August 2020

① The commutator subgroup of a group G, denoted by G', is the subgp. generated by all commutators $[x,y]=xyx^{-1}y^{-1}$ for $x,y\in G$. For an integer $n\geq 2$, define $G=\left\{\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}: a\in(\mathbb{Z}/n\mathbb{Z})^\times, b\in\mathbb{Z}/n\mathbb{Z}\right\}\subset GL_2(\mathbb{Z}/n\mathbb{Z})$.

(a) Show $N:=\left\{\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}: b\in\mathbb{Z}/n\mathbb{Z}\right\}$ is a normal subgp. of G and $G/N\cong(\mathbb{Z}/n\mathbb{Z})^\times$.

Pf: Define $\varphi: G\to(\mathbb{Z}/n\mathbb{Z})^\times$ by $\varphi\left(\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix}\right)=a$

Since $a\in(\mathbb{Z}/n\mathbb{Z})^\times$, this map is well-defined.

For $a_1,a_2\in(\mathbb{Z}/n\mathbb{Z})^\times$ and $b_1,b_2\in\mathbb{Z}/n\mathbb{Z}$, we have:

$\varphi\left(\begin{pmatrix} a_1 & b_1\\ 0 & 1\end{pmatrix}\begin{pmatrix} a_2 & b_2\\ 0 & 1\end{pmatrix}\right)=\varphi\begin{pmatrix} a_1a_2 & a_1b_2+b_1\\ 0 & 1\end{pmatrix}=a_1a_2=\varphi\left(\begin{pmatrix} a_1 & b_1\\ 0 & 1\end{pmatrix}\right)\varphi\left(\begin{pmatrix} a_2 & b_2\\ 0 & 1\end{pmatrix}\right)$

Therefore, φ is a homomorphism and it is onto.

Observe that $\ker(\varphi)=\{M\in G:\varphi(M)=1\}=\left\{\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}\in G: b\in\mathbb{Z}/n\mathbb{Z}\right\}=N$.

Therefore, $\ker(\varphi)=N$.

By the first isomorphism thm, $G/N\cong(\mathbb{Z}/n\mathbb{Z})^\times$.

Since N is the kernel of a homomorphism, we have that N is normal in G. □

(b) Show N is cyclic with generator $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$.

Pf: We claim $N=\left\langle\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\right\rangle$

We will show that $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^k=\begin{pmatrix} 1 & k\\ 0 & 1\end{pmatrix}$, by induction on k.

Base case: $k=1$: $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^1=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$

$k=2$: $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^2=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & 2\\ 0 & 1\end{pmatrix}$

Induction hypothesis: Assume this holds $\forall k$ $1\leq k\leq b-1$. Take $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^b$:

$\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^b=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^{b-1}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & b-1\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}$ ✓

Therefore, $N=\left\{\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}: b\in\mathbb{Z}/n\mathbb{Z}\right\}=\left\{\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^b: b\in\mathbb{Z}/n\mathbb{Z}\right\}=\left\langle\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\right\rangle$.

Thus, N is cyclic with generator $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$. □

(c) When $n\geq 3$ is odd, use (a) and (b) to show that $G'=N$.

(Skip for now)

---

② Let G be a group. Recall that an automorphism of G is an isomorphism $G\to G$. The two parts can be done independently.

(a) For a prime p, let G be a cyclic group of order p written multiplicatively. Prove that the automorphisms of G are precisely the functions $f:G\to G$ where $f(g)=g^k$ for all $g\in G$ and some exponent $k\not\equiv 0 \bmod p$.

Pf: First we will show that f is an automorphism. Let $k\not\equiv 0 \bmod p$.

Let $g_1,g_2\in G$.

Then $f(g_1g_2)=(g_1g_2)^k=g_1^kg_2^k=f(g_1)f(g_2)$ since G is cyclic (abelian).

Therefore, f is a homomorphism.

Observe that $\ker(f)=\{g\in G: f(g)=1\}=\{g\in G: g^k=1\}$

Let $k=a+np$, $0<a\leq p-1$, $a,n\in\mathbb{Z}$.

Then $g^k=1 \Rightarrow g^k=g^{a+np}=g^ag^{np}=g^a=1$. (since $|G|=p$, $g^{np}=1$.)

$g^a=1\Rightarrow |g|\leq a$

By Lagrange's Thm, every elt. has order dividing the group, so $|g|=1$ or p since $|G|=p$.

Since $0<a\leq p-1$, we get that $a=1$, so $|g|=1$.

