Dr. Marques Sophie
Office 519

Spring Semester 2017
marques@cims.nyu.edu

Problem Set #7

In the following, $\cong$ denotes a isomorphism of groups.

Exercise 0 :

Let G be a finite abelian group with $|G| = n$, we will see next week that $x^n = e$. Let $k > 0$ be an integer such that $\gcd(k, n) = 1$. Prove that every $g \in G$ can be written in the form $g = x^k$ for some $x \in G$.

Solution :

$gcd(k, n) = 1 \Rightarrow \exists r, s \in \mathbb{Z}$ such that $rk + sn = 1$. Now, by Lagrrange's theorem. $g^n = e$ for all $g \in G$. But,

$$g = g^1 = g^{rk+sn} = (g^r)^k \cdot (g^n)^s = (g^r)^k.e^S = (g^r)^k$$

Take $x = g^r$ to get $x^k = g$.

Exercise 1 :

In $\mathrm{GL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{C})$ define the subgroups of *scalar* matrices

$$\mathbb{C}^\times I = \{\lambda I : \lambda \neq 0 \text{ in } \mathbb{C}\} \qquad \Omega_n I = \{\lambda I : \lambda \in \Omega_n\}$$

where Ω_n are the complex n^{th} roots of unity.

(a) Prove that $\mathbb{C}^\times I$ and $\Omega_n I$ are normal in $\mathrm{GL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{C})$ respectively.

(b) Prove that $\mathrm{GL}(n, \mathbb{C})/\mathbb{C}^\times I \cong \mathrm{SL}(n, \mathbb{C})/\Omega_n I$

Hint : Use the Second Isomorphism Theorem. If $N = \mathbb{C}^\times I$ show that

$$N \cdot \mathrm{SL}(n, \mathbb{C}) = \mathrm{GL}(n, \mathbb{C})$$

□

Solution :

(a) If $g \in \lambda I$, $(\lambda \neq 0)$ then g commutes with every $A \in GL_n(\mathbb{C})$, so $A(\lambda I)A^{-1} = \lambda I \in \mathbb{C}^\times I$ for all $A \in G_N(\mathbb{C})$ and $\mathbb{C}^\times I$ normal in $GL_n(\mathbb{C})$. Likewise if $\lambda \in \Omega_n$, λI now belongs to $SL_n(\mathbb{C})$ since $det(\lambda I) = \lambda^n \cdot I = 1 \cdot I = I$, and again we have $B(\lambda \cdot I)B^{-1} = \lambda I$, $\forall B \in SL_n(\mathbb{C}) \Rightarrow \Omega_n I$ is normal in $SL_N(\mathbb{C})$.

(b) First, note that any $A \in GL_n(\mathbb{C})$ is λB with $det(B) = 1$, for a suitably chosen $a \neq 0$ in $\mathbb{C}$. If $n = det(A)$, it has n^{th} roots $\lambda \in \mathbb{C}$ $(\lambda^n = \mu)$ and then $B = 1/\lambda A$

has $det(B) = (1/\lambda)^n \cdot det(A) = 1/\mu \cdot \mu = 1$. Thus if $N = \mathbb{C}^* I$, we have N is a normal group of $GL_n(\mathbb{C})$ and $GL_n(\mathbb{C}) = \mathbb{C}^\times I \cdot SL_n(\mathbb{C})$.
Now apply 2nd Isomorphism theorem taking $A = SL_n(\mathbb{C})$, $N = \mathbb{C}^\times I$. Then

$$A \cap N = SL_n(\mathbb{C}) \cap \mathbb{C}^\times I = \{\lambda I : \lambda \neq 0 \ in\ \mathbb{C}\ and\ det(\lambda I) = \lambda^n\ is\ = 1\}$$

That means λ is an n^{th} root of unity, so $A \cap N = \Omega_n I$ and

$$GL_n(\mathbb{C}) = AN/N \simeq A/(A \cap N) = SL_n(\mathbb{C})/\Omega_n I$$

Exercise 2 :
If H is a subgroup of finite index in a group G, prove that there are only finitely many distinct "conjugate" subgroups aHa^{-1} for $a \in G$.
Solution :
Given $a \in G$, and $h \in H$, the element $x = ak$ conjugates H to the conjugates H to the subgroup $(ah)H(ah)^{-1} = ahHh^{-1}a^{-1}$, since $(xy)^{-1} = y^{-1}x^{-1}$. But $hHh^{-1} = H$, for all $h \in H$, so $(ah)H(ah)^{-1} = aHa^{-1}$ for all $h \in H$.
The group G is a union of n disjoint cosets $a_1H = H$, $a_2H, \dots, a_nH$, $(n = |G/H|)$ since H has finite index. All $x \in a_nH$ give the same "conjugate" xHx^{-1}, so there are at most n distinct conjugates, $H = eHe^{-1}$, $a_2Ha_2^{-1}, \dots, a_nHa_n^{-1}$.

