Dartmouth College
Mathematics 17

Assignment 5
due Wednesday, February 8

1. We investigate some general classes of groups. The symmetric group is defined as the set of permutations of the set $\{1, 2, \ldots, n\}$, that is, as a set $S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid f \text{ is a bijection}\}$.. The group operation is function composition, so that the group product $f * g$ is just the composite function $f \circ g$. The identity is the function f so that $f(k) = k$ for all k, $1 \leq k \leq n$, and any given function has an inverse precisely because it is one-to-one and onto. Convince yourself that the order of S_n, $|S_n|$, is $n!$.

   For concreteness, we shall consider the case of $n = 3$. While a bit cumbersome, we will denote an element in S_3 by $f = \begin{bmatrix} 1 & 2 & 3 \\ a & b & c \end{bmatrix}$ the function f defined by $f(1) = a$, $f(2) = b$, $f(3) = c$. The group operation is function composition, so $f * g$ is the function whose action on k is $f(g(k))$. In the permutation notation, this translates as follows:

$$f = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, g = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \mapsto fg = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix},$$

   that is

$$f(g(1)) = f(2) = 1; \quad f(g(2)) = f(1) = 3; \quad f(g(3)) = f(3) = 2.$$

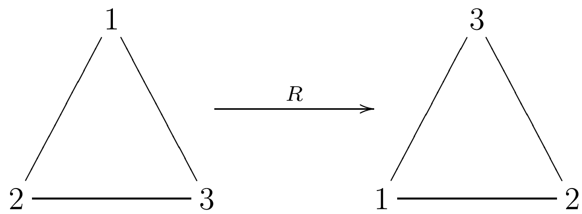
   (a) Let $\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ and $\tau = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Compute $\sigma, \sigma^2, \sigma^3$, τ, τ^2, τ^3, $\sigma\tau, \sigma^2\tau$.

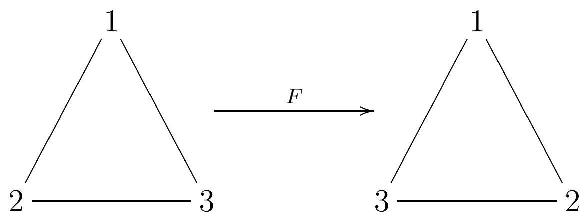
   (b) Fill in the Cayley table for S_3 using the elements listed in the first row or column. For example, don't enter $\tau\sigma$:

$\times$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e						
σ						
σ^2						
τ						
$\sigma\tau$						
$\sigma^2\tau$						

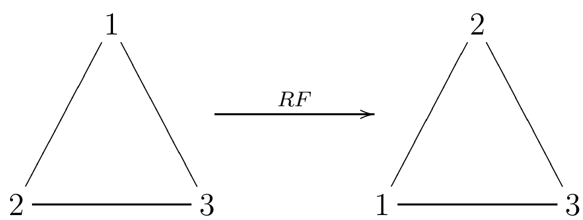
   (c) Determine whether S_3 is abelian.

2. The symmetries of a triangle for a finite group called D_3. Consider two basic symmetries of a an equilateral triangle, the first a counterclockwise rotation by 120 degrees (denoted R) and the second a flip (denoted F) about a vertical axis through the vertex labeled 1.





We compose like in function composition, so that RF means first act by F, then R:



(a) Compute $R, R^2, R^3,\ F, F^2, F^3,\ RF, R^2F$.

(b) Fill in the Cayley table for D_3 using the elements listed along the first row or column. For example, don't enter FR:

$\times$	e	R	R^2	F	RF	R^2F
e						
R						
R^2						
F						
RF						
R^2F						

(c) Notice that each symmetry can be thought of as a permutation of the three vertices. If we regard the numbers marking the vertices of the left-handle triangle as positions, the R can be described as the permutation $R = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$, and $F = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Describe R^2, F, RF, R^2F.

3. Show that D_3 is isomorphic to S_3; both are nonabelian groups of order 6. Now find two cyclic groups of order 6, one additive and one multiplicative and show they are isomorphic.

4. RSA, take two. In this problem, we use a 27-letter alphabet with $A \leftrightarrow 0$, $B \leftrightarrow 1$, $\ldots$, $Z \leftrightarrow 25$, space $\leftrightarrow 26$.

   We shall convert between alphabet and numeric plaintext messages by a common scheme: encoding as a base 27 number with a certain block size, in our case 5. We do this as follows: Suppose we want to convert the message 'Groups are fun'.

   First we break up our plaintext message into blocks of length 5, padding the last block if necessary: 'Group' 's are' ' funX'. Note we will not distinguish between upper and lower case, but this would easily be done by expanding the size of our alphabet.

   'Group' $\mapsto$ $06, 17, 14, 20, 15$; 's are' $\mapsto$ $18, 26, 00, 17, 04$; ' funX' $\mapsto$ $26, 05, 20, 13, 23$, where the numbers represent the base-27 digits. We now encode these as base 27 numbers:

$$\begin{aligned}
\text{`Group'} &\mapsto 06,17,14,20,15 \mapsto 27^4(06) + 27^3(17) + 27^2(14) + 27^1(20) + 27^0(15) = 3534018 \\
\text{`s are'} &\mapsto 18,26,00,17,04 \mapsto 27^4(18) + 27^3(26) + 27^2(00) + 27^1(17) + 27^0(15) = 10078170 \\
\text{` funX'} &\mapsto 26,05,20,13,23 \mapsto 27^4(26) + 27^3(05) + 27^2(20) + 27^1(13) + 27^0(23) = 13930835
\end{aligned}$$

   Let's choose primes p and q, so that $n = pq = 59753237$. We compute $\phi(n) = (p-1)(q-1) = 59737740$. I choose a common encryption exponent $e = 2^{16} + 1 = 65537$ (the last known Fermat prime).

   (a) Find the primes p and q; this is not necessary to break the code, but reinforces that knowing $\phi(n)$ is equivalent to factoring n.

   (b) Find my decryption exponent.

   (c) Decrypt the message consisting of two blocks of numerical ciphertext, i.e., $C = P^e \pmod n$: 10881312 29883226.

   The following Mathematica functions (note the syntax) will be of use:

   - `PowerMod[a,k,n]` Computes $a^k \pmod n$
   - `ExtendedGCD[a,n]` Computes $\{d, \{u, v\}\}$ where $d = \gcd(a, n) = au + nv$. You can do this via WolframAlpha (`http://www.wolframalpha.com/`)

$\times$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e						
σ						
σ^2						
τ						
$\sigma\tau$						
$\sigma^2\tau$						

$\times$	e	R	R^2	F	RF	R^2F
e						
R						
R^2						
F						
RF						
R^2F						