Therefore, $\ker(f)$ is trivial $\Rightarrow f$ is injective.

Since f is a map between G and itself (i.e., sets of the same cardinality) and f is injective, f must also be surjective.

Thus, f is an automorphism.

Now we want to show that any automorphism must have the form $f(g)=g^k$ for all $g\in G$ and some $k\not\equiv 0 \bmod p$.

Let f be an aut. of G.

Since G is cyclic, let $G=\langle g\rangle=\{1,g,g^2,\dots,g^{p-1}\}$

So $f(g)=g^j$ (b/c every elt. is a power of g)

$j\not\equiv 0 \bmod p$. Let $j=k$ and we are done. □

(b) For a prime p, let $G=(\mathbb{Z}/p\mathbb{Z})^2$. Show that the automorphisms of G are precisely the functions $f:G\to G$ where $f\begin{pmatrix} x\\ y\end{pmatrix}=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x\\ y\end{pmatrix}=\begin{pmatrix} ax+by\\ cx+dy\end{pmatrix}$ for some $a,b,c,d\in\mathbb{Z}/p\mathbb{Z}$ s.t. $ad-bc\not\equiv 0 \bmod p$.

Pf: Let $\begin{pmatrix} x\\ y\end{pmatrix},\begin{pmatrix} x'\\ y'\end{pmatrix}\in(\mathbb{Z}/p\mathbb{Z})^2$. Then:

$f\left(\begin{pmatrix} x\\ y\end{pmatrix}+\begin{pmatrix} x'\\ y'\end{pmatrix}\right)=f\left(\begin{pmatrix} x+x'\\ y+y'\end{pmatrix}\right)=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x+x'\\ y+y'\end{pmatrix}=\begin{pmatrix} a(x+x')+b(y+y')\\ c(x+x')+d(y+y')\end{pmatrix}=\begin{pmatrix} ax+by+ax'+by'\\ cx+dy+cx'+dy'\end{pmatrix}$

$=\begin{pmatrix} ax+by\\ cx+dy\end{pmatrix}+\begin{pmatrix} ax'+by'\\ cx'+dy'\end{pmatrix}=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x\\ y\end{pmatrix}+\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x'\\ y'\end{pmatrix}=f\left(\begin{pmatrix} x\\ y\end{pmatrix}\right)+f\left(\begin{pmatrix} x'\\ y'\end{pmatrix}\right)$.

Therefore, f is a homomorphism.

Injective: Let $\begin{pmatrix} x\\ y\end{pmatrix}\neq\begin{pmatrix} x'\\ y'\end{pmatrix}$.

Then $f\left(\begin{pmatrix} x\\ y\end{pmatrix}\right)=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x\\ y\end{pmatrix}=\begin{pmatrix} ax+by\\ cx+dy\end{pmatrix}$ and

$f\left(\begin{pmatrix} x'\\ y'\end{pmatrix}\right)=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x'\\ y'\end{pmatrix}=\begin{pmatrix} ax'+by'\\ cx'+dy'\end{pmatrix}$

$\begin{pmatrix} ax+by\\ cx+dy\end{pmatrix}\neq\begin{pmatrix} ax'+by'\\ cx'+dy'\end{pmatrix}$ since $ax+by=ax'+by'$, $a(x-x')\neq b(y'-y)$ $\begin{pmatrix} x\neq x'\\ y\neq y'\end{pmatrix}$

Surjective: Let $\begin{pmatrix} ax+by\\ cx+dy\end{pmatrix}\in G$.

Then $\exists\begin{pmatrix} x\\ y\end{pmatrix}\in G$ s.t. $f\left(\begin{pmatrix} x\\ y\end{pmatrix}\right)=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x\\ y\end{pmatrix}=\begin{pmatrix} ax+by\\ cx+dy\end{pmatrix}$

Therefore, f is an automorphism.

Suppose f is an aut. of G.

Let $f\begin{pmatrix} 1\\ 0\end{pmatrix}=\begin{pmatrix} a\\ c\end{pmatrix}$ and $f\begin{pmatrix} 0\\ 1\end{pmatrix}=\begin{pmatrix} b\\ d\end{pmatrix}$.

We claim that $f\begin{pmatrix} x\\ y\end{pmatrix}=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} x\\ y\end{pmatrix}$.

