SUMMER TERM ABSTRACT ALGEBRA
HANDOUT II: COSETS AND LAGRANGE'S THEOREM

SAMIR SIKSEK

1. Orientation

You're meant to tackle Handout II in Weeks 3 and 4. If you were ill/busy and missed out on Handout I don't worry: Handout II is independent of Handout I. Just crack on with Handout II. You can look forward to Handout I as a delicious treat to devour at some point during the summer. Still, you should read the advice on self-study under "What's this?" in Handout I.

Handout II revises cosets, and Lagrange's theorem, and explores some of the links with linear algebra. Just as with true love, the path to mathematical erudition never runs smooth. You need to keep going backwards and forwards between topics. You can't know abstract algebra properly until you know linear algebra and vice versa. And you need to do computations; with computations you acquire confidence and wisdom. As I said this before in Handout I, if you get stuck on something move on and come back later; hindsight is potent in maths just as it is in life.

2. Advice on writing out solutions

This term you are trying to cope without a supervisor. I think this can be a positive experience and help make you a better mathematician. Here is some advice on how that can be achieved.

- You should take the exercises seriously and write out full solutions to the best of your ability.
- Write in full sentences and avoid excessive notation. What you write should resemble how mathematics is written in textbooks (or for example in these handouts). The way your supervisor/tutor/lecturer writes on the blackboard is probably not a good model—blackboard style aims at quick and informal communication of ideas with many of the details said but not written.
- The level at which you write is important. Try imaginging that you are writing for a fellow first year student who will have to understand what you've written without second-guessing your mind.
- Be honest about gaps in your arguments. If there is a gap, just write down an explanation of what it is. For once, the objective is to learn and gain understanding, not to maximize marks.

Date: April 28, 2020.

- Come back to your answers after a couple of days and see if they still make sense, or if you can improve them.

I personally never write maths on bits of paper. Everything is Latexed so it can be edited and improved. If I change my mind about the ordering of an argument I can rearrange things by copying and pasting. I advise you to consider Latexing your answers. Yes it will slow you down at the beginning, but only at the beginning.

3. Past Exam Question

Here is a question from the 2015 Introduction to Abstract Algebra paper. As revision, we're going to work our way through this question. We're going to write far more than is necessary, and get distracted by some instructive examples. However, it might help you to have a go at the question first before reading on, and see how much you remember.

Question. Let G be a finite group and H a subgroup.

(i) Let $g \in G$. Define the *left coset* gH, and show that $\#H = \#gH$.
(ii) Show that any two left cosets of H in G are either disjoint or equal.
(iii) Define the *index* $[G : H]$ and show that $\#G = [G : H] \cdot \#H$.

Let $\mathbb{S} = \{\alpha \in \mathbb{C}^* \ : \ |\alpha| = 1\}$.

(iv) Show that $\mathbb{S}$ is a subgroup of $\mathbb{C}^*$.
(v) Show that $[\mathbb{C}^* : \mathbb{S}] = \infty$.

4. Subgroups

Recall the following definition.

Definition. Let $(G, \circ)$ be a group. A **subgroup** H is a subset of G such that H (or strictly speaking $(H, \circ)$) is a group with the same binary operation $\circ$.

Example 1. $\mathbb{R}^*$ is a subset of $\mathbb{R}$, both are groups, but $\mathbb{R}^*$ is **not** a subgroup of $\mathbb{R}$. When we talk about the group $\mathbb{R}$ we really mean the group $(\mathbb{R}, +)$. When we talk about the group $\mathbb{R}^*$ we really mean the group $(\mathbb{R}^*, \cdot)$. The binary operations are different.

Example 2. $\mathbb{Z}$ is a subgroup of $\mathbb{R}$. Strictly speaking we should say $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$. But only amateurs do that. Usually the intended binary operation is clear.

To check that H is a subgroup of the group G we normally use the following theorem.

