Mathematics 5310.
AlgebraNotes00
Background Information and Definition of a Group.

Relations.

Definition. Suppose that each of A and B is a set. Then the Cartesian product $A \times B$ is defined to be:

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Definition. The set R is a relation from A to B means that $R \subset A \times B$. If $(a, b) \in R$ then "a is related to b" is denoted by aRb. The symbol $\sim$ is often used for relations. Thus for the relation $\sim$, $a \sim b$ means *a is related to b* according to the given relation R. (And sometimes I may use subscript $\sim_R$ for emphasis.)

Definition. If R is a relation from the set A to the set B then the domain (Dom) and range (Rng) of R are defined as the following:

$$\begin{aligned} \text{Dom}(R) &= \{a \in A | \text{ there exists } b \in B \text{ such that } (a, b) \in R\} \\ \text{Rng}(R) &= \{b \in B | \text{ there exists } a \in A \text{ such that } (a, b) \in R\}. \end{aligned}$$

Definition. A relation f from the set A to the set B (denoted by $f : A \to B$) is said to be a function if for each $x \in \text{Dom}(f)$ there is a unique element $y \in B$ so that $(x, y) \in f$. Notation: If f is a function and $(x, y) \in f$ then the unique element y is denoted by $f(x)$.

Definition. If R is a relation from the set A to the set B then the inverse relation, written as R^{-1}, is a relation from the set B to the set A defined by:

$$R^{-1} = \{(b, a) | (a, b) \in R\}.$$

Definition. If R is a relation from the set A to the set B and S is a relation from the set B to the set C then the composition of S and R relation, written as $S \circ R$, is a relation from the set A to the set C defined by:

$$S \circ R = \{(a, c) | \text{ there exists } b \in B \text{ so that } (a, b) \in R, (b, c) \in S\}.$$

[Convince yourself that this implies that if $a \sim_R b$ and $b \sim_S c$ then $a \sim_{S\circ R} c$.]

Definitions. Suppose that R is a relation from the set A to itself. We will use the notation $a \sim b$ to mean that a and b are in A and a is related to b or equivalently $(a, b) \in R$. Then:
R is said to be *reflexive* if $x \sim x$ for all $x \in A$.
R is said to be *symmetric* if it is true that if $x \sim y$ then $y \sim x$.
R is said to be *transitive* if it is true that if $x \sim y$ and $y \sim z$ then $x \sim z$.

Definition. A relation from a set into itself is said to be an *equivalence relation* if it is reflexive, symmetric and transitive. If $\sim$ is an equivalence relation on the set X then $[x]_\sim$ denotes the equivalence class of x:

$$x_\sim = \{y \in X \mid x \sim y\}.$$

For ease of notation, the subscript is often omitted when the equivalence under consideration should be understood.

Definition. The function $f : A \to B$ is 1-to-1 (one-to-one) or injective means that if $f(x) = f(y)$ then $x = y$. It is onto or surjective if for each $b \in B$ there is an $a \in A$ so that $f(a) = b$. A bijection is a function that is both injective and surjective.

Groups.

A group $(G, \cdot)$ is a set of elements G with an operation $\cdot$ that has the following properties:

1. Closure: if $x \in G$ and $y \in G$ then
   $x \cdot y \in G$;
2. Associativity: if $x, y, z \in G$ then
   $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
3. Identity: there is an element $e \in G$ so that for each $x \in G$:
   $e \cdot x = x = x \cdot e$;
4. Inverses: for each $x \in G$ there is an element x^{-1} so that
   $x \cdot x^{-1} = e = x^{-1} \cdot x$.

Note: In the abstract the operation $\cdot$ is thought of as the function $\psi : G \times G \to G$ such that $\psi(x, y) = x \cdot y$. Furthermore, for east of notation and when no confusion is expected to arise, $x \cdot y$ is generally abbreviated xy.

