Solutions to HW2

1. (*Note:* I will use left-to-right composition of permutations since this is what GAP uses.) Coxeter-Todd coset enumeration on the cosets of $H = \langle a \rangle$ yields $[G : H] \leqslant 12$; see the attached worksheet. Since $|H| \leqslant 5$, this gives $|G| \leqslant 60$. At this point we should already suspect that $G \cong A_5$. Our coset table shows that the permutation representation of G on the twelve right cosets of H is given by

$$a \mapsto (2,3,4,5,6)(7,9,10,11,8); \qquad b \mapsto (1,2,3)(4,6,7)(5,8,9)(10,11,12).$$

We confirm our suspicions using GAP:

```
gap> g:=Group((2,3,4,5,6)(7,9,10,11,8),(1,2,3)(4,6,7)(5,8,9)(10,11,12));
Group([ (2,3,4,5,6)(7,9,10,11,8), (1,2,3)(4,6,7)(5,8,9)(10,11,12) ])
gap> Order(g);
60
gap> IsSimple(g);
true
gap>
```

While GAP has many sophisticated tools for group recognition, in this case it is an easy matter to identify $G \cong A_5$ since this is the unique simple group of order 60.

Alternatively, starting with the suspicion that $G \cong A_5$, it is not hard to find generators for A_5 satisfying the given presentation for G. For example, we may take $\alpha = (1,2,3,4,5)$ and $\beta = (2,5,3)$, so $\alpha\beta = (1,5)(3,4)$. Note that $\alpha^5 = \beta^3 = (\alpha\beta)^2 = \iota$. Now $\langle \alpha, \beta \rangle \leqslant A_5$ is a subgroup of order divisible by $\gcd(5,3,2) = 30$; and since A_5 is simple, it cannot have a subgroup of index 2. This proves that $\langle \alpha, \beta \rangle = A_5$. This shows that A_5 is a homomorphic image of G under an epimorphism satisfying $a \mapsto \alpha, b \mapsto \beta$. This gives the lower bound $|G| \geqslant 60$. We also have the upper bound $|G| \leqslant 60$ using coset enumeration. Putting these together gives $|G| = 60$ and our epimorphism $G \to A_5$ is an isomorphism.

Here is another GAP session in which we double-check our coset enumeration:

```
gap> f:=FreeGroup("a","b");
<free group on the generators [ a, b ]>
gap> g:=f/[f.1^5,f.2^3,(f.1*f.2)^2];
<fp group on the generators [ a, b ]>
gap> Order(g);
60
gap> IsSimple(g);
true
gap>
```

2. We first compute $|G| = 336$ using GAP:

```
gap> g:=Group((1,3,5,7,9,11,13)(2,4,6,8,10,12,14),
     (1,2)(3,6)(4,5)(7,8)(9,12)(10,13)(11,14));
Group([ (1,3,5,7,9,11,13)(2,4,6,8,10,12,14),
     (1,2)(3,6)(4,5)(7,8)(9,12)(10,13)(11,14) ])
gap> Order(g);
336
gap> k:=DerivedSubgroup(g);
Group([ (1,13,9)(2,12,10)(3,7,5)(4,8,6), (1,11,3)(4,14,12)(5,9,7)(6,10,8) ])
gap> Order(k);
168
gap> IsSimple(k);
true
gap> z:=Center(g);
Group(())
gap>
```

The derived subgroup $K = G' = [G, G]$ is the unique simple group of order 168, i.e. $K \cong PSL_2(\mathbb{F}_7) \cong GL_3(\mathbb{F}_2)$. Two candidates come to mind for G, and in fact it may be shown that these are the only possibilities: either we have a direct product $G \cong PSL_2(\mathbb{F}_7) \times 2$ or $G \cong PGL_2(\mathbb{F}_7)$. In the first case we would have a center $Z(G)$ of order 2. We used GAP to exclude this possibility; and given enough group theory we may conclude that $G \cong PGL_2(\mathbb{F}_7)$.

Next, we search for relations satisfied by the generators of G, which we label as ρ and σ. The only relations we need to check are alternating products of powers of ρ and σ, i.e. finite expressions of the form $\rho^i\sigma\rho^j\sigma\rho^k\sigma\cdots$ or $\sigma\rho^i\sigma\rho^j\sigma\rho^k\cdots$ where the exponents $i, j, k \in \{1, 2, \ldots, 6\}$. Fortunately, we do not have to check too many cases before we find suitable short relations of this form, using a continuation of our previous GAP session:

```
gap> rho:=g.1; sigma:=g.2;
(1,3,5,7,9,11,13)(2,4,6,8,10,12,14)
(1,2)(3,6)(4,5)(7,8)(9,12)(10,13)(11,14)
gap> rho*sigma;
(1,6,7,12,11,10,9,14)(2,5,8,13)(3,4)
gap> rho*sigma*rho^5*sigma;
(3,11)(4,10)(8,12)(9,13)
gap>
```

