Lior Silberman’s Math 322 Problem Set 1, due 14/9/2017

Practice and supplementary problems, and any problems specifically marked “OPT” (optional), “SUPP” (supplementary) or “PRAC” (practice) are not for submission. It is possible that the grader will not mark all problems.

Practice problems

The following problem is a review of the axioms for a vector space.

P1 Let $X$ be a set. Carefully show that pointwise addition and scalar multiplication endow the set $\mathbb{R}^X$ of functions from $X$ to $\mathbb{R}$ with the structure of an $\mathbb{R}$-vectorspace. Meditate on the case $X = [n] = \{0, 1, \ldots, n-1\}$.

P2 (Euclid’s Lemma) Let $a, b, q, r$ be four integers with $b = aq + r$. Show that the pairs $\{a, b\}$ and $\{a, r\}$ have the same sets of common divisors, hence the same greatest common divisor.

P3. Consider the equation $7x + 11y = 1$ for unknowns $x, y \in \mathbb{Z}$.

(a) Exhibit infinitely many solutions.

(*b) Show that you found all the solutions.

The integers

1. Show that for any integer $k$, one of the integers $k, k+2, k+4$ is divisible by 3.

2. (Modular arithmetic; see notes for the notation or wait for Tuesday lecture)
   (a) Give a simple rule for the remainder obtained when dividing $3^n$ by 13, for $n \in \mathbb{Z}_{\geq 0}$.
   PRAC Check that $2^{12} \equiv 1 \pmod{13}$.
   (b) Let $k$ be the smallest positive integer such that $2^k \equiv 1 \pmod{13}$. Show that $k|12$.
   PRAC Check that $2^6 \equiv -1 \pmod{13}$, $2^4 \equiv 3 \pmod{13}$.
   (c) Use the last check to show that $k = 12$.
   (d) Show that $2^i \equiv 2^j \pmod{13}$ iff $i \equiv j (12)$.

3. Let $a, n$ be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \equiv 1 \pmod{n}$ has a solution iff $d = 1$.

4. Let $f : \mathbb{Z} \to \mathbb{Z}$ be additive, in that for all $x, y \in \mathbb{Z}$ we have $f(x+y) = f(x) + f(y)$.
   PRAC Check that for any $a \in \mathbb{Z}$, $f_a(x) = ax$ is additive.
   (a) Show that $f(0) = 0$ (hint: $0 + 0 = 0$).
   (b) Show that $f(-x) = -f(x)$ for all $x \in \mathbb{Z}$.
   (c) Show by induction on $n$ that for all $n \geq 1$, $f(n) = f(1) \cdot n$.
   (d) Show that every additive map is of the form $f_a$ for some $a \in \mathbb{Z}$.
   RMK Let $H$ be the set of additive maps $\mathbb{Z} \to \mathbb{Z}$. We showed that the function $\phi : H \to \mathbb{Z}$ given by $\phi(f) = f(1)$ is a bijection (with inverse $\psi(a) = f_a$).
   SUPP Show that the bijections $\phi, \psi$ are themselves additive maps (addition in $H$ is defined pointwise).

(hints on reverse)
(for 2(a): try the first few values to find the pattern, then use induction)
(for 2(b): divide 12 by \(k\) using the theorem on division with remainder)
(for 2(c): consider in turn each proper divisor of 12)
(for 2(d): as in part b replace \(i, j\) with their remainders mod 12. Then, assuming \(i > j\), consider \(2^{i+(12-j)}\)

**Supplementary problems I: Functions**

The following problem will be used in the upcoming discussion of permutations.

**A.** Let \(X, Y, Z, W\) be sets and let \(f: X \rightarrow Y, g: Y \rightarrow Z\) and \(h: Z \rightarrow W\) be functions. Recall that the composition \(g \circ f\) is the function \(g \circ f: X \rightarrow Z\) such that \((g \circ f)(x) = g(f(x))\) for all \(x \in X\).

(a) Show that composition is **associative**: that \(h \circ (g \circ f) = (h \circ g) \circ f\) (recall that functions are equal if they have the same value at every \(x\)).

