \rtimes H = N \times H = P_{13} \times P_5 P_{31}$
and this is normal ?

5. Let $\zeta = \frac{1+\sqrt{-3}}{2}$, and R denote the subring $\mathbb{Z}[\zeta]$ of $\mathbb{C}$.

(a) Show that $R = \mathbb{Z} + \zeta \cdot \mathbb{Z}$.

(b) For $a \in R$, show that $|a|^2 = a\bar{a}$ is an integer, where $\bar{a}$ is the complex conjugate.

(c) For $a \in \mathbb{C}$ show that there are $q \in R$, and $r \in \mathbb{C}$, with

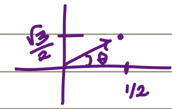
$$a = q + r \text{ and } |r| < 1$$

(d) (Division Algorithm)
Show that for $a, b \in R$ with $b \neq 0$ there are $q, r \in R$ with

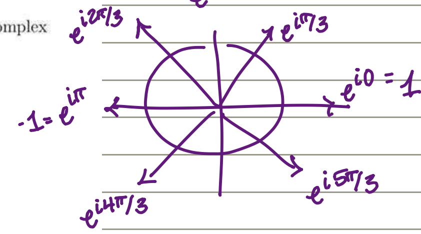
$$a = bq + r \text{ and } |r| < |b|$$

(e) Show that R is a principal ideal domain.

$\zeta = \frac{1+\sqrt{-3}}{2} = \frac{1+\sqrt{3}i}{2}$
$= e^{i\pi/3}$



$\theta = \pi/3$



$e^{i\pi/3} = \frac{1+\sqrt{-3}}{2}$
$e^{i2\pi/3} = \frac{-1+\sqrt{-3}}{2} = \frac{1+\sqrt{-3}}{2} - 1$
$e^{i4\pi/3} = \frac{-1-\sqrt{-3}}{2} = -\frac{1+\sqrt{-3}}{2}$
$e^{i5\pi/3} = -\left(\frac{1+\sqrt{-3}}{2} - 1\right)$

a.) $R = \mathbb{Z}[\zeta] = \{\sum_{i=1}^{n} c_i \zeta^i \mid c_i \in \mathbb{Z}\}$

$\zeta^1 = \zeta \qquad \zeta^4 = -\zeta$
$\zeta^2 = \zeta - 1 \qquad \zeta^5 = -\zeta + 1$
$\zeta^3 = -1 \qquad \zeta^6 = 1$
$\zeta^k = \zeta^{k \bmod 6}$

can be written as a deg 1 poly
$\rightarrow$ Then whole poly consists of lin. combos of deg 1 polys (= 1 deg 1 poly in $\mathbb{Z}[\zeta]$)

Then the degree k term of any poly in $\mathbb{Z}[\zeta]$ can be written as $\underset{\in\mathbb{Z}}{c_k}(\zeta^k) = c_k(\pm 1 \cdot \zeta \pm 1) = c_k(a_k\zeta + b_k) = d_k\zeta + b_k = \mathbb{Z}\cdot\zeta + \mathbb{Z}$
$a_k, b_k, c_k \in \mathbb{Z}$

b.) $a \in R = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\cdot\zeta$

WTS: $|a|^2 = a\bar{a} \in \mathbb{Z}$

If $a \in \mathbb{Z}$, then $\bar{a} = a$ so $a\bar{a} = a^2 \in \mathbb{Z}$

If $a = \zeta$, then $\bar{a} = \zeta^5 = -\zeta + 1$, so $a\bar{a} = \left(\frac{1+\overset{+i\sqrt{3}}{\sqrt{-3}}}{2}\right)\left(\frac{1-\overset{-i\sqrt{3}}{\sqrt{-3}}}{2}\right) = \frac{1}{4}(1-(-3)) = \frac{4}{4} = 1 \in \mathbb{Z}$

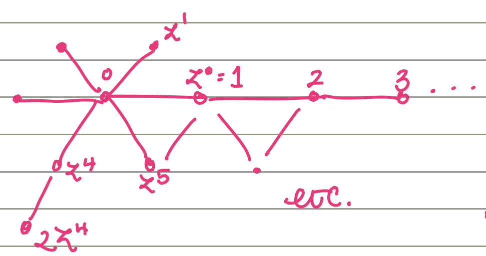
If $a = \mathbb{Z} + \mathbb{Z}\cdot\zeta = x + y\zeta = x + y\left(\frac{1+\sqrt{-3}}{2}\right) = x + \frac{y}{2} + \frac{y}{2}i\sqrt{3}$

$a\bar{a} = \left[(x+\frac{y}{2}) + i\left(\frac{y\sqrt{3}}{2}\right)\right]\left[(x+\frac{y}{2}) - i\left(\frac{y\sqrt{3}}{2}\right)\right] = (x+\frac{y}{2})^2 + \left(\frac{y\sqrt{3}}{2}\right)^2 = x^2 + \frac{y^2}{4} + \frac{3y^2}{4} = x^2 + \frac{4y^2}{4} = x^2 + y^2 \in \mathbb{Z}$ ✓

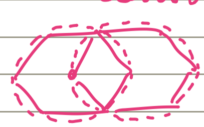
c.) $a \in \mathbb{C} \Rightarrow \exists\, q \in R, r \in \mathbb{C}$ w/ $a = q + r$ & $|r| < 1$
$R = \mathbb{Z}[\zeta]$ $\quad$ $\hookrightarrow \leq$?

$a = se^{i\theta} \qquad q = x + ye^{i\pi/3} \qquad x, y \in \mathbb{Z}$

Elements in R form a hexagonal lattice



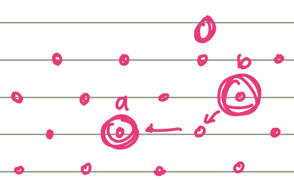
Each vertex of hexagon is dist 1 from center, & hexagons overlap.
Construct disk of radius 1 containing each hexagon.



any $a \in \mathbb{C}$ is inside at least 1 disk, so can be reached by vertex of hexagon + some vector w/ $|v| < 1$

d.) $a = bq + r$ $\quad$ for any $a, b \in R$
find $q, r \in R$ $\quad$ $|r| < |b|$

By part (a),
$b = a + b\omega \qquad b \cdot q = (a + b\omega)(c + d\omega)$
$q = c + d\omega \qquad = ac + (bc + ad)\omega + bd\omega^2$



FINISH THIS

$\boxed{S16}$

1. Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients, and assume that $P(0)$ and $P(1)$ are odd integers. Prove that $P(x)$ has no integer roots.

$P(x) = a_n x^n + \ldots + a_1 x + a_0$
$P(0) = a_0$
$P(1) = a_n + \ldots + a_1 + a_0$ } both odd
$\Rightarrow a_n + \ldots + a_1 = \text{even}$

If $r/s \in \mathbb{Q}$ is a root of a poly in $\mathbb{Z}[x]$ (r, s rel prime)
then $r | a_0$ & $s | a_n$
↳ r is odd

$P(r) = 0 = a_n r^n + \ldots + a_1 r + \underbrace{a_0}_{\text{odd}}$

all powers of r odd
even · odd = even
odd · odd = odd

$a_1 + \ldots + a_n = \text{even}$
must have an even # of odds
odd coeffs:
odd · odd = odd } even # of these, so sum to even
even coeffs:
even · odd = even

So $a_n r^n + \ldots + a_1 r = \text{even}$ no matter what
$0 = (\text{even}) + \underbrace{a_0}_{\text{odd}}$ cannot happen!

2. Let M denote the additive group $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$ and let $\mathrm{End}(M)$ denote the set of homomorphisms $\phi : M \to M$. Show that $\mathrm{End}(M)$ is infinite and noncommutative.

auto → iso
homo → endo

$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ Two copies of $\mathbb{Z}$

$\varphi((x,1)) = (nx, 1)$
$\varphi((x,1)+(y,1)) = \varphi((x+y, 0))$
$= (n(x+y), 0)$
$\varphi((x,1)) + \varphi((y,1)) = (nx, 1) + (ny, 1)$
$= (nx+ny, 0)$ ✓

can pick any n & produce a homo.
all of these maps are homos (but may not include all homos!)
However, at least ∞ many! ✓
$\Rightarrow$ End(M) is infinite ✓

Find φ, ψ which don't commute
i.e. $\psi(\varphi(m)) \neq \varphi(\psi(m))$
for some $m \in M$
↳ recall relation is composition

Try: $\varphi(x, 1) = (x \bmod 2, 1)$
$\psi(x, 1) = (2x, 1)$

$\psi(\varphi(\overset{2n+1}{x}, 1)) = \psi(1, 1) = (2, 1)$
$\varphi(\psi(x, 1)) = \varphi(\underset{2(2n+1) = 2n+2}{2x}, 1) = (0, 1)$ } $\neq$

Then End(M) is also noncommutative ✓

3. Let $A \in M_n(\mathbb{C})$ be a matrix such that $A^k = A$ for some integer $k \geq 2$. Prove that A is diagonalizable.

Note: A has $\lambda_1^{m_1}, \lambda_2^{m_2}, \dots, \lambda_n^{m_n}$
Then A^k has $\lambda_1^{m_1+k}, \dots, \lambda_n^{m_n+k}$
↳ see from J^k

A is $n \times n$, entries in $\mathbb{C}$
$A^k = A$ for some $k \geq 2$

$A = PJP^{-1}$ (Jordan form)
$A^k = (PJP^{-1})^k = PJ^kP^{-1}$
$A^k = A \Rightarrow PJP^{-1} = PJ^kP^{-1}$
$\Rightarrow J = J^k$
Then $J = J^k$ requires that J is diagonal

$$J^k = \begin{bmatrix} \lambda_1 & 1 & & \\ & \lambda_2 & 1 & \\ & & \ddots & 1 \\ & & & \lambda_n \end{bmatrix}^k = \begin{bmatrix} \lambda_1^k & k\lambda & \dots & \\ & & \ddots & k\lambda \\ & & & \lambda_n^k \end{bmatrix}$$

So for $J^k = J$, need λ's to be 1's (or roots of unity)

Remark: $c_A(x) \in \mathbb{C}[x]$
By Fund. Thm. of Algebra, $c_A(x)$ splits into linear factors

Linear factors $\Rightarrow$ Jordan blocks of size 1
$\Rightarrow J$ is diagonal

But FTA doesn't guarantee linear factors w/ multiplicity 1

So: $A^k = A \Rightarrow A^k - A = 0$
$A(A^{k-1} - 1) = 0$
A is a root of $p(x) = x(x^{k-1} - 1)$ w/ $p(x) \in \mathbb{C}[x]$
$p(x)$ has roots 0 + the $k-1$th roots of unity, hence has k distinct roots ...

4. Let F be a field whose multiplicative group F^* is cyclic. Prove that F is finite.

$F^\times$ is cyclic $\Rightarrow F^\times = \langle g \rangle$
so every $h \in F^\times$ has $h = g^k = g \times \dots \times g$ for some $k \geq 0$

F field, so every $h \in F^\times$ has mult inverse h^{-1}
$h^{-1} = g^j$ for some $j \geq 0$
$1 = h \cdot h^{-1} = g^k g^j = g^{k+j}$
Since generator has finite order $k+j$

5. Let G be a group of order 108. Prove that G is not simple.

$108 = 4 \cdot 27 = 2 \cdot 2 \cdot 27$
Not simple $= \exists N \trianglelefteq G$
$P \in Syl_p(G)$ has $P \trianglelefteq G$ if $n_p = 1$

$|P_2| = 4$
$\exists\ P_2 \in Syl_2$ + $P_{27} \in Syl_{27}$
$n_{27} \equiv 1 \bmod 27$ + $n_{27} | 4$ → only possibility is $n_{27} = 1$,
↳ $n_{27} = 1, 2, 4$

Dept sols available

$\boxed{716}$

1. Let G be an abelian group and for each positive integer n, define

$$G[n] = \{g \in G \mid ng = 0\}.$$

(a) Show that if m and n are positive integers and m divides n, then $G[m] \subseteq G[n]$ and $G[n]/G[m]$ is isomorphic to a subgroup of $G[n/m]$.
(b) Give an example in which m divides n but $G[n]/G[m] \not\cong G[n/m]$. Prove your assertion.

a) $G[n] = \{g \in G \mid ng = 0\}$ $\quad m|n$
$G[m] = \{g \in G \mid mg = 0\}$

Take $g \in G[m]$. $\Rightarrow mg = 0$. $m|n$, so $mg = (kn)g = 0$
$\Rightarrow ng = 0$
$\Rightarrow g \in G[n]$

$G[n]/G[m] \Rightarrow \{g \in G \mid mg = 0\} \mapsto 0$
keep only $\{g \in G \mid ng = 0, \ldots$
$G[n/m] = \{g \in G \mid (n/m) g = 0\}$

want to use 1st Iso Thm: $G/\ker \cong \mathrm{Im}$
Define map $\varphi : G[n] \to ???$ so $\ker = G[m]$
$\mathrm{Im} = G[n/m]$

$\ker = G[m] \Rightarrow$ make $\varphi(g) = mg$
$\varphi(g) + \varphi(h) = mg + mh = m(g+h) = \varphi(g+h)$ homo ✓
$\mathrm{Im}(\varphi) = ?$
$\forall g \in G[n]$, $\varphi(g) = mg$
$k\varphi(g) = kmg = ng = 0$ $\Big\}$ Then for $h \in \mathrm{Im}(\varphi)$, $kh = 0$, so $h \in G[k]$ $\Rightarrow \mathrm{Im}(\varphi) \leq G[k] = G[m/n]$

First Iso Thm: $G[n]/G[m] \cong \underbrace{H}_{\mathrm{Im}(\varphi)} \leq G[m/n]$ ✓

b.) Example where $m|n$ but $G[n]/G[m] \cong G[n/m]$
want things to be "annihilated" by k that aren't by m
$n = m \cdot k$

Dept Sol: $m = p^2$, $n = p^3$ p prime
$G[n] = G = G[m]$ so $G[n]/G[m] = 0$
$|G[n/m]| = |G[p]| = p$

2. Let T be a square matrix over $\mathbb{C}$. $\to T^{-1}$ exists
(a) Show that if T is invertible and T^k is diagonalizable for some positive integer k, then T is diagonalizable.
(b) Show that the invertibility hypothesis cannot be omitted in (a).

*Note that diag $\not\Leftarrow$ linear factors, only that J-blocks are diag-able

Diagonalizable $\Leftarrow$
$T = PDP^{-1} \Leftarrow J = D$
$\Leftarrow$ every J-block size 1
$\Leftarrow C_T(x)$ all linear factors

$T = PDP^{-1}$
$T^k = PD^kP^{-1}$
$\hookrightarrow$ still diag.

T has $\lambda_1^{m_1}, \ldots, \lambda_n^{m_n}$
T^k has $\lambda_1^{m_1+k}, \ldots, \lambda_n^{m_n+k}$

3. Let I be an ideal in a principal ideal domain R. Show that if $I \neq R$, then

$$\bigcap_{n=1}^{\infty} I^n = (0).$$

(Here I^n is the ideal generated by all products $x_1 \cdots x_n$ such that $x_i \in I$ for all $i = 1, \ldots, n$.)

All PIDs are Noetherian

PID $\Rightarrow$ Noetherian
$\Rightarrow$ every ideal is fin gen

$I = (a)$ for $a \in R$. Given $I \neq R$.
$I^n = \{x_1 \ldots x_n \mid x_i \in I \ \forall i \in [1,n]\}$
Note that $I^n = (a^n)$ this is just true

If $I = (0)$, trivially true
AFSOC $\bigcap_{n=1}^{\infty} I^n \neq (0)$
Intersection of ideals must be an ideal, + all ideals gen by a single ele.
Then $\bigcap_{n=1}^{\infty} I^n = (b)$ for $b \neq 0$.
Then $\forall n$, $b = a^n r_n$ for some $r_n \in R$
$\Rightarrow a^1 r_1 = a^2 r_2 = \ldots = a^n r_n = a^{n+1} r_{n+1} = \ldots$
$\Rightarrow r_n = a r_{n+1}$

$I \neq R$, so a cannot be a unit (else $aa^{-1} = 1 \in I$, so $1r = r \in I$ $\forall r \in R$)
Then $(r_n) \subsetneq (r_{n+1})$ $\forall n$, +
$(r_1) \subsetneq (r_2) \subsetneq \ldots \subsetneq (r_n) \subsetneq (r_{n+1}) \subsetneq \ldots$
is an inf. chain of ascending ideals. Cannot happen since R is Noetherian $\lightning$

4. Let B be a nondegenerate symmetric bilinear form on a 2-dimensional vector space V over the finite field F_p of p elements, where p is prime. Assume that $p \neq 2$. Show that there is always a vector $v \in V$ such that $B(v, v) = 1$.

2-dim v.s. over F_p $\Rightarrow$ basis $\{e_1, e_2\}$ where e_1, e_2 have entries in F_p
$\hookrightarrow$ orthogonal: $B(e_1, e_2) = 0$

symmetric bilinear form:
- $B(u,v) = B(v,u)$
- $B(u+v, w) = B(u,w) + B(v,w)$
- $B(\lambda v, w) = \lambda B(v,w)$

Nondegenerate bilinear:
$B(u,v) = 0 \ \forall v \Rightarrow x = 0$
(no nonzero u exists like this)

Nondegenerate $\Rightarrow B(e_1, e_1) \neq 0$
$B(e_2, e_2) \neq 0$
($e_1, e_2 \neq 0$ since basis elements)

* B is a v.s. over F_p, so $B(u,v) \in F_p$
WTS: $B(v,v) = 1$, aka some ele v "squared" under B gives id.

FINISH THIS!

