DAY 20: Exam I - Friday

Defs: Group, isomorphism of two algebraic structures, subgroup

Also: Subgroup Theorem

Office hours: I'll be around this afternoon; Th: 12-2

Recall $S_3$. If $a, b \in S_3$. Then the notation for the motion $a$ followed by the motion $b$ would be $ba$. Know how to do the computations given $(1 \ 2 \ 3)$

Ways to write $G$, a cyclic group of order $n \in \mathbb{Z}^+$.

$G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

$G \cong \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ modulo $n$

is isomorphic to

Theorem: Let $G$ be a cyclic group with $n$ elements which is generated by $a$. Let $b = a^s \in G$. Then $b$ generates a cyclic subgroup $H$ of $G$ containing $n/d$ elements where $d = \gcd(s, n)$.

Cor: If $a$ is a generator of a finite group $G$ of order $n$, then the other generators of $G$ are the elements of the form $a^r$ where $r$ is relatively prime to $n$.

Cor: An integer $k$ is a generator of $\mathbb{Z}_n$ iff $\gcd(k, n) = 1$. 
ex: \( \mathbb{Z}_{15} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 \} \)

\( |\mathbb{Z}_{15}| = |\langle 1 \rangle| = 15 \)

Underline the elements that generate \( \mathbb{Z}_{15} \).
(Note \( 15 = 3 \cdot 5 \))

Write down the distinct proper subgroups and underline generators.

\( \langle 0 \rangle = \{ 0 \} \)
\( \langle 3 \rangle = \{ 0, 3, 6, 9, 12 \} \)
\( \langle 5 \rangle = \{ 0, 5, 10 \} \)

Subgroup diagram

```
\begin{array}{ccc}
\langle 0 \rangle & \langle 3 \rangle & \langle 5 \rangle \\
| & \Uparrow & |
\end{array}
```

"Line segment" or edge designates the lower is a subgroup of the upper.

E.g. \( \langle 3 \rangle \rightarrow \langle 1 \rangle \)

I suggest you make an outline
Absence of a NO is a YES
Note some items are crossed out

\[ e, a \in S \quad \text{membership, 1} \]
\[ \emptyset \quad \text{empty set, 1} \]
\[ \varnothing, a \notin S \quad \text{nonmembership, 1} \]
\[ \{ x \mid P(x) \} \quad \text{set of all } x \text{ such that } P(x), 1 \]
\[ B \subseteq A \quad \text{set inclusion, 2} \]
\[ B \subset A \quad \text{subset } B \neq A, 2 \]
\[ A \times B \quad \text{Cartesian product of sets, 3} \]
\[ \mathbb{Z} \quad \text{integers, 3} \]
\[ \mathbb{Q} \quad \text{rational numbers, 3} \]
\[ \mathbb{R} \quad \text{real numbers, 3} \]
\[ \mathbb{C} \quad \text{complex numbers, 3} \]
\[ \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+ \quad \text{positive elements of } \mathbb{Z}, \mathbb{Q}, \mathbb{R}, 3 \]
\[ \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^* \quad \text{nonzero elements of } \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, 3 \]
\[ \mathbb{P} \quad \text{relation, 3} \]
\[ |A| \quad \text{number of elements in } A, \text{ as order of group, 50} \]
\[ \phi : A \to B \quad \text{mapping of } A \text{ into } B \text{ by } \phi, 4 \]
\[ \phi(a) \quad \text{image of element } a \text{ under } \phi, 4 \]
\[ \phi[A] \quad \text{image of set } A \text{ under } \phi, 4 \]
\[ \Rightarrow \quad \text{one-to-one correspondence, 4} \]
\[ \phi^{-1} \quad \text{the inverse function of } \phi, 5 \]
\[ n \quad \text{cardinality of } \mathbb{Z}^+, 5 \]
\[ x \quad \text{cell containing } x \in S \text{ in a partition of } S, 6 \]
\[ \equiv_n, a = b (\text{mod } n) \quad \text{congruence modulo } n, 7 \]
\[ \mathcal{P}(A) \quad \text{power set of } A, 9 \]
\[ U \quad \text{set of all } z \in C \text{ such that } |z| = 1, 15 \]
\[ \mathbb{R}_c \quad \text{set of all } x \in \mathbb{R} \text{ such that } 0 \leq x < c, 16 \]
\[ +_c \quad \text{addition modulo } c, 16 \]
\[ U_n \quad \text{group of } n \text{th roots of unity, 18} \]
\[ \mathbb{Z}_n \quad \{0, 1, 2, \ldots, n - 1\}, 18 \]
\[ \text{cyclic group } \{0, 1, \ldots, n - 1\} \text{ under addition modulo } n, 54 \]
\[ \text{group of residue classes modulo } n, 137 \]
\[ \text{ring } \{0, 1, \ldots, n - 1\} \text{ under addition and multiplication modulo } n, 169 \]
\[ *, a * b \quad \text{binary operation, 20} \]
\[ \circ, f \circ g, \circ \tau \quad \text{function composition, 22, 76} \]
\[ (S, *) \quad \text{binary structure, 29} \]
\[ \cong, S \cong S' \quad \text{isomorphic structures, 30} \]
\[ e \quad \text{identity element, 32} \]
\[ M_{m \times n}(S) \quad m \times n \text{ matrices with entries from } S, 40 \]
\[ M_n(S) \quad n \times n \text{ matrices with entries from } S, 40 \]
\[ \text{GL}(n, \mathbb{R}) \quad \text{general linear group of degree } n, 40 \]
\[ \det(A) \quad \text{determinant of square matrix } A, 46 \]
\[ a^{-1}, -a \quad \text{inverse of } a, 49 \]
\[ H \leq G; K \leq L \quad \text{subgroup inclusion, 50; substructure inclusion, 173} \]
\[ H < G; K < L \quad \text{subgroup } H \neq G, 50; \text{substructure } K \neq L, 173 \]
\[ (a) \quad \text{cyclic subgroup generated by } a, 54 \]
\[ n \mathbb{Z} \quad \text{principal ideal generated by } n, 250 \]
\[ m \mathbb{Z} \quad \text{ideal of } \mathbb{Z}, 250 \]
\[ \gcd \quad \text{greatest common divisor, 62, 250, 395} \]
\[ \cap \quad \text{intersection of sets, 60} \]