Math 322 Fall 2015: Problem Set 2, due 24/9/2015

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

Number Theory

1. (The Chinese Remainder Theorem)
   (a) Let p be an odd prime. Show that the equation $x^2 = [1]_p$ has exactly two solutions in $\mathbb{Z}/p\mathbb{Z}$ (aside: what about $p = 2$?)
   (b) We will find all solutions to the congruence $x^2 \equiv 1\,(91)$.
      (i) Find a "basis" a, b such that $a \equiv 1\,(7)$, $a \equiv 0\,(13)$ and $b \equiv 0\,(7)$, $b \equiv 1\,(13)$.
      (ii) Solve the congruence mod 7 and mod 13.
      (iii) Find all solutions mod 91.

Permutations

2. On the set $\mathbb{Z}/12\mathbb{Z}$ consider the maps $\sigma(a) = a + [4]$ and $\tau(a) = [5]a$ (so $\sigma([2]) = [6]$ and $\tau([2]) = [10]$)
   DEF $(f \circ g)(x) = f(g(x))$ is composition of functions.
   (a) Find maps σ^{-1}, τ^{-1} such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \tau \circ \tau^{-1} = \tau^{-1} \circ \tau = \mathrm{id}$.
   (b) Compute $\sigma\tau, \tau\sigma, \sigma^{-1}\tau$.
   (c) For each $a \in \mathbb{Z}/12\mathbb{Z}$ compute $a, \sigma(a), \sigma(\sigma(a))$ and so on until you obtain a again. How many distinct cycles arise? List them.
   RMK The relation "a, b are in the same cycle" is an equivalence relation.

SUPP [R1.29] On $\mathbb{Z}/11\mathbb{Z}$ let $f(x) = 4x^2 - 3x^7$. Show that f is a permutation and find its cycle structure and its inverse.

3. Let X be a set, $i \in X$. Say $\sigma \in S_X$ *fixes* i if $\sigma(i) = i$, and let $P_i = \mathrm{Stab}_{S_X}(i) = \{\sigma \in S_X \mid \sigma(i) = i\}$ be the set of such permutations.
   (a) Show that P_i is non-empty and closed under composition and under inverses (i.e. that if $\sigma, \tau \in P_i$ then $\sigma \circ \tau$ and $\sigma^{-1} \in P_i$).
   RMK You've shown that P_i is a *subgroup* of S_X.
   — Suppose that $\rho(i) = j$ for some $\rho \in S_X$. Define $f \colon S_X \to S_X$ by $f(\sigma) = \rho \circ \sigma \circ \rho^{-1}$.
   (b) Show that $f(\sigma \circ \tau) = f(\sigma) \circ f(\tau)$ for all $\sigma, \tau \in S_X$ and that $f(\sigma^{-1}) = (f(\sigma))^{-1}$.
   (c) Show that if $\sigma \in P_i$ then $f(\sigma) \in P_j$.
   (d) Show that f is a bijection ("isomorphism") between P_i and P_j.

Operations in a set of sets

Let X be a set, $P(X)$ (the "powerset") the set of its subsets (so $P(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$.

The *difference* of $A,B \in P(X)$ is the set $A - B \overset{\text{def}}{=} \{x \in A \mid x \notin B\}$ (so $[0,2]-[-1,1] = (1,2]$).

The *symmetric difference* is $A\Delta B \overset{\text{def}}{=} (A-B)\cup(B-A)$ (so $[0,2]\,\Delta\,[-1,1] = [-1,0)\cup(1,2]$).

4. (Checking that $(P(X), E, \Delta)$ is a commutative group).
   PRAC Show that $A\Delta B$ is the set of $x \in X$ which belong to *exactly one* of A,B. Note that this shows the *commutative law* $A\Delta B = B\Delta A$.
   (a) (associative law) Show that for all $A,B,C \in P(X)$ we have $(A\Delta B)\,\Delta C = A\Delta(B\Delta C)$.
   (b) (neutral element) Find $E \in P(X)$ such that $A\Delta E = A$ for all $A \in P(X)$.
   (c) (negatives) For all $A \in P(X)$ find a set $\bar{A} \in P(X)$ such that $A\Delta\bar{A} = E$.

5. (A quotient construction) Fix $N \in P(X)$ and say that $A,B \in P(X)$ *agree away from* N if $A - N = B - N$. Denote this relation $\sim$ during this problem. For example, as subsets of $\mathbb{R}$, the intervals $[-1,1]$ and $[0,1]$ agree "away from the negative reals".
   PRAC Show that $A \sim B$ iff for all $x \in X - N$ either x belong to both A,B or to neither.
   (a) Show that $\sim$ is an equivalence relation. We will use $[A]$ to denote the equivalence class of $A \subset X$ under $\sim$.
   (b) Show that if $A \sim A'$, $B \sim B'$ then $(A\Delta B) \sim (A'\Delta B')$.
   RMK This means the operation $[A]\,\tilde{\Delta}[B] \overset{\text{def}}{=} [A\Delta B]$ is well-defined: it does not depend on the choice of representatives.
   (c) Show that every equivalence class has a *unique* element which also belongs to $P(X-N)$ (that is, exactly one element of the class is a subset of $X-N$).
   (d) Show that $P(X-N) \subset P(X)$ is non-empty and closed under Δ (it is automatically closed under the "bar" operation of 4(c))
   RMK It follows that $\left(P(X)/\sim, [\emptyset], \tilde{\Delta}\right)$ and $(P(X-N), \emptyset, \Delta)$ are essentially the same algebraic structure (there is an operation-preserving bijection between them). We say "they are *isomorphic*".