5. Let G be a finite group acting transitively on a set Ω and suppose that $|\Omega| = p^m$ for some prime p and positive integer m. Let P be a Sylow p-subgroup of G (for the same prime p). Prove: P acts transitively on Ω.

transitive = one orbit

$|\Omega| = p^m$ $\quad |P| = p^n$ same p

$p \mid |G| \rightsquigarrow |G| = p^n \cdot \ell$ since P is Sylow p-subgp of G

<u>Group action:</u> $G \times A \to A$

$1 \cdot a = a$

$g_1 \cdot (g_2 \cdot a) = (g_1 \cdot g_2) \cdot a$

orbit-stabilizer: $|Orb_G| \cdot |Stab_G| = |G|$

Transitive, so $|Orb_G| = |\Omega| = p^m$ and then $|Stab_G| = p^{n-m}\ell$

↳ recall action maps Ω to itself, so 1 orbit $\Rightarrow |orb| = |\Omega|$

also have $|Orb_P| \cdot |Stab_P| = |P| = p^n$

$Stab_P = \{ w \in \Omega \mid p \cdot w = 1 \ \forall p \in P \}$ → lagrange!

* $Stab_P = P \cap Stab_G$ and $Stab_P \leq P$

FINISH THIS LATER

$\boxed{S17}$

1. Prove that any complex square matrix A is similar to its transpose matrix.

$\Leftrightarrow$ same JCF

$A = PJP^{-1}$ $\quad J = \begin{bmatrix} J_{\lambda_1,k_1} & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_n,k_n} \end{bmatrix}$ $\quad$ let $B = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}$

$\hookrightarrow$ eigenval λ_i has mult k_i

$\hookrightarrow$ invertible

<u>claim</u>: Each Jordan block is similar to its transpose $J_{\lambda_i,k_i} \sim J_{\lambda_i,k_i}^T$

$$B J_{\lambda_i,k_i} B^{-1} = (BJ)B^{-1} = \begin{bmatrix} 0 & & 1 & \lambda_i \\ & \iddots & \lambda_i & \\ 1 & \iddots & & \\ \lambda_i & & & 0 \end{bmatrix} B^{-1} = \begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix} = J_{\lambda_i,k_i}^T$$

$A = PJP^{-1}$

$A^T = (PJP^{-1})^T = (P^{-1})^T J^T P^T$ $\quad$ so $A^T = Q^{-1} J^T Q$

$= Q^{-1} J^T Q$

$A^T = Q^{-1}(BJB^{-1})Q$

$= Q^{-1}B(P^{-1}AP)B^{-1}Q$

$= R^{-1}AR$ $\quad$ $R = PB^{-1}Q$

$\Rightarrow A^T \sim A$ $\quad$ $\Rightarrow R^{-1} = Q^{-1}BP^{-1}$ ✓

2. Prove that if the ring of polynomials $R[x]$ over a commutative domain R with identity is a principal ideal ring then R is a field.

chapter 8 corollary 8. D&F

<u>WTS</u>:

$R[x]$ PID $\Rightarrow$ R a field

Recall if $R[x]$ a PID, then $R[x]/M$ (for M a max ideal) is a field

(x) is a max ideal in $R[x]$, so $R[x]/(x)$ is a field.

$R[x]/(x) = R$, so R a field ✓

$\hookrightarrow$ prime $\Leftrightarrow$ max in PID

$R[x]/(x) \cong R$ an ID, so (x) <u>prime</u>

3. Prove that there are no simple groups of order 18.

$|G| = 18 = 2 \times 3^2$

By Sylow Thms, $\exists P \in Syl_3(G)$ s.t. $|P| = 3^2$

by Sylow again,

$n_3 \equiv 1 \mod 3$ & $n_3 \mid 2$ $\Rightarrow$ $n_3 = 1$

since $\exists! P \in Syl_3(G)$, $P \trianglelefteq G$. Then G is not simple as $\exists$ a nontrivial normal subgp.

4. Prove that the groups D_6 and A_4 are not isomorphic. (*Here, D_6 is the symmetry group of the hexagon and A_4 is the alternating group of even permutations on 4 letters.*)

$D_6 : \langle r^6 = s^2 = 1 \rangle$

D_6:
r^3, s, sr^3 have order 2
r^2, r^4 have order 3
$r, r^5, sr^n \; \forall n \in [1,5]$ have order 6

Orders of eles don't match up, so can't be isomorphic!

A_4 : even perms of A_4 (even # transpositions)
Transposition pairs have order 2
There are 3 of these: $(12)(34)$
$(13)(24)$
$(14)(23)$
Three cycles have order 3
There are 8 of these: $(123)(132)$
$(124)(142)$
$(134)(143)$
$(234)(243)$

5. Let p be prime and let G be a p-group. Let X be a finite set with $|X|$ not divisible by p. Suppose that G ~~acts on~~ X. Prove that there exists $x \in X$ with orbit $G \cdot x = \{x\}$, that is, the action of G on X must have at least one fixed point.

$\rightarrow |G| = p^n$

$\rightarrow |X| = m$

WTS: $\mathrm{Stab}(x) = G$

$|\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)| = |G| = p^n$

$\Rightarrow$ Both orb + stab have prime power order (true for any O/S)

Recall orbits are equivalence classes, so they partition the set

$|X| = m = \Sigma p^{k_j} \qquad k < n$

$m = p^{k_1} + p^{k_2} + \ldots + p^{k_j} = p^{k_i}(p^{k_1 - k_i} + \ldots + p^{k_j}) \qquad k_i = \max\{k_j\}$

m is NOT divisible by p ↯

Then one of p^{k_i} must be $= 1$ $(k_i = 0)$
So $\exists$ x w/ orb of size 1
$1 \cdot x = x$ always, so $G \cdot x = \{x\}$ ✓

1. Let G be a group and let $H \subset G$ be a proper subgroup containing all other proper subgroups of G. Show the following:
a) H is normal.
b) G is a cyclic group.
c) G is a finite group.

$\boxed{F17}$

a.) $H \subset G$ proper subgp. Normal if $gHg^{-1} = H \quad \forall g \in G$
Take $g \in G \setminus H$.
i.) If $G \setminus H = \{g\}$, then
$gHg^{-1} = G$
$gH = Gg = G$
$H = g^{-1}G = G \qquad H = G$ (H not proper ↯)
ii.) $G \setminus H \neq \{g\}$ Then
$gHg^{-1} \leq G$ (not hard to show. True since $H \leq G$)
Since $\exists g' \in G \setminus H$, $gHg^{-1} \subset G$ (is proper)
Then since H contains all proper subgps, $gHg^{-1} \subset H$
$\Rightarrow gH \subset Hg$
$\Rightarrow H \subset g^{-1}Hg \quad \Rightarrow H = gHg^{-1}$ for $g \in G \setminus H$
obviously $gHg^{-1} = H$ when $g \in H$, so $gHg^{-1} = H \quad \forall g \in G$, & $H \trianglelefteq G$ ✓

b.) Let $g \in G \setminus H$. Then $\langle g \rangle \not\subseteq H$. But $\langle g \rangle$ is a subgp, so the only way for $\langle g \rangle \not\subseteq H$ is if $\langle g \rangle$ is not proper, i.e. $G = \langle g \rangle$. Then G is cyclic.

c.) AFSOC $|G| = \infty$. From part (b), we know $G = \langle g \rangle$. Consider subgp $\langle g^p \rangle$ for $p \geq 2$ prime. Note $\langle g^p \rangle$ is a proper subgp of G, so $\langle g^p \rangle \subset H$. This must be true for any (so all) prime p, but then H contains all possible powers of g. Hence, H is no longer proper. ↯

2. Let g be an invertible $n \times n$ complex matrix. Show that g can be written as

$$g = su = us,$$

where s is diagonalizable and all eigenvalues of u are equal to 1.

Consider JCF of g: $g = BJB^{-1}$ where $J = \begin{bmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \\ & & & \lambda \end{bmatrix}$
since g invertible, $\lambda \neq 0$
Then we can pull out λ w/o worrying about divide by 0

$$\begin{bmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \\ & & & \lambda \end{bmatrix} = \lambda \begin{bmatrix} 1 & 1/\lambda & & \\ & 1 & 1/\lambda & \\ & & \ddots & \\ & & & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{bmatrix}}_{\lambda I} \begin{bmatrix} 1 & 1/\lambda & & \\ & \ddots & \ddots & \\ & & & 1/\lambda \\ & & & 1 \end{bmatrix}$$

$= \text{Diag} \times$ matrix w/ eigenvals $= 1 \quad = D \times A \quad = A \times D$

Then $g = BJB^{-1} = B(DA)B^{-1} \qquad = B(AD)B^{-1}$
$= \underbrace{BDB^{-1}}_{=S} \underbrace{BAB^{-1}}_{=u} \qquad = \underbrace{BAB^{-1}}_{=u} \underbrace{BDB^{-1}}_{=S}$

$\Rightarrow g = su = us$
where $s = BDB^{-1}$ is diag'able
$u = BAB^{-1}$ has eigenvals all $= 1$ since similar matrices u & A have same eigenvals

3. List, up to isomorphism, all finite abelian groups G such that the order of every element of G divides 55, and the number n_{55} of elements of order exactly 55 satisfies $|g| = 1, 5, 11,$ or 55

$$10^2 \leq n_{55} \leq 10^3.$$

You must prove that your list is accurate.

To have at least 100 eles of orders at most 55, must use a direct sum (else indiv. orders get too big!)

*Order of eles in direct sum is the lcm of orders of componentwise eles from constituent gps, i.e.

$\mathbb{Z}_5 \oplus \mathbb{Z}_{11} \rightsquigarrow (4,0)$ has order $\text{lcm}(5,1) = 5$

$(0,10)$ has order $\text{lcm}(1,11) = 11$

$(4,10)$ has order $\text{lcm}(5,11) = 55$

Clearly $\mathbb{Z}_5 \oplus \mathbb{Z}_{11}$ doesn't give enough eles to have $n_{55} \geq 100$ (only 55 to begin with)

So, let's try...

$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11} = \{(a,b,c) \mid a,b \in \mathbb{Z}_5,\ c \in \mathbb{Z}_{11}\}$

(a,b,c) has order 55 iff a or $b \neq 0$ AND $c \neq 0$

$n_{55} = \underbrace{4 \times 5 \times 10}_{\text{a any, b nonzero}} + \underbrace{1}_{\text{zero}} \times \underbrace{4}_{\text{nonzero}} \times 10 = 50 + 40 = 90 \quad < 100 \quad \times$

OR

$\mathbb{Z}_5 \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11} = \{(a,b,c) \mid a \in \mathbb{Z}_5,\ b,c \in \mathbb{Z}_{11}\}$

need $a \neq 0$, b or $c \neq 0$

$n_{55} = 4 \times 10 \times 11 + 4 \times 1 \times 10 = 440 + 40 = 480 \quad 100 \leq n_{55} \leq 1000$ ✓

$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11}$ (next smallest w/ lcm = 55)

one of $a,b,c \neq 0$, $d \neq 0$

$n_{55} = 4 \times 5 \times 5 \times 10 + 1 \times 4 \times 5 \times 10 + 1 \times 1 \times 4 \times 10 = 1000 + 200 + 40 = 1240 > 1000 \times$

Remaining sums all too large! So only $G = \mathbb{Z}_5 \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$ works!

4. Let G be a nontrivial finite group of prime power order, and let H be a normal subgroup of G. Show that H contains at least one non-identity element of the center of G.

$|G| = p^\alpha$. *Normal subgps are unions of conjugacy classes.

Gp of prime power order has nontrivial center (by class eq.)

also, each conjugacy class has order p^β for $\beta < \alpha$ as orb-stab says $|\text{orb}| \,\big|\, |G|$ under conjugation as gp action

$H \trianglelefteq G$, so $1 \in H$. H is the orbit of H under conj. action by G. Then, by orbit-stabilizer,

$|H| = |\text{Orb}| \mid |G| = p^\alpha \implies |H| = p^\beta$

Recall $H \trianglelefteq G \implies H$ is the union of conjugacy classes.

$1 \in Z(G)$, + if H contained no other eles of center, we obtain

$|H| = 1 + p^\beta$ so $|H| \nmid p^\alpha$

Thus, we need $Z(G) \subseteq H$ (since $|Z(G)| = p^\gamma$) and since $Z(G)$ nontrivial, H contains at least one nontrivial center element

Yuqiao: $|G| = |Z(G)| + \sum_{g \notin Z(G)} |cl(G)|$

Either $cl(g) \subset H$ or $cl(g) \cap H = \emptyset \quad \forall g \in G$

Hence $|H| = |H \cap Z(G)| + \sum_{\substack{g \notin Z(G) \\ g \in H}} |cl(g)|$

For each $g \in H - Z(G)$

FINISH

5. Let $GL(n,F)$ denote the group of $n \times n$ invertible matrices with entries in the field F. Prove that $g_1, g_2 \in GL(n,\mathbb{Q})$ are conjugate in $GL(n,\mathbb{Q})$ if and only if they are conjugate in $GL(n,\mathbb{R})$.

Cor. 18, Section 12.2 D&F

g_1, g_2 conj in $GL_n(F) \Rightarrow \exists A \in GL_n(F)$ s.t. $A^{-1} g_1 A = g_2$

* Two matrices conj $\boxed{\text{iff}}$ similar $\boxed{\text{iff}}$ same RCF

* If F subfield of K, then RCF of A is same over F & K → D&F pg. 477

($\Leftarrow$) assume g_1 & g_2 conj in $GL_n(\mathbb{R})$, i.e. have same RCF. Since $\mathbb{Q}$ a subfield of $\mathbb{R}$ & RCF is unique, RCFs of g_1 & g_2 are same over $\mathbb{Q}$ as over $\mathbb{R}$. Since RCFs were equal over $\mathbb{R}$, also equal over $\mathbb{Q}$, so g_1 & g_2 conj in $GL_n(\mathbb{Q})$, too.

($\Rightarrow$) assume g_1 & g_2 conj in $GL_n(\mathbb{Q})$. (can use same theorem/idea, or...)

Then $\exists A \in GL_n(\mathbb{Q})$ s.t. $A^{-1} g_1 A = g_2$.

$GL_n(\mathbb{Q}) \subset GL_n(\mathbb{R})$, so $A \in GL_n(\mathbb{R})$, too.

Hence $A^{-1} g_1 A = g_2$ holds in $GL_n(\mathbb{R})$ as well, & thus g_1 & g_2 are conj in $GL_n(\mathbb{R})$.

S18

This exam is particularly difficult

1. Prove that any homomorphism from a finitely generated abelian group *onto* itself is an automorphism.

Every fin gen abelian gp is an R-module.
Let M be an R-module, so $M = Rm_1 + \ldots + Rm_n$ w/ $\{m_i \mid i \in [1,n]\}$ fin gen set

Define an onto map $\phi: M \to M$

Hint: Use Nakayama's Lemma ← also not on qual syllabus
I an arbitrary comm ring A, fin gen module M satis. $M = IM$, then $\exists\, a \in I$ s.t. $\forall m \in M$, $m = am$

2. Let K be a field. Let $K[[x]]$ denote the ring of formal power series, whose elements are expressions of the form $\sum_{n=0}^{\infty} a_n x^n$ with $a_n \in K$ and the usual addition and multiplication. Find, with proof, all ideals of $K[[x]]$.

$K[x] \Rightarrow f = a_0 + a_1 x + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i$
$K[[x]] \Rightarrow f = a_0 + a_1 x + \ldots + a_n x^n + \ldots = \sum_{i=0}^{\infty} a_i x^i$ infinite!
* $K[x] \subset K[[x]]$

Every ideal of $K[[x]]$ is of the form (x^m) for some $m \in \mathbb{Z}_{\geq 0}$

When is $f \in K[[x]]$ a unit? (A: iff a_0 invertible) → any $a_0 \neq 0 \in K$ is invertible since K is a field
Then the only non-units of $K[[x]]$ are eles w/ $a_0 = 0$

$1 = f \cdot g = (\sum_{i=0}^{\infty} a_i x^i) \cdot (\sum_{j=0}^{\infty} b_j x^j)$
$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i b_j x^{i+j}$ all pairwise combos
$= \sum_{k=0}^{\infty} \sum_{\ell=0}^{k} (a_\ell b_{k-\ell}) x^k$ another pairwise consideration

need $\sum_{\ell=0}^{k} (a_\ell b_{k-\ell}) = 0$ whenever $k > 0$ so that x terms drop out
but $a_0 b_0 x^0 = a_0 b_0 = 1$ as const term
Hence a_0 invertible is <u>necessary</u> for f to be a unit

If a_0 invertible, then for $f \cdot g$:
$\sum_{k=0}^{\infty} \sum_{\ell=0}^{k} a_\ell b_{k-\ell} x^k = a_0 b_0 + \sum_{k=1}^{\infty} \sum_{\ell=0}^{k} a_\ell b_{k-\ell} x^k$
$= 1 + \sum_{k=1}^{\infty} (a_0 b_k + \sum_{\ell=1}^{k} a_\ell b_{k-\ell}) x^k$
$= b_0 + b_0 \sum_{k=1}^{\infty}$ "
$= b_0 + \sum_{k=1}^{\infty} (b_k + b_0 \sum_{\ell=1}^{k} a_\ell b_{k-\ell}) x^k$
↳ for some fixed k, solve recursively for b_k so $b_k = -b_0 \sum_{\ell=1}^{k} a_\ell b_{k-\ell}$ to get zero coeffs on each x^k

Then invertible a_0 is also <u>sufficient</u> for inverse $g(x)$ to exist (+ be constructable) for $f(x)$

*Proper ideals cannot contain a unit! Once $u \in I$, $I = K[[x]]$.
Hence any proper + nonzero ideal is gen by a poly w/ $a_0 = 0$, most simply (x^m) for some $m \geq 1$.
To include trivial ideals in our categorization, say m can be 0. Then all ideals of $K[[x]]$ are of the form (x^m) for $m \in \mathbb{Z}_{\geq 0}$
✓

3. (A) Prove that for any square matrices A and B of size n with coefficients in some field the characteristic polynomial of AB equals that of BA.

(B) Give an example of square matrices A and B such that the minimal polynomial of AB does not equal that of BA.

Cr: Stack + AJ

a.) Char poly: $\chi_{AB} = \det(xI - AB)$

Note: Similar matrices have the same char. poly!

