Solutions to Exercises for TATA55, batch 2, 2022

November 19, 2022

1 Part one: computer assistance is helpful

In particular, the laboration that we did in class (and which is available on the course homepage) should be easy to modify to perform the necessary calculations.

1. (6p)

   (a) Let $f(n,k)$ denote the number of elements of order k in C_n. Tabulate $f(n,k)$ for $1 \leq k,n \leq 12$.

   (b) Guess a formula for $f(n,k)$.

   (c) Prove the formula!

   Solution:

```
var('n,k')
from collections import Counter
def f(n,k):
    return [a.order() for a in Integers(n)].count(k)

A = matrix(QQ,12,12,lambda n,k:f(n+1,k+1))
```

   gives

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 0 \\ 1 & 1 & 2 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

   From the textbook we know that if $G = \langle g \rangle$ is cyclic of order n, then $o(g^a) = \frac{n}{\gcd(a,n)}$. Hence $f(n,k) = 0$ when $k \not| n$, and when $k | n$ we want to count the number of $1 \leq a \leq n$ such that

$k = \frac{n}{\gcd(a,n)}$ i.e the number of $1 \leq a \leq n$ such that $\gcd(a,n) = \frac{n}{k}$. This is equivalent to finding $1 \leq r \leq k$ with $\gcd(r,k) = 1$ and putting $a = r\frac{n}{k}$. The number of such r is given by $\phi(k)$, so $f(n,k) = \phi(k)$ when $k \mid n$.

2. (6p) Same question for the dihedral group (but with $1 \leq k, n \leq 6$).

   Solution:

```
var('n,k')
from collections import Counter
def g(n,k):
    G = DihedralGroup(n)
    return [a.order() for a in G].count(k)

B = matrix(QQ,6,6,lambda n,k:g(n+1,k+1))
```

   gives

$$B = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 \\ 1 & 3 & 2 & 0 & 0 & 0 \\ 1 & 5 & 0 & 2 & 0 & 0 \\ 1 & 5 & 0 & 0 & 4 & 0 \\ 1 & 7 & 2 & 0 & 0 & 2 \end{pmatrix}$$

   Since D_n consists of n rotations, which form a cyclic subgroup, and of n reflections, which all have order two, we get that $g(n,k) = f(n,k)$ for $k \neq 2$ and that

$$g(n,2) = f(n,2) + n = \begin{cases} n+1 & n \text{ even} \\ n & n \text{ odd} \end{cases}$$

3. (6p) Same question for the symmetric group (but with $1 \leq k, n \leq 4$).

   Solution:

```
var('n,k')
from collections import Counter
def h(n,k):
    G = SymmetricGroup(n)
    return [a.order() for a in G].count(k)

C = matrix(QQ,4,4,lambda n,k:h(n+1,k+1))
```

   gives

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 3 & 2 & 0 \\ 1 & 9 & 8 & 6 \end{pmatrix}$$

   We know

- The number of permutations in S_n with cycle type $\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_\ell^{m_\ell}$ is given by

$$\frac{n!}{\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_\ell^{m_\ell}m_1!\cdots m_\ell!}$$

- The order of a permutation with cycle type $\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_\ell^{m_\ell}$ is $\gcd(\lambda_1,\dots,\lambda_\ell)$.

So the number of permutations in S_n of order k is

$$\sum_{\lambda_1^{m_1}\cdots\lambda_\ell^{m_\ell}\in T}\frac{n!}{\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_\ell^{m_\ell}m_1!\cdots m_\ell!}$$

where

$$T=\left\{\lambda_1^{m_1}\cdots\lambda_\ell^{m_\ell}\,\middle|\,\sum_j m_j\lambda_j=n,\ \gcd(\lambda_1,\dots,\lambda_\ell)=k\right\}$$

For the special cases $k=2$ we should sum

$$\sum_{m_1+2m_2=n,\,m_2>0}\frac{n!}{1^{m_1}2^{m_2}m_1!m_2!}=\sum_{m_2=1}^{\lfloor n/2\rfloor}\frac{n!}{2^{m_2}(n-2m_2)!m_2!}$$

As an example, for $n=4$ we get

$$\frac{4!}{1^2 2^1 2!}+\frac{4!}{2^2 2!}=6+3=9$$

We can turn the general half-explicit formula into an explicit one using some combinatorial machinery such as inclusion-exclusion and generating functions, but this is a bit beyond the scope of this course.