Examples 0.1 and Exercises: For each of the following sets and indicated operation, determine if the object is a group; if it isn't a group, indicate which group properties are not satisfied.

a.) Set = integers $\mathbb{Z}$, operation = usual addition.

b.) Set = integers $\mathbb{Z}$, operation = usual multiplication.

c.) Set = integers $\mathbb{Z}$, operation = usual subtraction.

d.) Set = real numbers $\mathbb{R}$, operation = usual addition.

e.) Set = real numbers $\mathbb{R}$, operation = usual multiplication.

f.) Set = positive real numbers $\{x \in \mathbb{R} | x > 0\}$, operation = usual multiplication.

g.) Set = 2×2 matrices each entry of which is a real number $\mathbb{R}$, operation = usual addition.

h.) Set = 2×2 matrices each entry of which is a real number $\mathbb{R}$, operation = usual multiplication.

i.) Set = 2×2 matrices each entry of which is a real number $\mathbb{R}$ and whose determinant is 1, operation = usual multiplication.

j.) Set = 2×2 matrices each entry of which is a real number $\mathbb{R}$ and whose determinant is ± 1, operation = usual multiplication.

k.) Set = $\{-1, 1\}$, operation = usual multiplication.

l.) Set = $\{0, 1\}$, operation = usual multiplication.

m.) Set = $\prod_{i=1}^{n} \{-1, 1\}$, operation = termwise multiplication.

n.) Set = the set of one-to-one onto functions from $\{1, 2, 3\}$ onto itself, operation = composition of functions $\circ$.

Theorem 0.1 [Uniqueness of the identity]. Suppose that G is a group with identity e. If $\hat{e}$ is an element of G so that for all $x \in G$, $\hat{e}x = x = x\hat{e}$ then $e = \hat{e}$.

Theorem 0.2 [Uniqueness of the inverse]. Suppose that G is a group with identity e and $x \in G$. Then there is a unique element $x' \in G$ so that $x \cdot x' = x' \cdot x = e$. [Notation: the unique inverse of the element x is denoted by x^{-1}.]

Theorem 0.3. Suppose that G is a group and $x, y, z \in G$ are arbitrary elements. Then:

1. $(x^{-1})^{-1} = x$.
2. $(xy)^{-1} = y^{-1}x^{-1}$.

3. $(xy = xz) \Rightarrow (y = z)$.
4. $(yx = zx) \Rightarrow (y = z)$.

Definition. A group G is said to be Abelian (or to be a commutative group) if and only if $xy = yx$ for all $x, y \in G$.

Exercise 0.2. Determine which groups from Examples 0.1 are Abelian - i.e. for those for which the operation turns out to produce a group, determine if the group is abelian.

Definition. Suppose that G is a group with operation $\cdot$ and $H \subset G$. Then H is said to be a subgroup of G if H with the operation $\cdot$ is a group.

Definition. Suppose that each of G and H are groups with operations $\otimes$ and $\boxtimes$ respectively and that $\varphi : G \to H$ is a function. Then φ is called a *homomorphism* if the following holds for all $x, y \in G$:

$$\varphi(x \otimes y) \quad = \quad \varphi(x) \boxtimes \varphi(y).$$

A homomorphism that is 1-to-1 and onto is called an *isomorphism*.

Notation. If G is a group with identity element e and $g \in G$ then:
i. g^0 denotes e;
ii. g^1 denotes g;
iii. for a positive integer $n > 1$, g^n is defined inductively as:

$$g^n = g^{n-1} \cdot g.$$

Theorem 0.4. Suppose that G is a group with the usual notation for the operation. Then:

$$\begin{array}{lll} a. & (g^{-1})^n = (g^n)^{-1} & \text{for } g \in G, n \in \mathbb{Z}^+ \\ b. & g^n \cdot g^m = g^{n+m} & \text{for } g \in G, n, m \in \mathbb{Z}^+ \end{array}$$

Theorem 0.5. Suppose that G is a group and H is a subgroup of G. Define the relation $\sim$ on G by $g \sim h$ if and only if $gh^{-1} \in H$. Then:
a. $\sim$ is an equivalence relation on G.

b. Let $p \in G$ and define $Hp = \{hp | h \in H\}$; then the function $f : H \to Hp$ defined by $f(h) = hp$ is 1-to-1 and onto.

c. $[e]_\sim = H$.

d. The collection $\{Hg | g \in G\}$ is a partition of G.

e. The function $\varphi : H \to Hx$ defined by $\varphi(h) = hx$ is a bijection.

Theorem 0.6. If G is a finite group and H is a subgroup of G then $|H| \Big| |G|$.