Indeed $f\begin{pmatrix} x\\ y\end{pmatrix}=f\left(\begin{pmatrix} x\\ 0\end{pmatrix}+\begin{pmatrix} 0\\ y\end{pmatrix}\right)=f\begin{pmatrix} x\\ 0\end{pmatrix}+f\begin{pmatrix} 0\\ y\end{pmatrix}=xf\begin{pmatrix} 1\\ 0\end{pmatrix}+yf\begin{pmatrix} 0\\ 1\end{pmatrix}=x\begin{pmatrix} a\\ c\end{pmatrix}+y\begin{pmatrix} b\\ d\end{pmatrix}$

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

Moreover, a matrix M over a field F is invertible iff $\det(M)\neq 0$.

Since $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ is invertible, $\det=ad-bc\neq 0$ in $\mathbb{Z}/p\mathbb{Z}$.

Therefore, each aut. must be of this form. □

---

③ Fix a group H and a group automorphism $f\in \mathrm{Aut}(H)$. Let $\varphi:\mathbb{Z}\to\mathrm{Aut}(H)$ by $\varphi(n)=f^n$.

(a) In $H\rtimes_\varphi\mathbb{Z}$, prove (h,n) has finite order if and only if h has finite order and $n=0$.

Pf: • Let $(h,n)\in H\rtimes_\varphi\mathbb{Z}$ s.t. $h^k=0$ and $n=0$.

If h has finite order, then $h^k=0$ for some $k\in\mathbb{Z}$. Let $n=0$.

Observe that:

$(h,0)^2=(h,0)(h,0)=(h\varphi_0(h),0)$

$(h,0)^3=(h,0)^2(h,0)=(h\varphi_0(h),0)(h,0)=(h\varphi_0(h)\varphi_0(h),0)$
$=(h\varphi_0(h)^2,0)$

⋮

$(h,0)^k=(h\varphi_0(h)^{k-1},0)=(h\cdot h^{k-1},0)=(h^k,0)=(0,0)$

Therefore, $(h,0)^k$ has finite order.

• Suppose (h,n) has finite order: $(h,n)^k=(0,0)$

The second coordinate is $n^k=0\Rightarrow n=0$ $(n\in\mathbb{Z})$

So we have $(h,0)^k=(0,0)$.

$(h,0)^k=(h\varphi_0(h)^{k-1},0)=(0,0)\Rightarrow h\varphi_0(h)^{k-1}=0$
$h\cdot h^{k-1}=0$
$h^k=0\Rightarrow h$ has finite order. □

(b) Let $\psi:\mathbb{Z}\to\mathrm{Aut}(H)$ by $\psi(n)=f^{-n}$. Prove that $H\rtimes_\varphi\mathbb{Z}\cong H\rtimes_\psi\mathbb{Z}$ as gps.

Pf: Define $\Phi: H\rtimes_\varphi\mathbb{Z}\to H\rtimes_\psi\mathbb{Z}$ by $\Phi((h,n))=(h,-n)$.

We can see that Φ is bijective since $\Phi^{-1}(h,n)=(h,-n)$.

We WTS Φ is a homomorphism:

Let $(h_1,n_1),(h_2,n_2)\in H\rtimes_\varphi\mathbb{Z}$, then

$\Phi((h_1,n_1)(h_2,n_2))=\Phi((h_1\varphi_{n_1}(h_2),n_1+n_2))$
$=(h_1f^{n_1}(h_2),-(n_1+n_2))$
$=(h_1f^{n_1}(h_2),-n_1-n_2)$
$=(h_1,-n_1)(h_2,-n_2)$
$=\Phi((h_1,n_1))\Phi((h_2,n_2))$

this equality follows from ↓ in $H\rtimes_\psi\mathbb{Z}$:

$(h_1,-n_1)(h_2,-n_2)=(h_1\psi_{-n_1}(h_2),-n_1-n_2)$
$=(h_1f^{-(-n_1)}(h_2),-n_1-n_2)$
$=(h_1f^{n_1}(h_2),-n_1-n_2)$

Therefore, Φ is a homomorphism.

Thus, Φ is an isom.: $H\rtimes_\varphi\mathbb{Z}\cong H\rtimes_\psi\mathbb{Z}$. □

---

④ For a finite subset $\{r_1,\dots,r_k\}$ of $\mathbb{Q}$, the ring $\mathbb{Z}[r_1,\dots,r_k]$ is the set of all sums of products of nonnegative powers of $r_1,\dots,r_k$ w/ coefficients in $\mathbb{Z}$.

(a) For relatively prime integers a and b with $b\neq 0$, prove $\mathbb{Z}[a/b]=\mathbb{Z}[1/b]$.

