KMB, 10/11/2014

# M2PM2 Algebra II, Solutions to Sheet 4.

**1.** (a) $D_{20}$ has an element of order 10, and $S_5$ doesn't (check cycle types for example). So $S_5$ has no subgroup isomorphic to $D_{20}$.

(b) Let $x = (1\,2\,3)\,(4\,5)$ and $y = (1\,2)$. Then $x$ has order 6, $y$ has order 2, and check that $yx = x^{-1}y$. These are the equations which determine the multiplication table of $D_{12}$, so $\{e, x, x^2, \ldots, x^5, y, xy, \ldots, x^5y\}$ is a subgroup of $S_5$ isomorphic to $D_{12}$.

**2.** (a) $C_{p^r} = \{x \in \mathbb{C} : x^{p^r} = 1\}$. This has a subgroup $C_{p^{r-1}}$, and I claim that all elements not in this subgroup have order $p^r$. For if $z \in C_{p^r}$ then the order of $z$ is some divisor of $p^r$, so it's $p^s$ for some $0 \leq s \leq r$, and $s < r$ if and only if the order divides $p^{r-1}$ if and only if $z \in C_{p^{r-1}}$.

So the number of elements of order $p^r$ is $p^r - p^{r-1}$. Similarly (applying the argument to $C_{p^{r-1}}$, $C_{p^{r-2}}$ and so on) for each $1 \leq i \leq r$, number of elements of order $p^i$ is $p^i - p^{i-1}$. (And of course there is 1 element of order 1.)

(b) Pretty much the same as in (a). If $g \in (C_{p^r})^k$ then $g^{p^r} = 1$ so $g$ has order $p^s$ for some $s \leq r$, and $s < r$ if and only if $g \in (C_{p^{r-1}})^k$. So there are $p^{(r-1)k}$ elements of order less than $p^r$, leaving $p^{rk} - p^{(r-1)k}$ elements of order exactly $p^r$.

**3.** Need to prove $G_{\mathbf{a}} \cong G_{\mathbf{b}} \Rightarrow \mathbf{a} = \mathbf{b}$ (reverse is trivial).

This is tough. Here's the trick. The elements of order dividing $p^n$ in $G_{\mathbf{a}}$ are simply the subgroup $C_{p^{\min\{n,a_1\}}} \times C_{p^{\min\{n,a_2\}}} \times \cdots \times C_{p^{\min\{n,a_k\}}}$, which has size $p^{A(n)}$, with $A(n) = \sum_{i=1}^{k} \min\{n, a_i\}$. Letting $B(n)$ denote the corresponding function for $G_{\mathbf{b}}$, we deduce $A(1) = B(1)$, $A(2) = B(2)$ and so on. Now $A(1) = k$ and $B(1) = l$ so $k = l$. Similarly $A(2) = A(1) + (k - t)$ where $t$ is the number of $i$ such that $a_i = 1$, and so $A(2) = B(2)$ implies that the number of $a_i$ which are 1 equals the number of $b_i$ which are 1. Continuing this way, get $\mathbf{a} = \mathbf{b}$.

**4.** This is tougher! Here is a very brief sketch of the solution. By the structure theorem, and the fact that $C_m \times C_n \cong C_{mn}$ if $hcf(m, n) = 1$ (applied repeatedly) we can deduce that every group is a product of cyclic groups of prime power order. Hence every group is isomorphic to a group of the form mentioned in the question.

Now uniqueness. Note first that given an abelian group $G$ and a prime dividing the order of $G$, we know from the paragraph about that we *can* write $G \cong G_{\mathbf{a}} \times H$ with $G_{\mathbf{a}}$ of the type in Q3 (we write $G$ as a product of cyclic groups of prime power order and then just group together the ones for which the order is a power of our fixed prime $p$). What we want to do of course is to figure out the subgroup $G_{\mathbf{a}}$ attached to $p$ in this way, intrinsically in terms of $G$ only. A little more precisely: we need to show that if if $G \cong G_{\mathbf{a}} \times H_1 \cong G_{\mathbf{b}} \times H_2$ with the orders of $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ a power of $p$, and the orders of $H_1$ and $H_2$ both prime to $p$, then $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ are isomorphic. The reason for this is that both

of these groups are isomorphic to the subgroup of $G$ consisting of elements of order some power of $p$! So $G_{\mathbf{a}} \cong G_{\mathbf{b}}$. Now we use Q3 and then repeat for each prime dividing the order of $G$ to finish.

**5** and **6**: see **7**!

**7.** Let $|G| = 2p$ with $G$ non-abelian and $p$ prime. The non-identity elements of $G$ have orders 2, $p$ or $2p$. There isn't one of order $2p$ (otherwise $G$ would be cyclic, hence abelian). Not all have order 2, otherwise $G$ would be abelian by Sheet 2, Q6. Hence $G$ has an element $x$ of order $p$. It also has an element $y$ of order 2 by Proposition 5.2.