Theorem 3. *Let G be a group and H a subset of G. The subset H is a subgroup if and only if*

(i) $1 \in H$;
(ii) $ab \in H$ *for all* $a, b \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

In this theorem we're using multiplicative notation for the group G. When we write $1 \in H$ in (i) what are we really saying? Here 1 is the identity element of G, and one of the things we need for H to be a subgroup of G is for that identity element to also belong to H. Then G and its subgroup H share the same identity element. What does (ii) mean? It means that if take two elements a, b of H and *compose them using the binary operation on* G we obtain an element of H. What does (iii) mean?

Exercise 1. Let $\mathbb{S} = \{\alpha \in \mathbb{C}^* \ : \ |\alpha| = 1\}$. Sketch $\mathbb{S}$ and show that it's a subgroup of $\mathbb{C}^*$.

Exercise 2. Let

$$A = \{\alpha \in \mathbb{C}^* \ : \ \frac{1}{2} < |\alpha| < 2\}.$$

Sketch A. Is A a subgroup of $\mathbb{C}^*$?

Exercise 3. Let K be a field and $n \geq 2$. Write $M_n(K)$ for the set of all $n \times n$ matrices with entries in K (in your Linear Algebra notes this set is denoted by $K^{n,n}$). Let

$$\mathrm{GL}_n(K) = \{A \in M_n(K) \ : \ \det(A) \neq 0\}$$

and

$$\mathrm{SL}_n(K) = \{A \in M_n(K) \ : \ \det(A) = 1\}.$$

Show that $\mathrm{GL}_n(K)$ is a group and $\mathrm{SL}_n(K)$ is a subgroup of $\mathrm{GL}_n(K)$. Here are some points to bear in mind.

- You can assume the standard properties of matrices and determinants that you know from Linear Algebra or school maths.
- **You** need to decide on the binary operation that is intended here. I am treating you as an adult, and expect you to work it out yourself. Is it addition, subtraction, multiplication, division or something exotic? Of course if had some exotic operation in mind I would have told you what it is. I don't like exotic things myself. The whole point of abstract algebra is to attain a better understanding of the operations (addition, multiplication, ...) and objects (numbers, matrices, functions, polynomials, ...) that we already know and love.
- One thing you should decide on pretty early is whether $\mathrm{GL}_n(K)$ is a subgroup of $M_n(K)$.

You will recall that Theorem 3 is written a little differently when G is an additive group.

Theorem 4. *Let* G *be an additive group and* H *a subset of* G. *The subset* H *is a subgroup if and only if*

(a) $0 \in H$;
(b) $a + b \in H$ *for all* a, $b \in H$;

(c) $-a \in H$ *for all* $a \in H$.

Exercise 4. Which of the following subsets of $\mathbb{R}^2$ are subgroups? You probably **don't** want to write out full details here—that'll take forever!

(i) $\{\mathbf{0}\}$.
(ii) $\mathbb{R}^2$.
(iii) $\mathbb{Z}^2$.
(iv) $\mathbb{Q}^2$.
(v) Straight line passing through the origin.
(vi) Straight line not passing through the origin.
(vii) $\{(a, a) \ : \ a \in \mathbb{R}, \ a \geq 0\}$ (draw picture).
(viii) $\{(a, a) \ : \ a \in \mathbb{R}\} \cup \{(a, -a) \ : \ a \in \mathbb{R}\}$ (draw picture).
(ix) $\{(x, y) \in \mathbb{R}^2 \ : \ x + y \in \mathbb{Q}\}$.

5. Vector spaces are additive abelian groups

Let K be a field and let V be a K-vector space. Then V is also an additive abelian group. How do we know this? We have two operations defined on V, addition and scalar multiplication (i.e. multiplication by elements of K), and these satisfy a bunch of properties listed under the definition of vector spaces in your Linear Algebra notes (page 14). From that bunch of properties we notice that A1–A4 tell us that V is an additive abelian group.

Let's now recall the defintion of a subspace (page 23 of your Linear Algebra notes).

