Homework #9

Problems to hand in on Thursday, April 4, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) (a) Prove Fermat's Little Theorem: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

   (b) If G is a group of prime order p, then G is cyclic.

   (c) A nontrivial group G has no nontrivial proper subgroups if and only if G is finite and of order p where p is prime.

Solution.

(a) In general, if G is a group of order n, then $g^n = e$ for any $g \in G$, since the order of g divides n by Lagrange's Theorem. Since $\mathbb{Z}_p^\times$ is as group of order $p-1$, every element in $\mathbb{Z}_p^\times$ verifies $g^{p-1} = 1$. Given an integer a such that $p \nmid a$, the class of a is an elment of $\mathbb{Z}_p^\times$, and thus $a^{p-1} \equiv 1$.

(b) Suppose that G is a group of order p, and let $g \in G$ be an element that is not the identity in G. By Lagrange's Theorem, the order of g divides $|G| = p$, and since the order of g cannot be 1, we conclude it must be p. Therefore, $\langle g \rangle = G$, and G is cyclic.

(c) Suppose that G has no nontrivial subgroups. Given any $g \in G$ that is not the identity, $\langle g \rangle$ is a nontrivial subgroup of G, and so the only possibility is that $\langle g \rangle = G$. We conclude that G is cyclic. If G is infinite, then g has infinite order, and the powers $g, g^2, g^3, \cdots$ are all distinct. In particular, $g \notin \langle g^2 \rangle$, wicih implies that $\langle g^2 \rangle$ is a proper subgroup of G. Therefore, G must be finite. We conclude that G is isomorphic to $\mathbb{Z}_n$ for some $n = |G|$. If $n = ab$, then $[a]$ has order b, and since G has no nontrivial proper subgroups, we conclude that either $a = 1$ and $b = n$ or $a = n$ and $b = 1$. In other words, n must be prime.

On the other hand, suppose that G is a finite group of order p. We have seen that G must then be cyclic, so isomorphic to $\mathbb{Z}_p$. Consider any $a \in \mathbb{Z}$ such that $p \nmid a$. There exist $u, v \in \mathbb{Z}$ such that $au + pv = 1$, so $au \equiv 1 \mod p$ for some u. In particular, $\langle [a] \rangle = \langle [1] \rangle = \mathbb{Z}_p$. This shows there are no nontrivial proper subgroups of $\mathbb{Z}_p$.

2) The goal of this problem is to prove the following fact:

Given positive integers n and p, if p is prime then $n!$ divides $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

   (a) Describe a subgroup of $GL_n(\mathbb{Z}_p)$ that is isomorphic to $\mathbb{S}_n$.

   (b) Count the elements in $GL_n(\mathbb{Z}_p)$.

   (c) Prove the fact.

Solution.

(a) The permutation matrices: see G in the adventure sheet on permutation groups.

(b) This is just a generalization of what we did before for $n = 2$. The first column can be any nonzero vector (there are $p^n - 1$ options), the second column cannot be a multiple of the first column ($p^n - p$ choices), the third column cannot be a linear combination of the first two ($p^n - p^2$ choices), etc. For the k-th column, there are $p^n - p^{k-1}$ options. The total number of invertible $n \times n$ matrices is $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

(c) There is a subgroup of order $n!$ of a group of order $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$; by Lagrange's theorem, the order of a subgroup divides the order of the group.

3) Let X be any set and $\sim$ be an equivalence relation on X. Write $\mathscr{E}(x)$ to denote the equivalence class of x.

(a) Given $x, y \in X$, show that $x \sim y$ if and only if $\mathscr{E}(x) = \mathscr{E}(y)$.

(b) Given $x, y \in X$, show that either $\mathscr{E}(x) = \mathscr{E}(y)$ or $\mathscr{E}(x) \cap \mathscr{E}(y) = \emptyset$.

(c) Show that X is the disjoint union of all the equivalence classes for $\sim$.

Solution.

(a) If $x \sim y$, then $z \in \mathscr{E}(x)$ if and only if $z \sim x$, which by transitivity is equivalent to $z \sim y$, which happens if and only if $z \in \mathscr{E}(y)$.

(b) By symmetry, if $z \sim x$ and $z \sim y$, then $x \sim y$. Suppose $x \not\sim y$; then $z \sim x$ implies $z \not\sim y$, and $z \sim y$ implies $z \sim x$. If $z \in \mathscr{E}(x)$ then $z \sim x$, and thus $z \not\sim y$, so $z \notin \mathscr{E}(y)$. This shows that $\mathscr{E}(x) \cap \mathscr{E}(y) = \emptyset$ whenever $x \not\sim y$.

(c) We have shown that all the distinct equivalence classes are disjoint. On the other hand, every element $x \in X$ is in some equivalence class, by reflexivity.

4) Let $R = \mathbb{R}[x]$. Consider the group action of $G = \mathbb{Z}_2$ on R by the rules

$$[0]_2 \cdot f(x) = f(x) \qquad \text{and} \qquad [1]_2 \cdot f(x) = f(-x).$$

Show that the set of *invariant polynomials* $\{r \in R \mid g \cdot r = r \text{ for all } g \in G\}$ is a subring of R, and describe this subring explicitly.

Solution. Let S be the set of invariant polynomials. Note that a polynomial p is invariant if and only if $p(-x) = p(x)$.

- S contains 0 and 1.
- S is closed under addition:
  If $p, q \in S$, then $(p + q)(-x) = p(-x) + q(-x) = p(x) + q(x) = (p + q)(x)$.
- S is closed under multiplication:
  If $p, q \in S$, then $(pq)(-x) = p(-x)q(-x) = p(x)q(x) = (pq)(x)$.

- S is closed for additive inverses:
  If $p \in S$, then $(-p)(-x) = -p(-x) = -p(x) = (-p)(x)$.

Now note that all even polynomials are in S, meaning all the polynomials of the form $a_0 + a_2x^2 + \cdots + a_{2n}x^{2n}$. Indeed, all polynomials of this form can be obtained by adding and multiplying multiple copies of 1 and x^2, and $1, x^2 \in S$. On the other hand, these are all the polynomials in S. To see that, just note that given any polynomial

$$p(x) = a_0 + a_1x + \cdots + a_nx^n,$$

we have

$$p(x) - p(-x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} 2a_{2i+1}x^{2i+1}.$$

So $p(x) = p(-x)$ if and only if all the odd degree coefficients of p are zero.