Math 417 Review Sheet: Examples of Groups

This is a list of some of the examples of groups we have seen in this course, together with some basic facts about them. Any specific groups appearing on the exam are likely to be either on this list or similar to a group on this list.

1. Dihedral groups (symmetries of polygons)

The symmetry group of a regular n-gon is the dihedral group D_n. It has $2n$ elements: n rotations and n flips. We usually assume that the polygon is drawn in the plane, centered at the origin, and has a vertex on the positive x-axis. Let $r = r_{2\pi/n}$ be the rotation counterclockwise by $2\pi/n$ radians, and let j be the flip accross the x-axis. Then the group D_n has elements

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, j, rj, r^2j, \ldots, r^{n-1}j\}.$$

When written this way, the relations $r^n = e$, $j^2 = e$, and $jr = r^{-1}j$ suffice to compute the product of any two elements.

2. Symmetric groups (permutations)

Let X be a set. Define

$$\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ is a bijective function}\}.$$

Then $\mathrm{Sym}(X)$ is a group under composition of functions. Elements of $\mathrm{Sym}(X)$ are called permutations of X. In the case where $X = \{1, 2, \ldots, n\}$, we write $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$. This group is not abelian if $n \geq 3$.

If $a_1, a_2, \ldots, a_k$ is a finite sequence of pairwise disjoint elements of X, then the notation $\sigma = (a_1 a_2 \ldots a_k)$ refers to the permutation of X such that:

(1) for $1 \leq i \leq k-1$, $\sigma(a_i) = a_{i+1}$;
(2) $\sigma(a_k) = a_1$;
(3) $\sigma(x) = x$ if x does not appear in the list $a_1, a_2, \ldots, a_k$.

Such a permutation is called a k-cycle. When X is finite, any permutation may be written as a product of disjoint cycles (in an essentially unique way).

A 2-cycle $(a_1 a_2)$ is called a transposition. When X is finite, any permutation may be written as a product of transpositions, but this representation is not unique.

There is a homomorphism $\epsilon : S_n \to \{1, -1\}$. It can be defined as $\epsilon = \det \circ T$, where $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ is the determinant homorphism, and $T : S_n \to \mathrm{GL}(n, \mathbb{R})$ is the homomorphism that sends a permutation to the corresponding permutation matrix. This homomorphism has the property that, for any transposition τ, $\epsilon(\tau) = -1$. It follows that, for any permutation σ, we have $\epsilon(\sigma) = 1$ if and only if σ can be written as a product of an even number of transpositions, and $\epsilon(\sigma) = -1$ if and only if σ can be written as a product of an odd number of transpositions.

3. Additive groups of number systems

Consider the number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ (integers, rationals, reals, complex numbers, and integers modulo n). Each of these number systems has a notion of addition. In each case, addition makes the set into an abelian group.

When we are dealing with such examples of groups, we use a notation that is different from the abstract notation for groups. When dealing with abstract groups, we write the group operation as if it were multiplication: if $a, b \in G$, then the result of applying the group operation to a and b is denoted ab; also, the inverse of a is denoted a^{-1}. But when dealing with groups where the group operation is "really" some kind of addition, we write $a + b$ for the operation. Also, the identity element is denoted

by 0 or [0], and the inverse of a is denoted by $-a$. Furthermore, if H is a subset of such an "additive" group, then the cosets of H are denoted by $a+H$ (instead of aH as in the abstract setting).

4. Multiplicative groups of number systems

Consider again the number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$. Each of these sets has a notion of multiplication, which is commutative, associative, and has an identity element 1. However, not every element has a multiplicative inverse that lies in the same set. Nevertheless, if we remove the elements that do not have multiplicative inverses, we obtain an abelian group:

(1) The set of integers whose multiplicative inverse is also an integer is $\{1,-1\}$, so this is an abelian group under multiplication.
(2) A rational, real, or complex number is multiplicatively invertible if and only if it is not zero. So $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$, and $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$ are all abelian groups under multiplication.
(3) An element $[a]\in\mathbb{Z}_n$ is multiplicatively invertible if and only if $\gcd(a,n)=1$. Note that if $n=p$ is a prime number then $\gcd(a,p)=1$ if and only if $[a]\neq[0]$. Thus:
   (a) $\mathbb{Z}_n^* = \{[a]\in\mathbb{Z}_n \mid \gcd(a,n)=1\}$ is an abelian group under multiplication.
   (b) When p is prime, $\mathbb{Z}_p^* = \mathbb{Z}_p\setminus[0]$ is an abelian group under multiplication.

Other notable subgroups of the above groups include $\mathbb{R}_+$, the group of positive real numbers under multiplication, and the group of unit complex numbers

$$U = \{a+bi \mid a^2+b^2=1\} = \{e^{i\theta} \mid \theta\in\mathbb{R}\}.$$

Geometrically, U is a circle of radius 1 in the complex plane.