Definition. A subspace W of V is a non-empty subset $W \subseteq V$ such that

(i) $\mathbf{u} + \mathbf{v} \in W$ for all $\mathbf{u}$, $\mathbf{v} \in W$;
(ii) $\alpha \mathbf{u} \in W$ for all $\alpha \in K$ and $\mathbf{u} \in W$.

We can summarise by saying that a subspace is a non-empty subset that is closed under addition and scalar multiplication.

Lemma 5. *Let W be a subspace of the K-vector space V. Then W is a subgroup of V.*

Proof. You should have a go at the proof yourself before reading on. In Theorem 4 we take $G = V$, $H = W$ and we would like to check that W satisfies conditions (a), (b), (c) of Theorem 4. Condition (b) is the same as (i), so we have it for free. What about condition (c)? Let $\mathbf{u} \in W$. We want to show that $-\mathbf{u} \in W$. So we take $\alpha = -1 \in K$, and invoke (ii). Therefore (c) holds.

Finally we need to check (a). We're given that W is non-empty. So take any $\mathbf{u} \in W$. Then $-\mathbf{u} = (-1)\mathbf{u} \in W$ by (ii), and $\mathbf{0} = \mathbf{u} + (-\mathbf{u}) \in W$ by (i). Hence (a) is also satisfied. Therefore W is a subgroup of V. □

Exercise 5. As you know, $\mathbb{R}^2$ is an $\mathbb{R}$-vector space. Which of the subsets in Exercise 4 are subspaces of $\mathbb{R}^2$? Again you probably **don't** want to write

down all the details as it'll take too long. One of your conclusions should be that whilst every subspace is a subgroup, not every subgroup is a subspace. There are more subgroups than there are subspaces.

Example 6. Groups are much more complicated than vector spaces. If I take $\mathbb{R}^2$ and think of it as an $\mathbb{R}$-vector space, I can give a complete description of its subspaces. If I think of $\mathbb{R}^2$ as a group I don't know how to give a complete description of its subgroups.

Let's give a complete a description of the subspaces of $\mathbb{R}^2$. The dimension of $\mathbb{R}^2$ is 2. Therefore any subspace will have dimension at most 2. So if W is a subspace then $\dim(W) = 0, 1, 2$. If $\dim(W) = 0$ then $W = \{0\}$ is the zero subspace. If $\dim(W) = 2$ then $W = \mathbb{R}^2$. What if $\dim(W) = 1$? Then W has an $\mathbb{R}$-basis consisting of one vector $\mathbf{w}$. This vector is non-zero, as $\{\mathbf{w}\}$ is linearly indendent. Since $\mathbf{w}$ is an $\mathbb{R}$-basis, we have

$$W = \{\alpha\mathbf{w} \ : \ \alpha \in \mathbb{R}\}.$$

We see that 1-dimensional subspaces of $\mathbb{R}^2$ are precisely the straight lines passing through the origin.

Exercise 6. Give a complete description of the subspaces of $\mathbb{R}^3$. Give five examples of subgroups of $\mathbb{R}^3$ than aren't subspaces.

6. Cosets

Let G be a group and H a subgroup. Let g be an element of G. We call the set

$$gH = \{gh \ : \ h \in H\}$$

a **left coset** of H in G. Here of course, we're using multiplicative notation. If G is an additive group then a coset of H in G has the form

$$g + H = \{g + h \ : \ h \in H\}.$$

We write $[G : H]$ for the number of distinct left cosets of H in G and call it the index of H in G.

Example 7. $\mathbb{Z}$ is a subgroup of $\mathbb{R}$. Note that

$$\cdots = -1.9 + \mathbb{Z} = -0.9 + \mathbb{Z} = 0.1 + \mathbb{Z} = 1.1 + \mathbb{Z} = 2.1 + \mathbb{Z} = \cdots .$$

But

$$0.1 + \mathbb{Z} \neq 0.2 + \mathbb{Z}.$$

A very very important fact about cosets is the following:

$$g_1 + H = g_2 + H \implies g_1 = g_2$$

in the additive setting, and

$$g_1H = g_2H \implies g_1 = g_2$$

in the multiplicative setting.