$\chi_A = \det(xI - A)$ ← $A = P^{-1}BP$ if similar

$= \det(xI - P^{-1}BP)$

$= \det(xP^{-1}IP - P^{-1}BP)$

$= \det(P^{-1}(xIP - BP))$

$= \det(P^{-1}(xI - B)P)$ } rule of dets

$= \det(P^{-1})\det(xI - B)\det(P)$

$* \det(P^{-1})\det(P) = \det(P^{-1}P) = \det(I) = \text{const. } n$

$= \det(xI - B)$

$= \chi_B$

If A or B is invertible, then $AB \sim BA$, so by above argument, $\chi_{AB} = \chi_{BA}$

If A, B not invertible, need to do some extra work...

Schur's Formula: $\det\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det(A)\det(D - CA^{-1}B)$ if A invertible

$= \det(D)\det(A - BD^{-1}C)$ if D invertible

Consider $\begin{bmatrix} xI & A \\ B & I \end{bmatrix}$. $\det\begin{bmatrix} xI & A \\ B & I \end{bmatrix} =$

$= \det(xI)\det(I - B(xI)^{-1}A)$

$= \det(xI)\det(I - B\frac{1}{x}IA)$

$= \det(xI(I - \frac{1}{x}BIA))$

$= \det(xI - BA)$

$= \chi_{BA}$

$= \det(I)\det(xI - AI^{-1}B)$

$= \det(I)\det(xI - AB)$

$= \det(xI - AB)$

$= \chi_{AB}$

hence $\chi_{AB} = \chi_{BA}$ ✓

b.) $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

char poly $= \det(xI - M)$

$= \det\begin{pmatrix} x & -1 \\ 0 & x \end{pmatrix} = \det\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$

$= x^2 - 0$

$= x^2$

min poly is largest invariant factor AND $m_{AB}(AB) = 0$, $m_{BA}(BA) = 0$

Then $m_{BA}(x) = x$ since $BA = 0$

But $m_{AB}(x)$ cannot be simply x since $AB \neq 0$

$m_{AB}(x) = x^2$

So min polys are different

4. (A) Prove that a Sylow 2-subgroup of the symmetric group S_4 is isomorphic to the dihedral group D_4 of 8 elements.

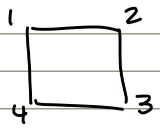
(B) Prove that a Sylow p-subgroup of the symmetric group S_n is non-abelian if and only if $n \geq p^2$.

a.) $|S_4| = 24 = 2^3 \cdot 3$

$\Rightarrow P_2 \in Syl_2(S_4)$ has order 8 $\rightarrow$ (Products of) 2- + 4-cycles

$D_4 = \langle r, f \mid r^4 = f^2 = 1,\ rf = fr^3 \rangle$

For isomorphism, need generator of order 4 + of order 2



$r \mapsto (1234)$

$f \mapsto (13)$

$\rightarrow$ FIX

b.) ($\Rightarrow$) assume $P \leq S_n$ not abelian. $\mathbb{Z}_p$ abelian, so $\mathbb{Z}_p \not\cong P$ thus $|P| = p^\alpha$ for $\underbrace{\alpha > 1}_{\alpha \geq 2}$. Then $p^\alpha \mid n!$, so $p^\alpha \mid m$ for some $m \leq n$.

Let $p^\alpha = p^2 \cdot p^\beta$ for $\beta \geq 0$. Thus $p^2 \cdot p^\beta \mid m$ for some $m \leq n$, and thus $p^2 \mid m$ for some $m \leq n$. If p^2 divides m, then $p^2 \leq m$, and this is true for some $m \leq n$, so $p^2 \leq m \leq n \Rightarrow p^2 \leq n$ ✓

($\Leftarrow$) assume $n \geq p^2$. $|S_n| = n!$, and $\forall m \leq n$, $m \mid n!$. Then if $p^2 \leq n$, $p^2 \mid n!$, so $\exists$ a Sylow p-subgp of S_n w/ order p^α for $\alpha \geq 2$.

NOT DONE

*any gp of order p^2 is abelian

5. Let I be a maximal ideal of $\mathbb{Z}[x]$. Prove that $\mathbb{Z}[x]/I$ is a finite field.

Can't use $F[x]/\overset{\text{max}}{I} \cong$ Field since $\mathbb{Z}$ not a field

Hint: $\mathbb{Z}_p$ is a field!

Show that max ideals are of the form (p, x) in $\mathbb{Z}[x]$

Since $\mathbb{Z}[x]$ is not a PID, any max ideal I cannot be principal.

Recall any maximal ideal cont. a prime (Fall 2021 P2)

$\hookrightarrow$ I max in $\mathbb{Z}[x] \Rightarrow I/(p)$ max in $\mathbb{Z}[x]/(p)$

$\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$

$\mathbb{Z}[x]/I \cong \underbrace{(\mathbb{Z}[x]/(p))}_{\mathbb{Z}_p[x]} / \underbrace{(I/(p))}_{= J \cong ?}$ 3rd Iso.

$\mathbb{Z}_p[x]$ is a PID, so the ideal $J = I/(p)$ is principal. Say $J = (f)$ for some poly $f \in \mathbb{Z}_p[x]$. Note since J is maximal in $\mathbb{Z}_p[x]$, f is irreducible + prime in $\mathbb{Z}_p[x]$. $\rightsquigarrow$ max = prime ideals in a PID

Then $\mathbb{Z}[x]/I \cong \mathbb{Z}_p[x]/(f) \cong \mathbb{Z}_p$ which is a finite field!

Note: Then any max ideal in $\mathbb{Z}[x]$ is of form (p, f) where f is an irred poly in $\mathbb{Z}_p[x]$

1. Give an example of an integral domain R and an ideal I in R such that *all* of the following statements hold. The ideal I is not principal, it is not maximal, and it is prime.

$\boxed{7/8}$

i.) I not principal (more than one generator)
ii.) I not maximal
iii.) I prime

$(7, x) = I$, $R = \mathbb{Z}[x,y]$

i.) Not principal
AFSOC $(7,x) = (p(x,y))$ for $p(x,y) \in \mathbb{Z}[x,y]$
Then $7 \in I$, so $p(x,y) \cdot q(x,y) = 7$ for some $q(x,y)$
Then $p(x,y) = 1$ or 7 (only 2 factors of 7)
If $p(x,y) = 1$, then $(p(x,y)) = (1) = \mathbb{Z}$ ↯ $x \notin \mathbb{Z}$
If $p(x,y) = 7$, then $(p(x,y)) = (7) = 7\mathbb{Z}$ ↯ $x \notin 7\mathbb{Z}$

ii.) Not maximal
$y \notin (7,x)$, and $(7,x) \subset (7,x,y) \subset \mathbb{Z}[x,y]$ something bigger exists

iii.) Prime
commutative R / prime I $\cong$ ID
$\mathbb{Z}[x,y]/(7,x) \cong \mathbb{Z}[y]/(7) = \mathbb{Z}_7[y]$ which is an ID
ID preserved under poly ring, so $\mathbb{Z}_7$ ID $\Rightarrow \mathbb{Z}_7[y]$ an ID
$\mathbb{Z}$ an ID, + since 7 is prime in $\mathbb{Z}$, $\nexists$ $a,b \in \mathbb{Z}_7$, $\neq 0$ s.t. $ab = 0$ (or $= 7$).
Hence $\mathbb{Z}_7$ is an ID, then $\mathbb{Z}_7[y]$ an ID, so I is prime in $\mathbb{Z}[x,y]$ ✓

2. Let p and q be distinct primes. Let $\bar{q} \in \mathbb{Z}/p\mathbb{Z}$ denote the class of q modulo p and let k denote the order of $\bar{q}$ as an element of $(\mathbb{Z}/p\mathbb{Z})^*$. Prove that no group of order pq^l with $1 \leqslant l \leqslant k$ is simple.
↳ no normal subgps

WTS: n_p or $n_q = 1$ so P or $Q \trianglelefteq G$
so G not simple

$\bar{q} \in \mathbb{Z}_p$ $(0 \le \bar{q} \le p-1)$
$\bar{q} = q \bmod p$
$(\bar{q})^k = 1 \bmod p$
$\Rightarrow q^k = 1 \bmod p$
$(q^j \neq 1 \bmod p \ \forall j \le k)$

$|G| = pq^l \Rightarrow$ By Sylow, $\exists P \in Syl_p(G)$
$\exists Q \in Syl_q(G)$

$n_p \equiv 1 \bmod p$, $n_p \mid q^l \Rightarrow 1$ or q^k where $k \mid l \Rightarrow k = l$ since $l \le k$
$n_q \equiv 1 \bmod q$, $n_q \mid p \Rightarrow$???

If $n_p = 1$, then $P \trianglelefteq G$ so G not simple ✓
If $n_p = q^l = q^k$, then recall since $|P| = p^1$ is prime (not, more generally, prime power)
the q^k p-subgps all intersect trivially, so there are $(p-1) \cdot q^k$ elements of order p in G
Total elements of G: $|G| = pq^l = \underset{\text{id}}{1} + (p-1)q^l + \underset{= \#\text{ elements of order } q}{x}$ $\Rightarrow x = pq^l - (p-1)q^l - 1$
$= q^l - 1$
$\Rightarrow n_q = 1$ since $|Q| = q^l$
Then $Q \trianglelefteq G$, so G has a normal subgp + thus not simple

3. Let M be a square matrix with complex coefficients. We consider the usual matrix exponential

$$\exp(M) = \sum_{j=0}^{\infty} \frac{1}{j!} M^j.$$

Prove that $\exp(M)$ is equal to the identity matrix if and only if M is diagonalizable with eigenvalues in $2\pi i\,\mathbb{Z}$.

Note: Pick eigenpair λ, x (so $Mx = \lambda x$)

$$\begin{aligned} \exp(M)x &= \textstyle\sum_{j=0}^{\infty} \frac{1}{j!} (M)^j x \\ &= \textstyle\sum_{j=0}^{\infty} \frac{1}{j!} M^j x \\ &= \textstyle\sum_{j=0}^{\infty} \frac{1}{j!} \lambda^j x \quad \text{ind.} \\ &= e^{\lambda} x \end{aligned}$$

$e^x = \sum_{j=0}^{\infty} \frac{1}{j!} x^j$

Then e^{λ} is an eigenvalue of $\exp(M)$!

$e^{\lambda} = 1$ iff $\lambda = 2\pi i n$ for $n \in \mathbb{Z}$

so eigenvalues of $\exp(M)$ are all 1 iff $\lambda = 2\pi i n$ for all eigenvals of M

M diagonalizable iff Jordan blocks of size 1 (n of them)
iff char poly factors linearly

M diag'able w/ $\lambda = 2\pi i n$ for $n \in \mathbb{Z}$ iff has n Jordan blocks

Recall M has λ w/ mult l
$\Leftrightarrow$ $\exp(M)$ has e^{λ} w/ mult. l

iff $\exp(M)$ has $\lambda = 1$ & Jordan blocks of size 1, so $\exp(M) = I$ ✓

4. Let $G = \mathbb{Q}/\mathbb{Z}$ be the quotient of the additive group of rational numbers by the subgroup of integers.

(A) Prove that every finitely generated subgroup of G is a finite cyclic group.

(B) Prove that G is not isomorphic to $G \oplus G$ as an abelian group.

a.) let $S = \{g_1, \ldots, g_n\}$ be a finite generating set s.t. $\langle S \rangle = H \leq G$.
Each g_i takes form $g_i = r_i/q_i$ for $r_i, q_i \in \mathbb{Z}$ but $q_i \nmid r_i$

Then $h \in H = \langle S \rangle$ takes form $h = \sum_{i=1}^{n} c_i \frac{r_i}{q_i}$ $\quad c_i \in \mathbb{Z}\ \forall i$

Then get a common denom: $\hookrightarrow$ mult each term by $\prod_{i=1}^{n} q_i$ top & bottom

$h = c_1 \frac{r_1}{q_1} + c_2 \frac{r_2}{q_2} + \ldots + c_n \frac{r_n}{q_n}$

$h = \frac{c_1 r_1 \prod_{i=1}^{n} q_i}{q_1 \cdot \prod_{i=1}^{n} q_i} + \frac{c_2 r_2 \prod_{i=1}^{n} q_i}{q_2 \cdot \prod_{i=1}^{n} q_i} + \ldots + \frac{c_n r_n \prod_{i=1}^{n} q_i}{q_n \cdot \prod_{i=1}^{n} q_i}$

$h = \frac{c_1 r_1 \prod_{i \neq 1} q_i + c_2 r_2 \prod_{i \neq 2} q_i + \ldots + c_n r_n \prod_{i \neq n} q_i}{\prod_{i=1}^{n} q_i}$

Then each $h \in H$ is some multiple of $1/\prod_{i=1}^{n} q_i$. Since $q_i \nmid r_i\ \forall i$, $q_i \neq 1\ \forall i$,
so $1/\prod_{i=1}^{n} q_i \notin \mathbb{Z}$, thus $1/\prod_{i=1}^{n} q_i \in \mathbb{Q}/\mathbb{Z}$ and $\langle S \rangle = \langle 1/\prod_{i=1}^{n} q_i \rangle$.

Note: clearly $\langle 1/\prod_{i=1}^{n} q_i \rangle$ is finite cyclic since $(\prod_{i=1}^{n} q_i) \cdot (1/\prod_{i=1}^{n} q_i) = 1$ $(= 0$ in $\mathbb{Q}/\mathbb{Z})$
so generator has finite order

b.) By part (a), every fin gen subgp is finite cyclic gp.
Would like to show that $\exists$ some fin gen subgp of $G \oplus G$ which is not cyclic.

Hint: Take advantage of both components $(g, 0)$ & $(0, g)$ in $G \oplus G$

Counterex: $\langle (0, \frac{1}{2}), (\frac{1}{2}, 0) \rangle$ not cyclic, but fin gen

5. Let G be a finite subgroup of the group of real $n \times n$ matrices with nonzero determinant such that all elements of G are symmetric matrices. Prove that G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for some $k \geqslant 0$. $A^T = A$

$G \cong (\mathbb{Z}_2)^k = \underbrace{(\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2)}_{k \text{ times}}$ = binary triples of length k } each have order 2

$\mathbb{Z}_2 = \{0,1\}$

*Recall: real symmetric matrices have real eigenvalues & are diagonalizable

For iso to exist, $|g| = 2 \ \forall g \in G$

$g^2 = I \Rightarrow \lambda = \pm 1 \ \forall g \in G$. Then

$(gh)^2 = 1$

$gh \cdot gh = 1 = gh(gh)^{-1}$

$\Rightarrow gh = hg$ so G is abelian

If G abelian & each element has order 2, then $G \cong (\mathbb{Z}_2)^k$ for some k

Need to prove every element of G has order 2

G finite, so every ele has finite order (i.e. $A^m = I$ for some $m \geq 1$)

Can decompose $A = UDU^{-1}$ (by spectral thm.)

$A^m = I \Rightarrow \lambda^m = 1 \ \forall \lambda$ of A

$D = \begin{bmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{bmatrix}$ of A

$A^m = (UDU^{-1})^m = UD^mU^{-1} = U\begin{bmatrix} \lambda^m & & \\ & \ddots & \\ & & \lambda^m \end{bmatrix}U^{-1}$

If $\lambda^m = 1$ for any λ of A, then $\lambda = \pm 1 \ \forall \lambda$

D is diagonal w/ entries ± 1,

so $D^2 = \begin{bmatrix} \pm 1 & & & \\ & \pm 1 & & \\ & & \ddots & \\ & & & \pm 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = I$

signs are same, so square to $+1$

Then $A^2 = UD^2U^{-1} = UIU^{-1} = UU^{-1} = I$

Hence $m = 2$, so any $g \in G$ has order 2 ✓

S19

1. Let P be a Sylow p-subgroup of a finite group G and H be a normal subgroup in G.

a) Prove that the intersection of P and H is a Sylow p-subgroup in H.

b) Find an example showing that for non-normal subgroups H the statement a) may not be valid.

a.) $P \in Syl_p(G)$, WTS: $P \cap H \in Syl_p(H)$, alt: $|P \cap H| = p^\alpha$

$P \in Syl_p(G) \Rightarrow |P| = p^\alpha$.

Since $P, H \le G$, $P\cap H \le G$, and additionally $P \cap H \le P$ and $P \cap H \le H$.

Then $|P\cap H| \mid |P|$, so $|P \cap H| \mid p^\alpha \Rightarrow |P\cap H| = p^\beta$ w/ $\beta \le \alpha$.

additionally, $|P \cap H| \mid |H|$ since $P \cap H \le H$, so $p^\beta \mid |H| \Rightarrow p \mid |H|$.

Then H has a Sylow p-subgp, i.e. $Syl_p(H) \neq \emptyset$.

$H \trianglelefteq G$, $P \le G \Rightarrow |PH| = \frac{|P|\cdot|H|}{|P\cap H|}$

$P \le G$ w/ $|P| = p^\alpha$, $|G| = p^\alpha m$. Then $|G|/|P| = m$, & $p \nmid m$

$PH \le G$, so $|PH| \mid |G|$, and thus $p \nmid |G|/|P| \Rightarrow p \nmid |PH|/|P|$

$|PH|/|P| = |H|/|P\cap H|$, so $p \nmid \frac{|H|}{|P \cap H|}$

Thus $P \cap H$ is a Sylow p-subgp of H

b.) $G = S_3$ $\quad |G| = 6 = 2 \times 3$

$P = \langle (12) \rangle = \{1, (12)\}$ $(p=2)$

$H = \langle (23) \rangle = \{1, (23)\}$

(12) (123)
(13) (132) } only normal subgp
(23) 1

Recall if $|G| = p^\alpha m$ w/ $p \nmid m$, then a group of order p^α is a Sylow p-subgp.

Then $P \cap H = \{1\}$. But $|H| = 2$, so for (a.) to be true, $|P \cap H| = 2^1$. But $|P\cap H| = 1$, so this doesn't work!

2. A ring is called completely left reducible if it is a direct sum of left ideals which are simple modules over the ring. For what integers n is the ring $\mathbb{Z}/n\mathbb{Z}$ completely left reducible?

let R be a ring, M a nonzero R-module.
The module M is simple (irreducible) if its only submodules are 0 + M

$\mathbb{Z}$ is a ring, $n\mathbb{Z}$ an ideal, so $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module
(R/I is an R-module)

For what n is $\mathbb{Z}/n\mathbb{Z} = \bigoplus_m \mathbb{Z}/m\mathbb{Z}$ for $\mathbb{Z}/m\mathbb{Z}$ irred, i.e. m prime

Recall direct product = direct sum in finite gp.

