1 Problem of the Week

There are weekly problems assigned which will be discussed in reading groups. A solution will also be given in the reading group. You are not expected to necessarily complete them, but it will be very useful to look through it and have some ideas about how you might go about solving the problem even if you are very unsure.

Weekly Problem 1. Let G be a finite semigroup, that is, G is closed under an associative operation $\cdot$. Assume that left and right cancellation holds in G, so $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$. Prove that G is a group.

Here is a lemma you may (and probably will) use:

Lemma 1.1. If G is a semigroup and $e \in G$ is a right identity and for all $x \in G$, x has a right inverse, then G is a group. Likewise, if G is a semigroup and $e \in G$ is a left identity and for all $x \in G$, x has a left inverse, then G is a group.

2 Basic Number theory

Some preliminaries for review:

- Euclidean division: Let $a, b \in \mathbb{Z}$. Then, there exists a unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.
- Bézout's lemma: Let $a, b \in \mathbb{Z}$. Then, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.
- An equivalence relation on X is a relation $\sim$ such that
  - For all $x \in X$, $x \sim x$ (reflexivity)
  - For all $x, y \in X$, $x \sim y$ implies $y \sim x$ (symmetry)
  - For all $x, y, z \in X$, $x \sim y$ and $y \sim z$ implies $x \sim z$ (transitivity)
- Let $\sim$ be an equivalence relation on X and $x \in X$. An equivalence class $[x]_\sim$ is defined as $\{y \in X | x \sim y\}$. $X/\sim$ is the set of equivalence classes of X under $\sim$. Furthermore, there is a natural map $\pi : X \mapsto X/\sim$ (also known as the canonical map, the projection map) defined as $\pi(x) = [x]_\sim$.

3 Monoids and Groups

Definition 1. Let X be a set. Then, a binary operation $\cdot$ is a map $X \times X \mapsto X$.

Definition 2. A semigroup $(X, \cdot)$ is a set X with a binary operation $\cdot$ such that for all $x, y, z \in X$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ is associative)

Definition 3. A monoid $(M, \cdot)$ is a set M with a binary operation $\cdot$ such that

- For all $x, y, z \in M$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ is associative)
- There exists $e \in M$ such that for all $x \in M$, $x \cdot e = e \cdot x = x$ (existence of identity)

Definition 4. A group $(G, \cdot)$ is a set G with a binary operation $\cdot$ such that

- For all $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ is associative)
- There exists $e \in G$ such that for all $x \in M$, $x \cdot e = e \cdot x = x$ (existence of identity)
- For all $x \in G$, there exists x^{-1} such that $x \cdot x^{-1} = e = x^{-1} \cdot x$ (existence of inverses)

In other words, a group is a monoid closed under inverses.

Definition 5. A group G is called abelian if for all $x, y \in G$, $x \cdot y = y \cdot x$ ($\cdot$ is commutative)

Definition 6. Given a monoid (respectively group) X, A submonoid (resp. subgroup) is a subset $Y \subseteq X$ such that Y is a monoid (resp. group) equipped with the operation on X.

Definition 7. The order of a group G is the number of elements in G. The order of an element $x \in G$ is the smallest $n \in \mathbb{N}$ such that $x^n = e$, if no such n exists, x has infinite order.

Here is some notation conventions

- Monoids are usually written as M
- Groups are usually written as G with H and K being used for subgroups. Other times, M, N can also be used. Be careful that G' is usually used for a different purpose.
- Elements of groups are usually written as g, g', h, x, y.
- The order of a group and of an element of a group are usually written $|G|, |x|$ or $\#G, \#x$
- $\cdot$ is usually omitted, i.e. $g \cdot h$ is written as gh. g^n denotes $g \cdot g \cdot g \ldots \cdot g$ done n times. g^{-1} denotes the inverse of g and g^{-n} denotes $(g^{-1})^n$.
- We usually call $\cdot$ multiplication even if the operation itself is different from multiplication.
- If H is a subgroup of G it is common to write $H \leq G$.

Proof. □

4 Exercises

These are exercises which will be worked through in the reading group. You are more than welcome to try them beforehand, but you are not expected to. Solutions will be posted after the reading section.

1. (a) Prove Lemma 1.1
   (b) Show that Lemma 1.1 is false if we assume G has a right identity and every x has left inverses by constructing a counterexample.
2. (a) Show that the statement in the weekly problem is false if we assume only one of the cancellation laws hold.
   (b) Show that the statement in the weekly problem is false if we assume G is infinite by constructing a counterexample.
3. (a) Show that if G is a group, then for all a, b the equations $ax = b$ and $ay = b$ have unique solutions.
   (b) Show that if G is a semigroup such that for all a, b the equations $ax = b$ and $ay = b$ have unique solutions, then G is a group.