One can also use the cycle-index polynomial of S_n, for which an easy recursion is known, namely

$$Z(S_n)=\frac{1}{n}\sum_{\ell=1}^{n}a_l Z(S_{n-1})$$

to get the number of elements of order k. As an example, the cycle index of S_4 is, in SAGE-MATHS idiosyncratic notation,

$$\frac{1}{24}p_{1,1,1,1}+\frac{1}{4}p_{2,1,1}+\frac{1}{8}p_{2,2}+\frac{1}{3}p_{3,1}+\frac{1}{4}p_4$$

so we se that the number of elements of order 2 is $4!(1/4+1/8)=9$ since the monomials $p_{2,1,1}$ and $p_{2,2}$ enumerate cycle types 1^2*2^1 and 2^2, that is to say, transpositions and products of disjoint transpositions, which are the only permutatins of order 2 in S_4.

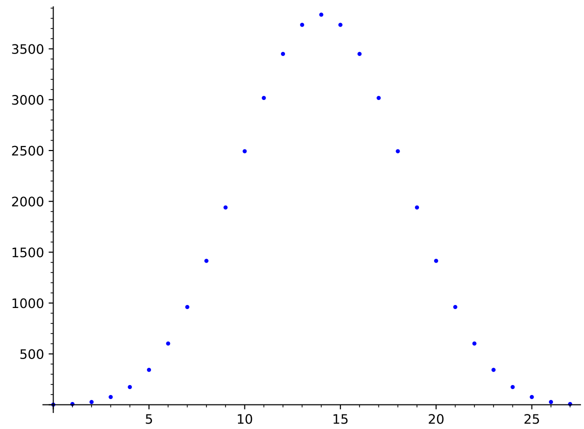
4. (4p) Let $g(n,k)$ denote the number of permutations in S_n with k inversions. Plot $g(8,k)$. Make an educated guess about the $g(n,k)$.

   Solution:

```
from collections import Counter
def j(n,k):
    Group = SymmetricGroup(n)
    numinvlist = [Permutation(g).number_of_inversions() for g in Group]
    return numinvlist.count(k)

max_k = 28
values = [j(8, x) for x in srange(0, max_k, 1)]
```

gives the follwing plot:



This looks normally distributed!

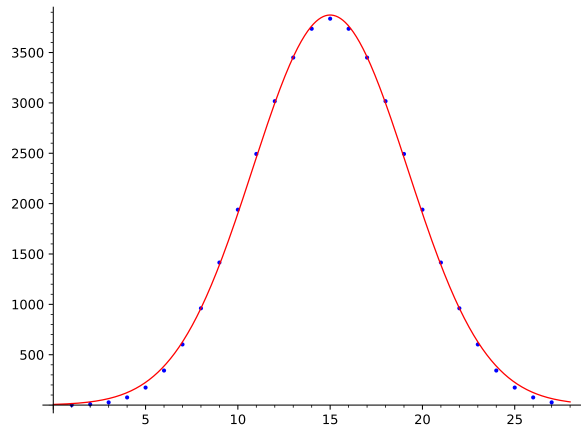
We try some data fitting:

```
data=[[x+1,values[x]] for x in srange(0, max_k-1, 1)]
var('sigma mu max x')
model(x) = max*(1/sqrt(2*pi*sigma**2))*exp(-(x-mu)**2/(2*sigma**2))
hm=find_fit(data, model,initial_guess=[3000,14,1])
```

gives

$$[max = 40702.97703256941, \mu = 15.000233170303714, \sigma = 4.193232194404608]$$

which seems to fit well (though maybe it was translated one step to the right):



The maximal number of inversions of a permutation in S_n is $1+2+\cdots+(n-1) = (n-1)n/2$, so we guess that the average number is half of that, $(n-1)n/4$.