(b) \(f\) is called **injective** or **one-to-one** (1:1) if \(x \neq x'\) implies \(f(x) \neq f(x')\). Show that if \(g \circ f\) is injective then so is \(f\).

(c) \(g\) is called **surjective** or **onto** if for every \(z \in Z\) there is \(y \in Y\) such that \(g(y) = z\). Show that if \(g \circ f\) is surjective then so is \(g\).

(d) Suppose that \(f, g\) are both surjective or both injective. In either case show that the same holds for \(g \circ f\).

(e) Give an example of a set \(X\) and \(f, g: X \rightarrow X\) such that \(f \circ g \neq g \circ f\).

**Supplementary Problems II: Subsemigroups of \((\mathbb{Z}_{\geq 0}, +)\)**

**B.** The Kingdom of Ruritania mints coins in the denominations \(d_1, \ldots, d_r\) Marks (\(d_i\) are positive integers, of course). Let \(d = \gcd(d_1, \ldots, d_r)\).

(a) Show that every payable sum (total value of a combination of coins) is a multiple of \(d\) Marks.

(b) Show that there exists \(N \geq 1\) such that any multiple of \(d\) Marks exceeding \(N\) can be expressed using the given coins.

(c) Let \(H \subset \mathbb{Z}_{\geq 0}\) be the set of sums that can be paid using the coins. Show that \(H\) is closed under addition.

**DEF** \(H\) is called the **subsemigroup of \(\mathbb{Z}_{\geq 0}\) generated by \{\(d_1, \ldots, d_r\}\}**.

**C.** (partial classification of subsemigroups of \(\mathbb{Z}_{\geq 0}\)) Let \(H \subset \mathbb{Z}_{\geq 0}\) be closed under addition.

(a) Show that either \(H = \{0\}\) or there are \(N, d \geq 1\) such that \(d\) divides every element of \(h\), and such that \(H\) contains all multiples of \(d\) exceeding \(N\).

**Hint:** Enumerate the elements of \(H\) in increasing order as \(\{h_i\}_{i=1}^{\infty}\) and consider the sequence \(\{\gcd(h_1, \ldots, h_n)\}_{m=1}^{\infty}\).

(b) Conclude that \(H\) is **finitely generated**: there are \(\{d_1, \ldots, d_r\} \subset H\) such that \(H\) is obtained as in problem C.
Supplementary Problems III: Additive groups in $\mathbb{R}$.

D. (just linear algebra)
   (a) Show that the usual addition and multiplication by rational numbers endow $\mathbb{R}$ with the structure of a vector space over the field $\mathbb{Q}$.
   (b) Let $f: \mathbb{R} \to \mathbb{R}$ be additive ($f(x+y) = f(x) + f(y)$). Show that $f$ is $\mathbb{Z}$-linear: that $f(nx) = nf(x)$ for all $x \in \mathbb{R}, n \in \mathbb{Z}$.
   (c) Show that $f$ is $\mathbb{Q}$-linear: $f(rx) = rf(x)$ for all $r \in \mathbb{Q}$.
   (d) Let $B \subset \mathbb{R}$ be a basis for $\mathbb{R}$ as a $\mathbb{Q}$-vector space (this is called a Hamel basis). Use $B$ to construct a $\mathbb{Q}$-linear map $\mathbb{R} \to \mathbb{R}$ which is not of the form $x \mapsto ax$.

E. (add topology ...) Let $f: \mathbb{R} \to \mathbb{R}$ be additive.
   (a) Suppose that $f$ is continuous. Show that $f(x) = ax$ where $a = f(1)$.
   (b) (If you have taken Math 420) Suppose that $f$ is Lebesgue (or Borel) measurable. Show that there is $a \in \mathbb{R}$ such that $f(x) = ax$ a.e.
   (c) (“$\mathbb{R}$ has no field automorphisms”) Let $f: \mathbb{R} \to \mathbb{R}$ satisfy $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$. Show that either $f(x) = 0$ for all $x$ or $f(x) = x$ for all $x$. 