(hint for 1(a): what does it mean that $x^2 \equiv 1\,(p)$ for $x \in \mathbb{Z}$?)
(hint for 3(a): given $\sigma(i) = i$ and $\tau(i) = i$, check that $(\sigma \circ \tau)(i) = i$)
(hint for 3(b): use the definition of f, and the idea of PS1 problem 4(b))
(hint for 3(c): what's $\rho^{-1}(j)$?)
(hint for 3(d): find f^{-1})

Supplementary Problems I: The Fundamental Theorem of Arithmetic

If you haven't seen this before, you *must* work through problem A.

A. By definition the empty product (the one with no factors) is equal to 1, and a product with one factor is equal to that factor.
   (a) Let n be the smallest positive integer which is not a product of primes. Considering the possibilities that $n = 1$, n is prime, or that n is neither, show that n does not exist. Conclude that every positive integer is a product of primes.
   (b) Let $\{p_i\}_{i=1}^r$, $\{q_j\}_{j=1}^s$ be sequences of primes, and suppose that $\prod_{i=1}^r p_i = \prod_{j=1}^s q_j$. Show that p_r occurs among the $\{q_j\}$ (hint: p_r divides a product ...)
   (c) Call two representations $n = \prod_{i=1}^r p_i = \prod_{j=1}^s q_j$ of $n \geq 1$ as a product of primes *essentially the same* if $r = s$ and the sequences only differ in the order of the terms. Let n be the smallest integer with two essentially different representations as a product of primes. Show that n does not exist.

The following problem is for your amusement only; it is not relevant to Math 322 in any way.

B. (The p-adic absolute value)
   (a) Show that every non-zero rational number can be written in the form $x = \frac{a}{b}p^k$ for some non-zero integers a, b both prime to p and some $k \in \mathbb{Z}$. Show that k is *unique* (only depends on x). By convention we set $k = \infty$ if $x = 0$ ("0 is divisible by every power of p").
   DEF The *p-adic absolute value* of $x \in \mathbb{Q}$ is $|x|_p = p^{-k}$ (by convention $p^{-\infty} = 0$).
   (b) Show that for any $x, y \in \mathbb{Q}$, $|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\} \leq |x|_p + |y|_p$ and $|xy|_p = |x|_p\,|y|_p$ (this is why we call $|\cdot|_p$ an "absolute value").
   (c) Fix $R \in \mathbb{R}_{\geq 0}$. Show that the relation $x \sim y \iff |x-y|_p \leq R$ is an equivalence relation on $\mathbb{Q}$. The equivalence classes are called "balls of radius R" and are usually denoted $B(x, R)$ (compare with the usual absolute value).
   (d) Show that $B(0, R) = \left\{x \,\middle|\, |x|_p \leq R\right\}$ is non-empty and closed under addition and subtraction. Show that $B(0, 1) = \left\{x \,\middle|\, |x|_p \leq 1\right\}$ is also closed under multiplication.

Supplementary Problem II: Permutations and the pigeon-hole principle

C. (a) Prove by induction on $n \geq 0$: Let X be any finite set with n elements, and let $f\colon X \to X$ be either surjective or injective. Then f is bijective.
   (b) conclude that if X, Y are sets of the same size n and $f\colon X \to Y$ and $g\colon Y \to X$ satisfy $f \circ g = \mathrm{id}_Y$ then $g \circ f = \mathrm{id}_X$ and the functions are inverse.

Supplementary Problem III: Cartesian products and the CRT

NOTATION. For sets X,Y we write X^Y for the set of functions from Y to X.

D. Let I be an index set, A_i a family of sets indexed by I (in other words, a set-valued function with domain I). The *Cartesian product* of the family is the set of all touples such that the ith element is chosen from A_i, in other words:

$$\prod_{i\in I} A_i = \left\{ a \in \left(\bigcup_{i\in I} A_i\right)^I \middle| \forall i \in I : a(i) \in A_i \right\}$$

(we usually write a_i rather than $a(i)$ for the ith member of the touple).

(a) Verify that for $i = \{1,2\}$, $A_1 \times A_2$ is the set of pairs.

(b) Give a natural bijection

$$\left(\prod_{i\in I} A_i\right)^B \leftrightarrow \prod_{i\in I} \left(A_i^B\right) .$$

(you have shown: a vector-valued function is the same thing as a vector of functions).

(b) Let $\{V_i\}_{i\in I}$ be a family of vector spaces over a fixed field F (say $F = \mathbb{R}$). Show that pointwise addition and multiplication endow $\prod_i V_i$ with the structure of a vector space.

DEF This vector space is called the *direct product* of the vector spaces $\{V_i\}$.

RMK Recall that, if W is another vector space, then the set $\mathrm{Hom}_F(W,V)$ of linear maps from W to V is itself a vector space.

(*c) Let W be another vector space. Show that the bijection of (a) restricts to an isomorphism of vector spaces

$$\mathrm{Hom}_F\left(W, \prod_{i\in I} V_i\right) \to \prod_{i\in I} \mathrm{Hom}_F\left(W, V_i\right) .$$

E. (General CRT) Let $\{n_i\}_{i=1}^r$ be divisors of $n \geq 1$.

(a) Construct a map

$$f\colon \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^r (\mathbb{Z}/n_i\mathbb{Z}) ,$$

generalizing the case $r = 2$ discussed in class.

(b) Show that f respects modular addition and multiplication.

(*c) Suppose that $n = \prod_{i=1}^r n_i$ and that the n_i are pairwise relatively prime (for each $i \neq j$, $\gcd\left(n_i, n_j\right) = 1$. Show that f is an isomorphism.