Exercise 3 :
Let $G = (\mathbb{R}^\times, \cdot)$ be the multiplicative group of nonzero real numbers, and let N be the subgroup consisting of the numbers ± 1. Let $G' = (0, +\infty)$ equipped with multiplication as its group operation. Prove that N is normal in G and that $G/N \cong G' \cong (\mathbb{R}, +)$.
Solution :

(a) G is abelian so all subgroups are normal; to see $G/N \simeq G'$ via first Isomorphism theorem. Let $\phi : G \to G'$ be the squaring map $f(x) = x^2$. This is a homomorphism since $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$. It is surjective since every $x > 0$ is $\phi(\sqrt{x})$. $Ker(\phi- = \{\pm 1\}$. By F.I.T, $G/N \simeq G'$.

(b) To see $G' = ((0, +\infty), \cdot) \simeq (\mathbb{R}, +)$. Taking $\phi(x) = ln(x)$. This is a bijection and $ln(xy) = ln(x) + ln(y)$ so $ln : G' \to (\mathbb{R}, +)$ is a group $\simeq$.

Exercise 4 :
If H is a subgroup of G, its *normalizer* is $N_G(H) = \{g : gHg^{-1} = H\}$. Prove that

(a) $N_G(H)$ is a subgroup.

(b) H is a normal subgroup in $N_G(H)$.

(c) If $H \subseteq K \subseteq G$ are subgroups such that H is a normal subgroup in K, prove that K is contained in the normalizer $N_G(H)$.

(d) A subgroup H is normal in $G \Leftrightarrow N_G(H) = G$.

Note : Part (c) shows that $N_G(H)$ is the largest subgroup of G in which H is normal.
Solution :

(a)Trivial. If $g_1, g_2 \in N_G(H)$ then

$$g_1g_2 \cdot H \cdot (g_1g_2)^{-1} = g_1(g_2Hg_2^{-1})g_1^{-1} = g_1Hg_1^{-1} = H$$

so $g_1g_2 \in N_G(H)$. Obviously, $g = e$ is in $N_G(H)$. Finally, $g \in N(H) \Rightarrow gHg^{-1} = H, \Rightarrow H = g^{-1}Hg = g^{-1}H(g^{-1})^{-1}$, so $g^{-1} \in N_G(H)$. Finally, $g \in N(H) \Rightarrow gHg^{-1} = H \Rightarrow H = g^{-1}Hg = g^{-1}H(g^{-1})^{-1}$ so $g^{-1} \in N(H)$. Done.

(b) H is normal in $N_G(H)$. Really trivial : $g \in N(H) \Rightarrow gHg^{-1} = H$, and clearly $H \subseteq N_G(H)$.

(c) Suppose $H \subseteq K$ are subgroups of G and that H is a normal subgroup K ($kHk^{-1} = H$, $\forall k \in K$). Prove that $K \subseteq N_G(H)$. Totally obvious from definition of $N_G(H)$.

(d) $(\Rightarrow)$ H normal subgroup of $G \Rightarrow gHg^{-1} = H$, $\forall g \in G \Rightarrow G = N_G(H)$. $(\Leftarrow)$ $N_G(H) = G \Rightarrow gHg^{-1} = H$, $\forall g \Rightarrow H$ is normal subgroup of G.

Exercise 5 :

If $x, y \in G$, products of the form $[x, y] = xyx^{-1}y^{-1}$ are called *commutators* and the subgroup they generate

$$[G, G] = \left\langle xyx^{-1}y^{-1} : x, y \in G \right\rangle$$

is the **commutator subgroup** of G. Prove that

(a) The subgroup $[G, G]$ is normal in G.

(b) The quotient $G/[G, G]$ is abelian.

Hint : In (a) recall that a subgroup H is normal if $\alpha_g(H) = gHg^{-1} \subseteq H$ for all $g \in G$. What do conjugations α_g do to the generators $[x, y]$ of the commutator subgroup ?