Then we want n s.t. n decomposes into unique primes

(note $\mathbb{Z}_{p^2} \not\cong \mathbb{Z}_p \times \mathbb{Z}_p$, only if $\gcd(p,q) = 1$)

Then $\mathbb{Z}/n\mathbb{Z}$ is left reducible iff n has a decomp into unique primes

3. Let A and B be operators in complex finite-dimensional vector space such that $AB - BA = B$.

a) Prove that for all integer $k > 0$ there holds $AB^k - B^kA = kB^k$.

b) Prove that operator B is nilpotent.

a.) Proof by induction

Base: $K=1 \Rightarrow AB^1 - B^1A = 1 \cdot B^1$

$AB - BA = B$ ✓ given

IH: assume $\forall K>0$, $AB^K - B^K A = KB^K$

IS: consider $K+1$ (WTS: $AB^{K+1} - B^{K+1}A = (K+1)B^{K+1}$)

By IH: $AB^K - B^K A = KB^K$

$(AB^K - B^K A)B = KB^K \cdot B$

$AB^{K+1} - B^K AB = KB^{K+1}$ $\qquad AB - BA = B$

$AB^{K+1} - B^K(B+BA) = KB^{K+1}$ $\qquad \Rightarrow AB = B + BA$

$AB^{K+1} - B^{K+1} - B^{K+1}A = KB^{K+1}$

$AB^{K+1} - B^{K+1}A = (K+1)B^{K+1}$ ✓

b.) B nilpotent $\Rightarrow \exists K>0$ s.t. $B^K = 0$

By pt (a.), $AB^K - B^K A = KB^K$

AJ Hint: Consider trace. $B^K = 0 \Leftrightarrow Tr(B^K) = 0 \ \forall K$

$Tr(KB^K) = Tr(AB^K - B^K A)$

$K\,Tr(B^K) = Tr(AB^K) - Tr(B^K A)$

$= Tr(AB^K) - Tr(AB^K)$

$= 0$

$K>0$, so $Tr(B^K) = 0$

$\Rightarrow B$ nilpotent

4. Show that the groups of automorphisms of the finite abelian groups $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/15\mathbb{Z}$ are isomorphic.

automorphisms of cyclic grp $\mathbb{Z}_n$ are of form $\sigma_a : \mathbb{Z}_n \to \mathbb{Z}_n$, $\sigma_a(x) = x^a$ for $x \in \mathbb{Z}_n$ iff a & n rel. prime

Then for $\mathbb{Z}_{15}$, automorphisms are σ_a for

$a = 1, 2, \cancel{3}, 4, \cancel{5}, \cancel{6}, 7, 8, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, 14, \cancel{15}$ = 8 autos

For $\mathbb{Z}_{30}$, automorphisms are σ_b for

$b = 1, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}$ = 8 autos

Exhibit isomorphism: ($\Phi : a \to b$ homo.)

Φ: a	1	2	4	7	8	11	13	14
b	1	7	11	13	17	19	23	29

$\Phi(1+14) = \Phi(15) = 0$

$\Phi(1) + \Phi(14) = 1 + 29 = 30 = 0$ ✓ etc.

5. Let R be an associative ring with identity. Assume that R has no proper one-sided ideals. Prove that R is a skew-field.

skew field = division ring
= every nonzero element has a mult. inverse

assume R has no proper one-sided ideals
let $I = (a)$ for some $a \in R$. No proper ideals $\Rightarrow I = R$
Then for any $r \in R$, $r = as$ for $s \in R$
$1 \in R$, so $\exists t \in R$ s.t. $1 = at$
Then $t = tat$
$0 = tat - t$
$0 = t(at - 1)$ } associativity

→ see below for proof

We want to be able to claim that R has no zero divisors, so either $t = 0$ or $at - 1 = 0$
If so, then
i.) $t = 0 \Rightarrow ta = 0 \neq 1$ ↯
ii.) $at - 1 = 0 \Rightarrow at = 1$, so t is both the left & right inverse of a
Hence any $a \in R$ has a mult inverse t, so R is a skew field

To show R is an ID:
let $x \in R$ w/ $x \neq 0$, & consider the ideal xR. Since xR not proper, $xR = R$.
Since $1 \in R$, $\exists s \in R$ s.t. $sx = 1$
Suppose $\exists y \in R$ w/ $y \neq 0$ s.t. $xy = 0$. Then:
$s(xy) = s(0) = 0$
$(sx)y = 1(y) = y$
} since R is associative, must be equal, but $y \neq 0$ by assumption ↯

Thus R must be an ID!

$\boxed{719}$

1. Classify all finite groups G of order 2019 up to isomorphism. (Hints: The prime factors of 2019 are 3 and 673. Also, $255^3 - 1$ is divisible by 673.)

↳ $3 \mid 255$, so $3 \mid 255^3$ + $255^3 = 1 \bmod 3$
plus $673 \mid 255^3$ ⟹ $673 = 1 \bmod 3$

$|G| = 2019 = 3 \times 673$

By Sylow: $\exists P_3 \in Syl_3(G)$ w/ $n_3 \equiv 1 \bmod 3$ + $n_3 \mid 673$ ⟹ $n_3 = 1$ or 673

$\exists P_{673} \in Syl_{673}(G)$ w/ $n_{673} \equiv 1 \bmod 673$ + $n_{673} \mid 3$ ⟹ $n_{673} = 1$

If $n_3 = 1$, $n_{673} = 1$, Then $P_3, P_{673} \trianglelefteq G$

$P_3 \cong \mathbb{Z}_3$, $P_{673} \cong \mathbb{Z}_{673}$ since 3 + 673 both prime

Then $G = \mathbb{Z}_3 \times \mathbb{Z}_{673} \cong \mathbb{Z}_{2019}$ as 3 + 673 coprime

If $n_3 = 673$, $n_{673} = 1$, then there are → $(3-1) \times 673 = 1346$
Then only $P_{673} \trianglelefteq G$, so $G \cong P_{673} \rtimes P_3$ $(673-1) \times 1 = 672$
Recall $P_{673} \rtimes P_3$ ⟹ $\exists$ homo $\phi: P_3 \to Aut(P_{673})$ $+ \; 1$ (id.)
If ϕ trivial, $G \cong P_{673} \rtimes P_3 \cong P_{673} \times P_3 \cong \mathbb{Z}_{2019}$ 2019 eles ✓
as in the above case

If ϕ nontrivial, $G = \langle x, y \mid x^{673} = 1 = y^3, yx = x^m y$ w/ $m^3 \equiv 1 \bmod 673 \rangle$

In general, $|G| = p \cdot q$ has these two forms

2. Let R be a ring (associative with 1) with finitely many elements. Prove that if R cannot be written as a direct product $R = R_1 \times R_2$ of smaller rings, then the number of elements of R is a power of a prime.

$|R| = N < \infty$, $R \neq R_1 \times R_2$ w/ $|R_1|, |R_2| < N$

<u>Contrapos:</u> $|R| \neq p^\alpha$ ⟹ $R = R_1 \times R_2$ CRT

$|R| \neq p^\alpha$ ⟹ $|R| = p_1 \times p_2 \times \ldots \times p_n$ as a prime decomp where $n \geq 2$ ↗ (might need more detail)

Then let $I_1 = (p_1)$ and $I_2 = (p_2, \ldots, p_n)$.

Note that I_1 + I_2 are comaximal as $I_1 + I_2 = \{x + y \mid x \in I_1, y \in I_2\} = R$

Then by Chinese Remainder Thm:

$R \cong R/I_1 \times R/I_2 = R_1 \times R_2$ ✓

↳ ↳ both are subrings of R

3. Let A be an $n \times n$ matrix over some field and let $f(t) = \det(A - tI_n)$ be its characteristic polynomial. Consider left multiplication by A

↳ function of t whose zeros are λs

$$M \mapsto AM$$

as a linear transformation L_A on the space of $n \times n$ matrices. Prove that the characteristic polynomial of L_A is equal to $f(t)^n$.

$L_A(M) = AM$ $\quad f(t) = \det(A - tI) = \prod_{i=1}^{n} (t - \lambda_i)$

↳ LT usually defined by action on basis vectors

can write as a matrix L:

$L = [L_A \cdot e_1, L_A \cdot e_2, \ldots, L_A \cdot e_n]$

$= [A \cdot e_1, A \cdot e_2, \ldots, A \cdot e_n]$

$= \begin{bmatrix} A & & 0 \\ & A & \\ 0 & & A \end{bmatrix}$

$A = n \times n$
$L = n$ copies of A in each dir, so $n^2 \times n^2$

Then $g(t) = \det(L - tI)$ ← char poly of L_A

$= \det\left(\begin{bmatrix} A & & \\ & A & \\ & & \ddots A \end{bmatrix} - \begin{bmatrix} t & & \\ & t & \\ & & \ddots t \end{bmatrix} \right)$ → must be $n^2 \times n^2$ for dims to work

$= \det \begin{pmatrix} A - tI & & \\ & A - tI & \\ & & \ddots A - t\,I \end{pmatrix}$ } n of these blocks along diagonal

↳ each $n \times n$ now

$= \det(A - tI)^n$

$= f(t)^n$ ✓

as desired

4. Let S be the subring of $\mathbb{C}[x, y]$ which consists of the polynomials $f(x, y)$ with $\underline{f(x, 0) = f(0, 0)}$. Prove that S is not Noetherian.

Not Noetherian = $\exists$ an ideal not fin gen
or ascending chain of ideals w/o max ele

$f(x,y) = \Sigma a_i x^i y^i$
If $f(x,0) = f(0,0)$, then there are no $a_i x^i$ terms, i.e. every power of x also has a y w/ it

Hence every x term is divisible by y
$x \notin S$ then $\nexists z \in S$ s.t.
$y \in S$ $xy \cdot z = x^2 y$, so $x^2y \notin (xy)$ and so on

$(1) \subset (xy) \subset (xy, x^2y) \subset (xy, x^2y, x^3y) \subset \ldots$
$\hookrightarrow$ is an ascending chain of ideals w/ no max element

5. Prove that for any prime p and any positive integer n, the group $GL(n, \mathbb{Z}/p\mathbb{Z})$ contains an element of order $(p^n - 1)$.
prime

$|GL_n(\mathbb{Z}_p)| = ?$

$n\left\{\underbrace{\left[\,|\;|\;|\;|\;\cdots\;|\,\right]}_{n}\right.$

GL_n is invertible $n \times n$ matrices, so cols are lin ind.

How many choices for cols w/ entries in $\mathbb{Z}_p$?

First col: Pick one of p elements n times, but can't have all 0's
$\Rightarrow \binom{p}{1}^n - 1^n = p^n - 1$
Second col: Pick another col, but you can't have dependence w/ first col. So eliminate any of p possible multiples of c_1 (note: this includes 0's)
$\Rightarrow \binom{p}{1}^n - p = p^n - p$
Third col: Pick another, but can't have any lin combo of first 2, so $c_3 \neq a_1 \cdot c_1 + a_2 \cdot c_2$. There are p possible values of a_1 & p possible for a_2, so $p \cdot p = p^2$ bad c_3's. Then:
$\Rightarrow p^n - p^2$

In general: Column j has $p^n - p^j$ possibilities

Order of $GL_n(\mathbb{Z}_p)$ = total # poss. combos of cols $c_1, \ldots, c_n$, so:
$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \ldots (p^n - p^{n-1})$

Since for any prime divisor of $|G|$, $\exists$ an element of that order, we conclude since $(p^n - 1) \mid |GL_n(\mathbb{Z}_p)|$ & $p^n - 1$ prime, $\exists A \in GL_n(\mathbb{Z}_p)$ s.t. $|A| = p^n - 1$ ✓

S20

1. Suppose that A is a not necessarily commutative, finite dimensional associative algebra with a unit over a field F and $P \lhd A$ is a two-sided ideal such that for $a, b \in A$, $ab \in P$ implies $a \in P$ or $b \in P$. Show that A/P must be a division algebra (i.e. every nonzero element has a multiplicative inverse).

alg over a field = vector space w/ scalars in F
w/ unit = has identity

let $P \lhd A$ be a 2-sided prime ideal ($a,b \in A$, $ab \in P \Rightarrow$ $a \in P$ or $b \in P$)
WTS: A/P is a division alg.
↳ every nonzero element has mult inverse

CR: Teddy
let $a \notin P$. Then for any $b \notin P$, $ab \notin P$
$A/P \to A/P$ defined by $a \cdot x$ is inj. as long as $a \neq 0$
($x \in A/P$)

A/P is fin dim., & an inj btwn 2 fin dim v.s. w/ same dim is bij., hence iso.
Then left mult by a must hit $1 \in A/P$, i.e. $\exists\, y \in A/P$ s.t. $a \cdot y = 1$
Hence a has a right inverse y

By same logic, right mult by a is also an inj. since for any $b \notin P$, if $a \notin P$ then $ba \notin P$. Again, see that right mult by a gives an inj., which $\Rightarrow$ isomorphism
So $\exists\, z \in A/P$ s.t. $za = 1$, hence a has a left inverse z.

To show that $y = z$ (so a has a single inverse)
Notice that $ay = 1$
$z \cdot ay = z \cdot 1$) left mult by z
$\underbrace{za}_{=1} \cdot y = z$ (associative)
$\Rightarrow y = z$ ✓

Then any $a \in A/P$ has an inverse, so A/P is a division algebra ✓

2. Show that every group of order 2020 contains a unique (and hence normal) subgroup of order 505.

$|G| = 2020 = 4 \times 505 = 2^2 \times 5 \times 101$
By Sylow: $\exists\, P_{101} \in Syl_{101}(G)$ w/ $n_{101} \equiv 1 \bmod 101$, $n_{101} \mid 4 \times 5$ $\Rightarrow n_{101} = 1$
Then $P_{101} \trianglelefteq G$ since it is the unique subgp of order 101
Consider $G' = G/P_{101}$ (since P_{101} normal), and note $|G'| = |G|/|P_{101}| = 2020/101 = 20$ $(= 2^2 \times 5)$
By Sylow again: $\exists\, Q_5 \in Syl_5(G')$ w/ $n_5 \equiv 1 \bmod 5$, $n_5 \mid 4$ $\Rightarrow n_5 = 1$
Then $Q_5 \trianglelefteq G'$
Since $Q_5 \trianglelefteq G/P_{101}$ and $P_{101} \trianglelefteq G$, let $N = Q_5 P_{101}$ and observe that $|N| = 505$ & $N \trianglelefteq G$
Hence N is a unique/normal subgp of G

3. Let M be a matrix with integer entries.

(a) Prove that the minimal polynomial of M over $\mathbb{C}$

$$f_{min}(t) = t^k + \sum_{i=0}^{k-1} a_i t^i$$

has integer coefficients.

(b) Prove that if M is diagonalizable over $\mathbb{Q}$ then there exists an integer N such that the matrix M mod p is diagonalizable over $\mathbb{Z}/p\mathbb{Z}$ for all $p > N$.

they are roots of polys w/ integer coeffs

Let $\lambda_1, \dots, \lambda_n$ be eigenvalues M

FACT: the λs of an integer matrix are algebraic integers

Char poly: $\prod_{i=1}^n (x-\lambda_i)$

min poly divides char poly over field $\mathbb{C}$

↳ coeffs are integral over $\mathbb{Z}$

↳ $\mathbb{Z}$ integrally closed, so coeffs in $\mathbb{Z}$

↳ Hey! Min poly has integer coeffs

b.) M diag'able over $\mathbb{Q}$ $\iff$ min poly factors into distinct linear factors over $\mathbb{Q}$

$D = A^{-1} M A$ A is $m \times m$ over $\mathbb{Q}$, D is $m \times m$ over $\mathbb{Z}$

Make A, A^{-1} s.t. all entries have same denom N

↳ mult by lcm top & bottom, so $N = \text{lcm}(\text{denoms})$

For any $p > N$, the same matrix comps from $\mathbb{Q}$ hold since no entry is great/eq p, so nothing zeros out/loops around

$\Rightarrow$ also diag (similar to diag) over $\mathbb{Z}_p$

4. Let F be a field and let L be the ring of Laurent polynomials $L = F[x, x^{-1}]$ (it is the subring of $F(x)$ generated over F by x and x^{-1}). We consider L as a module over the ring of polynomials $R = F[x]$.

(a) Show that L is not a finitely generated module over R.

(b) Show that every finitely generated submodule of L is free with a single generator.

↳ same idea as finite subgp of $\mathbb{Q}/\mathbb{Z}$ being cyclic

a.) $L = F[x, x^{-1}]$, $R = F[x]$

AFSOC L is fin gen over R. Then for any $l \in L[x, x^{-1}]$, $l = \sum_{i=1}^n r_i$ where $r_i \in R$ $\forall i$

Each r_i is of the form $r_i = \sum_{j=0}^{m_i} a_j x^j$, so $l = \sum_{i=1}^{n} \sum_{j=1}^{m_i} a_{i,j} x^j$

Note that $x^{-1} \in L$. Then $x^{-1} = \sum_{i=1}^n \sum_{j=0}^{m_i} a_{i,j} x^j$

$1 = \sum_{i=1}^n \sum_{j=0}^{m_i} a_{i,j} x^{j+1} = \sum_{k=0}^{M} a_k x^{k+1} = \sum_{k=1}^{M} a_{k-1} x^k$

But a finite sum of positive powers of x cannot be equal to 1, (or $\frac{1}{x}$ cannot be written as a sum of nonnegative powers of x)

Contradiction! So L cannot be fin gen by R

b.) Free w/ a single generator $\Rightarrow$ every fin gen submodule of L is gen by a single element in L

Let Y be a fin gen submodule of L. Then any $y \in Y$ can be written as $y = \sum_{i=1}^n c_i a_i$ for $c_i \in R$, $a_i \in A$ (finite gen set, $A \subseteq L$)

Each $a_i = \sum_{j=-1}^{m} b_j x^j$, so

$y = \sum_{i=1}^n a_i \sum_{j=-1}^{m} b_j x^j$
$= \frac{1}{x} \underbrace{\left(\sum_{i=1}^n a_i \sum_{j=0}^{m} b_j x^j \right)}_{\in R}$

any $y \in Y$ is a linear combo of $\frac{1}{x}$'s using coeffs in R

$\frac{1}{x} \in L$, so any fin gen submodule is free w/ single generator $\frac{1}{x}$

5. Let R be a commutative integral domain and let $I \lhd R$ be an ideal.

(a) Show that every alternating bilinear form

$$f : I \times I \to R$$

is zero.