(b) Let $N>1$ in $\mathbb{Z}$ have prime factn $p_1^{e_1}\cdots p_k^{e_k}$ for distinct primes $p_1,\dots,p_k$ and $e_j>0$. Prove that $\mathbb{Z}[1/N]=\{a/N^e: a\in\mathbb{Z}, e\geq 0\}$ and $\mathbb{Z}[1/N]=\mathbb{Z}[1/p_1,\dots,1/p_k]$.

(c) Prove that $\mathbb{Z}[1/N]$ has unit gp. $\langle -1,p_1,\dots,p_k\rangle=\{\pm p_1^{a_1}\cdots p_k^{a_k}: a_j\in\mathbb{Z}\}$.

(Skip for now)

---

⑤ Let A be an $n\times n$ matrix with complex entries.

(a) Show that A and its transpose A^T have the same eigenvalues in $\mathbb{C}$.

Pf: A and its transpose A^T have the same characteristic polynomial.

(Let $\lambda\in\mathbb{C}$ be the eigenvalues)

$\mathrm{char}_A=\det(A-I\lambda)$

$\mathrm{char}_{A^T}=\det((A-I\lambda)^T)=\det(A^T-I\lambda)$

$\det(A-I\lambda)=\det(A^T-I\lambda)$

Therefore, A and A^T have the same eigenvalues in $\mathbb{C}$. □

(b) If λ is an eigenvalue of A, with $Av=\lambda v$ and $A^Tw=\lambda w$ in $\mathbb{C}^n$, then prove that the matrix $B=vw^T$ commutes with A.

Pf: We want to show $AB=BA$:

$AB=A(vw^T)=(Av)w^T=(\lambda v)w^T=v(\lambda w^T)$ (λ is a scalar)
$=v(\lambda w)^T=v(A^Tw)^T=vw^TA^{T^T}$
$=BA$. □

---

⑥ Give examples as requested, with justification.

(a) A prime factn. of $3+i$ in $\mathbb{Z}[i]$.

Pf: $N(3+i)=(3+i)(3-i)=9+1=10$

Let $3+i=\alpha\beta$ for some $\alpha,\beta\in\mathbb{Z}[i]$.

Then $N(3+i)=10=N(\alpha)N(\beta)$.

WLOG, let $N(\alpha)=2$ and $N(\beta)=5$.

Let $\alpha=1-i$. Note that $N(1-i)=(1+i)(1-i)=2$
2 is prime $\Rightarrow 1+i$ is irred.

Let $\beta=1+2i$. Note that $N(1+2i)=(1+2i)(1-2i)=5$
5 is prime $\Rightarrow 1+2i$ is irred.

$\mathbb{Z}[i]$ is a Euclidean dom. $\Rightarrow$ PID $\Rightarrow$ UFD.

In UFD, {primes} = {irred.}.

Therefore, $3+i=(1-i)(1+2i)$ is a prime factn. of $3+i$ in $\mathbb{Z}[i]$. □

(b) A unit in $\mathbb{Z}[x]/(x^2)$ other than ± 1.

Pf: The elt. $1-x^2\equiv 1 \bmod x^2$

Notice that $1-x^2=(1+x)(1-x)$

Therefore, $1+x$ is a unit in $\mathbb{Z}[x]/(x^2)$ that is not ± 1. □

(c) A maximal ideal m in $\mathbb{Z}[x]$ s.t. $\mathbb{Z}[x]/m$ has order 27.

Pf: The max. ideals in $\mathbb{Z}[x]$ are of the form $(p,f(x))$ where p is prime and $f(x)$ is irred. mod p and monic.

Consider the ideal $(3,x^3+2x+1)$.

The poly. x^3+2x+1 is irred mod 3:

$0^3+2\cdot 0+1\equiv 1\ (3)$
$1^3+2\cdot 1+1\equiv 1\ (3)$
$2^3+2\cdot 2+1\equiv 1\ (3)$
} can do this test b/c the poly. is a cubic.

Observe that $\mathbb{Z}[x]/(3,x^3+2x+1)\cong(\mathbb{Z}/3)[x]/(x^3+2x+1)$, which has size 27 since we are mod-ing out by a cubic. (field; roughly looks like $\{ax^2+bx+c: a,b,c\in\mathbb{Z}/3\mathbb{Z}\}$; irred.)