Solution :

(a) If $x \in G$, $\alpha_x(g) = xgx^{-1}$ takes commutators to commutators :

$$\begin{aligned}
\alpha_x([a, b]) &= \alpha_x(aba^{-1}b^{-1}) \\
&= x(aba^{-1}b^{-1})x^{-1} \\
&= (xax^{-1}) \cdot (xbx^{-1}) \cdot (x(a^{-1})x^{-1}) \cdot (x(b^{-1})x^{-1}) \\
&= \alpha_x(a)\alpha_x(b)\alpha_x(a)^{-1}\alpha_x(b)^{-1} \\
&= [\alpha_x(a), \alpha_x(b)]
\end{aligned}$$

$[\alpha_x(g^{-1}) = (\alpha_x(g))^{-1}, \forall g]$.

Thus each operator α_x maps generators of $[G, G]$ to generators : if $S =$ (the set of all commutators $[x, y]$, $x, y \in G$) then $\alpha_x(S) \subseteq S$. We must show this $\Rightarrow \alpha_x(< S >) \subseteq < S >$, and that will prove normality of $< S >= [G, G]$.

In an earlier problem set we showed that the generated subgroup $< S >$ for any set $S \subseteq G$ consists of all "words of finite length" $w = a_1 \ldots a_r$ with $r \leqslant \infty$ and $a_i \in S$ or $a_i \in S^{-1}$. But for any such word, $\alpha_x(w) = \alpha_x(a_1) \ldots \alpha_x(a_r)$ is just another word of the same type because if $a_i = s \in S$, we have $\alpha_x(s) \in S$, and if $a_i = s^{-1}$ for $s \in S$ then $\alpha_x(a_i) = \alpha_x(s^{-1}) = (\alpha_x(s))^{-1} \in S^{-1}$. Thus, for $\forall x \in G$,

α_x maps words to words, and hence maps $< S >$ to $< S >$. Applying this to $S = (all\ commutators)$, we see $[G, G]$ is normal in G.

(b) As for abelian property of the quotient group, let $\pi : G \to G/[G, G] = \bar{G}$ be the quotient homomorphism. Then $\pi(aba^{-1}b^{-1}) = \bar{e}$, by definition of $[G, G]$. But the $e = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1}$, which implies $\pi(b)\pi(a) = \pi(a)\pi(b)$. (Elements in $range(\pi)$ commute. Since π is surjective, all elements in $barG$ commute.

Exercise 7 :

Let G be the group of all real 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \text{such that } ad \neq 0 \ .$$

Show that the commutator subgroup $[G, G]$ defined in Exercise 3.3.28 is precisely the subset of matrices in G with 1's on the diagonal and an arbitrary entry in the upper right corner.

Solution :

We do a brute force calculation of a typical commutator $ABA^{-1}B^{-1}$, remembering that these are the generators of $[G, G]$. If $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $B = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in G$. Then $ad, a'd' \neq 0$ and $A^{-1} = 1/(ad)\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$, $B^{-1} = 1/(a'd')\begin{pmatrix} d' & -b' \\ 0 & a' \end{pmatrix}$. All diagonal entries are nonzero. Then by direct matrix calculation

$$\begin{aligned} ABA^{-1}B^{-1} &= \begin{pmatrix} 1 & -b'/d - (a'b)/(dd') + (ab')/(dd') + b/d \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1/(dd')(-b'd' - a'b + ab' + bd') \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & b'(a - d')/(dd') + b(d' - a')/(dd') \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Take $d, d' \neq 0$ and a' such that $(d' - a')/(dd') = 1$; then the set $a = d'$ (b can be arbitrary in $\mathbb{R}$). We see that the set $S = \{ABA^{-1}B^{-1} : A, B \in G\}$ contains all elements of the form $C = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $b \in \mathbb{R}$.

Now $[G, G] =< S >$. But note that $S = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R}\}$ is already a group under the matrix multiplication($(det(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = 1 \neq 0$, and $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b + b' \\ 0 & 1 \end{pmatrix}$). Since $< S >=$ the smallest subgroup in G that contains the set of generators S, we must have $< S >= S = [G, G] = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R}\}$

Exercise 8 :

Consider the group $(\mathbb{Z}/12\mathbb{Z}, +)$.

(a) Identify the set of units U_{12}.

(b) What is the order of the multiplicative group $(\mathrm{U}_{12}, \cdot\,)$? Is this abelian group *cyclic* ?

