THE UNIVERSITY OF SYDNEY

MATH2008 Introduction to Modern Algebra

(http://www.maths.usyd.edu.au/u/UG/IM/MATH2008/)

Semester 2, 2003 | Lecturer: R. Howlett

Tutorial 11

1. Let H and K be subgroups of a finite group G, and let m be the order of H and n the order of K. By Question 4 of Tutorial 7, the intersection $H \cap K$ is also a subgroup. If $H \cap K$ has order d, prove that d is a common divisor of m and n.

Solution.

Because $H \cap K$ is a subgroup of H it follows from Lagrange's Theorem that d divides m. Similarly, since $H \cap K$ is a subgroup of K it follows that d divides n. Thus d divides both m and n.

2. If $m = 31$ and $n = 64$ in Question 1, what can you deduce about $H \cap K$?

Solution.

Since 31 and 64 have no common divisors greater than 1, the order of $H \cap K$ must be 1. Since $H \cap K$ is a subgroup it must contain the identity element e, and since its order is 1 it contains no other elements. Thus $H \cap K = \{e\}$.

3. If $m = 21$ and $n = 14$ in Question 1, show that $H \cap K$ is a cyclic group.

Solution.

Recall that a group is cyclic if and only if it contains an element whose powers give all the elements of the group. Such an element is called a *generator* of the cyclic group.

The only positive integers that are divisors of both 21 and 14 are 1 and 7; so these are the only possibilities for $\#(H \cap K$ (the order of $H \cap K$). If $\#(H \cap K) = 1$ then $H \cap K = \{e\}$, which is certainly a cyclic group (generated by e). Alternatively, suppose that $\#(H \cap K) = 7$. Then we can choose an element $x \in (H \cap K)$ with $x \neq e$. The set of all powers of x is then a subgroup of $H \cap K$ (called the cyclic subgroup generated by x). Call this subgroup L. Then $\#L$ is a divisor of $\#(H \cap K) = 7$, and $\#L > 1$ since L contains at least the two distinct elements e and x. So $\#L = 7$, which means that $L = H \cap K$. So $H \cap K$ is cyclic, generated by x.

4. Let G be the group of all nonzero complex numbers under multiplication. Using the representation of complex numbers as points in the plane, draw a sketch showing the subgroup H consisting of all complex numbers of modulus 1. Describe also the cosets of H in G.

Solution.

In the Argand diagram the complex numbers of modulus 1 constitute a circle of radius 1 with the origin as centre. Let t be an arbitrary element of G, and put $a = |t|$. Then a is a positive real number. The coset tH consists of all complex numbers of the form tx, where $x \in H$, and since $|x| = 1$ for all $x \in H$ we see that $|tx| = |t|\,|x| = a|x| = a$. So all elements of tH have modulus a. Conversely, if u is a complex with $|u| = a$ then $u \neq 0$ and we have $u = tx$, where $x = tu^{-1}$. Now since $a = |u| = |tx| = |t|\,|x| = a|x|$ it follows that $|x| = 1$; thus $x \in H$, and so $u = tx \in tH$. This shows that all complex numbers of modulus a lie in tH. Thus the coset tH is a circle of radius a centred at the origin. Every positive real number a occurs as the modulus of a nonzero complex number; so we conclude that the set of all cosets of H in G is the set of all circles of positive radius centred at the origin.

5. Let a be a group element of order 79. Determine the order of a^{59}.

Solution.

Any element of any group must generate a cyclic subgroup of that group. If the group is finite then the order of the subgroup must also be finite, and by Lagrange's Theorem must be a divisor of the order of the group. And if the cyclic subgroup generated by g has order k then the element g has order k. In summary, the elements of a finite group all have finite order, and for each element the order is a divisor of the order of the group.

Recall that a group element g has order k if and only if k is the least positive integer m such that $g^m = e$ (the identity). If g has order k then $g^m = e$ if and only if m is a multiple of k.

We are given that a is an element of a group G and that a has order 79. Thus $a^m = e$ if and only if m is a multiple of 79. Let H be the cyclic subgroup of G generated by a. Then $\#H = 79$. Since a^{59} is an element of H, the order of a^{59} is a divisor of $\#H = 79$. Since 79 is prime, it follows that the order of a^{59} is either 79 or 1. If it were 1 then we would have that $a^{59} = e$, which is false since 59 is not a multiple of 79. So the order of a^{59} is 79.

6. Let D be the group of symmetries of a regular hexagon. Show that any subgroup of D containing both a reflection and the rotation anticlockwise through 60° must be all of D.

Solution.

Let ρ be the anticlockwise rotation through $60°$ and let σ be any reflection symmetry of the hexagon. Let H be the subgroup of D generated by ρ and σ. Since ρ^n is a rotation through $60n°$, we see that ρ has 6 distinct powers (namely, anticlockwise rotations through $0°$, $60°$, $120°$, $180°$, $240°$ and $300°$). The subgroup H contains these 6 elements and also σ. Since σ is not a rotation—reflections are distinguished from rotations by the fact that a reflection fixes exactly two points on the perimeter of the hexagon, whereas non-identity rotations do not fix any and the identity fixes them all—it follows that H contains at least 7 elements. The order of H is a divisor of the order of D, which is 12 (since D consist of 6 rotations and 6 reflections). So $|H| = 12$, and so $H = D$.