Example 8. Let's go back to the exam question and show $[\mathbb{C}^* : \mathbb{S}] = \infty$. We did this before in lectures, and it's also in the lecture notes. But I want to go through it again. A coset of $\mathbb{S}$ in $\mathbb{C}^*$ has the form $\alpha\mathbb{S}$ where α is in $\mathbb{C}^*$ (i.e. α is a non-zero complex number). As such, we can write $\alpha = re^{i\theta}$, where r is positive (it is the absolute value of α), and θ is the argument of α. Consider $e^{i\theta}\mathbb{S}$. Multiplying any complex number by $e^{i\theta}$ simply rotates anticlockwise through angle θ about the origin. So $e^{i\theta}\mathbb{S} = \mathbb{S}$. Now $\alpha\mathbb{S} = r\mathbb{S}$. What does multiplying by r do? It scales the circle $\mathbb{S}$ by a factor of r. Two different positive real numbers $r_1 \neq r_2$ will give different cosets $r_1\mathbb{S} \neq r_2\mathbb{S}$, since the first has radius r_1 and the second has radius r_2. See Figure 1. So

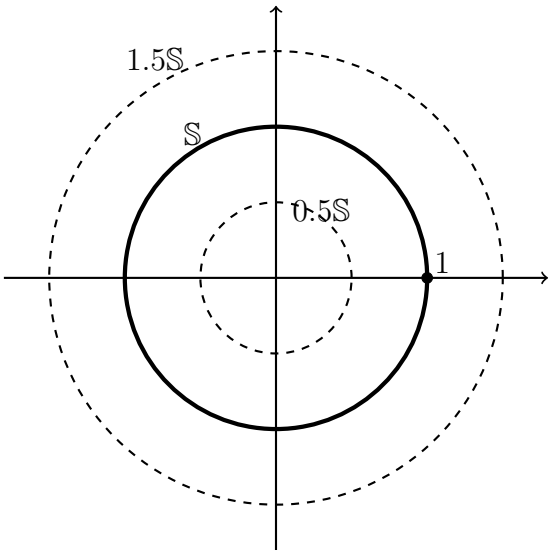

FIGURE 1. $\mathbb{S}$ and its cosets $0.5\mathbb{S}$ and $1.5\mathbb{S}$ in $\mathbb{C}^*$.

$\mathbb{S}$ has as many cosets in $\mathbb{C}^*$ as there are positive real numbers. In particular $[\mathbb{C}^* : \mathbb{S}] = \infty$.

Summary: $\mathbb{S}$ is the circle centred at the origin of radius 1, and its cosets in $\mathbb{C}^*$ are the circles centred at the origin (of positive radius).

7. Equivalence Relations and Equivalence Classes

We are going to prove Lagrange's Theorem in a slightly different way from MA136 lectures. Both proofs are instructive, and you should feel at home with both. The proof is going to make use of the concepts of equivalence relation and equivalence classes that you've met before in Foundations (pages 68–70) of your lecture notes. Recall the following defintion.

Definition. Let X be a set and let $\sim$ be a relation on X. We say that $\sim$ is an **equivalence relation** on X if the following three conditions are satisfied.

- **Reflexivity**: $x \sim x$ for all $x \in X$.
- **Symmetry**: for all x, $y \in X$, if $x \sim y$ then $y \sim x$.
- **Transitivity**: for all x, y, $z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.

Example 9.
- Equality is an equivalence relation whatever X is.
- Let $m \geq 2$. Congruence modulo m is an equivalence relation on $\mathbb{Z}$.
- $\leq$ is not an equivalnce relation on $\mathbb{R}$; it is reflexive and transitive but not symmetric.
- Let A be a set and $\mathcal{P}(A)$ its powerset. Then $\subseteq$ is not an equivalence relation on $\mathcal{P}(A)$; again it is reflexive and transitive without being symmetric.
- $<$ is neither reflexive nor symmetric on $\mathbb{R}$, and so is certainly not an equivalence relation.