Hint : What is the maximal order of any element $g \in \mathrm{U}_{12}$?

Solution :

(a) In $\mathbb{Z}/12\mathbb{Z}$ the multiplication units are $U_{12} = \{[1], [5], [7], [11]\}$.

(b) $|U_{12}| = 4$; elements can be have orders $o(x) = 1, 2, 4$ by Lagrange. Now :

$$o([1]) = 1; o([5]) = 2; \textit{ since } [1], [5], [25] = [1] \textit{ are pairs as } x^k$$

$$o([7]) = 2 \textit{ since } [1], [7], [7]^2 = [49] = [1]$$

$$o([11]) = 2 \textit{ since } [11] = [-1] \textit{ and } (-1)^2 = [1]$$

This group is not cyclic since no x has order $o(x) = 4$.

Exercise 9 :

Let G be any group and let $\mathrm{Int}(G)$ be the set of conjugation operations $\alpha_g(x) = gxg^{-1}$ on G. Prove that

(a) Each map α_g is a homomorphism from $G \to G$.

(b) Each map α_g is a bijection, hence an automorphism in $\mathrm{Aut}(G)$.

(c) $\alpha_e = \mathrm{id}_{G}$, the identity map on G.

$\square$.

Solution :

If $\alpha_g(x) = gxg^{-1}$ then $\alpha_e(x) = exe^{-1} = x$, so $\alpha_e = Id_G$. Also,

$$\alpha_{g_1g_2}(x) = g_1g_2x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = \alpha_{g_1}(\alpha_{g_2}(x)), \forall x$$

So, $\alpha_{g_1g_2} = \alpha_{g_1} \circ \alpha_{g_2}$.

$$\alpha_{g^{-1}} \circ \alpha_g(x) = \alpha_{g^{-1}g}(x) = \alpha_e(x) = x$$

which implies $\alpha_{g^{-1}} = (\alpha_g)^{-1}$.

Additional : Show that each α_g is an isomorphism $G \to G$ (so $\alpha_g \in Aut(G)$). Since α_g is invertible, it is a bijection, one need only show α_g is a homomorphism :

$$\alpha_g(xy) = gxyg^{-1} = gxg^{-1}gxg^{-1} = \alpha_g(x) \cdot \alpha_g(y)$$

Exercise 10 :

Show that the group $\mathrm{Int}(G)$ of inner automorphisms is a *normal* subgroup in $\mathrm{Aut}(G)$.

Note : The quotient $\mathrm{Aut}(G)/\mathrm{Int}(G)$ is regarded as the group of *outer automorphisms* $\mathrm{Out}(G)$.

Solution :

Let α be an arbitrary automorphism and $\alpha_g \in Int(G)$. If $x \in G$. Then

$$\begin{aligned}
\alpha \circ \alpha_g \circ \alpha^{-1}(x) &= \alpha(g\alpha^{-1}(x)g^{-1}) \\
&= \alpha(g)\alpha(\alpha^{-1}(x))\alpha(g^{-1}) \\
&= \alpha(g) \cdot x \cdot \alpha(g^{-1}) = \alpha(g) \cdot x \cdot \alpha(g)^{-1} = \alpha_{\alpha(g)}(x)
\end{aligned}$$

Therefore $\alpha \circ \alpha_g \alpha^{-1}$ is automorphism. Thus $\alpha \circ Int(G) \circ \alpha^{-1} \subseteq Int(G)$, and $Int(G)$ is a normal sugroup of $Aut(G)$.

Exercise 11 :
The permutation group $G = S_3$ on three objects has $6 = 3!$ elements

$$S_3 = \{e, (12), (23), (13), (123), (132)\}$$

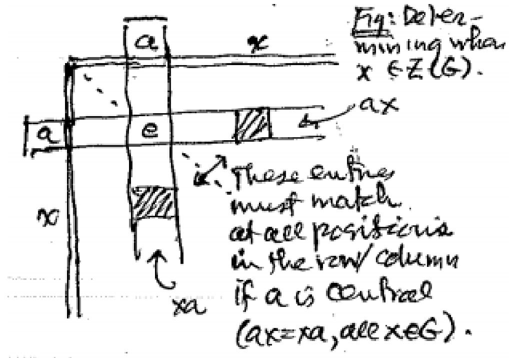
Prove by direct calculation the center of S_3 is trivial (Note : you have proven that $G \cong \mathrm{Int}(G)$). **Solution :**
$G = S_3$; Show that $G \simeq Int(G)$. This happens if and only if $Z(G) = (e)$. So our problem is to compute $Z(S_3)$ and show it is trivial. For this permutation group we can list all its elements and compute the 6×6 multiplication table shown above. We have $S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. We omit these routine calculations (they may be simplified by noting that if $x = (1,2)$ and $y = (1,2,3)$. Then $(1,3,2) = y^{-1}$ and $o(y) = 3$ because

$$(1,2,3)(1,3,2) = (1,3,2)(1,2,3) = e$$
$$(1,2,3)^2 = (1,3,2)$$
$$(1,2,3)^3 = e$$

