Algebra Exam 1 Note Sheets

1.2 Binary Operations

Definitions:

Binary Operation: A binary operation $*$ on set S is a function from $S \times S$ to S. We denote an output as $a*b$. Big Idea: Take 2 elements from S, (a, b) and the operation gives $a * b$, which is an element of S.

Commutative: If $a * b = b * a$ for all $a, b \in S$.

Associative: If $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Closed: Suppose $*$ is a binary operation on S and $H \subset S$. We say H is $\underline{\text{closed under } *}$ if for all $a, b \in H$, $a * b \in H$.

Identity: There exists $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.

Inverse: For all $a \in G$, there exists $a' \in G$ such that $a*a' = a'*a = e$.

Examples:

1. Let $L = \{n^2 \mid n \in \mathbb{N}\}$. Is L closed under $+$? No: $16 + 4 \notin L$.

2. Is L closed under $\cdot$? Yes. Let $a, b \in L$. There exists $n, m \in L$ such that $a = n^2$ and $b = m^2$. Then $a \cdot b = n^2 \cdot m^2 \implies a \cdot b = (nm)^2$. Since $n, m \in \mathbb{N}$, $a, b \in L$. Therefore, L is closed under $\cdot$.

3. For tables, calculations are made from the column element to the row element. Commutativity and associativity can be checked by testing all possible combinations.

4. Suppose that $*$ is an associative and commutative binary operation on a set S. Show that $H = \{a \in S \mid a * a = a\}$ is closed under $*$. (The elements of H are **idempotents** of the binary operation $*$.)

   Solution. Suppose that $*$ is an associative and commutative binary operation on set S. Let $a, b \in H$ and consider the following:

$$\begin{aligned}
(a * b) * (a * b) &= (b * a) * (a * b) && \text{commutative property,}\\
&= b * (a * a) * b && \text{associative property,}\\
&= b * a * b && \text{definition of } H,\\
&= b * b * a && \text{commutative property,}\\
&= (b * b) * a && \text{associative property,}\\
&= b * a && \text{property of } H,\\
&= a * b && \text{commutativity property.}
\end{aligned}$$

   Therefore, H is closed because $a * b \in H$.

1.3 Isomorphisms

Definitions:

Isomorphism: Let $\langle G, * \rangle$ and $\langle G', *' \rangle$ be 2 binary structures. We say they are *isomorphic* if there exists an function $\phi : G \to G'$ such that

1. ϕ is a bijection
2. ϕ preserves the operation ($\forall a, b \in G$, $\phi(a * b) = \phi(a) *' \phi(b)$).

One-to-One: If $f(a) = f(b)$, then $a = b$.

Onto: Let $f : X \to Y$. f is *onto* if for every $y \in Y$, there exists at least one $x \in X$ such that $f(x) = y$.

Examples:

1. $\langle \mathbb{Z}, + \rangle$ with $\phi : \mathbb{Z} \to 2\mathbb{Z}$ and $\langle 2\mathbb{Z}, + \rangle$ with $\phi(x) : 2x$. This is one-to-one (just draw a diagram and line them up to each other), and onto because every element in y has an x that is mapped to it. It's a homomorphism because $\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b)$.

To prove that two groups are not isomorphic, you must rely on *structural properties.* Consider the following examples to demonstrate structural property differences:

2. The sets $\mathbb{Z}$ and $\mathbb{Z}^+$ both have cardinality $\aleph_0$, and there are lots of one-to-one functions mapping $\mathbb{Z}$ onto $\mathbb{Z}^+$. However, the binary structures $\langle \mathbb{Z}, \cdot \rangle$ and $\langle \mathbb{Z}^+, \cdot \rangle$, where $\cdot$ is the usual multiplication, are not isomorphic. In $\langle \mathbb{Z}, \cdot \rangle$, there are two elements x such that $x \cdot x = x$, namely 0 and 1. However, in $\langle \mathbb{Z}^+, \cdot \rangle$, there is only the single element 1.

3. The binary structures $\langle \mathbb{C}, \cdot \rangle$ and $\langle \mathbb{R}, \cdot \rangle$ under the usual multiplication are not isomorphic. (It can be shown that $\mathbb{C}$ and $\mathbb{R}$ have the same cardinality.) The equation $x \cdot x = c$ has a solution x for all $c \in \mathbb{C}$, but $x \cdot x = -1$ has no solution in $\mathbb{R}$.

