

HW 4: solution sketches

- (1) A permutation of cycle type $(i j)$ is called a transposition. Show that the symmetric group S_n is generated by the transpositions it contains. Equivalently, show that every element of S_n is a product of transpositions.

Any permutation may be written as a product of disjoint cycles, so it is enough to show that any cycle is a product of transpositions. Here is one way to show this. Check that:

$$(a_1 a_2 \cdots a_n) = (a_1 a_2)(a_2 a_3) \cdots (a_{n-2} a_{n-1})(a_{n-1} a_n).$$

- (2) Recall that D_n denotes the symmetry group of a regular n -gon. Show that if n is divisible by m , then D_n has a subgroup isomorphic to D_m .

Assume that $n = md$ and let $R = r^d, F = f$. The elements

$$\{1, R, R^2, \dots, R^{m-1}, F, RF, \dots, R^{m-1}F\} = \{1, r^d, r^{2d}, \dots, r^{(m-1)d}, f, r^d f, \dots, r^{(m-1)d} f\}$$

are (i) distinct elements of D_n , (ii) closed under the group operations of D_n , and (iii) satisfy the relations that define D_m : $R^m = 1, F^2 = 1$, and $FR = R^{-1}F$. Items (i)-(iii) are enough to show that these elements form a subgroup isomorphic to D_m .

More detail for (iii): $R^m = r^{md} = r^n = 1, F^2 = f^2 = 1$, and $FR = fr^d = r^{-1}fr^{d-1} = r^{-2}fr^{d-2} = \dots = r^{-d}f = R^{-1}F$.

- (3) An element of order 2 in a group is called an involution. Show that D_n is generated by two involutions. (Hint: find two reflections that generate all elements of D_n .)

The problem should state that $n > 1$. We should exclude the case $n = 1$, since if $n = 1$ we have $|D_1| = 2$ hence D_1 contains at most one involution.

Recall that $D_n = \langle r, f \mid r^n = 1, f^2 = 1, fr = r^{-1}f \rangle$. (This states that D_n is generated by the elements r and f subject to the relations $r^n = 1, f^2 = 1, fr = r^{-1}f$ and to no other relations that are not consequences of these.)

The elements r and f generate D_n . The elements rf and f suffice to generate r (since $r = (rf) \cdot f$). Hence the set $\{rf, f\}$ generates $\{r, f\}$, which generates D_n . On Quiz 4 you showed that $(rf)^2 = 1$. If $rf \neq 1$, then rf is an involution, in which case $\{rf, f\}$ is a generating set for D_n consisting of two involutions.

This is all you were meant to do, but there is one more thing to be concerned about. What if $rf = 1$? Then, according to the definition, rf is not an involution, so we should not use it in the generating set. Let's explain why this case can never occur.

If $rf = 1$, then $r = (rf)f = 1f = f$, in which case the elements of D_n can only be $\{1, f\}$ so n must be 1. But when $n = 1$ we do not have $rf = 1$ since in D_1 we have $r = 1$ and $f \neq 1$. Thus, we never have $rf = 1$ in D_n .