(b) Show that if R is a principal ideal domain, then every alternating bilinear form

$$f : I \times I \to M$$

to any R-module M is zero.

D+F pg. 368

alternating: $\forall v \in V$, $B(v,v) = 0$

Bilinear: $B(u+v,w) = B(u,w) + B(v,w)$ $\quad u,v,w \in I$
$B(u,v+w) = B(u,v) + B(u,w)$
$B(\lambda u, v) = \lambda B(u,v)$ $\quad \lambda \in R$
$B(u,\lambda v) = \lambda B(u,v)$

alternating $\Rightarrow$ antisymmetric
$B(u,v) = -B(v,u)$

a.) $\forall a \in I$, $f(a,a) = 0$

$f(a,a) = f(a+0, a+0) = f(a+0,a) + f(a+0,0)$
$= \cancel{f(a,a)}^{\,0} + f(0,a) + f(a,0) + \cancel{f(0,0)}^{\,0}$
$= f(0,a) + f(a,0)$

Note $f(0,a) = f(\underset{\lambda=0}{\lambda a}, a) = \lambda \underbrace{f(a,a)}_{=0} = 0$. Same for $f(a,0)$ (by same logic or since $f(a,0) = -f(0,a)$)

Let $a,b \in I$. If a or $b = 0$, then $f(a,b) = 0$ by argument above

Else, consider $f(ab,ab) = 0$

$0 = f(ab,ab) = \underset{b \in I \subseteq R}{b} f(a,ab) = \underset{a \in I \subseteq R \text{ + R comm.}}{ab} f(a,b)$ since R an ID, $ab \neq 0$ when $a,b \neq 0$.

Then $0 = ab\, f(a,b) \Rightarrow f(a,b) = 0$

Then $f \equiv 0$ as $f(a,b) = 0$ for any $a,b \in I$.

b.) R is a PID, so for any I of R, $I = (a)$ for some $a \in R$

Take any 2 elements $x,y \in I$, + note $x = ra$, $y = sa$ for some $r,s \in R$

$f(x,y) = f(ra,sa) = r f(a,sa) = rs \underbrace{f(a,a)}_{=0} = 0$

Then $f \equiv 0$ again as $f(x,y) = 0$ for any $x,y \in I$

$\boxed{F20}$

1. Prove that for any pair of commuting $n \times n$-matrices with complex entries there exists a common eigenvector.

A, B

Let x, λ be an eigenvector/eigenvalue pair for A, so $Ax = \lambda x$. Since A, B commute, $AB = BA$, so:

$$ABx = BAx = B\lambda x = \lambda Bx$$

$\Rightarrow ABx = \lambda Bx$, so Bx is an eigenvector of A

Since x + Bx are both in the eigenspace of A under λ
Thus B takes each eigenvector x to some other member of the eigenspace
Then each Bx is a lin combo of eigenbasis vectors
The restriction of $B|_{E_\lambda}$ (eigenspace of λ) must have an eigenvector, which is the common eigenvector of A + B ✓

2. Prove that there exists no simple group of order 56.

*RECALL: SUBGP OF ORDER p^α IS A SYLOW $\underline{\underline{P}}$-SUBGP

$|G| = 56 = 7 \times 8 = 7 \times 2^3$

Sylow $\Rightarrow \exists P_7 \in Syl_7(G)$ s.t. $n_7 \equiv 1 \bmod 7$, $n_7 \mid 8$ $\Rightarrow n_7 = 1$ or 8

$\exists P_2 \in Syl_2(G)$ s.t. $n_2 \equiv 1 \bmod 2$, $n_2 \mid 7$ $\Rightarrow n_2 = 1$ or 7

$\hookrightarrow |P_2| = 2^3$

If $n_7 = 1$, then $P_7 \trianglelefteq G$, so G not simple ✓

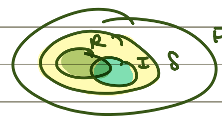
If $n_7 = 8$, then $\exists\, (7-1) \times 8 = 48$ elements of order 7 in G.
$\hookrightarrow$ not identity

Then there are $(56 - \underset{\text{id.}}{1}) - 48 = 7$ elements of order 2
$\hookrightarrow = (2^3 - 1)$ elements
$\Rightarrow n_2 = 1$, so $P_2 \trianglelefteq G$, so G is not simple ✓

Check-In: Why not consider n_2?
The Sylow 7-subgroups are all distinct as they intersect only trivially. But the Sylow 2-subgps of order 8 may not intersect trivially

3. Prove that a ring (S) which contains a principal ideal ring R, and which is contained in the field of fractions (F) of R, is a principal ideal ring.

PID $\subset R \subset$ Fracs(R)
Give things better names:
$R \subset S \subset F$ Given R a PID, WTS: S a PID



Let I be an ideal of S (WTS: principal)
Take $a \in I$. $I \subset F$, so $a \in F$ so $a = \frac{x}{y}$ for $x, y \in R$.
By def of an ideal, since $y \in R \subset S$, $y \in S$, and $ay = \frac{x}{y} \cdot y = x \in I$
$\hookrightarrow$ ideal of S, too!

The intersection of ideals is an ideal, so $I \cap R$ is an ideal, + is an ideal of R (and S)
Since R is a PID, $I \cap R = (r)$ for some $r \in R$. (WTS: $I = (r)$ in S)
Recall $x \in I$, but $x \in R$ by def., so $x \in I \cap R$. Then: $x = kr$ for some $k \in S$ (since $I \cap R = (r)$)

$$\Rightarrow \frac{x}{y} = \frac{k}{y} r$$

$$\Rightarrow a = \underbrace{\frac{k}{y}}_{\in F} r$$

Then any $a \in I$ is of form fr for $f \in F$,
so $I = (r)$ in F. Since $S \subset F$, $I = (r)$ in S, too. ✓

4. Let A and B be two projection linear maps in a vector space over a field K. Prove that if $A+B$ is a projection linear map and $char K \neq 2$ then $AB = BA = 0$.

CR: KAYLEE

A, B proj. linear maps $\Rightarrow A^2 = A$, $B^2 = B$

$A+B$ proj. $\Rightarrow A+B = (A+B)^2 = A^2 + AB + BA + B^2$

$= A + AB + BA + B$

$\cancel{A}+\cancel{B} = \cancel{A}+\cancel{B}+AB+BA$

$0 = AB + BA$

$AB = -BA$

But also: $AB = (A^2)B = A\underbrace{AB}_{=-BA} = -A\underbrace{BA}_{=BA} = BAA = BA^2 = BA$

$\Rightarrow AB = BA$

If $AB = BA$ AND $AB = -BA$, then $AB = BA = 0$ ✓

5. Prove that in the group $\mathbf{Q}/\mathbf{Z}$ for any natural number n there exists exactly one subgroup of order n.

$\mathbb{Q}/\mathbb{Z} = \{ p/q \mid p, q \in \mathbb{Z},\ |q| \nmid |p| \}$

Yugico's hint:

Existence: $\langle \frac{1}{n} \rangle$ has order n $\forall n \in \mathbb{N}$

and no ele of $\langle \frac{1}{n} \rangle$ is an integer except the identity, so $\langle \frac{1}{n} \rangle \leq \mathbb{Q}/\mathbb{Z}$

Then need $\langle \frac{1}{n} \rangle$ to be unique

AFSOC $\exists H \leq \mathbb{Q}/\mathbb{Z}$ w/ $H \neq \langle \frac{1}{n} \rangle$ & $|H| = n$ for some n

$\forall$ $p/q \in H$ w/ $|\frac{p}{q}| = n \Rightarrow n\frac{p}{q} = z \in \mathbb{Z}$

$\Rightarrow p/q = z/n$

Then for any $p/q \in H$, p/q is an integer multiple of $\frac{1}{n}$, so $H \leq \langle \frac{1}{n} \rangle$

Since $|H| = |\langle \frac{1}{n} \rangle| = n$

1. The following are four classes of commutative rings, in alphabetical order

- fields;
- integral domains (IDs);
- principal ideals domains (PIDs);
- unique factorization domains (UFDs).

These are contained in one-another, in some order, so that

$$A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq A_4.$$

(a) Determine the order;

(b) Give an example in each class to show that the inclusions are proper.

FEPUI!
pg. 292 in D+F

$\boxed{S21}$

a.) Fields $\subset$ PIDs $\subset$ UFDs $\subset$ IDs

b.) Field : $\mathbb{R}$
PID : $\mathbb{Z}$ no mult inverses
UFDs : $\mathbb{Z}[x]$ $(2, x)$ not principal ideal
IDs : $\mathbb{Z}[\sqrt{-5}]$ $(2-\sqrt{-5})(2+\sqrt{-5}) = 4-(-5) = 9$
But $3 \times 3 = 9$, so 9 has 2 factorizations into nonunits
Hence $\mathbb{Z}[\sqrt{-5}]$ not a UFD

2. (a) If R is a commutative ring, define what it means for R to be Noetherian and state Hilbert's basis theorem.

(b) Give an example of a non-Noetherian commutative ring.

a.) R is Noetherian if every ideal is finitely generated
alternatively, R is Noetherian if every ascending chain of ideals has a maximal element, i.e. if $I_1 \subset I_2 \subset I_3 \subset \ldots$ has some I_m s.t. $\forall n \geq m$, $I_n = I_m$

Hilbert's Basis Thm: If R is Noetherian, so is $R[x]$

b.) Example: $R[x_1, x_2, \ldots]$
Counterex: $R[x_1] \subset R[x_1, x_2] \subset R[x_1, x_2, x_3] \subset \ldots$
is an ascending chain of ideals w/o a maximal element

3. Let G be a group of order 105 and let P_3, P_5, and P_7 be Sylow 3, 5, and 7 subgroups, respectively. Assuming the Sylow theorems, prove the following:

(a) At least one of P_5 or P_7 is normal in G;

(b) G has a cyclic subgroup of order 35;

(c) Both P_5 and P_7 are normal in G.

$|G| = 105 = 3 \times 5 \times 7$
By Sylow Thms: $\exists P_3 \in Syl_3(G)$
$\exists P_5 \in Syl_5(G)$
$\exists P_7 \in Syl_7(G)$

a.) For $P_i \trianglelefteq G$, need $n_i = 1$
Note $n_i \equiv 1 \bmod i$ + $n_i \mid m$
So $n_5 \equiv 1 \bmod 5$, $n_5 \mid 3 \times 7 \Rightarrow n_5 = 1, 21$
$n_7 \equiv 1 \bmod 7$, $n_7 \mid 3 \times 5 \Rightarrow n_7 = 1, 15$
AFSOC neither $n_5, n_7 = 1$. Then $n_5 = 21$ and $n_7 = 15$.
$\left.\begin{array}{l}\text{Eles of order 5: } (5-1) \times 21 = 84 \\ \text{Eles of order 7: } (7-1) \times 15 = 90\end{array}\right\} \Rightarrow 84 + 90 = 174 > 105$
↳ ignore identity
Since eles of different orders are distinct, we obtain 174 elements in G, but this is more than $|G|$, so this can't be.
Thus at least one of n_5 or $n_7 = 1$, so at least one of P_5 or P_7 is normal in G

b.) By part (a.), one of P_5 or $P_7 \trianglelefteq G$. Both are subgps.
$|P_5| = 5$ + $|P_7| = 7$ are coprime, so $P_5 \times P_7 \cong \mathbb{Z}_{35}$ is a subgp, and is cyclic

$\boxed{\text{Note:}}$ $H, J \trianglelefteq G \Rightarrow$ (HJ subgp $\Leftrightarrow HJ = JH$)
$|HJ| = |H| \cdot |J| / |H \cap J|$

c.) WLOG, say $P_5 \trianglelefteq G$. Then quotient G/P_5 exists, and in fact $|G/P_5| = |G|/|P_5| = 105/5 = 21$
Let $G' = G/P_5$. Then $|G'| = 21 = 3 \times 7$, so by Sylow $\exists\, Q_7 \in Syl_7(G')$
$n_7 \equiv 1 \bmod 7$, $n_7 | 3 \Rightarrow n_7 = 1$
so $Q_7 \trianglelefteq G'$

Then $P_5 \times Q_7$ is a subgp of G of order $5 \times 7 = 35$
In fact, since $P_5 \trianglelefteq G$ and $Q_7 \trianglelefteq G/P_5$, $P_5 \times Q_7 \trianglelefteq G$
By part (b.), $N = P_5 \times Q_7$ is cyclic
Then $P_7 \trianglelefteq N \trianglelefteq G \Rightarrow P_7 \trianglelefteq G$ ✓

4. Find all similarity classes of 2×2 matrices A with entries in $\mathbb{Q}$ satisfying $A^4 = I$. What are the corresponding rational canonical forms?

$x^4 = 1 \Rightarrow x^4 - 1 = 0$ can have only entries in $\mathbb{Q}$
$(x^2-1)(x^2+1) = 0$
$(x+1)(x-1)(x^2+1) = 0$

monic which divides char poly ($x^4 - 1 = 0$)
This divides the char poly

min poly	invar factors	RCF	
$x-1$	$x-1$	$[1]$	
$x+1$	$x+1$	$[-1]$	
x^2+1	x^2+1	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$x^2 \; x^1$
$(x-1)(x+1) = x^2 - 1$	$(x-1), (x+1)$	$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$x^2 \; x^{-1}$

5. (a) Find the possible Jordan Canonical Forms of any matrix such that $A^4 = I$ over $F = \mathbb{F}_5$.
(b) Give an example of a matrix B over $F = \mathbb{F}_3$ satisfying $B^4 = I$, such that B is not diagonalizable.

a.) $x^4 = 1 \Rightarrow x^4 - 1 = 0$
$(x^2-1)(x^2+1) = 0$
$(x+1)(x-1)(x^2+1) = 0$ In $\mathbb{F}_5$, $x^2 + 1 = x^2 - 4$
$(x+1)(x-1)(x+2)(x-2) = 0$ $= (x+2)(x-2)$
* Since the char poly splits into linear factors, the matrix is diagonalizable, so all Jordan blocks are diagonal. Then we have all possible Jordan blocks + hence all JCFs

b.) In $\mathbb{F}_3$: $x^4 = 1 \Rightarrow x^4 - 1 = 0$
$(x^2-1)(x^2+1) = 0$
$(x+1)(x-1)(x^2+1) = 0$
companion matrix
Consider the invar factor $x^2 + 1$ above, then the companion matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $x^2 \; x^1$
+ $[1], [-1]$
This block has eigenvalues $\pm 1, \pm i$
not in $\mathbb{F}_3$, so blocks are not all diagonal, so the entire matrix is not diagonalizable

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

1. Let G be a group and $Z(G)$ the center of G. a.) Show that the group $G/Z(G)$ does not have prime order. b.) Find a group G such that $G/Z(G)$ has 4 elements.

$\boxed{721}$

a.) <u>WTS:</u> $|G/Z(G)| \neq p$

AFSOC $|G/Z(G)| = p$. Recall if $|H| = p$, $H \cong \mathbb{Z}_p$, so H is cyclic

If $G/Z(G)$ is cyclic, then $G/Z(G) = \langle gZ(G) \rangle$ for some $g \in G \setminus Z(G)$

Then any $hZ(G) \in G/Z(G)$ written as $hZ(G) = (gZ(G))^k = \underbrace{gZ(G) \cdot gZ(G) \cdot \ldots \cdot gZ(G)}_{k \text{ times}} = g^k Z(G)$ stays in coset

commutes w/ all!

<u>Note:</u> a, b in the same coset of H iff $b^{-1}a \in H$
$aH = bH \Leftrightarrow b^{-1}aH = H$

Recall that $Z(G) \trianglelefteq G$. Then if $hZ(G) = g^k Z(G)$, $h + g^k$ are in the same coset of $Z(G)$, so $(g^k)^{-1} h \in Z(G)$

$\Rightarrow \exists z \in Z(G)$ s.t. $z = (g^k)^{-1} h \Rightarrow g^k z = h$

This is true for any $h \in G/Z(G)$, so taking $h_1, h_2 \in G/Z(G)$ gives

$$\left.\begin{array}{l} h_1 = z_1 g^{k_1} \\ h_2 = z_2 g^{k_2} \end{array}\right\} \begin{aligned} h_1 h_2 &= z_1 g^{k_1} \cdot z_2 g^{k_2} \\ &= g^{k_1} g^{k_2} z_1 z_2 \\ &= g^{k_1+k_2} z_1 z_2 \\ &= g^{k_1+k_2} z_2 z_1 \\ &= g^{k_2} g^{k_1} z_2 z_1 \\ &= g^{k_2} z_2 g^{k_1} z_1 \\ &= h_2 h_1 \end{aligned}$$

$z_1, z_2 \in Z(G)$, so commute w/ everything

Then any 2 eles of $G/Z(G)$ commute, so $G/Z(G)$ is abelian
But this means that $G = Z(G)$, so $G/Z(G) = 1$ ↯ not prime order!

