Number Theory
Spring 2022

Assignment 3
Due March 2

Exercise 1. Given $a \in \mathbb{Z}$ and nonempty $S, T \subseteq \mathbb{Z}$, define

$$S + T = \{s + t \,|\, s \in S, t \in T\},$$
$$aS = \{as \mid s \in S\},$$

which are both subsets of $\mathbb{Z}$ as well. Throughout our work with subgroups of $\mathbb{Z}$, we made implicit use of the following identities regarding these operations: for all $a, b \in \mathbb{Z}$ and all $S, T \subseteq \mathbb{Z}$ one has

$$a(S + T) = aS + aT,$$
$$a(bS) = (ab)S.$$

Prove these carefully using double-containment arguments. Determine (with proof) whether or not $(a + b)S = aS + bS$ is also a valid identity.

Exercise 2. Let $S, T, U, V \subseteq \mathbb{Z}$.

a. Prove that if $S \subseteq U$ and $a \in \mathbb{Z}$, then $aS \subseteq aU$.

b. Prove that if $S \subseteq U$ and $T \subseteq V$, then $S + T \subseteq U + V$.

Exercise 3. Given nonzero $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, define their *greatest common divisor* $(a_1, a_2, \ldots, a_r)$ to be the largest $a \in \mathbb{N}$ so that $a|a_i$ for all i. Using the techniques of subgroups that we have introduced in class, without appealing to Bézout's lemma, prove that

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_r\mathbb{Z} = (a_1, a_2, \ldots, a_r)\mathbb{Z}.$$

Conclude that every common divisor of the a_i must in fact divide $(a_1, a_2, \ldots, a_r)$.