7. Let H be the group formed by the complex numbers 1, -1, i, $-i$ under multiplication. Find a group of permutations that is isomorphic to H.

Solution.

These four complex numbers form a cyclic group of order 4, generated by i (and also generated by $-i$). All cyclic groups of order 4 are isomorphic to H: if x is a generator of a cyclic group L of order 4 then the function $f\colon H \to L$ given by $f(i) = x$, $f(-1) = x^2$, $f(-i) = x^3$ and $f(1) = x^4 = e$ is an isomorphism (that is, a one-to-one correspondence that preserves multiplication). So to answer this question we just have to find a permutation x of order 4. The most obvious choice is the 4-cycle $x = (1,2,3,4)$. Then $x^2 = (1,3)(2,4)$ and $x^3 = (1,4,3,2)$ (and $x^4 = \mathrm{id}$).

There are other possibilities too: for example $(1,2,3,4)(5,6)$ has order 4: this would give an isomorphism with $i \leftrightarrow (1,2,3,4)(5,6)$, $-1 \leftrightarrow (1,3)(2,4)$, $-i \leftrightarrow (1,4,3,2)(5,6)$ and $1 \leftrightarrow \mathrm{id}$. In general, a permutation has order 4 if and only if its expression as a product of disjoint cycles consists of 4-cycles and 2-cycles, with at least 1 4-cycle.

8. (*i*) Let G be an abelian group. Suppose that $x, y \in G$, x has order 2 and y has order 3. Show that xy has order 6.

(*ii*) Find an example of a group G containing an element x of order 2 and an element y of order 3 such that G contains no elements of order 6. (Note that G must be non-abelian, by Part (*i*).)

Solution.

(*i*) If $xy = e$ (the identity) then $x = xe = x(xy) = x^2y = ey = y$, since we are given that x has order 2 (and so $x^2 = e$). But $x \neq y$ since x has order 2 and y has order 3. So $xy \neq e$.

As G is abelian, $xy = yx$. So $(xy)^2 = xyxy = xxyy = x^2y^2 = ey^2 = y^2$. Note that $y^2 \neq e$ since y has order 3, and 2 is not a multiple of 3. So $(xy)^2 \neq e$.

Similarly, $(xy)^3 = xyxyxy = x^3y^3 = x$, since $x^3 = x$ and $y^3 = e$. And $x \neq e$ since x has order 3, not 1. So $(xy)^3 \neq e$.

Since $(xy)^6 = xyxyxyxyxyxy = x^6y^6 = e$, the order of xy must be a divisor of 6. It is not 1, 2 or 3 since xy, $(xy)^2$ and $(xy)^3$ are all not equal to e. So the order of xy is 6.

(*ii*) The group $G = \mathrm{Sym}(3)$ has the required property. It has 6 elements: three transpositions $(1,2)$, $(1,3)$ and $(2,3)$, which all have order 2, two 3-cycles $(1,2,3)$ and $(1,3,2)$, both of order 3, and the identity (of order 1). It has no elements of order 6.

9. Let G be a finite group and H, K subgroups of G such that $H \cap K = \{e\}$ (where e is the identity). Let m, n be the orders of H and K. Show that the mn products hk, where h is in H and k is in K, give mn distinct elements of G. (Hint: If $h_1k_1 = h_2k_2$ then $k_1k_2^{-1} = h_1^{-1}h_2$, and this element is both in K and in H.)

Solution.

Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$, and suppose that $h_1k_1 = h_2k_2$. Then $h_1^{-1}(h_1k_1)k_2^{-1} = h_1^{-1}(h_2k_2)k_2^{-1}$. But $h_1^{-1}h_1k_1k_2^{-1} = ek_1k_2^{-1} = k_1k_2^{-1}$, and similarly $h_1^{-1}(h_2k_2)k_2^{-1} = h_1^{-1}h_2$. So $k_1k_2^{-1} = h_1^{-1}h_2$. Call this element t.

Since $h_1, h_2 \in H$ and H is closed under the formation of inverses and under multiplication, the element $h_1^{-1}h_2$ is in H. So $t \in H$. Similarly $t = k_1k_2^{-1} \in K$. So $t \in H \cap K$, and so $t = e$ since we are given that $H \cap K = \{e\}$.

Thus $k_1k_2^{-1} = e$, and so $k_1 = k_1(k_2^{-1}k_2) = (k_1k_2^{-1})k_2 = k_2$. Similarly, since $h_1^{-1}h_2 = e$ it follows that $h_2 = h_1h_1^{-1}h_2 = h_1$.

The above calculations show that as h runs through all m elements of H and k runs through all n elements of K, distinct pairs (h,k) give distinct products hk. So we get mn distinct elements of G, as claimed.