Therefore, $m=(3,x^3+2x+1)$ is such an ideal. □

(d) A ring theoretic property that $\mathbb{Q}[x]/(x^2-1)$ and $\mathbb{Q}[x]/(x^2)$ do not share (so the rings are not isomorphic).

Pf: Nilpotent elements.

$\mathbb{Q}[x]/(x^2)$ has one nonzero nilpotent element, namely x $(x^2=x\cdot x=0)$

$\mathbb{Q}[x]/(x^2-1)$ does not have any nonzero nilpotent elements. □

January 2020

① Let p be a prime number.

(a) Show every group of order p^n where $n\geq 1$ has nontrivial center.

Pf: Let G be a finite group s.t. $|G|=p^n$, p prime, $n\geq 1$.

Let G act on itself by conjugation.

Then by fixed point congruence, we have

$|G|\equiv|\mathrm{Fix}_G(G)| \bmod p\Rightarrow|G|\equiv|Z(G)| \bmod p$.

Observe that $|G|=p^n\equiv 0 \bmod p\Rightarrow|Z(G)|\equiv 0 \bmod p$
$\Rightarrow p\,|\,|Z(G)|$

Since $|Z(G)|\geq 1$ and $p\,|\,|Z(G)|$, we get that $|Z(G)|\geq p$.

Therefore, G has a nontrivial center $(Z(G)\neq\{1\})$. □

(b) Use part (a) to show every group whose order is p^2 is abelian.

Pf: Let G be a finite group s.t. $|G|=p^2$.

Since G is a p-group, by part (a), we have that $Z(G)$ is nontrivial.

Therefore, $|Z(G)|=p$ or $|Z(G)|=p^2$.

If $|Z(G)|=p^2$, then since $Z(G)\leq G$, we have $Z(G)=G$.

Thus, G is abelian.

If $|Z(G)|=p$, then $\left|G/Z(G)\right|=\frac{|G|}{|Z(G)|}=\frac{p^2}{p}=p$

$\Rightarrow G/Z(G)\cong\mathbb{Z}/p\mathbb{Z}$, so $G/Z(G)$ is cyclic.

Therefore, G is abelian. □

* $G/Z(G)$ cyclic $\Rightarrow G$ is abelian.

---

② For $a\in\mathbb{Z}$ and $u=(u_1,u_2,u_3)\in\mathbb{R}^3$, define $a*u=(u_1,au_1+u_2,a^2u_1+2au_2+u_3)$.

(a) Prove the above formula defines an action of the additive group $(\mathbb{Z},+)$ on $\mathbb{R}^3$.

Pf: We WTS that for $0\in\mathbb{Z}$ and $u\in\mathbb{R}^3$, $0*u=u$, and that for $a,b\in\mathbb{Z}$ and $u\in\mathbb{R}^3$, $a*(b*u)=(a+b)*u$.

• First, let $0\in\mathbb{Z}$ and $u=(u_1,u_2,u_3)\in\mathbb{R}^3$: (0 is the additive identity)

$0*(u_1,u_2,u_3)=(u_1,0\cdot u_1+u_2,0^2\cdot u_1+2\cdot 0\cdot u_2+u_3)=(u_1,u_2,u_3)$ ✓

• Now let $a,b\in\mathbb{Z}$ and $u=(u_1,u_2,u_3)\in\mathbb{R}^3$:

$a*(b*(u_1,u_2,u_3))=a*(u_1,bu_1+u_2,b^2u_1+2bu_2+u_3)$
$=(u_1,au_1+bu_1+u_2,a^2u_1+2a(bu_1+u_2)+b^2u_1+2bu_2+u_3)$
$=(u_1,(a+b)u_1+u_2,a^2u_1+2abu_1+2au_2+b^2u_1+2bu_2+u_3)$
$=(u_1,(a+b)u_1+u_2,(a+b)^2u_1+2(a+b)u_2+u_3)$

$(a+b)*(u_1,u_2,u_3)=(u_1,(a+b)u_1+u_2,(a+b)^2u_1+2(a+b)u_2+u_3)$

$\Rightarrow a*(b*u)=(a+b)*u$ ✓

Therefore, the above formula defines an action of the additive group $(\mathbb{Z},+)$ on $\mathbb{R}^3$. □

(b) Show a vector $u=(u_1,u_2,u_3)$ in $\mathbb{R}^3$ has a finite $\mathbb{Z}$-orbit for this action if and only if $u_1=u_2=0$.

Pf: If $u_1=u_2=0$, then $u=(0,0,u_3)$.