This yields the relations $\rho^7 = \sigma^2 = (\rho\sigma)^8 = (\rho\sigma\rho^5\sigma)^2 = 1$. While searching for suitable relations we also found a number of other less helpful relations (which were too long, leading to inconclusive coset enumeration problems which did not terminate in a reasonable time). We have deleted these less helpful relations from our output. Now we show that

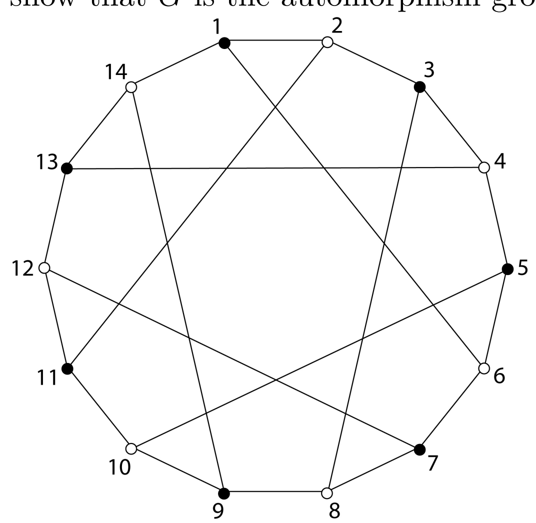
$$G \cong \langle a, b \,:\, a^7 = b^2 = (ab)^8 = (aba^5b)^2 = 1\rangle$$

using GAP to perform the coset enumeration:

```
gap> f:=FreeGroup("a","b");
<free group on the generators [ a, b ]>
gap> a:=f.1; b:=f.2;
a
b
gap> g:=f/[a^7,b^2,(a*b)^8,(a*b*a^5*b)^2];
<fp group on the generators [ a, b ]>
gap> Order(g);
336
gap> k:=DerivedSubgroup(g);
Group([ (1,13,9)(2,12,10)(3,7,5)(4,8,6), (1,11,3)(4,14,12)(5,9,7)(6,10,8) ])
gap> Order(k);
168
gap> IsSimple(k);
true
gap> Center(g);
Group(())
gap>
```

It is not hard to find elements generating $PGL_2(\mathbb{F}_7)$ and satisfying the indicated relations. Take $A = \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$ in $GL_2(\mathbb{F}_7)$. We compute $(AB)^8 = (ABA^5B)^2 = \left[\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right]$ so the desired relations are satisfied in the quotient group $PGL_2(\mathbb{F}_7) = GL_2(\mathbb{F}_7)/Z$ where $Z = \left\{\left[\begin{smallmatrix}a&0\\0&a\end{smallmatrix}\right] : a = 1,2,3,4,5,6\right\}$. Now if we interpret A and B as the corresponding elements of $PGL_2(\mathbb{F}_7)$, the subgroup $\langle A, B\rangle$ is a homomorphic image of G. But the only normal subgroups of G are the subgroups $\{1\}, K, G$ so every homomorphic image of G has order 1, 2 or 336. It follows that the epimorphism $G \to PGL_2(\mathbb{F}_7)$, $a \mapsto A$, $b \mapsto B$ is an isomorphism.

It is also not hard to show that G is the automorphism group of the graph shown.



The black and white vertices represent the points and lines of the projective plane of order 2, i.e. the 1- and 2-dimensional subspaces of $\mathbb{F}_3$. Edges of the graph represent incidence (containment). The full automorphism group of the projective plane is the group $GL_3(\mathbb{F}_2) \cong K$ of order 168, acting naturally on $\mathbb{F}_2^3$ by linear transformations. The remaining 168 elements of G act as dualities of $\mathbb{F}_2^3$, interchanging points and lines (the black and white vertices).

3. Let G_1 and G_2 be the groups in #1 and #2 respectively. Each of these groups can be generated by $m = 2$ elements. In order for both groups to be homomorphic images of $B(2, n)$, we need n to be divisible by the orders of all the elements of both groups. Clearly we can take $n = 840 = \mathrm{lcm}(|G_1|, |G_2|)$ for this purpose.

Indeed, 840 is the smallest value that works. We have

$$\begin{aligned} a &\in G_1 \quad \text{of order } 5; \\ b &\in G_1 \quad \text{of order } 3; \\ \rho &\in G_2 \quad \text{of order } 7; \\ \rho\sigma &\in G_2 \quad \text{of order } 8 \end{aligned}$$

and the least common multiple of these orders is 840.

The *exponent* of a group G is the least common multiple of the orders of its elements. Thus G_1 has exponent 60 and G_2 has exponent 168. So the exponent of a finite group G is an integer dividing the order of the group; it is the least positive integer n such that g^n for every element $g \in G$. An infinite group may have finite or infinite exponent. The Burnside group $B(m, n)$ is the most general (or universal) group of exponent dividing m, generated by n elements.