These are a list of possible structural and nonstructural properties:

Structural Properites

1. The set has 4 elements.
2. The operation is commutative.
3. $x * x = x$ for all $x \in S$.
4. The equation $a * x = b$ has a solution x in S for all $a, b \in S$

Nonstructural Properties

1. The number 4 is an element.
2. The operation is called "addition."
3. The elements of S are matrices.
4. S is a subset of $\mathbb{C}$.

1.4 Groups

Definitions:

Group: A *group* $\langle G, * \rangle$ is a set G closed under a binary operation $*$ such that there is an inverse, an identity element, and the associative property is upheld.

Examples:

Let $*$ be defined on $\mathbb{Q}^+$ as $a * b = \frac{ab}{2}$. Show this is a group:

- **Associativity:** Let $a, b, c \in \mathbb{Q}^+$. $(a*b)*c = \frac{ab}{2} * c = \frac{abc}{4} = \frac{2(bc/2)}{2} = a * \frac{bc}{2} = a * (b * c)$.
- **Identity:** $a * e = a \implies e = 2$.
- **Inverses:** $a * a' = 2 \implies \frac{aa'}{2} = 2 \implies aa' = 4 \implies a' = \frac{4}{a} \implies a * \frac{4}{a} = \frac{a(4/a)}{2} = 2$. So, the identity is $a' = \frac{4}{a}$, and this exists in the group.

1.5 Subgroups

Definitions:

Subgroup: Let G be a group, where $H \subseteq G$. H is called a *subgroup* of G if:

1. H is closed under the operation.
2. Identity element belongs to H.
3. Each element of H must have its inverse in H.

Note: For finding subgroups of some modulo integer set, just use the divisors of the set.

Examples:

1. Determine whether the group consisting of the $n \times n$ matrices with determinant -1 or 1 is a subgroup of $GL(n, \mathbb{R})$.

   Let H be the set of all $n \times n$ matrices with determinant -1 or 1. We will show that H is a subgroup of $GL(n, \mathbb{R})$ by verifying the subgroup criterion:

   - **Identity:** The identity matrix I_n has a determinant of 1, so $I_n \in H$.
   - **Closure:** Let $A, B \in H$. Then $\det(A) = \pm 1$ and $\det(B) = \pm 1$. The determinant of the product AB is given by $\det(AB) = \det(A)\det(B) = (\pm 1)(\pm 1) = \pm 1$. Thus, $AB \in H$.
   - **Inverses:** Let $A \in H$. Then $\det(A) = \pm 1$. The determinant of the inverse A^{-1} is given by $\det(A^{-1}) = \frac{1}{\det(A)} = \pm 1$.. Thus, $A^{-1} \in H$.

1.6 Cyclic Groups

Definitions:

Cyclic: A group is *cyclic* if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$. We call the element $a \in G$ a generator.

Order: For any $b \in G$, $\langle b \rangle$ is a cyclic subgroup. The *order* of element b is the cardinality of b.

Relatively Prime: If two integers are *relatively prime*, then their $\gcd(r, s) = 1$. Thus, there exists $n, m \in \mathbb{Z}$ such that $nr + ms = 1$.

The Division Algorithm for $\mathbb{Z}$: Let m be a positive integer, and n be any integer. Then there exists unique q and r such that $n = m \cdot q + r$ with $0 \leq r < m$ (where q is the quotient, r is the remainder). Idea: $n = 42$, $m = 8$, $42 = 8(5) + 2$ and $n = -42$, $m = 8$, $-42 = 8(-6) + 6$.

Proof. On a number line where we have 0, m, $2m$, etc. n is either a multiple of m or it falls between two multiples of m. Let q be the largest integer such that $qm \leq n$. Then $r = n - qm$. Hence, $0 \leq r < m$. □

Theorems:

Theorem 1: Every subgroup of a cyclic group is cyclic.

Theorem 2: Let G be a cyclic subgroup. If G is infinite, then $G \simeq \mathbb{Z}$. If G is finite, with order n, then $G \simeq \mathbb{Z}_n$. ($\simeq$ is equivalence relation.)

Theorem 3: Let G be a cyclic group with n elements with generator a and $b = a^s$. Then b generates a cyclic subgroup of G of which contains $\frac{n}{d}$ elements where $d = \gcd(s, n)$. Also $\langle a^s \rangle = \langle a^t \rangle \iff \gcd(s, n) = \gcd(t, n)$.

1.7 Generating Sets

Properties of Cayley Digraphs:

1. The graph is always connected.
2. At most, 1 arc can go from 1 vertex to another.
3. Each vertex has exactly 1 type of each arc starting at the vertex and ending at the vertex.
4. If two sequences of arc types starting at one vertex end at the same place, then the same two sequences starting at a common vertex will end at the same place.

Any digraph that has these properties is a group.