<u>Conclusion:</u> $G/Z(G)$ cyclic $\Rightarrow G$ abelian

b.) Example where $|G/Z(G)| = 4 \Rightarrow$ 4 cosets of $Z(G)$

$D_4 = \langle r, f \mid r^4 = f^2 = 1, rf = fr^3 \rangle$

Cosets: $\{1, r^2\}$ $\{f, r^2 f\}$
$\{r, r^3\}$ $\{rf, r^3 f\}$

Recall cosets of $Z(G)$ partition G since $Z(G) \trianglelefteq G$

2. Show that every prime ideal P in $\mathbf{Z}[x]$ which is not principal contains a prime number

Let f, g be distinct irred elements of $\mathbb{Z}[x]$
Then $\gcd(f, g) = 1 \subseteq \mathbb{Q}[x]$

By Bezout's Lemma: $\exists n \in \mathbb{Z}$ s.t. $(nf, ng) = (n) \subseteq \mathbb{Z}[x]$
Thus $(n) \subseteq P$ + since P is a prime ideal, there must be some prime dividing n contained in (n)

3. Show that every finite noncyclic group is a finite union of proper subgroups, and that if a group maps surjectively to a finite noncyclic group then it is a finite union of proper subgroups and use this to determine for which positive integers the product of n copies of the integers is a finite union of proper subgroups.

a.) Let G be a finite noncyclic gp. (WTS: $G = \bigcup_{i=1}^{N} H_i$ for $H_i < G$ $\forall i$)
Take $g \in G$. Since G not cyclic, $\langle g \rangle \neq G$, so $\langle g \rangle < G$.
Then $G = \bigcup_{g \in G} \langle g \rangle$ since $h \in \bigcup_{g\in G} \langle g \rangle$ for any $h \in G$, and union is finite since $|G|$ finite

b.) Let $\varphi: G' \to G$ be a surj group ~~map~~ homomorphism to finite, noncyclic G.
Since φ is surj, $\forall g \in G$, $\exists h \in G'$ s.t. $\varphi(h) = g$.
$\varphi^{-1}(g) = \{h \in G' \mid \varphi(h) = g\} \neq \emptyset$ (WTS: $\varphi^{-1}(\langle g \rangle) < G'$)
$1 \in \langle g \rangle$ by definition, so $\varphi^{-1}(\langle g \rangle) \ni 1_{G'}$ by def of homo. φ
If $k \in \langle g \rangle \Rightarrow k = g^m$ for some m
Then $k^{-1} = g^{n-m}$ if $g^n = 1$. Since $g^{n-m} \in \langle g \rangle$, $k^{-1} \in \langle g \rangle$
By φ homo, $\varphi^{-1}(k), \varphi^{-1}(k^{-1}) \in \varphi^{-1}(\langle g \rangle)$
Then for any $g \in G$, $\varphi^{-1}(\langle g \rangle)$ is a subgp. of G'
additionally, since $\langle g \rangle < G$, $\varphi^{-1}(\langle g \rangle) < G'$ (φ is a function, so one element cannot map to more than one thing)

also, since φ is a homo., $\langle \varphi^{-1}(g) \rangle = \varphi^{-1}(\langle g \rangle)$
Then $G' = \bigcup_{i=1}^{N} J_i$ for $J_i = \langle \varphi^{-1}(g) \rangle < G'$
↳ $g \in G$, finite # of them

c.) For what $n \in \mathbb{Z}^+$ is $\mathbb{Z}^n$ ($= \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n \text{ times}}$) a finite union of proper subgps?
A: whenever $\mathbb{Z}^n$ is not cyclic
$\mathbb{Z}^1$ cyclic, so won't work (gen by 1 ele.)
But any $\mathbb{Z}^n$ for $n \geq 2$ has $\Phi: \mathbb{Z}^n \to G$, then employ part (b.)
↳ noncyclic finite

$\boxed{\text{e.g.}}$ $\mathbb{Z}^2 = \langle (0,1) \rangle \times \langle (1,0) \rangle$
$\Phi: \mathbb{Z}^2 \to G$
$(0,1), (1,0) \mapsto g_1$
$\vdots$
$(0,N), (N,0) \mapsto g_N$

In general: $\mathbb{Z}^n = \langle (1,0,\ldots,0) \rangle \times \langle (0,1,\ldots,0) \rangle \times \ldots \times \langle (0,0,\ldots,1) \rangle$
$(1,0,\ldots,0), \ldots, (0,\ldots,0,1) \mapsto g_1$
$\vdots$
$(N,0,\ldots,0), \ldots, (0,\ldots,0,N) \mapsto g_N$

Then $\varphi((N+1,0)) = \varphi((N,0)) + \varphi((1,0))$
etc.
?

4. Let A and B be two square matrices over a field F. Suppose $diag(A, A)$ and $diag(B, B)$ are similar. Show that A and B are similar.

assume $\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \sim \begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix}$.

Two matrices similar iff they have the same JCF, so consider the invariant factors of A + B as follows:
$a_1(x), a_2(x), \ldots, a_n(x)$ and $b_1(x), b_2(x), \ldots, b_m(x)$
Then the companion matrices of A + B respectively are:
$C_{a_1}, C_{a_2}, \ldots, C_{a_n}$ and $C_{b_1}, C_{b_2}, \ldots, C_{b_m}$

$$\Rightarrow A \sim \begin{bmatrix} C_{a_1} & & & \\ & C_{a_2} & & \\ & & \ddots & \\ & & & C_{a_n} \end{bmatrix} + B \sim \begin{bmatrix} C_{b_1} & & & \\ & C_{b_2} & & \\ & & \ddots & \\ & & & C_{b_m} \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \sim \begin{bmatrix} C_{a_1} & & & & & 0 \\ & \ddots & & & & \\ & & C_{a_n} & & & \\ & & & C_{a_1} & & \\ & & & & \ddots & \\ 0 & & & & & C_{a_n} \end{bmatrix} + \begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix} \sim \begin{bmatrix} C_{b_1} & & & & & 0 \\ & \ddots & & & & \\ & & C_{b_m} & & & \\ & & & C_{b_1} & & \\ & & & & \ddots & \\ 0 & & & & & C_{b_m} \end{bmatrix}$$

$$= \begin{bmatrix} C_{a_1} & & & & 0 \\ & C_{a_1} & & & \\ & & \ddots & & \\ & & & C_{a_n} & \\ 0 & & & & C_{a_n} \end{bmatrix} \qquad = \begin{bmatrix} C_{b_1} & & & & 0 \\ & C_{b_1} & & & \\ & & \ddots & & \\ & & & C_{b_m} & \\ 0 & & & & C_{b_m} \end{bmatrix}$$

By def of invar factors:
$a_1(x) \mid a_2(x) \mid \ldots \mid a_n(x)$
$b_1(x) \mid b_2(x) \mid \ldots \mid b_m(x)$
also
$a_1(x) \mid a_1(x) \mid \ldots \mid a_n(x) \mid a_n(x)$
$b_1(x) \mid b_1(x) \mid \ldots \mid b_m(x) \mid b_m(x)$
Then
$$\left.\begin{matrix} a_1(x), a_1(x), \ldots, a_n(x), a_n(x) \\ b_1(x), b_1(x), \ldots, b_m(x), b_m(x) \end{matrix}\right\} \text{invar factors of } \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} + \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} \text{ resp.}$$
Since $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \sim \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}$, conclude that $n = m$
so $a_i(x) = b_i(x)$ $\forall i$
$\Rightarrow$ Then $A \sim B$ ✓

5.

(A) Suppose that p and q are distinct primes and a group G is generated by elements of order p and also by elements of order q. Show that any homomorphism of G to an abelian group is trivial.

(B) Show that for $n \geq 5$ the alternating group A_n of even permutations of n obhjects is generated by elements of order 2, and also by elements of order 3, so that for such n the only homomorphisms to abelian groups are trivial.

→ even # of transpos.

a.) $G = \langle a_1, \dots, a_n, b_1, \dots, b_m \mid a_i^p = b_j^q = 1 \ \forall i \in [1,n], j \in [1,m] \rangle$

If G nonabelian then any $\phi: G \to H$ where H abelian must be trivial since if h_1, h_2 commute in H, then $\phi^{-1}(h_1), \phi^{-1}(h_2)$ must commute in G. (g_1, g_2)

In abelian gp, everything commutes w/ everything, so if g_1, g_2 do not commute, they cannot map to nontrivial elements in H.

There seems to be a typo in this problem. Not sure what it's trying to ask, but here's a counterexample:
$G = \mathbb{Z}_3 \times \mathbb{Z}_5 = \langle a, b \mid a^3 = b^5 = 1 \rangle$
cyclic, so abelian, and $\phi: \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$ is not trivial

b.) $s \in S_n$ has order = lcm of cycle lengths
⇒ order 2 means products of disjoint transpositions
⇒ order 3 means products of 3 cycles

WTS: any s = even # transpos. can be written as product of

Case 1: If all of the even transpos are distinct, then s is an element of order 2, hence generated by eles of order 2 ✓

Case 2: some subset not disjoint. Then compose 2 overlapping transpos to get a 3-cycle. Then any non-overlapping (hence disjt) transpos are left behind, so s is a product of distinct transpos (have order 2) + 3-cycles (have order 3)

$\boxed{\text{e.g.}}$ $(ab)(bc) = (abc)$
$(ab)(bc)(ca) = (abc)(ca)$

⇒ any $s \in A_n$ can be written as product of eles of orders 2 & 3, so can be generated by eles of these orders

Then by part (a.), any $\phi: A_n \to G$ for G abelian is trivial

1. Prove that the rings $\mathbb{Q}[x]/\langle x^2-1\rangle$ and $\mathbb{Q}\oplus\mathbb{Q}$ are isomorphic.

S22

Define map $\varphi: \mathbb{Q}[x] \to \mathbb{Q}\oplus\mathbb{Q}$
↳ Idea: Get $\langle x^2-1\rangle = \ker\varphi$, then use First Iso Thm
$\varphi: \mathbb{Q}[x] \to \mathbb{Q}\oplus\mathbb{Q}$
$x \mapsto -1$
So $\mathbb{Q}[x]/\langle x^2-1\rangle \cong \mathbb{Q}\oplus\mathbb{Q}$ as desired
Then $(x^2-1) \mapsto 0$ as desired

alt: $I=(x+1)$, $J=(x-1)$ $\Rightarrow I\cap J = (x^2-1)$
By Chinese Rem Thm: $\mathbb{Q}[x]/I\cap J \cong \mathbb{Q}[x]/I \oplus \mathbb{Q}[x]/J \cong \mathbb{Q}\oplus\mathbb{Q}$
$\mathbb{Q}[x]/(x+1)$
↳ $x+1 \mapsto 0 \Rightarrow x\mapsto -1$
so $\mathbb{Q}[x]/(x+1) \cong \mathbb{Q}$
$\mathbb{Q}[x]/(x-1)$
↳ $x-1\mapsto 0 \Rightarrow x\mapsto 1$
so $\mathbb{Q}[x]/(x-1) \cong \mathbb{Q}$

2. Let p be a prime. Show that any element of order p in $GL_2(\mathbb{Z}/p\mathbb{Z})$ can be conjugated to the matrix $\begin{pmatrix}1&1\\0&1\end{pmatrix}$. *Hint*: You may consider the p-Sylow subgroups of $GL_2(\mathbb{Z}/p\mathbb{Z})$.

$|GL_2(\mathbb{Z}_p)| = ???$ (Need decomp to use Sylow)
General linear = invertible $\Rightarrow$ cols lin ind.
For $\begin{bmatrix}a&c\\b&d\end{bmatrix}$:

- $\begin{bmatrix}a\\b\end{bmatrix}$ has $\underbrace{\binom{p}{1}}_{a}\underbrace{\binom{p}{1}}_{b}$ choices, but can't have $\binom{0}{0}$, so $\binom{p}{1}\binom{p}{1}-1 = p^2-1$ choices
- $\begin{bmatrix}c\\d\end{bmatrix}$ has $\underbrace{\binom{p}{1}}_{c}\underbrace{\binom{p}{1}}_{d}$ choices, but can't take any multiple $n\begin{bmatrix}a\\b\end{bmatrix}$ for $n\in[0,p-1]$
so $\binom{p}{1}\binom{p}{1} - p = p^2-p$ choices
↳ p possible values of n

↳ Then $|GL_2(\mathbb{Z}_p)| = (p^2-1)(p^2-p) = p(p^2-1)(p-1)$
↳ $p \mid |GL_2(\mathbb{Z}_p)|$, so $\exists P\in Syl_p(GL_2(\mathbb{Z}_p))$
Then $P\cong \mathbb{Z}_p$

- all Sylow p-subgps are conjugate
- any ele of order p gen a Sylow p-subgp

If $K\in GL_2(\mathbb{Z}_p)$ w/ $|K|=p$, then $\langle K\rangle$ is a Sylow p-subgp, + $\langle K\rangle$ is conj. to any other p-subgp.
$\begin{pmatrix}1&1\\0&1\end{pmatrix}$ is an ele of order p:
$\begin{pmatrix}1&1\\0&1\end{pmatrix}^n = \begin{pmatrix}1&n\\0&1\end{pmatrix} \Rightarrow \begin{pmatrix}1&1\\0&1\end{pmatrix}^p = \begin{pmatrix}1&p\\0&1\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix}$
Then $\langle K\rangle$ conj. to $\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\rangle$
Then K conj to $\begin{pmatrix}1&n\\0&1\end{pmatrix}$ for some n

<u>WTS</u>: $K\sim\begin{pmatrix}1&1\\0&1\end{pmatrix}$
Know already $K\sim\begin{pmatrix}1&n\\0&1\end{pmatrix}$, to get $K\sim\begin{pmatrix}1&1\\0&1\end{pmatrix}$ show $\begin{pmatrix}1&n\\0&1\end{pmatrix}\sim\begin{pmatrix}1&1\\0&1\end{pmatrix}$
conj matrices:
$A = P^{-1}BP \Rightarrow PA = BP$
Find P s.t. $P\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}1&n\\0&1\end{pmatrix}P$

Eventually get $\begin{pmatrix}n&n\\0&1\end{pmatrix}$ ✓

Then $K\sim\begin{pmatrix}1&1\\0&1\end{pmatrix}$ as desired!

3. Let a and b be elements of a field of order 2^n where n is odd. Prove that if $a^2+ab+b^2=0$ then $a=b=0$.

let $a^2+ab+b^2=0$, AFSOC $b\neq 0$.
Then we can divide by b & see what breaks!
$\frac{a^2}{b^2}+\frac{a}{b}+1=0$
let $\frac{a}{b}=c$, then $c^2+c+1=0$
$\Rightarrow$ c is a root of x^2+x+1
$\Rightarrow$ c is a root of $(x^2+x+1)(x-1)=x^3-1$
$\Rightarrow c^3=(\frac{a}{b})^3=1$
$\Rightarrow a^3=b^3 \Rightarrow a=b$

$a^2+ab+b^2=0$
$a^2+a^2+a^2=0$
$3a^2=0$
$a^2=0$
But $a=b$, so $a=b=0$

Not necessarily true in field w/ some char.

alt: $c^3=(\frac{a}{b})^3=1$, and $c\in F_{2^n}$
By def, for F, $\underbrace{F\setminus\{0\}}_{=F^\times}$ is a group under mult.

In F, $2^n(x)=0$. But in $F^\times$, $x^{2^n-1}=1$
↳ $F^\times$ cyclic, & $F^\times$ has $2^n-\underbrace{1}_{\{0\}}$ elements, so each element has order 2^n-1 in $F^\times$

$c^3=1 \Rightarrow 3\mid 2^n-1$ since $c^{2^n-1}=1$, too
$3\mid 2^n-1 \Rightarrow 2^n\equiv 1 \bmod 3$, but this can't happen if n is odd ↯
n odd $\Rightarrow n=2k+1$
$2^n=2^{2k+1}=2^{2k}\cdot\underbrace{2}_{=-1 \bmod 3}=-1\cdot 2^{2k}=-1\cdot\underbrace{4^k}_{\text{any power of 4 is 1 mod 3}}=-1\cdot 1=-1 \bmod 3 \neq 1 \bmod 3$ ✓

check on this

4. Let A, B be linear operators on a nonzero finite-dimensional vector space V over $\mathbb{C}$ such that $A^2=B^2=\mathrm{Id}$. Prove that there exists a nonzero subspace W of V which is invariant under A and B and $\dim W\leq 2$.

Invariant: $Aw\in W$ $\forall w\in W$
$Bw\in W$

One thing to notice:
If $w, Aw\in W$, then
$A\cdot w\in W$
$A\cdot Aw=Iw\in W$

Then need:
$Bw \in W$?
$B(Aw)\in W$?

$A^2=B^2=I$
$\Rightarrow \lambda^2=1$
$\Rightarrow \lambda=\pm 1 \quad \forall\lambda$

exists since A & B each have nonzero eigenvector
let w be eigenvector of BA
CL: Build $W=\{w, Aw\}$
Invar under A ✓

These are 2 lin ind eles of W, & there can't be anything else in W ind of (x, Ax), so $\dim W\leq 2$ by construction

WTS: Invar under B
$\Rightarrow$ w is an eigenvector of BA
$BAw=\lambda w$ $\quad B(Aw)\in W$
Remains to show $Bw\in W$
$BBAw=\lambda Bw$
$Aw=\lambda Bw$ $\Rightarrow Aw=\pm Bw$
$w=Iw=AAw$ $\quad$ since $Aw\in W$, $Bw\in W$ ✓ (?)
$=A\lambda Bw$
$=\lambda ABw$ $\Rightarrow w=\pm ABw$

5. Let A be a complex $n \times n$ matrix. Let a_k denote the dimension of the null space of A^k (in particular, $a_0 = 0$). Prove that $a_k + a_{k+2} \le 2a_{k+1}$ for all $k \ge 0$.

Given $a_0 = 0$.

Note $\ker(A) \subseteq \ker(AB)$. So $\ker(A^k) \subseteq \ker(A^{k+1})$ and in fact $\ker(A^k) \subseteq \ker(A^{k+j})$

Then $\text{nullity}(A^k) \le \text{nullity}(A^{k+j})$ $\forall j \ge 0$

↳ = dim(nullspace)

$a_k + a_{k+2} \le 2a_{k-1}$

$\Leftrightarrow a_k - a_{k+1} + a_{k+2} - a_{k+1} \le 0$

since $a_k \le a_{k+1}$ and $a_{k+1} \le a_{k+2}$ by the above argument, then

$a_{k+1} - a_k \le 0$ $\quad a_{k+2} - a_{k+1} \ge 0$

For $\underbrace{(a_k - a_{k+1})}_{\le 0} + \underbrace{(a_{k+2} - a_{k+1})}_{\ge 0} \le 0$, need $|a_{k+2} - a_{k+1}| \le |a_k - a_{k+1}|$

$\dim(A) = \text{rank}(A) + \text{null}(A)$

$\dim(A) = \dim(A^k)$ $\forall k$

The decrease in rank from A^k to A^{k+1} must be nonincreasing.

