Groups and Group Actions, Sheet 4, HT20

Modular Arithmetic. Cosets and Lagrange's Theorem. Applications.

Main course

1. (i) Let x, n be integers with $n \geqslant 2$ and n not dividing x. Show that the order $o(\bar{x})$ of $\bar{x} \in \mathbb{Z}_n$ is

$$o(\bar{x}) = \frac{n}{\mathrm{hcf}(x,n)}.$$

(ii) Let G, H be finite groups with $g \in G$ and $h \in H$. Show that the order of (g,h) in $G \times H$ is given by

$$o((g,h)) = \mathrm{lcm}\{o(g), o(h)\}.$$

2. $\bar{x} \in \mathbb{Z}_n$ is said to be a *unit* if there exists $\bar{y} \in \mathbb{Z}_n$ such that $\bar{x}\bar{y} = \bar{1} \pmod{n}$.
(i) Show that the units of $\mathbb{Z}_n$ form a group under multiplication. We denote this group $\mathbb{Z}_n^*$.
(ii) Use Bézout's Lemma to show that $\bar{x}$ is a unit of $\mathbb{Z}_n$ if and only if $\mathrm{hcf}(x,n) = 1$.
(iii) List the units in $\mathbb{Z}_9$ and write out the Cayley table for $\mathbb{Z}_9^*$.
(iv) Show that $\mathbb{Z}_9^*$ is cyclic. What are the generators of $\mathbb{Z}_9^*$?

3. (i) Use Fermat's Little Theorem to compute $5^{15} \pmod{7}$ and $7^{13} \pmod{11}$.
(ii) Use the Fermat-Euler Theorem to compute $4^{43} \pmod{15}$ and $2^{51} \pmod{21}$.
(iii) Show that $5^{14} = 10 \pmod{15}$. [You might try to find 5^{14} modulo 3 and modulo 5 first.]

4. Let p be a prime and let g, h be elements, both of order p, in a group G. What are the possible orders of $\langle g \rangle \cap \langle h \rangle$?

Show that if G is finite then the number of elements of order p in G is a multiple of $p-1$.

Deduce that a group of order 35 contains an element of order 5 and an element of order 7.

5. Suppose that every element x in a group G satisfies $x^2 = e$. Prove that G is Abelian.

Show also that if H is any subgroup of G and $g \in G \setminus H$ then $K = H \cup gH$ is a subgroup of G.

Show further that K is isomorphic to $H \times C_2$.

Deduce that if G is finite then G is isomorphic to $(\mathbb{Z}_2)^n$ for some non-negative integer n.

6. Let G_1 and G_2 be finite groups and let $K \leqslant G_1 \times G_2$.

(i) Set $H_1 = \{g \in G_1 : (g,e) \in K\}$ and $H_2 = \{g \in G_2 : (e,g) \in K\}$. Show that

$$H_1 \leqslant G_1; \qquad H_2 \leqslant G_2; \qquad H_1 \times H_2 \leqslant K.$$

(ii) Suppose that $|G_1|$ and $|G_2|$ are coprime. Show that $K = H_1 \times H_2$.

(iii) Show that this result need not follow if $|G_1|$ and $|G_2|$ are not coprime.

Starter

S1. In this question we work in $\mathbb{Z}_8$. For each $a \in \mathbb{Z}_8$, find a^7. How does this relate to Fermat's Little Theorem and to the Fermat-Euler Theorem?

S2. Consider the dihedral group $D_8 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$ with the notation from lectures. Find all the left cosets of $\langle r \rangle$ in D_8. Find all the right cosets of $\langle r \rangle$. How do these lists compare? Now repeat for the subgroup $\langle s \rangle$.

S3. For each of the following, give a proof or a counterexample.

(i) A group with order 20 cannot have a subgroup of order 10.

(ii) A group with order 22 cannot have a subgroup of order 10.

(iii) A group with order 10 cannot have a subgroup of order 22.

(iv) A group with order 10 must have a subgroup of order 10.

(v) A group with order 12 must have a subgroup of order 6.

Pudding

P1. Let $F = 2^{32} + 1$. Let p be a prime dividing F. What is the order of 2 in $\mathbb{Z}_p^*$? Deduce that $p \equiv 1 \pmod{64}$. Use this to show that F is not prime.

P2. We say that $n \geqslant 2$ is a *Carmichael number* if n is not prime and $a^{n-1} \equiv 1 \pmod{n}$ for all a coprime to n. Show that if $n = (6k+1)(12k+1)(18k+1)$ where k is a positive integer such that $6k+1$, $12k+1$ and $18k+1$ are all prime, then n is a Carmichael number. Use this construction to find two Carmichael numbers.

P3. Let G be a group of order n with a subgroup H of order $n-1$. What can you say about n?