August 2020

martes, 20 de diciembre de 2022 5:50 p.m.

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 $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}^b=\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}$, by induction on b.

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

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

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

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

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 $f(g_1 g_2) = (g_1 g_2)^k = g_1^k g_2^k = f(g_1) f(g_2)$ 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 $k = a + np$, $0 < a \le p-1$, $a, n \in \mathbb{Z}$.

Then $g^k = 1 \Rightarrow g^k = g^{a+np} = g^a \underbrace{g^{np}}_{\substack{\text{since } |G| = p, \\ g^{np} = 1.}} = g^a = 1$.

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

By Lagrange's Thm., every elt. has order dividing the group, so $|g| = 1$ or p since $|G| = p$.
Since $0 < a \le p-1$, 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 $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{p-1}\}$
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.

$\square$

(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.

$\square$

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:

$$\begin{aligned}
(h,0)^2 &= (h,0)(h,0) = (h\varphi_0(h), 0) \\
(h,0)^3 &= (h,0)^2(h,0) = (h\varphi_0(h),0)(h,0) = (h\varphi_0(h)\varphi_0(h), 0) \\
&\qquad\qquad = (h\varphi_0(h)^2, 0) \\
&\vdots \\
(h,0)^k &= (h\varphi_0(h)^{k-1}, 0) = (h \cdot h^{k-1}, 0) = (h^k, 0) = (0,0)
\end{aligned}$$

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 $(h,0)^k = (0,0)$.

$$\begin{aligned}
(h,0)^k = (h\varphi_0(h)^{k-1}, 0) = (0,0) \Rightarrow\ & h\varphi_0(h)^{k-1} = 0 \\
& h \cdot h^{k-1} = 0 \\
& h^k = 0 \Rightarrow h \text{ has finite order.}
\end{aligned}$$

□

(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 $\Phi: H \rtimes_\varphi \mathbb{Z} \longrightarrow H \rtimes_\psi \mathbb{Z}$ 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

$$\begin{aligned}
\Phi((h_1,n_1)(h_2,n_2)) &= \Phi((h_1\varphi_{n_1}(h_2), n_1+n_2)) \\
&= (h_1 f^{n_1}(h_2), -(n_1+n_2)) \\
&= (h_1 f^{n_1}(h_2), -n_1-n_2) \\
&= (h_1,-n_1)(h_2,-n_2) \\
&= \Phi((h_1,n_1))\Phi((h_2,n_2))
\end{aligned}$$

this equality follows from ↓

in $H \rtimes_\psi \mathbb{Z}$:

$$\begin{aligned}
(h_1,-n_1)(h_2,-n_2) &= (h_1\psi_{-n_1}(h_2), -n_1-n_2) \\
&= (h_1 f^{-(-n_1)}(h_2), -n_1-n_2)
\end{aligned}$$

$$= (h_1 f^{n_1}(h_2), -n_1 - n_2)$$

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)

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

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

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

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 $A^T w = \lambda w$ in $\mathbb{C}^n$, then prove that the matrix $B = vw^T$ commutes with A.

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

λ is a scalar

$$AB = A(vw^T) = (Av)w^T = (\lambda v)w^T = v(\lambda w^T)$$
$$= v(\lambda w)^T = v(A^T w)^T = vw^T A^{T^T}$$
$$= BA.$$

□

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, $\{\text{primes}\} = \{\text{irred.}\}$.

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

(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. $\square$

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

$$\left.\begin{aligned} 0^3 + 2\cdot 0 + 1 &\equiv 1 \ (3) \\ 1^3 + 2\cdot 1 + 1 &\equiv 1 \ (3) \\ 2^3 + 2\cdot 2 + 1 &\equiv 1 \ (3) \end{aligned}\right\} \text{can do this test b/c the poly. is a cubic.}$$

field

roughly looks like $\{ax^2+bx+c : a, b, c \in \mathbb{Z}/3\mathbb{Z}\}$

Observe that $\mathbb{Z}[x]/(3, x^3+2x+1) \cong (\mathbb{Z}/3)[x]/\overset{\text{irred.}}{(x^3+2x+1)}$, which has size 27 since we are mod-ing out by a cubic.

Therefore, $\mathfrak{m} = (3, x^3+2x+1)$ is such an ideal. $\square$

(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.

$\square$