Then increase in nullity must be nonincreasing, hence

$a_{k+1} - a_k \ge a_{k+2} - a_{k+1}$

precisely as desired.

1. Let G be a finite simple group. Prove that $G \times G$ has exactly 4 normal subgroups (including $G \times G$) if and only if G is non-abelian.

$\boxed{722}$

G finite, simple (only normal subgps are 1 + itself)

Note that 1×1, $G \times 1$, $1 \times G$, and $G \times G$ are all normal subgps of $G \times G$

($\Rightarrow$) By contrapos: G abelian $\Rightarrow$ there are not 4 subgps.

Know from above that there are at least 4 subgps of $G \times G$, so WTS: more than 4

Assume G is abelian. Then $gh = hg$ $\forall g, h \in G$, so $ghg^{-1} = h$. Let $g \neq 1$.

Then (g, g) is a normal subgp of $G \times G$, but $(g, g) \neq 1 \times 1, G \times 1, 1 \times G$, or $G \times G$.

Hence there are more than 4 subgps of $G \times G$

($\Leftarrow$) Assume that G is nonabelian. WTS: the aforementioned subgps are the only subgps of $G \times G$.

AFSOC $\exists N \trianglelefteq G \times G$ s.t. $N \neq 1$. Then $\exists (a, b) \in N$ s.t. at least one of $a, b \neq 1$. Assume $a \neq 1$. Then, since G nonabelian, $\exists g \in G$ s.t. $ga \neq ag$, so $gag^{-1} \neq a$ and $gag^{-1}a^{-1} \neq 1$.

Then $(g, 1)(a, 1)(g^{-1}, 1) = (gag^{-1}, 1) \neq (1, 1)$

$(g, 1)(a, b)(g^{-1}, 1) = (gag^{-1}, b) \in N$ since N normal (conj. stays in N)

$\underbrace{(gag^{-1}, b)}_{\in N}\underbrace{(a^{-1}, b^{-1})}_{\in N \text{ as inverse of } (a,b)} = (gag^{-1}a^{-1}, 1) \in N$ since N closed

$\rightarrow$ note $gag^{-1}a^{-1} \neq 1$

Then for any $h \in G$:

$(h, 1)(gag^{-1}a^{-1}, 1)(h^{-1}, 1) = (hgag^{-1}a^{-1}h^{-1}, 1) \in N$

Since conj. of $gag^{-1}a^{-1}$ generates all of G, we see that $G \times 1 \leq N$.

Similarly, if $b \neq 1$ then $1 \times G \leq N$.

If $b = 1$ $\forall (a, b) \in N$, then $N = G \times 1$

If $a = 1$ $\forall (a, b) \in N$, then $N = 1 \times G$

If $\exists (a, b) \in N$ s.t. $a \neq 1$, then $G \times 1 \leq N$

and if $\exists (c, d) \in N$ s.t. $b \neq 1$, then $1 \times G \leq N$

so $(G \times 1) \times (1 \times G) = G \times G \leq N \Rightarrow N = G \times G$

$\hookrightarrow$ Then if N normal + nontrivial, it is one of the normal subgps we have already accounted for. Hence the 4 normal subgps above are the only normal subgps of $G \times G$.

2. Let R be a principal ideal domain and I and J be ideals of R. Show that $I \cap J = IJ$ holds if and only if $I = 0$ or $J = 0$ or $I + J = R$.

$I \cap J = \{a \mid a \in I, a \in J\}$

$IJ = \{\Sigma_i^n a_i b_i \mid a_i \in I, b_i \in J\}$

Note: $IJ \subseteq I \cap J$ always

$a \in I, r \in R \Rightarrow ra \in I$ Then $a_i b_j \in I$ $\forall b_j \in J$

+ I closed under (+) so $\Sigma a_i b_j \in I$ (same for J)

Hence $IJ \subseteq I \cap J$

($\Rightarrow$) Let $I \cap J = IJ$. Recall $IJ \subseteq I \cap J$ ALWAYS!

$I = (a)$ + $J = (b)$ (PID) ASSUMES NONZERO IDEALS!

$I + J = (a) + (b) = \{a^n + b^m\}$

ideal $I + J = (c)$ w/ $c = (\gcd(a, b))$

$I \cap J = (d)$ w/ $d = (\mathrm{lcm}(a, b))$

$IJ = (a)(b) \Rightarrow IJ = (ab)$

(*) $I + J \subseteq R$ (ideal)

Need to show $R \subseteq I + J$

Since $IJ = I \cap J$, $(ab) = (\mathrm{lcm}(a, b))$

$\Rightarrow a \cdot b = \mathrm{lcm}(a, b)$ so a + b are coprime

Then $\gcd(a, b) = 1$, so $I + J = (1)$

Then $\forall r \in R$, $r \cdot 1 = r \in I + J$ ✓

Q.E.D.

($\Leftarrow$) $I = 0$ or $J = 0$ or $I + J = R$

- $I = 0 \Rightarrow I \cap J = 0$

Note $IJ \subseteq I \cap J$, so $IJ = 0$

Then $I \cap J = IJ$. Same if $J = 0$.

- If $I + J = R$ then $r = a + b$ $\substack{a \in I \\ b \in J}$ $\forall r \in R$

I ideal, so $x \in I$, $r \in R \Rightarrow xr \in I$

$xr = x(a + b) = xa + xb$

Recall $IJ \subseteq I \cap J$, so just need $I \cap J \subseteq IJ$

$x \in I \cap J \Rightarrow x \in I$, $x \in J$, $x \in R$ so $x = a_0 + b_0$

Then every $x \in I \cap J$ is a lin combo of $a_0 \in I$, $b_0 \in J$

Hence $x \in IJ$. Then $I \cap J \subseteq IJ$ ✓

3. Let $A \in M_n(\mathbb{R})$ be a symmetric matrix with real coefficients. Show that all eigenvalues of A are non-negative if and only if $A = P^T P$ for some matrix $P \in M_n(\mathbb{R})$.

($\Rightarrow$) assume all $\lambda \geq 0$ for symmetric A.
Then we can write $A = QDQ^{-1}$ for D diagonal w/ λ's down diag.
Since all λ's are nonneg, then main diag entries are nonneg, so we define

$$D' = \begin{bmatrix} \sqrt{\lambda_1} & & & \\ & \sqrt{\lambda_2} & & \\ & & \ddots & \\ & & & \sqrt{\lambda_n} \end{bmatrix} \quad \text{when } D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

since diag matrix, $D' = (D')^T$

Then $A = QDQ^T = Q(D')^2Q^T = QD' \cdot D'Q^T = \underbrace{QD'}_{=P} \cdot \underbrace{(D')^T Q^T}_{=P^T}$

Hence $A = PP^T$ for $P \in M_n(\mathbb{R})$ ✓

($\Leftarrow$) assume symmetric A can be written as $A = P^T P$ for $P \in M_n(\mathbb{R})$ (conj. transpose)
Then $A = P^+ P$. Let λ, x be an eigenvalue/eigenvector pair for A. Then:

$Ax = \lambda x$ $\quad$ $x^+ Ax = x^+ \lambda x = \lambda x^+ x = \lambda \|x\|^2$

$\Rightarrow P^+ P x = \lambda x$ $\quad$ $x^+ P^+ P x = (Px)^+ Px = \|Px\|^2 \geq 0$ $\quad$ ≥ 0 (by def of norm)

$x^+ A x = x^+ P^+ P x \Rightarrow \underbrace{\lambda \|x\|^2}_{\geq 0} = \underbrace{\|Px\|^2}_{\geq 0}$

Then $\lambda \geq 0$ as well. True for any λ of A, so all eigenvals of A are nonneg.

4. Let R be an integral domain and $R[x,y,z]$ the polynomial ring in three variables over R. Show that $I = \langle x^3 - y^2, y^3 - z^2 \rangle \subset R[x,y,z]$ is a prime ideal. Hint: Show that I is the kernel of a ring homomorphism $R[x,y,z] \to R[t]$.

$\varphi : R[x,y,z] \to R[t]$

For $I = \langle x^3 - y^2, y^3 - z^2 \rangle$ to be the kernel, need:

$x^3 - y^2 \mapsto 0$ $\quad$ Then define: $\varphi(x) = t^a$ $\quad$ $t^{3a} - t^{2b} = 0$ $\quad$ $3a - 2b = 0$ $\quad \Rightarrow$ $a = 4$

$y^3 - z^2 \mapsto 0$ $\quad$ $\varphi(y) = t^b$ $\quad$ $t^{3b} - t^{2c} = 0$ $\quad$ $3b - 2c = 0$ $\quad$ $b = 6$

$\varphi(z) = t^c$ $\quad$ $c = 9$

Then $\varphi : R[x,y,z] \to R[t]$

$x \mapsto t^4$

$y \mapsto t^6$

$z \mapsto t^9$

Note: clearly $I \subseteq \operatorname{Ker} \varphi$ since $x^3 - y^2, y^3 - z^2 \mapsto 0$
But $\operatorname{Ker} \varphi \subseteq I$ as well since R is an ID, so no nonzero elements of R can map to 0 under a homomorphism

By First Iso Thm: $G/\operatorname{Ker} \varphi \cong \operatorname{Im} \varphi$
So $R[x,y,z]/I \cong R[t]$

Since R is an ID, so is $R[t]$ (ID is preserved by poly rings)
an ideal I of R is prime iff R/I is an ID.
Because $R[x,y,z]/I \cong R[t]$ is an ID, I is prime! ✓

5. Let A and B be commuting complex matrices. Assume that $B \notin \mathbb{C}[A]$, that is, B cannot be written as a polynomial in A. Show that some eigenspace of A has dimension at least two.

→ set of eigenvectors assoc. w/ an eigenvalue

Proof: Let x, λ be an eigenpair for A. Then $Ax = \lambda x$.
A, B commute, so $AB = BA$. Then: $ABx = BAx$
$= B\lambda x$
$= \lambda Bx$

So $Ax = \lambda x$
$A(Bx) = \lambda(Bx)$
Hence Bx is also an eigenvector of A for eigenvalue λ

Since $B \notin \mathbb{C}[A]$, we have $B \neq C_n A^n + \dots + C_1 A + C_0$

If $B \in \mathbb{C}[A]$, then

$$B = C_n A^n + \dots + C_1 A + C_0$$

$$Bx = C_n A^n x + \dots + C_1 A x + C_0 x$$

$$= C_n A^{n-1} \lambda x + \dots + C_1 \lambda x + C_0 x$$

$$\vdots$$

$$= C_n \lambda^n x + \dots + C_1 \lambda x + C_0 x$$

so Bx is not actually a new eigenvector in the eigenspace, it is a lin combo of x's

Then, the fact that $B \notin \mathbb{C}[A]$ tells us that Bx and x are distinct eigenvectors for the same eigenvalue λ, so the eigenspace of A for λ has dimension at least 2

↳ has 2 lin ind elements!

S23

1. Classify all groups of order 309, up to isomorphism.

$309 = 3 \cdot 103$

By Sylow 1, $\exists P \in Syl_3(G)$ & $\exists Q \in Syl_{103}(G)$

By Sylow 3, $n_p \equiv 1 \mod p$ and $n_p \mid m$

$n_3 \equiv 1 \mod 3$ & $n_3 \mid 103 \Rightarrow n_3 = 1$ or 103

$n_{103} \equiv 1 \mod 103$ & $n_{103} \mid 3 \Rightarrow n_{103} = 1$

If $n_3 = n_{103} = 1$,
each of P & Q are unique Sylow p-subgps, so both are normal in G.
Then $|P||Q| = |PQ|$ so $PQ \cong G$. Since P, Q both normal,
$3 \cdot 103 = 309$ $\quad P \times Q \cong PQ$, and $|P| = 3 \Rightarrow P \cong \mathbb{Z}_3$
$|Q| = 103 \Rightarrow Q \cong \mathbb{Z}_{103}$

Thus $G \cong \mathbb{Z}_3 \times \mathbb{Z}_{103} \cong \mathbb{Z}_{309}$ since $3, 103$ coprime

If $n_3 = 103$, $n_{103} = 1$, then $G \cong P_{103} \rtimes P_3$, $\Rightarrow \exists$ homo $\phi: P_3 \to Aut(P_{103})$

If ϕ trivial, same as above case: $G \cong P_{103} \rtimes P_3 \cong P_{103} \times P_3 \cong \mathbb{Z}_{103} \times \mathbb{Z}_3 \cong \mathbb{Z}_{309}$

If ϕ nontrivial, then $G \cong \langle x, y \mid x^3 = 1 = y^{103},\ xy = y^m x$ for $m^3 \equiv 1 \mod 103 \rangle$

2. Let A be the abelian group with generators x, y, z and the relations

$$4x + 3y + z = 0, \quad x + 2y + 3z = 0, \quad 3x + 2y + 5z = 0$$

Show that A is a cyclic abelian group, and determine its order.

Smith Normal Form again?

$\hookrightarrow$ all gen by one ele $\rightarrow$ put generators in terms of each other

$A = \langle x, y, z \rangle$

$4x + 3y + z = 0$
$x + 2y + 3z = 0$
$3x + 2y + 5z = 0$

$$\begin{bmatrix} 4 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 2 & 5 \end{bmatrix}$$

HELP!

3. Let A be a complex $n \times n$ matrix. Prove that there is an invertible complex $n \times n$ matrix B such that $AB = BA^t$. (A^t is the transpose of A.)

Jordan Block Problem

$AB = BA^T \Rightarrow A^T = B^{-1}AB$ (means A & A^T similar)

Two matrices similar iff they have the same JCF

matrix facts (from Kaylee)

$B_n = \begin{pmatrix} 0 & & 1 \\ & ⋰ & \\ 1 & & 0 \end{pmatrix}$ $\quad H_n = \begin{pmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$ $\quad B_n H_n = H_n^T B_n$
so $H_n = B_n^{-1} H_n^T B_n$

invertible series of column swaps gives I

Jordan block of size n for λ has $J_n(\lambda) = J_n(0) + \lambda I$

JCF of A: $A = P^{-1}JP \Rightarrow J = PAP^{-1} = \begin{bmatrix} J_1(\lambda_1) & & \\ & \ddots & \\ & & J_m(\lambda_m) \end{bmatrix} = \begin{bmatrix} \lambda_1 I + H_1 & & \\ & \ddots & \\ & & \lambda_m I + H_m \end{bmatrix}$

By fact #2, write $H_n = B_n^{-1} H_n^T B_n$

$$= \begin{bmatrix} \lambda_1 I + B_1^{-1} H_1^T B_1 & & \\ & \ddots & \\ & & \lambda_m I + B_m^{-1} H_m^T B_m \end{bmatrix}$$

Let $Q = \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_m \end{bmatrix}$ so $Q^{-1} = \begin{bmatrix} B_1^{-1} & & \\ & \ddots & \\ & & B_m^{-1} \end{bmatrix}$ then

$$= Q^{-1} \begin{pmatrix} \lambda_1 I + H_1^T & & \\ & \ddots & \\ & & \lambda_m I + H_m^T \end{pmatrix} Q$$

$= Q^{-1} (PAP^{-1})^T Q$

$= Q^{-1} (P^T)^{-1} (PA)^T Q$

$= Q^{-1} (P^T)^{-1} A^T P^T Q$

$\Rightarrow A = P^{-1} (Q^{-1} (P^T)^{-1} A^T P^T Q) P$

$= \underbrace{(P^{-1} Q^{-1} (P^T)^{-1})}_{=B^{-1}} A^T \underbrace{(P^T Q P)}_{=B}$

Tada!

If U Practice Everything First

4. Prove that the subring $\mathbb{Z}[3i]$ of $\mathbb{C}$ is not a Principal Ideal Domain (PID).

Not a PID $\Rightarrow$ $\exists$ an ideal which is not principal i.e. not generated by one element

counterex: $(2, 3i)$

Stack:
PID $\Rightarrow$ PID/(max) = field so contradict this
Prime = max in PID, so find prime ideal
Note: $\mathbb{Z}[3i] \cong \mathbb{Z}[x]/(x^2+9)$

alt: UFDs $\supset$ PIDs
$\mathbb{Z}[3i]$ not a UFD
e.g. $-9 = -3 \cdot 3$
$-9 = 3i \cdot 3i$ } these are the same
↳ this is probably the move

$10 = 2 \times 5 = (1-3i)(1+3i)$
↳ all irreds, but two unique factorizations

Ideals gen by prime eles are prime

5. If $R = \mathbb{Z}[x]$, show that the sequence

$$R \xrightarrow{f} R^2 \xrightarrow{g} R$$

is exact, where $f(a) = (ax, -2a)$ and $g(c, d) = 2c + dx$.

To be exact: ~~f inj~~ ~~g surj~~ $\quad \mathrm{Im}(f) = \mathrm{Ker}(g)$
↳ show exact (?)

$\mathrm{Im}(f) = \{(ax, -2a) \mid a \in \mathbb{Z}[x]\}$
↳ = polys in $\mathbb{Z}[x]$ w/ no const term
↳ $= -2$(poly in $\mathbb{Z}[x]$) so a_n's are even

$\mathrm{Ker}(g) = \{(c, d) \mid 2c + dx = 0\}$
$2c = -dx$

$\mathrm{Ker}(g) \subseteq \mathrm{Im}(f)$
(c, d) s.t. $2c + dx = 0$
show (c, d) of form $(ax, -2a)$

$2c + dx = 0 \Rightarrow 2c = -dx$
$(c, d) \Rightarrow$ d is even (divisible by 2)
c is a poly w/ no const term
Let $c = ax$ for some $a \in \mathbb{Z}[x]$
$2c = 2ax = -dx \quad (2c = -dx)$
$\Rightarrow 2a = -d$

Then $d = -2a$
So $\mathrm{Ker}(g) \subseteq \mathrm{Im}(f)$

$\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$
$(ax, -2a)$ for $a \in \mathbb{Z}[x]$
$\;\;\, c \quad\;\; d$
Then $2c + dx = 2(ax) + (-2a)x$
$= 2ax - 2ax = 0$ ✓
so $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$

1. Classify the groups of order $2023 = 7 \times 17^2$ up to isomorphism. (You may use without proof the well-known result that if p is a prime, then every group of order p^2 is abelian.)