Let $a\in\mathbb{Z}$. Then $a*u=a*(0,0,u_3)=(0,0,u_3)$, so u has a finite $\mathbb{Z}$-orbit for this action.

Assume that $u=(u_1,u_2,u_3)$ in $\mathbb{R}^3$ has a finite $\mathbb{Z}$-orbit for this action.

Then there exists a nonzero $a\in\mathbb{Z}$ s.t. $a*u=u$.

$a*u=(u_1,au_1+u_2,a^2u_1+2au_2+u_3)=(u_1,u_2,u_3)$

$\Rightarrow au_1+u_2=u_2\Rightarrow u_1=0$ $(au_1=0$, since $a\neq 0\Rightarrow u_1=0)$

$\Rightarrow a^2u_1+2au_2+u_3=u_3\Rightarrow u_1=0, u_2=0$

(we know $u_1=0$, so $2au_2+u_3=u_3\Rightarrow 2au_2=0$ $\Rightarrow u_2=0$ since $a\neq 0$)

Therefore, u has to equal $(0,0,u_3)$, i.e., $u_1=u_2=0$. □

---

③ The goal of this problem is to classify all groups of order 35 up to isomorphism.

(a) Determine all abelian groups of order 35 up to isomorphism.

Pf: $35=5\cdot 7$

By the fundamental thm for finitely generated abelian groups, the only abelian group of order 35 is $\mathbb{Z}/35\mathbb{Z}$, which is isomorphic to $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$ since $(5,7)=1$. □

(b) Show that every group of order 35 is abelian.

Pf: Let G be a finite group w/ $|G|=35=5\cdot 7$.

By the first Sylow theorem, there exists a 5-Sylow subgp. P w/ $|P|=5$ and a 7-Sylow subgp. Q w/ $|Q|=7$.

By the third Sylow theorem, we have

$n_5\equiv 1 \bmod 5$ and $n_5\,|\,7\Rightarrow n_5=1$
$n_7\equiv 1 \bmod 7$ and $n_7\,|\,5\Rightarrow n_7=1$
} P and Q are the unique 5-Sylow and 7-Sylow subgroups, respectively

$\Rightarrow P\trianglelefteq G$, $Q\trianglelefteq G$

Since $P\trianglelefteq G$ (and $Q\trianglelefteq G$), it follows that PQ is a subgroup of G.

Observe that $|P\cap Q|=1$: $P\cap Q\leq P$ and $P\cap Q\leq Q$, so by Lagrange's Thm, $|P\cap Q|\,|\,|P|$ and $|P\cap Q|\,|\,|Q|$, but $(|P|,|Q|)=(5,7)=1$, so $|P\cap Q|=1$.

Therefore, $|PQ|=\frac{|P||Q|}{|P\cap Q|}=\frac{5\cdot 7}{1}=35=|G|\Rightarrow PQ=G$.

Note that $|P|=5$, so P is abelian (cyclic b/c 5 is prime) and $|Q|=7$, so Q is abelian (cyclic b/c 7 is prime).

We want to show that the elements of P and Q commute:

Let $x\in P$, $y\in Q$. Then

$xyx^{-1}y^{-1}=xyx^{-1}y^{-1}\in P\cap Q=\{1\}\Rightarrow xyx^{-1}y^{-1}=1\Rightarrow xy=yx$.

($\in P$; $\in P$ since $P\trianglelefteq G$; $\in Q$ since $Q\trianglelefteq G$; $\in Q$)

Therefore, the elements of P and Q commute with each other.

Thus, we conclude that G is abelian. □

---

④ Let I be the ideal $(7,1+\sqrt{-13})$ in $\mathbb{Z}[\sqrt{-13}]$.

(a) Show the ring homomorphism $\mathbb{Z}/7\mathbb{Z}\to\mathbb{Z}[\sqrt{-13}]/I$ given by $a \bmod 7\mathbb{Z}\mapsto a \bmod I$ is an isomorphism.

Pf: Let $\varphi:\mathbb{Z}/7\mathbb{Z}\to\mathbb{Z}[\sqrt{-13}]/(7,1+\sqrt{-13})$ given by $a \bmod 7\mathbb{Z}\mapsto a \bmod I=(7,1+\sqrt{-13})$

We are given that φ is a ring homomorphism, so it remains to show that φ is bijective.

