Margaret Bilu
Office 604

bilu@cims.nyu.edu

Algebra homework 4
Laws of composition, groups, subgroups

Exercise 1. We define a law of composition $*$ on $\mathbf{R}$ by $x * y = x - y$.

(a) Is it associative?

(b) Is it commutative?

(c) Does it have an identity?

Exercise 2. We consider the set $\mathcal{F}(\mathbf{R}, \mathbf{R})$ of functions from $\mathbf{R}$ to $\mathbf{R}$. We saw in lectures that the composition of functions $\circ$ is an associative law of composition on this set, with identity the function $\mathrm{id} : \mathbf{R} \to \mathbf{R}$ defined by $\mathrm{id}(x) = x$. For the following elements of $\mathcal{F}(\mathbf{R}, \mathbf{R})$, determine if they have an inverse for $\circ$, and if yes, give it.

(a) The function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = 3x + 2$.

(b) The function $g : \mathbf{R} \to \mathbf{R}$ given by $g(x) = x^2 - 1$.

(c) The function $h : \mathbf{R} \to \mathbf{R}$ given by $h(x) = e^x$.

Exercise 3. Determine the set $(\mathbf{Z}/8\mathbf{Z})^\times$ and give the Cayley table of the group $((\mathbf{Z}/8\mathbf{Z})^\times, \odot)$.

Exercise 4. If $n > 2$, show that the group of units $(\mathbf{Z}/n\mathbf{Z})^\times$ of $\mathbf{Z}/n\mathbf{Z}$ contains an element a such that $a \neq 1$ but $a^2 = 1$. (Here 1 denotes the identity element of $(\mathbf{Z}/n\mathbf{Z})^\times$, that is, the congruence class of the integer 1 modulo n.)

Exercise 5. Let $S = \mathbf{R} \setminus \{-1\}$ and define a law of composition on S by $x * y = x + y + xy$. Show that $(S, *)$ is an abelian group. Can you explain why we had to remove -1 from $\mathbf{R}$ to make this work?

Exercise 6. Let G be a group such that for every $x \in G$ we have $x^2 = e$, where e is the identity element of g. Show that G must be abelian.

Exercise 7. Let G be a group with law of composition $*$. Show that

$$Z(G) = \{x \in G,\ x * g = g * x \text{ for all } g \in G\}$$

is a subgroup of G. It is called the *center* of G.

Exercise 8. Prove that

$$G = \{a + b\sqrt{2},\quad a, b \in \mathbf{Q},\ a, b \text{ not both zero}\}$$

is a subgroup of the group $(\mathbf{R}^\times, \cdot)$.