Math 322: Problem Set 3 (due 25/9/2014)

Practice problems

P1 Which of the following are groups? If yes, prove the group axioms. If not, show that an axiom fails.
(a) The "half integers" $\frac{1}{2}\mathbb{Z} = \left\{\frac{a}{2} \mid a \in \mathbb{Z}\right\} \subset \mathbb{Q}$, under addition.
(b) The "dyadic integers" $\mathbb{Z}[\frac{1}{2}] = \left\{\frac{a}{2^k} \mid a \in \mathbb{Z}, k \geq 0\right\} \subset \mathbb{Q}$, under addition.
(c) The non-zero dyadic integers, under multiplication.

P2. [DF1.1.7] Let $G = [0,1)$ be the half-open interval, and for $x, y \in G$ define $x * y = \begin{cases} x+y & \text{if } x+y < 1 \\ x+y-1 & \text{if } x+y \geq 1 \end{cases}$.
(a) Show that $(G, *)$ is a commutative group. It is called "$\mathbb{R}$ mod $\mathbb{Z}$".
(b) Give an alternative construction of G using the equivalence relation $x \equiv y\,(\mathbb{Z})$ if $x - y \in \mathbb{Z}$

P3. [DF1.1.9] Let $F = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$.
(a) Show that $(F, +)$ is a group.
(*b) Show that $(F \setminus \{0\} \cdot)$ is a group.
RMK Together with the distributive law, (a),(b) make F a *field*.

Symmetric Groups

1. Show that every element of A_n is a product of 3-cycles (hint: start with $(12)(13) \in A_3$ and $(12)(34) \in A_4$).

2. Call $\sigma, \tau \in S_X$ *conjugate* if there is $\rho \in S_X$ such that $\tau = \rho\sigma\rho^{-1}$.
(a) Show that "σ is conjugate to τ" is an equivalence relation.
(b) Let β be an r-cycle. Show that $\rho\beta\rho^{-1}$ is also an r-cycle.
(c) Show that if $\sigma = \prod_{i=1}^{t} \beta_i$ is the cycle decomposition of σ, then $\rho\sigma\rho^{-1} = \prod_{i=1}^{t}\left(\rho\beta_i\rho^{-1}\right)$ is the cycle decomposition of $\rho\sigma\rho^{-1}$.
RMK We have shown: if σ is conjugate to τ then they have the same *cycle structure*: for each r they have the same number of r-cycles.
(*d) Suppose σ, τ have the same cycle structure. Show that they are conjugate.

3. A *permutation matrix* is an $n \times n$ matrix which is zero except for exactly one 1 in each row and column (example: the identity matrix). The *Kroncker delta* is defined by $\delta_{a,b} = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$.
(a) Given $\sigma \in S_n$ let $P(\sigma)$ be the matrix with $(P(\sigma))_{ij} = \delta_{i,\sigma(j)}$. Show that P is a bijection between S_n and the set of permutation matrices of size n.
(b) Show that $P \colon S_n \to M_n(R)$ has $P(\sigma\tau) = P(\sigma)P(\tau)$.
(c) Show that the image of P consists of invertible matrices.
RMK $\det(P(\sigma)) = \mathrm{sgn}(\sigma)$.

Groups and homomorphisms

4. Which of the following are groups? If yes, prove the group axioms. If not, show that an axiom fails.
   (a) The non-negative real numbers with the operation $x * y = \max\{x, y\}$.
   (b) $\mathbb{R} \setminus \{-1\}$ with the operation $x * y = x + y + xy$.

5. Let $*$ be an associative operation on a set G (that means $(x*y)*z = x*(y*z)$, and let $a \in G$. We make the rescursive definition $a^1 = a$, $a^{n+1} = a^n * a$ for $n \geq 1$.
   (a) Show by induction on m that if $n, m \geq 1$ then $a^n * a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.
   SUPP If G is a group, set $a^0 = e$ and $a^{-n} = \left(a^{-1}\right)^n$ and show that for all $n, m \in \mathbb{Z}$ we have $a^n * a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.
   — From now on suppose G is a group.
   (c) [R1.31] Let m, n be relatively prime integers and suppose that $a^m = e$. Show that there is $b \in G$ such that $b^n = a$ (hint: Bezout's Theorem).
   (d) Let $a \in G$ satisfy $a^n = e$ for some $n \neq 0$ and let $k \in \mathbb{Z}_{\geq 1}$ be minimal such that $a^k = e$. Show that $k|n$.
   DEF We call k the *order* of a. We have shown that $a^n = e$ iff n is divisible by the order of a.