$\boxed{723}$

By Sylow Thms, since $|G| = 7 \times 17^2$, $\exists\ P \in Syl_7$ and $Q \in Syl_{17}$
$p_1{}' \times p_2{}^2$ ↳ $|P| = 7$ ↳ $|Q| = 17^2$

Recall that for $|G| = p^k m$, $n_p \equiv 1 \bmod p$ and $n_p \mid m$

Then $n_7 \equiv 1 \bmod 7$ and $n_7 \mid 17^2 \Rightarrow n_7 = 1$

$n_{17} \equiv 1 \bmod 17$ and $n_{17} \mid 7 \Rightarrow n_{17} = 1$

Then since $|G| = |P| \cdot |Q|$, we have that $G \cong P \times Q$.

Since $|P| = 7$ (prime), $P \cong \mathbb{Z}_7$

Since $|Q| = 17^2$ (prime^2), $Q \cong \mathbb{Z}_{17^2}$ or $\mathbb{Z}_{17} \times \mathbb{Z}_{17}$

Thus $G \cong \mathbb{Z}_7 \times \mathbb{Z}_{17^2}$ or $G \cong \mathbb{Z}_7 \times \mathbb{Z}_{17} \times \mathbb{Z}_{17}$

($\cong \mathbb{Z}_{2023}$ since $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ iff m,n coprime)

2. Let $\mathbb{R}[x, y]$ be the polynomial ring over $\mathbb{R}$ in the variables x, y and let I be the principal ideal generated by $f(x, y) = x^2 + y^2 + 1$. Prove that the ring $R = \mathbb{R}[x, y]/I$ has infinitely many maximal ideals.

$R = \mathbb{R}[x,y]/(x^2+y^2+1)$ ⤳ x^2+y^2+1 is irred since it's a deg 2 poly w/ no roots

↳ $x^2+y^2+1 = 0 \Rightarrow x^2 = \underbrace{-(1+y^2)}_{>0}$

But can't have $x^2 < 0$ for $x \in \mathbb{R}$, so no roots

- $\mathbb{R}[x]$ a PID, and in PIDs prime ideals = max ideals also, irred polys generate prime ideals

⇒ In a PID, irred polys generate max ideals

↳ To find ∞ max ideals, find ∞ many irred polys in $\mathbb{R}[x]$

Quotient from R to $\mathbb{R}[x]$:

$R = \mathbb{R}[x,y]/(x^2+y^2+1)$

Divide by ideal gen by poly w/ y: $(y-a)$ for $a \in \mathbb{R}$ → irred since linear polys are always irred.

$R/(y-a) \Rightarrow y - a \mapsto 0 \Rightarrow y = a$

$R/(y-a) = \mathbb{R}[x]/(x^2+a^2+1)$

↳ x^2+a^2+1 irred as a deg 2 poly w/ no roots

$x^2+a^2+1 = 0 \Rightarrow x^2 = \underbrace{-(a^2+1)}_{>0}$ and again, $x^2 < 0$ can't happen for $x \in \mathbb{R}$

$F[x]/(f(x))$ for $f(x)$ irred is a field, so $\mathbb{R}[x]/(x^2+a^2+1)$ is a field

PID$/(f(x))$ field iff $f(x)$ irred (so $(f(x))$ is prime = max)

$\mathbb{R}[x]/(x^2+a^2+1)$ field $\Rightarrow R/(y-a)$ is a field. R is a PID, so $(y-a)$ is max ideal in R

↳ We can choose any $a \in \mathbb{R}$, so there are ∞ many max ideals in R of form $(y-a)$, $a \in \mathbb{R}$

3. Let $A = \mathbb{Z} \oplus \mathbb{Z}$ be the free abelian group of rank 2. Compute the number of subgroups $B \subseteq A$ of index 3. ?

Free = gen set (integers, no relations)
rank 2 = gen set has size 2
↳ 2 integers?

Every subgp of A is also free abelian of rank @ most 2

Smith Normal Form (?)
Write out basis vectors for $\mathbb{Z} \oplus \mathbb{Z}$: $\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix}$
Then $\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ is Smith Normal Form, & since subgp B is gen from the same basis (at most has same rank)
Then index = |det| = |-1-1| = 2 ?

should be 4, I think

$= \sum_{d|n} d = 1+3 = 4$ subgps of index $n=3$

DANAE'S METHOD

$A = \mathbb{Z} \oplus \mathbb{Z}$ rank 2, want $B \subseteq A$ of index 3

Given A abelian ⇒ every subgp is normal
Normal subgps are kernels of homos
B has index 3, i.e. there are 3 cosets of B in A
Then B is ker of $\underbrace{\varphi : A \to \mathbb{Z}/3\mathbb{Z}}_{\text{ker}}$

B has index 3 iff ker of surj homo $\varphi : A \to \mathbb{Z}/3\mathbb{Z}$

*all homos of free gps are determined by where generators are sent

$\varphi(a) = \{0,1,2\}$
$\varphi(b) = \{0,1,2\}$
What does each mapping produce as a kernel (for B?)

A has rank 2, so gen by set of size 2 ($\{a,b\}$)
So we want to know $\varphi(a)$ + $\varphi(b)$

What else (a,b) map to (0,0)?
$a \mapsto 0,\ b \mapsto 0 \Rightarrow$ ker = A any $(a,b) \mapsto (0,0)$ not surj
$a \mapsto 1,\ b \mapsto 0 \Rightarrow$ ker = $\{(3k, b) \mid k \in \mathbb{Z}\} = B_1$ $3a \mapsto 3(1) = 0$, $b \mapsto 0$
$a \mapsto 2,\ b \mapsto 0 \Rightarrow$ ker = $\{(3k, b) \mid k \in \mathbb{Z}\} = B_1$
$a \mapsto 0,\ b \mapsto 1 \Rightarrow$ ker = $\{(a, 3k) \mid k \in \mathbb{Z}\} = B_2$
$a \mapsto 1,\ b \mapsto 1 \Rightarrow$ ker = $\{(a,b) \mid a = -b \bmod 3\} = B_3$
$a \mapsto 2,\ b \mapsto 1 \Rightarrow$ ker = $\{(a,b) \mid a = b \bmod 3\} = B_4$
$a \mapsto 0,\ b \mapsto 2 \Rightarrow$ ker = $\{(a, 3k) \mid k \in \mathbb{Z}\} = B_2$
$a \mapsto 1,\ b \mapsto 2 \Rightarrow$ ker = $\{(a,b) \mid a = b \bmod 3\} = B_4$
$a \mapsto 2,\ b \mapsto 2 \Rightarrow$ ker = $\{(a,b) \mid a = -b \bmod 3\} = B_3$

$(na, mb) = n(1) + m(1) = n+m$
$\equiv 0 \bmod 3$ when $m = -n \bmod 3$
$(na, mb) = n(2) + m(2) = 2n + 2m$
$\equiv 0 \bmod 3$ when $2m = -2n \bmod 3$
$m = -n \bmod 3$
$(na, mb) = n(1) + m(2) = n + 2m$
$\equiv 0 \bmod 3$ when $m = n \bmod 3$
$(na, mb) = n(2) + m(1) = 2n + m$
$\equiv 0 \bmod 3$ when $m = n \bmod 3$

4 possible B's

For the following questions, recall that an element r of a ring R is said to be *nilpotent* if there exists a positive integer k such that $r^k = 0$.

4.

(i) [7 pts] Prove that if N is a nilpotent $n \times n$ matrix over $\mathbb{C}$ and I is the $n \times n$ identity matrix, then there exists an $n \times n$ matrix A over $\mathbb{C}$ such that $A^2 = I + N$.

(ii) [3 pts] Prove that there does not exist a 2×2 matrix B over the field $\mathbb{F}_2$ with 2 elements such that

$\hookrightarrow = \{0, 1\}$

$$B^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

i.) N nilpotent $\Rightarrow N^k = 0$

Try $A^2 - I = N$

$(A^2 - I)^k = N^k$

$(A^2 - I)^k = 0$

$A^{2k} - A^{2k-1} + A^{2k-2} - \ldots + A - I = 0$

By the way, $N = J_m(\lambda)$ J-block of size m for eigen λ

$= J_m(0) + \lambda I$

$\hookrightarrow \begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$

$(J_m(0) + \lambda I)^k = J_m(0)^k \lambda I + \ldots J_m(0)\lambda^{k-1} I + \lambda^k I$

$(J_m(0))^2 = [0]$

e.g. $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

For $J_m(0)^k$ w/ $k \geq 2$, $J_m(0)^k = 0$

$= J_m(0) \cdot \lambda^{k-1} I + \lambda^k I = \lambda^k I$

$= \begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \begin{bmatrix} \lambda^{k-1} & & \\ & \lambda^{k-1} & \\ & & \ddots \\ & & & \lambda^{k-1} \end{bmatrix} = [0]$

$N = \begin{bmatrix} J_1(\lambda_1) & & 0 \\ & J_2(\lambda_2) & \\ 0 & & \ddots J_m(\lambda_m) \end{bmatrix}$

$N^k = \begin{bmatrix} J_1(\lambda_1)^k & & 0 \\ & J_2(\lambda_2)^k & \\ 0 & & \ddots J_m(\lambda_m)^k \end{bmatrix}$

$N^k = \begin{bmatrix} (J_1(0) + \lambda_1 I)^k & & \\ & \ddots & \\ & & (J_m(0) + \lambda_m I)^k \end{bmatrix}$

$= \begin{bmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_m^k \end{bmatrix} = [0]$

$\Rightarrow$ nilpotent matrices can only have $\lambda_i = 0 \ \forall i$

$N = P^{-1} J P \qquad J = \begin{bmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix} \qquad \lambda = 0 \ \forall \lambda \Rightarrow J = \begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$

$\Rightarrow$

come back

5. Let R be an associative commutative ring with identity 1. Prove that an element $f(z) = a + bz$ of the polynomial ring $R[z]$ is a unit if and only if a is a unit in R and b is nilpotent in R.

units of $R[z]$ are the units of R

($\Rightarrow$) assume $f = a + bz$ is a unit of $R[z]$. Then it is also a unit of R. Since $z \notin R$, the multiplicative inverse $\frac{1}{z} \notin R$, and so $b = 0$ (thus $b^2 = 0$, so b is nilpotent) otherwise f is not a unit in R. Then $f = a + 0$, and since f is a unit, so is a.

$1/f \in R[z]$

$\frac{1}{f}(a+bz) = 1$

$\frac{a}{f} + \frac{bz}{f} = 1$

($\Leftarrow$) Let a be a unit & b be nilpotent in R. Consider $f = a + bz$ in $R[z]$. Since a is a unit in R, a also a unit in $R[z]$. Since b nilpotent, say $b^k = 0$

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

$= b^{k-1}a + \cancel{b^k z}^{\,0z}$

$b^{k-1} f = b^{k-1} a + 0$

$f = a$

Since a is unit in R, a is unit in $R[z]$, and thus f is a unit in $R[z]$

1. Let G be a finite group and let p be the smallest prime divisor of $|G|$. Show that any subgroup H of G of index p is normal in G.
Hint: Consider maps $G \to S_p$.

S24

Index $p \Rightarrow$ there are p cosets of H in G
$1H = g_1 H, g_2 H, \ldots, g_p H$
$g \cdot H = g_i H$ for some $i \in [1, p]$
induces permutation of p cosets
$\Phi : G \to S_p$ *Recall $H \trianglelefteq G$ iff
$g \mapsto \sigma$ $H = \mathrm{Ker}(\Phi)$
$\mathrm{Ker}\,\Phi = \{ g \mid g \cdot g_i H = g_i H \ \forall i \}$
$\Rightarrow g \cdot 1H = 1H$, so $g \in H$. Then $\mathrm{Ker}\,\Phi \subseteq H$.

D&F Section 4.2
corollary 5(?)
after Cayley's Thm

Consider $G/\mathrm{Ker}\,\Phi \cong \mathrm{Im}\,\Phi$. $G/\mathrm{Ker}\,\Phi \leq G$, so $|G/\mathrm{Ker}\,\Phi| \mid |G|$.
$\mathrm{Im}\,\Phi \leq S_p$, so $|\mathrm{Im}\,\Phi| \mid p!$. For $G/\mathrm{Ker}\,\Phi \cong \mathrm{Im}\,\Phi$ to have order dividing both $p!$ and $|G|$, order must be p since p is the smallest prime dividing $|G|$.
Then: $p = |G/\mathrm{Ker}\,\Phi| = [G : \mathrm{Ker}] = \underbrace{[G:H]}_{=p}[H : \mathrm{Ker}]$ $\Rightarrow H = \mathrm{Ker}$, so $H \trianglelefteq G$ since it is the kernel of a group homo.

2. Let R be a principal ideal domain, and F a free R-module of finite rank. Show that any surjective R-module homomorphism $f : F \to F$ is an isomorphism.

abelian

F free module $\Rightarrow s \in F$ can be written $s = r_1 a_1 + \ldots + r_n a_n$ $r_i \in R$, $a_i \in A \subseteq F$ ↳ gen set

some condition of free module has lin dep so $s = 0$ iff $r_i = 0 \ \forall r_i \in R$
Then $f(s) = f(r_1 a_1) + \ldots + f(r_n a_n)$ since f homo
Surj, so any $s \in F$ has $t \in F$ s.t. $f(t) = s$
$\mathrm{Ker}(f) = \{ t \in F \mid f(t) = 0 \}$
If $0 = s = f(t) = f(r_1 a_1) + \ldots + f(r_n a_n)$
↳ $= r_1' b_1 + \ldots + r_n' b_n$
Requires all $r' = 0$ ...

PIDs $\subset$ IDs so there are no zero divisors

So f is inj (trivial kernel)
Since is inj + surj (bij) homo, is isomorphism

3. Let R be a noetherian domain with the property that if I and J are principal ideals in R, then $I + J$ is also a principal ideal. Prove that R is a principal ideal domain.

Noetherian = every ideal fin gen.
let I be ideal of R, WTS: is principal (i.e. $\exists a$ s.t. $I = (a)$)
Fin gen $\to I = RA = \{ r_1 a_1 + \ldots + r_n a_n \mid r_i \in R, a_i \in A \}$
$= Ra_1 + Ra_2 + \ldots + Ra_n$
$= (a_1) + (a_2) + \ldots + (a_n)$
↳ all principal
By ind on sum, $I = RA$ also principal by properties of R
Then R a PID since any ideal is principal

4. Let X, Y be nonzero 3×3 matrices over the real numbers $\mathbb{R}$ satisfying

$$X^3 + X = 0.$$

a) Show that X and Y need not be similar over the complex numbers $\mathbb{C}$.
b) Show that X and Y must be similar over $\mathbb{R}$.

$A^3 + A = 0$
$A(A^2+1) = 0$
$A(A+i)(A-i) = 0$

* JCF has Jordan blocks for each elementary divisor, i.e. the linear factors (maybe w/ powers) of each $\underbrace{\text{invariant factor}}_{\text{divide min poly}}$

elem divs are powers of irred factors
prime powers of invar factors

3x3 matrix ⇒ total degree of invar factors = 3
In $\mathbb{R}$: x, x^2+1
can't have x, x, x since this means $x^3 = 0$ ⇒ $x = 0$ & x, y nonzero
so can only have x, x^2+1 invar factors

In $\mathbb{C}$: $x, (x+i), (x-i)$
invar factors must divide each other
can have more than one invar factor decomp
could have, for ex: $(x-i), (x-i)(x+i)$ ⇝ degree of product = 3
$(x+i), (x+i)(x-i)$
etc.

similar ⟺ RCF
same RCF ⟺ same invar factor decomp
↳ must be same in $\mathbb{R}$, but not necessarily in $\mathbb{C}$

5. a) Show that every finite subgroup of $\mathbb{C}^\times$ is cyclic.
b) Suppose that A is a finite abelian group, and $f : A \to \mathbb{C}^\times$ is a homomorphism with $f(A) \neq \{1\}$. Show that $\sum_{a \in A} f(a) = 0$ in $\mathbb{C}$.

a.) $z \in \mathbb{C}$ takes the form $z = re^{i\theta}$, H
In a finite order subgroup, every element must have finite order, so say order n
$z^n = r^n e^{in\theta} \in H$. Then $r^n = r$, so $r = 1$ for the subgp to be closed.
additionally, $1 = e^0, e^{i\theta}, e^{2i\theta}, \dots, e^{(n-1)i\theta} \in H$
These are precisely the n^{th} roots of unity, so $\langle \zeta_n \rangle \subseteq H$
If another element $z' \in H$, $|z'| < \infty$ (say $|z'| = m$) and so once again if $z' = r'e^{i\phi}$, $r' = 1$.
Then $1 = e^0, e^{2i\phi}, \dots, e^{(m-1)i\phi} \in H$
If n.m coprime, then H contains both the n^{th} + m^{th} roots of unity, which is equivalent to the $m \times n$-th roots of unity $\mathbb{Z}_n \cong$ $\mathbb{Z}_m \cong$
$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ for m.n coprime
Else, we have the lcm(m,n)-th roots of unity. Regardless, the n-th roots of unity $\cong \mathbb{Z}_n$, so $H = \langle \zeta_n \rangle$ and H is cyclic

b.) A finite abelian, $f : A \to \mathbb{C}^\times$ w/ $f(A) \neq \{1\}$ nontriv.
f is a homo., so $f(A)$ is still finite abelian. By pt (a.), any finite subgp. of $\mathbb{C}^\times$ is cyclic.
Then if $|A| = n$, $f(A) \cong \mathbb{Z}_n \cong \langle \zeta_n \rangle = \{\zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}, \zeta_n^n = 1\}$
Then $\sum_{a \in A} f(a) = \zeta_n + \zeta_n^2 + \dots + \zeta_n^{n-1} + 1 = 0$, as desired