Injective: $\ker(\varphi)=\{a\in\mathbb{Z}/7\mathbb{Z}:\varphi(a)=0\}$
$=\{a\in\mathbb{Z}/7\mathbb{Z}: a \bmod 7\mapsto 0 \bmod I\}\Rightarrow a\equiv 0 \bmod 7$

Therefore, $\ker(\varphi)$ is trivial.

Surjective: Let $a+b\sqrt{-13}\in\mathbb{Z}[\sqrt{-13}]/I$, then for all $a,b\in\mathbb{Z}$

$a+b\sqrt{-13}\equiv a+b(-1) \bmod (1+\sqrt{-13})$
$\equiv a-b \bmod (1+\sqrt{-13})$

and then we are left with $a-b \bmod 7$ in $\mathbb{Z}[\sqrt{-13}]/I$, where $a,b\in\mathbb{Z}$.

There exists $a-b\in\mathbb{Z}/7\mathbb{Z}$ s.t. $a-b \bmod 7\mapsto a-b \bmod I$

Therefore, φ is surjective.

Thus, φ is a bij. hom., so $\mathbb{Z}/7\mathbb{Z}\cong\mathbb{Z}[\sqrt{-13}]/I$ □

(b) Show I is not principal.

Pf: Suppose that $(7,1+\sqrt{-13})=(\alpha)$ for some $\alpha\in\mathbb{Z}[\sqrt{-13}]$.

Then $7\in(\alpha)$, so $7=\alpha\beta$ for some $\beta\in\mathbb{Z}[\sqrt{-13}]$.

By taking norms, we get:

$N(7)=49=N(\alpha)N(\beta)\Rightarrow N(\alpha)=\pm 7$

(if $N(\alpha)=\pm 1$, then $(\alpha)=\mathbb{Z}[\sqrt{-13}]$)

We also have $1+\sqrt{-13}\in(\alpha)$, so $1+\sqrt{-13}=\alpha\gamma$ for some $\gamma\in\mathbb{Z}[\sqrt{-13}]$.

By taking norms, we get:

$N(1+\sqrt{-13})=(1+\sqrt{-13})(1-\sqrt{-13})=14=N(\alpha)N(\gamma)$

Let $\alpha=a+b\sqrt{-13}$. Then $N(\alpha)=a^2+13b^2$.

If $N(\alpha)=\pm 7$, then $a^2+13b^2=\pm 7$ has a solution in $\mathbb{Z}$.

$a^2+13b^2\neq -7$ since $a^2+13b^2\geq 0$
$a^2+13b^2\neq 7$ for any $a,b\in\mathbb{Z}$
} Therefore, there is no elt. in $\mathbb{Z}[\sqrt{-13}]$ with norm ± 7.

Therefore, $(7,1+\sqrt{-13})\neq(\alpha)$

Thus, the ideal I is not principal. □

---

⑤ Let p be a prime number.

(a) Prove $\mathbb{Z}[x]/p\mathbb{Z}[x]\cong(\mathbb{Z}/p\mathbb{Z})[x]$ as rings.

Pf: Let $\varphi:\mathbb{Z}[x]\to(\mathbb{Z}/p\mathbb{Z})[x]$ by $f(x)\mapsto f(x) \bmod p$ be the redn. map, so φ is a homomorphism and it is onto.

Then $\ker(\varphi)=\{f(x)\in\mathbb{Z}[x]:\varphi(f(x))=0 \bmod p\}=p\mathbb{Z}[x]$ since $\varphi(f(x))=0$ only if $f(x)$ reduces to 0 mod p, which only happens if $f(x)$ has p-multiple coefficients, i.e., $f(x)\in p\mathbb{Z}[x]$.

Therefore, by the first Isom. thm, we get that $\mathbb{Z}[x]/p\mathbb{Z}[x]\cong(\mathbb{Z}/p\mathbb{Z})[x]$. □

(b) Prove that a maximal ideal in $\mathbb{Z}[x]$ that contains p must have the form $(p,f(x))$ where $f(x)$ is monic in $\mathbb{Z}[x]$ and $f(x)$ mod p is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$.

Pf: By part (a), we have that $\mathbb{Z}[x]/p\mathbb{Z}[x]\cong(\mathbb{Z}/p\mathbb{Z})[x]$.

In order for an ideal M containing p to be maximal, we need to have $\mathbb{Z}[x]/M$ is a field.

Note that $\mathbb{Z}/p\mathbb{Z}$ is a field, but $(\mathbb{Z}/p\mathbb{Z})[x]$ is not, so we want to mod out by a polynomial s.t. $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))\cong\mathbb{Z}/p\mathbb{Z}$, $f(x)\in\mathbb{Z}[x]$.

