Math 342 Problem set 12 (not for submission)

The subgroup generated by an element

1. Let G be a group, $g \in G$. Define a function $f \colon \mathbb{N} \to G$ by setting $f(0) = e$, $f(n+1) = f(n) \cdot g$. Extend f to a function $f \colon \mathbb{Z} \to G$ by setting $f(-n) = f(n)^{-1}$.
   (a) What is $f(1)$?
   (b) Show that for all $m,n \in \mathbb{N}$, $f(m+n) = f(m) \cdot f(n)$.
   (c) Let $n,m \in \mathbb{N}$ with $n > m$. Show that $f((-m)+n) = f(-m) \cdot f(n)$.
   Hint: Show that $f(m) \cdot f((-m)+n) = f(m) \cdot (f(-m) \cdot f(n))$ [for the LHS use part (b), for the second associativity] then use problem 3.
   (d) Show that $f(n+m) = f(n) \cdot f(m)$ for all $n,m \in \mathbb{Z}$.
   We have shown: for any group G and element $g \in G$ there exists a group homomorphism $f \colon (\mathbb{Z}, 0, +) \to G$ such that $f(1) = g$.
   OPTIONAL Show that such f is *unique.*
   Because of this we usually write $f(n)$ as g^n.

2. (Continuation)
   (a) Let $I = \{n \in \mathbb{Z} \mid f(n) = e\}$. Show that $0 \in I$ and that I is closed under addition.
   (b) Show that I is closed under multiplication by elements of $\mathbb{Z}$.
   Hint: Multiplication is repeated addition.
   OPTIONAL Show that f descends to an injection $g \colon \mathbb{Z}/I \hookrightarrow G$.

Subgroups and Lagrange's Theorem

Let $G = \mathrm{GL}_2(\mathbb{F}_p)$, and let $B = \left\{ \begin{pmatrix} a & b \\ & d \end{pmatrix} \in G \right\}, N = \left\{ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \in G \right\}, T = \left\{ \begin{pmatrix} a & \\ & d \end{pmatrix} \in G \right\}$.

In Problem Set 11 we saw that the order of G (the number of its elements) is $(p+1)p(p-1)^2$.

3. (orders of the groups)
   (a) Find the order of N.
   (b) Find the order of T.
   (c) Find the order of B.
   (d) Check that $\#B = \#N \cdot \#T$.

4. (Lagrange's Theorem) Among the groups G,B,N,T find all pairs such that one is a subgroup of the other. In each case verify that the order of the subgroup divides the order of the larger group. (For example: N is a subgroup of G so its order must divide the order of G).

5. (B/T; see Example 181 in the notes)
   (a) Let $n_1, n_2 \in N$ be distinct. Show that $n_1 \not\equiv_L n_2\,(T)$. Conclude that all elements of N belong to different costs modulu T.
   Hint: what is $n_2^{-1} n_1$? When would it belong to T?
   (b) Use Lagrange's Theorem and your answer to 1(d) to show that N is a complete system of representatives for B/T.
   Hint: Can the number of cosets be larger than $\#N$?

(c) Let $g = \begin{pmatrix} a & b \\ & d \end{pmatrix} \in B$ and let $t = \begin{pmatrix} \alpha & \\ & \delta \end{pmatrix} \in T$. Calculate the product $gt \in B$.

(d) Given g, find t so that $gt \in N$. Conclude that every element of B belongs to the coset of an element of N and again show that N is a complete system of representatives.

OPTIONAL Following the same steps, show that T is a system of coset representatives for G/N.

A group isomorphism

6. Let F be a field, $G = \mathrm{GL}_n(F)$, $V = F^n$, $X = V \setminus \{\underline{0}\}$ the set of non-zero vectors.
   (a) Show that for any $g \in G$, $x \in X$, we also have $gx \in X$.
   (b) Show that for any $g \in G$, the map $\sigma_g \colon X \to X$ given by $\sigma_g(x) = gx$ is a bijection of X to itself.
   Hint: find an inverse to the map.
   (c) Show that the map $g \mapsto \sigma_g$ is a group homomorphism $G \to S_X$.
   (d) Assume that σ_g is the identity permutation. Show that g is the identity matrix. Conclude that the map from part (c) is injective.
   (e) Now assume $F = \mathbb{F}_2$, $n = 2$. What are the sizes of G? Of V? of X? Show that in this case the map from part (c) is surjective, hence an isomorphism.

Optional Problems

A. Let R be a commutative ring, $I \subset R$ an ideal (a non-empty subset closed under addition and under multiplication by elemenets of R). Consider the relation $f \equiv g\,(I) \iff f - g \in I$ defined for $f, g \in R$.

(a) Show that $f \equiv g\,(R)$ is an equivalence relation.

(b) Show that the set R/I of equivalence classes has a natural ring structure so that the map $Q\colon R \to R/I$ given by $Q(f) = [f]_I$ is a surjective ring homomorphism.

(c) Let J be an ideal of R/I. Show that $F^{-1}(J)$ is an ideal of R.

(d) Assume that every ideal of R is principal. Show that every ideal of R/I is principal.

B. Let F be a field, $R = F[x]$, $I = (x^n - 1) = \{f(x^n - 1) \mid f \in R\}$, $\bar{R} = R/I$. Show that the restriction of the quotient map $Q\colon R \to \bar{R}$ to the subset $F[x]^{<n}$ is bijective. It is an isomorphism of vector spaces over F.

C. The cyclic group C_n acts on F^n by cyclically permuting the co-ordinates. Show that under the usual identifications of F^n with $F[x]^{<n}$ and $F[x]^{<n}$ with $F[x]/(x^n - 1)$, the action of the generator of C_n in F^n corresponds to multiplication by x in $\bar{R}$.

D. Let $C \subset F^n$ be a *cyclic code*, that is a code for which if $\underline{v} = (v_1, \ldots, v_n)$ is a code word then $(v_2, v_3, v_{4,}, \ldots, v_n, v_1)$ is also a codeword. Show that under the correspondence above a cyclic code C is the same as an ideal in $\bar{R}$.

Hint: Let $J \subset F[x]$ be a linear subspace closed under multiplication by x. Show by induction on the degree of $f \in F[x]$ that J is closed under multiplication by f.

E. Let C be a cyclic code, $J \subset \bar{R}$ the corresponding ideal. Let $g \in R$ be a polynomial of minimal degree such that $Q(g)$ generates J (this exists by problem A(d)). Show that $GCD(g, x^n - 1)$ also generates J. Conclude that $g | x^n - 1$.