We can verify this guess (argument stolen from internet):

Define $c \in S_n$ by $c(k) = n+1-k$, i.e. reversal. Then $\{i,j\}$ is an inversion for $\sigma \in S_n$ iff it is not an inversion for $\sigma \circ c$, and $\sum_{\sigma\in S_n} \mathrm{inv}(\sigma) = \sum_{\sigma\in S_n} \mathrm{inv}(\sigma \circ c)$ since $\sigma \mapsto \sigma \circ c$ is a bijection on S_n, so

$$2\sum_{\sigma\in S_n} \mathrm{inv}(\sigma) = \sum_{\sigma\in S_n} \mathrm{inv}(\sigma) + \sum_{\sigma\in S_n} \mathrm{inv}(\sigma\circ c) = \sum_{\sigma\in S_n} \mathrm{inv}(\sigma)+\mathrm{inv}(\sigma\circ c) = \sum_{\sigma\in S_n} \binom{n}{2} = n!\binom{n}{2}$$

so the average number of inversions is $\binom{n}{2}/2$.

We leave the calculation of the standard deviation to the student!

5. (4p) Describe the elements of the (full) symmetry group of the regular dodecaedron and list their orders. Find the conjugacy classes.

Solution:

```
Q = polytopes.dodecahedron()
G = Q.restricted_automorphism_group()
s=""
for clr in G.conjugacy_classes_representatives():
    cl = ConjugacyClass(G,clr)
    cll = cl.list()
    L = len(cll)
    s += f"{clr.order()} \t {L} \t {clr}\n"
```

gives the table

```
1   1   ()
2   15   (1,3)(2,4)(5,7)(8,9)(11,12)(13,14)(16,17)(18,19)
3   20   (20,11,12)(1,7,19)(2,14,17)(3,18,5)(4,16,13)(6,9,8)
2   15   (10,20)(1,4)(2,3)(5,12)(6,15)(7,11)(8,17)(9,16)(13,14)(18,19)
10   12   (10,20,5,4,8,15,6,17,1,12)(2,14,9,16,13,3,18,11,7,19)
5   12   (10,20,5,19,11)(1,18,2,8,16)(3,12,7,4,14)(6,17,13,9,15)
6   20   (10,1,13,15,4,19)(20,3,18,6,2,14)(5,11,12,17,9,8)(7,16)
5   12   (10,1,11,12,3)(20,17,19,18,16)(2,15,4,9,8)(5,13,14,7,6)
10   12   (10,2,6,11,7,15,3,20,9,16)(1,5,13,14,12,4,17,19,18,8)
2   1   (10,15)(20,6)(1,4)(2,3)(5,17)(7,16)(8,12)(9,11)(13,19)(14,18)
```

We analyse this:

- There are two conjugacy classes with $12 + 12$ elements of order 5, which are rotations by multiples of $2\pi/5$ around axes that go through centers of opposite faces. These rotations fix no vertex.
- There is one conjugace class with 20 elements of order 3, which are rotations by $2\pi/3$ around axes that go through opposite vertices (hence fix 2 vertices)
- There is one conjugacy class with 15 elements of order 2, which are rotations by π around axes through midpoints of opposite edges
- There is the class of the identity, 1 elem of order 1
- $12 + 12 + 20 + 15 + 1 = 60$ makes all the rotations
- There are also 60 reflections, which all have order 2
- Their conjugacy classes are all antipodal times conjugacy class of rotations, order is doubled, same number of elements

2 Part two: no computer necessary

6. (4p) Let G be a group, and let A, B be subgroups of G. Put

$$AB = \{ab | a \in A,\ b \in B\}, \quad BA = \{ba | a \in A,\ b \in B\}.$$

Show that AB is a subgroup if and only if $AB = BA$.