Since the ideal M contains p, the surjective homomorphism $\mathbb{Z}[x]\to\mathbb{Z}[x]/M$ kills p and thus induces a surjective ring homomorphism: $\psi:(\mathbb{Z}/p\mathbb{Z})[x]\to\mathbb{Z}[x]/M$

The $\ker(\psi)=\{\pi(x)\in(\mathbb{Z}/p\mathbb{Z})[x]:\psi(\pi(x))=0$ in $\mathbb{Z}[x]/M\}$ has to be maximal in $(\mathbb{Z}/p\mathbb{Z})[x]$, so it is $(\pi(x))$ for some monic irreducible $\pi(x)\in(\mathbb{Z}/p\mathbb{Z})[x]$.

Let $f(x)$ be a monic lifting of $\pi(x)$ to $\mathbb{Z}[x]$:
$f(x)$ is monic and $\pi(x)=\bar{f}(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

That $\psi(\pi(x))=0$ in $\mathbb{Z}[x]/M$ implies that $f(x)\equiv 0 \bmod M$, so the monic irreducible $f(x)$ must also be in the maximal ideal, i.e., $f(x)\in M$ in $\mathbb{Z}[x]$. Therefore, $M=(p,f(x))$.

Thus, a maximal ideal in $\mathbb{Z}[x]$ that contains p must have the form $(p,f(x))$ where $f(x)$ is monic in $\mathbb{Z}[x]$ and $f(x)$ mod p is irred. in $(\mathbb{Z}/p\mathbb{Z})[x]$. □

---

⑥ Give examples as requested, with justification.

(a) A nonabelian group of order 21.

Pf: Consider the semidirect product $G=\mathbb{Z}/7\mathbb{Z}\rtimes_\psi\mathbb{Z}/3\mathbb{Z}$ with

$\psi:\mathbb{Z}/3\mathbb{Z}\to\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})\cong(\mathbb{Z}/7\mathbb{Z})^\times$. $(|\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})|=|(\mathbb{Z}/7\mathbb{Z})^\times|=6)$

$|\psi(1)|\,|\,3$, so $|\psi(1)|=1$ or 3

If $\psi(1)=1$, then we get the trivial hom.

Since $3\,|\,|\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})|$ $(3\,|\,6)$, we have the nontrivial hom. given by $|\psi(1)|=3$. (this means $\exists$ a nontrivial hom. ψ)

Therefore, $\mathbb{Z}/7\mathbb{Z}\rtimes_\psi\mathbb{Z}/3\mathbb{Z}$ is a nonabelian group of order 21. □

(b) An expression of (12345) as a product of transpositions.

Pf: Consider $(12)(23)(34)(45)$.

Then $(12)(23)(34)(45)=(12345)$.

Thus, $(12)(23)(34)(45)$ is an expression of (12345) as a product of transpositions. □

(c) Gaussian integers γ and ρ s.t. $7+2i=(2+3i)\gamma+\rho$ and $N(\rho)<N(2+3i)$.

Pf: $\frac{7+2i}{2+3i}\cdot\frac{(2-3i)}{(2-3i)}=\frac{14-21i+4i+6}{4+9}=\frac{20-17i}{13}=\frac{20}{13}-\frac{17i}{13}$.

Let $\gamma=1-i$. Then $\rho=7+2i-(2+3i)(1-i)$
$=7+2i-(2-2i+3i+3)$
$=7+2i-(5+i)$
$=2+i$.

$N(\rho)=N(2+i)=(2+i)(2-i)=5$
$N(2+3i)=(2+3i)(2-3i)=13$
} $N(\rho)=5<13=N(2+3i)$ ✓

Check: $7+2i=(2+3i)(1-i)+(2+i)$ ✓

Therefore, $\gamma=1-i$ and $\rho=2+i$. □

(d) A homomorphism of commutative rings $f:R\to S$ and an ideal I in R such that $f(I)$ is not an ideal in S.

Pf: Let $R=\mathbb{Z}$ and $S=\mathbb{Q}$, so $f:\mathbb{Z}\to\mathbb{Q}$ is the inclusion map.

Then $\mathbb{Z}$ is an ideal in $\mathbb{Z}$

Observe that $f(\mathbb{Z})$ is not an ideal of $\mathbb{Q}$ b/c the only ideals of $\mathbb{Q}$ are (0) and $\mathbb{Q}$. □