6. Let G be a group, and suppose that $f(x) = x^{-1}$ is a group homomorphism $G \to G$. Show that $xy = yx$ for all $x, y \in G$ (we call such G *abelian*).

Supplementary Problems I: Permutations

A. In this problem we will give an alternative proof of the cycle decomposition of permutations. Fix a set X (which may be infinite) and a permutation $\sigma \in S_X$.
   (a) Define a relation $\sim$ on X by $i \sim j \leftrightarrow \exists n \in \mathbb{Z} : \sigma^n(i) = j$. Show that this is an equivalence relation.
   DEF We'll call the equivalence classes the *orbits* of σ on X.
   (b) Let O be an orbit, and let $\kappa_O = \sigma \restriction_O$ be the *restriction* of σ to O: the function $O \to X$ defined by $\kappa_O(i) = \sigma(i)$ if $i \in O$. Show that $\kappa_O \in S_O$ (note that you need to show that the range of κ_O is in O!)
   (c) Choose $i \in O$ and suppose O is finite, of size r. Show that κ_O is an r-cycle: that mapping $[j]_r \mapsto \kappa_O^j(i)$ gives a well-defined bijection $\mathbb{Z}/r\mathbb{Z} \to O$ (equivalently, that if we set $i_0 = i$, $i_1 = \sigma(i)$, $i_{j+1} = \sigma(i_j)$ and so on we get $i_r = i_0$).
   RMK Note that $r = 1$ is possible now – every fixed point is its own 1-cycle.
   (d) Choose $i \in O$ and suppose O is infinite. Show that κ_O is an infinite cycle: that mapping $j \mapsto \kappa_O^j(i)$ gives bijection $\mathbb{Z} \to O$.
   RMK We'd like to say

$$\sigma = \prod_{O \in X/\sim} \kappa_O$$

   but there very well may be infinitely many cycles if X is infinite. We can instead interpret this as σ being the union of the κ_O: for every $i \in X$ let O be the orbit of i, and then $\sigma(i) = \kappa_O(i)$.

B. In this problem we give an alternative approach to the sign character.

(a) For $\sigma \in S_n$ set $t(\sigma) = \#\{1 \leq i < j \leq n \mid \sigma(i) > \sigma(j)\}$ and let $s(\sigma) = (-1)^{t(\sigma)} = \begin{cases} 1 & t(\sigma) \text{ even} \\ 0 & t(\sigma) \text{ odd} \end{cases}$.

Show that for an r-cycle κ we have $s(\kappa) = (-1)^{r-1}$.

(b) Let $\tau \in S_n$ be a transposition. Show that $t(\tau\sigma) - t(\sigma)$ is odd, and conclude that $s(\tau\sigma) = s(\tau)s(\sigma)$.

(c) Show that $s\colon S_n \to \{\pm 1\}$ is a group homomorphism.

(d) Show that $s(\sigma) = \mathrm{sgn}(\sigma)$ for all $\sigma \in S_n$.

Supplementary Problems II: Automorphisms

C. (The automorphism group) Let G be a group.

(a) An isomorphism $f\colon G \to G$ is called an *automorphism* of A. Show that the set $\mathrm{Aut}(G)$ of all automorphisms of G is a group under composition.

DEF Fix $a \in G$. For $g \in G$ set $\gamma_a(g) = aga^{-1}$. This is called *"conjugation by a"*.

(b) Show that $\gamma_a \in \mathrm{Hom}(G, G)$.

(*c) Show that $\gamma_a \in \mathrm{Aut}(G)$ and that the map $a \mapsto \gamma_a$ is a group homomorphism $G \to \mathrm{Aut}(G)$.

DEF The image of this map is called the group of *inner* automorphisms and is denoted $\mathrm{Inn}(G)$.

D. Let F be a field. A map $f\colon F \to F$ is an *automorphism* if it is a bijection and it respects addition and multiplication.

(a) Show that $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of the field from problem P3.

(b) Show that complex conjugation is an automorphism of the field of real numbers.

RMK $\mathbb{C}$ has many other automorphisms.

(c) Supplementary Problem F to PS1 shows that $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.