Solution: Suppose that $AB = BA$. Take $h \in AB$, $h = ab$ with $a \in A$, $b \in B$. Then $\ni h^{-1} = b^{-1}a^{-1} \in BA = AB$. Take furthermore $k = cd, c \in A$, $d \in b$. Then $hk = abcd = a(bc)d$. Since $bc \in BA = AB$ there exists $r \in A$, $s \in B$ with $bc = rs$. Thus $hk = a(rs)d = (ar)(sd) \in AB$.

Conversely, suppose that $AB \leq G$. Take $a \in A$, $b \in b$, and put $h = ab$. Then $h^{-1} \in AB$. But $h^{-1} = b^{-1}a^{-1} \in BA$. Since every $k \in AB$ is $(k^{-1})^{-1}$, the result follows.

7. (3p) Let G be a group, and suppose that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Show that G is abelian.

Solution: Multiplying $abab = aabb$ with a^{-1} to the left and b^{-1} to the right yields $ba = ab$.

8. (6p) Let G be a group, and let $H \subseteq G$, such that $e \in H$ and $HH \subseteq H$.

   (a) Show that $HH = H$.
   (b) If $|G| < \infty$, show that $H \leq G$.
   (c) Is it enough that $|H| < \infty$?

   Solution:

   (a) $eh = h$.
   (b) We need only to show that $H^{-1} \subseteq H$. Pick $h \in H$. Consider the map

   $$\phi_h : H \to H$$
   $$\phi_h(x) = hx$$

   This map is injective: if $\phi_h(x) = \phi_h(y)$ then $hx = hy$ so $x = y$ by cancellation. However, since H is finite (beeing a subset of the finite set G), any injective map from H to itself is in fact bijective! Thus, $e \in \phi_h(H)$, that is to say, there is some $x \in h$ with $e = \phi_h(x) = hx$. Thus h has a right inverse x, which, by group laws, is also a left inverse.
   (c) Yes.

9. (4p)

   (a) Let G be a finite group, and let $H \leq G$ be a proper, nontrivial subgroup of size k. If there is no other subgroup of G of size k, show that H is normal in G.
   (b) Give a (non-abelian) example of this situation.

   Solution: For $g \in G$, gHg^{-1} is another subgroup of size k. If there is only one such subgroup, $gHg^{-1} = H$, for any g, so H is normal in G.

   The alternating group A_n has index 2 in S_2, so it is the unique subgroup of that size, hence normal.

10. (6p) Give examples of

    (a) A non-normal subgroup (not of S_n or D_n, be creative)
    (b) $A \leq B \leq C$ and $A \triangleleft B$ but not $A \triangleleft C$.
    (c) $H_1 \triangleleft G$, $H_2 \triangleleft G$, $H_1 \neq H_2$, $|H_1| = |H_2| < \infty$.

    Solution: The subgroup of 2×2 diagonal matrices is not normal in $GL(2)$, since any symmetric matrix is conjugate to a diagonal matrix.

    Matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ form a normal subgroup of upper triangular matrices; the latter subgroup of $GL(2)$ is not normal.

    If H, K are different finite groups of the same size then (their images) are both normal in $H \times K$.

11. (4p) Let p be an odd prime number. Show that the set of matrices

$$G = \left\{ \begin{bmatrix} 1 & a & -a & b \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \middle| \, a, b \in \mathbb{Z}_p \right\}$$

is (under multiplication) a finite abelian group. What direct product of cyclic groups of prime power order is it isomorphic to?

Solution:

We have that

$$\begin{bmatrix} 1 & a & -a & b \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c & -c & d \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+c & -a-c & b+d \\ 0 & 1 & 0 & b+d \\ 0 & 0 & 1 & b+d \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and that

$$\begin{bmatrix} 1 & a & -a & b \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a & a & -b \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & -b \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

So this is indeed a group.

We see that

$$\mathbb{Z}_p \times \mathbb{Z}_p \ni (a, b) \mapsto \begin{bmatrix} 1 & a & -a & b \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \in G$$

is a surjective group homomorphism. The kernel is trivial, so it is an isomorphism.