5. Matrix groups

Consider the set of $n\times n$ matrices with entries in some number system, which we can take to be $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ or $\mathbb{Z}_n$. Matrix multiplication is an associative operation, and it has an identity element, which is the identity matrix (1 on the diagonal and 0 off the diagonal). However, not every matrix is invertible. The general fact is that a matrix (with entries in some number system) is invertible if and only if its determinant is invertible (in that number system). This gives us the following examples

(1) $\mathrm{GL}(n,\mathbb{Q})$ is the group of $n\times n$ matrices with rational entries and nonzero determinant.
(2) $\mathrm{GL}(n,\mathbb{R})$ is the group of $n\times n$ matrices with real entries and nonzero determinant.
(3) $\mathrm{GL}(n,\mathbb{C})$ is the group of $n\times n$ matrices with complex entries and nonzero determinant.
(4) $\mathrm{GL}(n,\mathbb{Z})$ is the group of $n\times n$ matrices with integer entries whose determinant is 1 or -1. (If the determinant is nonzero, but not ±1, then the determinant of the inverse matrix will be a fraction, and so it cannot have integer entries.)
(5) When p is prime, $\mathrm{GL}(n,\mathbb{Z}_p)$ is the group of $n\times n$ matrices with $\mathbb{Z}_p$ entries, whose determinant is not $[0]\in\mathbb{Z}_p$.

We can also consider the subgroup of matrices whose determinant is equal to 1.

(1) $\mathrm{SL}(n,\mathbb{Q})$ is the group of $n\times n$ matrices with rational entries and determinant equal to 1.
(2) $\mathrm{SL}(n,\mathbb{R})$ is the group of $n\times n$ matrices with real entries and determinant equal to 1.
(3) $\mathrm{SL}(n,\mathbb{C})$ is the group of $n\times n$ matrices with complex entries and determinant equal to 1.
(4) $\mathrm{SL}(n,\mathbb{Z})$ is the group of $n\times n$ matrices with integer entries and determinant equal to 1.
(5) When p is prime, $\mathrm{SL}(n,\mathbb{Z}_p)$ is the group of $n\times n$ matrices with $\mathbb{Z}_p$ entries and determinant equal to [1].

We can also obtain subgroups by restricting the "shape" of the matrix. A matrix is called *upper triangluar* if all entries below the diagonal are zero. For instance, a 3×3 upper triangular matrix looks

like

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}$$

A *lower triangular* matrix has all zeros above the diagonal. A *diagonal* matrix is one which is both upper and lower triangular, that is, it only has nonzero entries along the main diagonal.

Proposition 1. *The set of upper triangular $n \times n$ matrices is closed under multiplication. So are the sets of lower triangular matrices and of diagonal matrices. Moreover, if such a matrix is invertible, its inverse has the same shape.*

Proposition 2. *Let $A = (a_{ij})$ be an $n \times n$ matrix that is either upper triangular, lower triangular, or diagonal. Then the determinant of A is equal to the product of the entries on the main diagonal:*

$$\det(A) = \prod_{i=1}^{n} a_{ii}.$$

For example, the set

$$\left\{ \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} \mid a, b, c, d, e, f \in \mathbb{R}, a \neq 0, d \neq 0, f \neq 0 \right\}$$

is a group under matrix multiplication; it is a subgroup of $\mathrm{GL}(3, \mathbb{R})$.

6. Direct products and vectors

We can build many more groups by taking direct products of the groups listed in the previous sections. Recall that if A and B are groups, then $A \times B$ is the group whose elements are ordered pairs (a, b) with $a \in A$ and $b \in B$, and with the binary operation

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

A related construction is the following. Let A be a group, and let $n \geq 1$ be an integer. Then we can consider the set A^n of all n-tuples whose coordinates are elements of A:

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A \text{ for all } i\}.$$

This set is also a group under coordinate-wise operations:

$$(a_1, a_2, \ldots, a_n)(a_1', a_2', \ldots, a_n') = (a_1 a_1', a_2 a_2', \ldots, a_n a_n')$$

The most commonly encountered instance of this construction is when A is the additive group of a number system. So let $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_k$, with addition as the group operation. Then we write the coordinate-wise operation additively:

$$(a_1, a_2, \ldots, a_n) + (a_1', a_2', \ldots, a_n') = (a_1 + a_1', a_2 + a_2', \ldots, a_n + a_n').$$

In other words, the groups $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$, and $\mathbb{Z}_k^n$ are the groups of *n-dimensional vectors* with entries in each number system. In particular, $\mathbb{R}^n$ and $\mathbb{C}^n$ are the standard vector spaces of traditional linear algebra, regarded as abelian groups with respect to addition.