Exam I Review

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

- Group $(G,*)$: i) Closure ii) Associativity iii) Identity iv) Inverses
  - □ abelian (eg. $(\mathbf{Z}_n, +_{[\,]})$, $(\mathbf{Z}_n^\times, \cdot_{[\,]})$) v.s. nonabelian (eg. $S_n, n \geq 3$)
  - □ finite (eg. $|\mathbf{Z}_n| = n$, $|\mathbf{Z}_n^\times| = \varphi(n)$) v.s. infinite (eg. $(\mathbf{Z}, +)$)
- Subgroup $(H,*)$: i), iii), iv) $\Leftrightarrow H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$
  - ◇ $|H| < \infty$: H is a subgroup $\Leftrightarrow H \neq \emptyset$ and $ab \in H$ for all $a, b \in H$
  - ◇ Cyclic subgroup $\langle a \rangle$ is the *smallest* subgroup of G containing $a \in G$.
  - ◇ G is cyclic if $G = \langle a \rangle$; $|\langle a \rangle| = o(a)$; If $o(a) < \infty$, then $a^k = e \Leftrightarrow o(a)|k$
  - ◇ **Lagrange's Theorem:** If $|G| < \infty$ and $H \subseteq G$, then $|H|\big||G|$.
    - ▷ $o(a)\big||G|$ for any $a \in G$. $\rightsquigarrow$ Euler's Theorem
    - ▷ Any group of prime order is cyclic.
- Constructing (sub)groups:
  - ◦ $H \cap K$ is the *largest* subgroup contained in both H and K.
  - ◦ Product HK is not always a subgroup of G.
    - ⊙ $h^{-1}kh \in K$ ✓ $\rightsquigarrow$ HK is the *smallest* subgroup containing both H and K
    - ⊙ $|HK| = |H||K|/|H \cap K|$ if $|G| < \infty$.
  - ◦ Direct product $G_1 \times G_2$ is a group under the operation $(*_1, *_2)$.
    - ⊙ $o((a_1, a_2)) = [o(a_1), o(a_2)]$; $|G_1 \times G_2| = |G_1| \cdot |G_2|$ if G_1, G_2 are finite.
    - ⊙ $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow \gcd(n, m) = 1$.
  - ◦ Subgroup $\langle S \rangle$ generated by S; New groups defined over a field F.

Let $S = \mathbf{R} - \{-1\}$. Define $*$ on S by $a * b = a + b + ab$, for all $a, b \in S$. Show that $(S, *)$ is an abelian group.

Proof: i) **Closure:** To show $a * b \in S$, i.e., $a + b + ab \neq -1$ for all $a, b \in S$

Proof by contradiction: Assume $a + b + ab = -1$ for some $a, b \in S$

$$a + b + ab + 1 = 0 \quad \Rightarrow (a+1)(b+1) = 0 \quad \Rightarrow a \overset{!}{=} -1 \text{ or } b \overset{!}{=} -1$$

ii) **Associativity:** $(a * b) * c = \cdots = a * (b * c)$ for all $a, b, c \in S$

Commutativity: $a * b = \cdots = b * a$ for all $a, b \in S$

iii) **Identity:** 0 By **Commutativity**, we only need to check one equation

$$a * 0 = \cdots = a \quad \text{for all } a \in S.$$

iv) **Inverses:** $\dfrac{-a}{a+1}$ By **Commutativity**, only need to check one equation

$$a * \frac{-a}{a+1} = \cdots = 0 \quad \text{for all } a \in S.$$

Let H be any subgroup of G and $a \in G$. Then aHa^{-1} is a subgroup of G.

Proof: Note that $aHa^{-1} = \{g \in G : g = aha^{-1} \text{ for some } h \in H\}$.

Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}$. Then $g_1g_2 = a(h_1h_2)a^{-1} \in aHa^{-1}$.

Identity: $e = aea^{-1} \in aHa^{-1}$.

Inverses: $g = aha^{-1} \in aHa^{-1} \quad \Rightarrow g^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$. □

Way 2: Nonempty e; $\quad g_1g_2^{-1} = ah_1a^{-1}(ah_2a^{-1})^{-1} = ah_1h_2^{-1}a^{-1}$ □

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N := \{g \in G : g = a^n \text{ for some } a \in G\}.$$

Then N is a subgroup of G.

Way 2: To show N is nonempty and $g_1g_2^{-1} \in N$ for all $g_1, g_2 \in N$.

- The identity element $e \in N$ since $e = e^n$.
- Let $g_1 = a_1^n$ and $g_2 = a_2^n$ for some $a_1, a_2 \in G$. Then

$$g_1g_2^{-1} = a_1^n(a_2^n)^{-1} = a_1^na_2^{-n} = a_1^n(a_2^{-1})^n \overset{!}{=} (a_1a_2^{-1})^n \in N.$$ □

Let H, K, L be subgroups of the group G and $H \subseteq K$. Prove that

$$H(K \cap L) = K \cap HL.$$

Note: This is an equality of sets, since they may not be subgroups.

Proof: $\subseteq$: For any $a \in H(K \cap L)$, there exist $h \in H, t \in K \cap L$ such that

$$a = ht. \quad \rightsquigarrow \begin{cases} a \in K \quad \text{[Why?]} \\ \\ a \in HL \quad \text{[Why?]} \end{cases}$$

$\supseteq$: For any $a \in K \cap HL$, there exist $h \in H$ and $\ell \in L$ such that

$$a = h\ell \quad \text{and} \quad a = k \text{ for some } k \in K. \qquad (\star)$$

To show $\ell \in K$ since $\ell \in H$ already. $\overset{(\star)}{\Longrightarrow} \ell = h^{-1}k \overset{!}{\in} K$ [Why?]