Let $H$ be the cyclic subgroup $\langle x \rangle = \{e, x, x^2, \ldots, x^{p-1}\}$ of $G$. Then $y \notin H$, so $H$ and $Hy$ are the two different right cosets of $H$ in $G$, so

$$G = H \cup Hy = \{e, x, x^2, \ldots, x^{p-1}, y, xy, x^2y, \ldots, x^{p-1}y\}. \tag{1}$$

Now consider the element $yx \in G$. It is in the above list, and is not equal to any $x^i$ (as $y \notin \langle x \rangle$). If $yx = xy$ we easily see that $G$ is abelian, a contradiction. So $yx = x^i y$ for some $i$ with $2 \leq i \leq p-1$.

Now we need to think a little – this is where the general case gets trickier than the $|G| = 6$ case. What is the order of $yx$? Well, $(yx)^2 = yxyx = x^i yyx = x^{i+1}$. If $i < p-1$ then $x^{i+1}$ has order $p$, but $yx$ can't have order $p$, because if it did then we get the following contradiction: $p$ is odd so $(yx)^p = x^j y^p = x^j y$ (for some $j$), and $x^j y$ can't be the identity element. Hence $yx$ has order $2p$ and $G$ is cyclic.

The remaining case is when $i = p-1$; then and $yx = x^{p-1}y = x^{-1}y$. We now have all the equations defining the dihedral group $D_{2p}$: $x^p = y^2 = e$ and $yx = x^{-1}y$, and hence $G \cong D_{2p}$.

**8.** (a) Easy.

(b) By (a) we will get all the matrices $A^r B^s$ if we take $0 \leq r \leq 3$ and $0 \leq s \leq 1$ (note the upper limit 1 rather than 3 for $s$, since we can replace $B^2$ by $A^2$). These matrices are

$$\pm I, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(c) We check the 3 subgroup properties:

(1) $I \in Q_8$

(2) Closure: using the equation $BA = A^3B$, we see that any product $(A^r B^s)(A^t B^u)$ is again of the form $A^m B^n$, so is in $Q_8$.

(3) Inverses: the inverse of $A^r B^s$ is $B^{-s} A^{-r}$, and using the equation $BA = A^3 B$, we see this is again of the form $A^m B^n$, so is in $Q_8$.

Hence $Q_8$ is a subgroup of $GL(2, \mathbb{C})$.

(d) Check from the list of matrices in (b) that $Q_8$ has only 1 element of order 2 (namely $-I$). Since $D_8$ has 5 elements of order 2, it follows that $Q_8 \ncong D_8$.

**9.** (a) Let $G$ be a non-abelian group with $|G| = 8$. The elements of $G$ have order 1,2,4 or 8 by Lagrange. Now $G$ has no element of order 8 (otherwise $G \cong C_8$ which is abelian), and not every element $x$ satisfies $x^2 = e$ (otherwise $G$ would be abelian by Sheet 2, Q6). Hence $G$ has an element $x$ of order 4.

(b) We are given that $y \neq x^2$, and also $y \neq x$ or $x^{-1}$ as these have order 4. So $y \in G - \langle x \rangle$ and

$$G = \langle x \rangle \cup \langle x \rangle y = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}.$$

Consider the product $yx$. It is clearly not $e, x, x^2, x^3$ or $xy$ (the last would force $G$ to be abelian). So $yx = x^2y$ or $x^3y$. If $yx = x^2y$ then there are lots of ways of fiddling around to get a contradiction. Here's one:

$$yx = x^2y \Rightarrow x^2 = yxy^{-1} \Rightarrow e = (x^2)^2 = (yxy^{-1})(yxy^{-1}) = yx^2y^{-1} \Rightarrow x^2 = e$$

which is a contradiction.

Hence $yx = x^3y$. Now we have the equations

$$x^4 = e,\ y^2 = e,\ yx = x^3y.$$

These equations determine the multiplication table of $G$, and as they are also the equations determining the multiplication table of $D_8$, it follows that $G \cong D_8$.

**10.** By Q9(a), $G$ has an element $x$ of order 4. Pick $y \in G - \langle x \rangle$. Then

$$G = \langle x \rangle \cup \langle x \rangle y = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}.$$

Consider the product $yx$. Show exactly as in Q9(b) that $yx = x^3y$.

If $y$ has order 2 then $G \cong D_8$ by Q9(b). The only other possibility is that $y$ has order 4, so assume this now. Consider $y^2$. It cannot be equal to $e, x$ or $x^3$ (the latter two have order 4). It cannot be $y, xy, x^2y, x^3y$ as $y \notin \langle x \rangle$. So $y^2 = x^2$. We now have the equations

$$x^4 = e,\ x^2 = y^2,\ yx = x^3y.$$

These equations determine the mult table of $G$, and as they are also the equations determining the mult table of $Q_8$, it follows that $G \cong Q_8$.