Math 342 Problem set 11 (due 29/11/11)

Reed-Solomon decoding

1. Working over the field $\mathbb{F}_5$, the sender has enocded two-digit messages by evaluating the associated linear polynomial at the 4 non-zero points of $\mathbb{F}_5$ in order. You receive the transmissions below, which may contained corrupted bits. For each 4-tuple find the linear polynomial which passes through as many points as possible.
   (a) $\underline{v}' = (1,2,3,3)$.
   (b) $\underline{v}' = (4,1,3,0)$.
   (c) $\underline{v}' = (2,4,3,1)$.

The symmetric group

2. Multiply (compose) the following permutations in S_4. Explain why the answers to (b) and (d) are the same.
   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
   (c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
   (d) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

3. Let S_3 be the symmetric group on three letters, C_6 the group $(\mathbb{Z}/6\mathbb{Z}, [0]_6, +)$.
   (a) Show that both C_6 and S_3 have six elements.
   (b) Find two elements a, b of S_3 which do not commute (that is, such that $ab \neq ba$.
   (c) Using (b) explain why the groups S_3 and C_6 cannot be "the same group".
   (d) For the a, b you found calculate $c = (ab)(ba)^{-1} = aba^{-1}b^{-1}$. This is called the "commutator" of a, b.
   (e) Let $f\colon S_3 \to C_6$ be a group homomorphism (that is: $f(\mathrm{id}) = [0]_6$, $f(\sigma\tau) = f(\sigma) + f(\tau)$, $f(\sigma^{-1}) = -f(\sigma)$ for all $\sigma, \tau \in S_3$). Show that $f(c) = [0]_6$.
   Hint: Calculate $f(c)$ in terms of the (unknown) $f(a), f(b)$ and simplify your answer using properties of modular addition.
   (f) Conclude that any group homomorphism $f\colon S_3 \to C_6$ is not injective, in particular not an isomorphism.

Orders

4. (General cancellation property) Let G be a group and let $x, y, z \in G$. Show that if $xz = yz$ then $x = y$ and that if $zx = zy$ then also $x = y$.

5. For each $\sigma \in S_3$ find the smallest k such that $\sigma^k = \mathrm{id}$. This is called the *order* of σ.

Supplementary problems

A. Direct products and sums.

(a) Let G,H be groups. On $G \times H$ define a binary operation by $(g_1,h_1)\cdot(g_2,h_2) \stackrel{\text{def}}{=} (g_1g_2,h_1h_2)$. Together with the identity element (e_G,e_H) show that this makes $G \times H$ into a group called the *direct product* of G,H.

(b) More generally, let $\{G_i\}_{i\in I}$ be a family of groups. Let $\prod_{i\in I} G_i$ be the set of all functions f with domain I such that $f(i) \in G_i$ for all i. Give $\prod_{i\in I} G_i$ the structure of a group. This is the *direct product* of the family. When the G_i are all isomorphic to a fixed group G this is usually denoted G^I.

(c) Let $\Sigma_{i\in I}G_i \subset \prod_i G_i$ be the set of *finitely supported* functions, that is those functions f such that $f(i) = e_{G_i}$ for all but finitely many i. Show that $\sum_{i\in I} G_i$ is a group, called the *direct sum* of the groups G_i. When the G_i are all isomorphic to a fixed group G this is sometimes denoted $G^{\oplus I}$.

B. Distinguishing direct products and sums.

(a) Show that $C_2^{\oplus\mathbb{N}}$ is not isomorphic to $C_2^{\mathbb{N}}$, and that $\mathbb{Z}^{\oplus\mathbb{N}}$ is not isomorphic to $\mathbb{Z}^{\mathbb{N}}$.
Hint: In both cases show that the direct sum is countable and that the direct product has the cardinality of the continuum.

(b) Show that every element of $\sum_{n=1}^{\infty} C_n$ has finite order.

(c) Show that $\prod_{n=1}^{\infty} C_n$ has elements of infinite order.