Math 5330 Online Review. April 26, 2018

- A group is best defined as an algebraic structure with three operations. One is binary and usually called multiplication or addition, one is unary, called inversion and one is nullary, called unit or zero. Example: $(\mathbb{R}\backslash\{0\}, \cdot, ^{-1}, 1)$ is the group of real numbers different from zero with multiplication. $(\mathbb{R}, +, -, 0)$ is the additive group of real numberfs with addition.

- For groups we have three laws: associativity, $x \cdot (y \cdot z) = (x \cdot y) \cdot z, x \cdot e = e \cdot x, x \cdot x^{-1} = x^{-1} \cdot x = e$

- For any set X the set of bijections on X is a group where the operations are composition, taking the invers map, identity on X, : $(S_X, \circ, ^{-1}, id_X)$ is the symmetry group on X.

- A subset H of a group is called closed if whenever $x, y \in H$ then $x \cdot y \in H, x^{-1} \in H, e \in H$. A closed subset is with the operations of G restricted to elements of H a group. It is called a subgroup of G.

- The rational numbers different from zero with multiplication form a subgroup of all real numbers different from zero with multiplication.

- A group is commutative if the binary operation is commutative: $x \cdot y = y \cdot x$.

- A group is cyclic, generated by x, if every element is a power of $x : C =< x >= \{x^n | n \in \mathbb{Z}\}$

- Any cyclic group is commutative. $(\mathbb{Z}, +)$ is cyclic. Z_n is cyclic. Z is generated by $1, Z_n$ is generated by $[1]_n$.

- Any finite group of order 4 is commutative.

- A map $\varphi : G \to H$ between groups is a homomorphis if $\varphi(xy) = \varphi(x)\varphi(y), \varphi(x^{-1}) = \varphi(x)^{-1}, \varphi(e_G) = e_H$. Only the first property for a map between groups is needed to make it to a homomorphism: $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G), e_H = \varphi(e_G)^{-1}\varphi(e_G) = \varphi(e_G)^{-1} \cdot (\varphi(e_G) \cdot \varphi(e_G)) = \varphi$ $e_H = \varphi(e_G)$. And then $e_H = \varphi(e_G) = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$. Therefore $\varphi(x)^{-1} = \varphi(x^{-1})$.
- $(\mathbb{Z}, +) \twoheadrightarrow < x >, n \mapsto x^n$ is a surjective homomorphism from the additive group of integers onto the cyclic group generated by x.
- For any homomorphism $\varphi : G \to H, N = \ker(\varphi) = \{g | \varphi(g) = e_H\}$ is a normal subgroup of G and $im(\varphi) = \{h | h = \varphi(g)$ for some $g \in G\}$ is a subgroup of H.
- A subgroup N is normal if for every x one has that $xN = Nx$ iff $xNx^{-1} = N$ iff left cosets equal right cosets $xN = Nx$ iff N is the kernel of a homomorphism.

Indeed, if N is normal then $(xN) \cdot (y) = (x \cdot y)N$ defines a group multiplication on the set G/N of all co-sets and $G \to G/N, x \mapsto xN,$ is a homomorphism with kernel N.

- For any homomorphism $\varphi : G \to H$ one has that $G/N \cong im(\varphi)$. Under φ all elements of the coset xN have the same image $\varphi(x)$. The map $G/N \to im(\varphi), [x]_N = xN \mapsto \varphi(x)$ is a bijective homomorphism. This is the fundamental theorem for groups.

- Given any map $f : A \to B$ between any two sets. Then $a_1 \sim a_2$ iff $f(a_1) = f(a_2)$ is an equivalence $\ker(f)$ relation on A. It partitiones the set A into classes on which f is constant. The set of classes is called $A/\ker(f)$. The map $A/\ker(f) \to im(f), [a] \to f(a)$ is a bijection from the set of equivalence classes to the image of f.
- Here is a trivial example. Let $A = \{1,2,3,4,5\}, B = \{a,b,c,d\}, f(1) = f(2) = a, f(3) = b, f(4) = f(5) = c$. Then $A/\ker(f) = \{\{1,2\},\{3\},\{4,5\}\}$ has three classes and each class corresponds to an element of $im(f)$: $[1] = [2] = \{1,2\} \mapsto a, [3] \mapsto b, [4] = [5] \mapsto c$.
- In the homomorphism theorem we have that the equivalence classes for a homomorphism φ the class of the unit e is a (normal) subgroup N. Each other class $[x]$ is determined by the class of e, it is just xN. All classes have the same number of elements as N has. The classes form a group, the coset group G/N which is isomorphic to $im(\varphi)$.
- According to the homomorphism theorem, andy cyclic group is either isomorphic to $(\mathbb{Z}, +)$ or isomorphic to the integers $\bmod n$.
- The positive reals $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ and the additive group $(\mathbb{R}, +, -, 0)$ of all reals are isomorphic groups. $\log : \mathbb{R}^+ \to \mathbb{R}$ is the isomorhism. The log laws: $\log(x \cdot y) = \log(x) + \log(y), \log(x^{-1}) = -\log(x), \log(1) = 0$ state that the function $\log$ is homomorphic. The inverse of $\log$ is the exponential function to base $e = 2.71\ldots$ That the exponential function is homomorphic are the exponential laws: $e^{x+y} = e^x \cdot e^y, e^{-x} = \frac{1}{e^x}, e^0 = 1$
- It was an interesting homework exercise to show that the groups $(\mathbb{R}\backslash\{0\}, \cdot, ^{-1}, 1)$ and $(\mathbb{R}, +, -, 0)$ are **not isomorphic**.