Obviously $x^2 = e$, since $(1,2)(1,2) = e$ (all the 2-cycle have order $= 2$). Finally, $xyx = y^{-1}$, by direct calculation. That means $S_3 =< x, y >$ is isomorphic to the dihedral group D_3, which has trivial center because ($n = 3$ is odd))
Even if you don't adopt these tricks it is still simple (but tedious to compute the multiplication table $Z(G)$ can be read out of this table as shown above the table. Inspection shows that $g = e$ is the only element in S_3.

Table $a \cdot b =$ $(G = S_3)$

$a \backslash b$	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)



Exercise 12 :
For any group G prove that the commutator subgroup $[G,G] =< xyx^{-1}y^{-1}|x,y \in G >$ is a *characteristic subgroup* that is for any $\sigma \in Aut(G)$, we have $\sigma([G,G]) = [G,G]$.
Hint : What does an automorphism do to the generators of $[G,G]$?
Note : This example shows that if G is abelian its automorphism gorup may nevertheless be noncommuative (while $\text{Int}(G)$ is trivial).
Solution :
If $c = [x,y]$ is any commutator in S then

$$\alpha(x) = \alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} = [\alpha(x), \alpha(y)]$$

is just another commutator in S is again in S is again in S because

$$[xy]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x]$$

is a commutator in S. Thus $S = S^{-1} = S \cup S^{-1}$. Now $[G,G] =< S >$ means : a typical element in $[G,G]$ is a word $g = c_1c_2 \dots c{-}r$ with $r < \infty$ and $c_i \in S$. Then $\alpha(g) = \alpha(c_1) \dots \alpha(c_r)$ is just another word in $[G,G]$ so $\alpha([G,G]) \subseteq [G,G]$. Likewise, taking α^{-1} in place of α, $\alpha^{-1}[G,G] \subseteq [G,G]$ which yields the reverse inclusion $[G,G] \subseteq \alpha[G,G] \subseteq [G,G]$. So $\alpha[G,G] = [G,G]$ as claimed.

Exercise 13 :
If G is a group, Z is its center, and the quotient group G/Z is *cyclic*, prove that G must be abelian.
Solution :
Let $\bar{a} = \pi(a) \in G/Z$ $(a \in G)$ be a cyclic generator of G/Z, where $\pi : G \to G/Z$ is the quotient homomorphism. Let $A =< a >$ in G. The product set $A \cdot Z$ is a subgroup in G because $z, z' \in Z \to (a'z') \cdot (az) = (a'a) \cdot (z'z) \in AZ$.
Furthermore : $\pi(AZ) = \pi(A) \cdot \pi(Z)$ and $\pi(Z) = \bar{e}$ (identity in G/Z) we get

$$\pi(AZ) = \pi(A) = \pi\{a^k : k \in \mathbb{Z}\} = \{(\bar{a})^k : k \in \mathbb{Z}\} =< \bar{a} >= G/Z$$

Thus if $g \in G$, $\exists x \in AZ$ such that $\pi(x) = \pi(g)$, which implies $gZ = xZ$, and in particular, $\exists z_0 \in Z$ such that $g = g \cdot e = xz_0 \in (AZ) \cdot z_0 = AZ$. Hence, $G \subseteq AZ$, so $G = AZ$.
If $xy \in G$, we can find $a_i \in A$, $z_i \in Z$ such that $x = a_1z_1$, $y = a_2z_2$. But $A =< a >$ is

obviously abelian (as is any cyclic subgroup) and the $z_i \in Z(G)$ commute with everybody, so we get

$$xy = a_1z_1 \cdot a_2z_2 = a_1a_2 \cdot z_1z_2 = a_2a_1 \cdot z_2z_1 = (a_2z_2) \cdot (a_1z_1) = y \cdot x$$

G is abelian.