Definition. Let $\sim$ be an equivalence relation on X and let $x \in X$. The **equivalence class of** x is the set

$$[x] = \{y \in X \ : \ y \sim x\}. \tag{1}$$

Example 10. Take the equivalence relation $=$ on X. The equivalence class of $x \in X$ is

$$[x] = \{y \in X \ : \ y = x\} = \{x\}.$$

Thus the set of equivalence classes here is the set of singletons.

Example 11. Let $m \geq 2$, and consider congruence modulo m on $\mathbb{Z}$. The equivalence class of $a \in \mathbb{Z}$ is

$$[a] = \{b \in \mathbb{Z} \ : \ b \equiv a \pmod{m}\} = \{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}.$$

In Introduction to Abstract Algebra we denote $[a]$ by $\overline{a}$. The set of equivalence classes is $\mathbb{Z}/m\mathbb{Z}$.

Exercise 7. Let $\sim$ be the relation on $\mathbb{R}^2$ given by

$$(r, s) \sim (u, v) \iff r - s - u + v \in \mathbb{Z}.$$

Show that $\sim$ is an equivalence relation on $\mathbb{R}^2$. Sketch the equivalence class $[(0, 0)]$.

Lemma 12. *Let $\sim$ be an equivalence relation on X. Let x, $y \in X$. Suppose that $y \in [x]$. Then $[x] = [y]$.*

Proof. Note $y \in [x]$ simply tells us that $y \sim x$ by definition of the equivalence class $[x]$ in (1). We want to show that $[x] = [y]$. This means that every element of $[x]$ belongs to $[y]$ and vice versa.

Suppose $z \in [x]$. Thus $z \sim x$. We know that $y \sim x$ so $x \sim y$ by symmetry. Now we have $z \sim x$ and $x \sim y$. By transitivity, $z \sim y$. Hence $z \in [y]$.

Your turn! Suppose $z \in [y]$ and show that $z \in [x]$. Once you've done that the proof would be complete. $\square$

Definition. Let X be a set and let $\mathcal{A}$ be a collection of subsets of X. We say that $\mathcal{A}$ is a **partition of** X if and only if the following three conditions are satisfied.

(I) $A \neq \emptyset$ for every $A \in \mathcal{A}$.
(II) If A, $B \in \mathcal{A}$ and $A \neq B$ then $A \cap B = \emptyset$.
(III) $\displaystyle\bigcup_{A \in \mathcal{A}} A = X$.

Example 13. Let $X = \{1, 2, 3, 4\}$.

- $\mathcal{A} = \{\{1, 2\}, \{2, 3\}, \{4\}\}$ is not a partition of X since $A = \{1, 2\}$ and $B = \{2, 3\}$ belong to $\mathcal{A}$ and violate condition (II).
- $\mathcal{B} = \{\{1, 2\}, \{4\}\}$ is not a partition of X, since
$$\bigcup_{B \in \mathcal{B}} = \{1, 2\} \cup \{4\} = \{1, 2, 4\} \neq X,$$
violating condition (III).
- $\mathcal{C} = \{\{1\}, \{2, 3, 4\}, \emptyset\}$ is not a partition of X as one of the elements is empty violating condition (I).
- $\mathcal{D} = \{\{1\}, \{2, 3, 4\}\}$ is a partition of X, and so is $\mathcal{E} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$ and so is $\mathcal{F} = \{\{1, 2, 3, 4\}\}$.

Example 14. $\{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$ is a partition of $\mathbb{Z}$, since every integer is either even or odd but can't be both.

Example 15. Let $n \geq 2$. Recall that we refer to a permutation $\sigma \in S_n$ as **even** if it is a product of an even number of transpositions, and **odd** if it is a product of an odd number of transpositions. One of the key theorems of MA136 says that every permutation is either odd, or even but not both. This is Theorem XIV.40 of your MA136 lecture notes. We wrote A_n for the subset of even permutations in S_n and discovered that it is a subgroup. Let's write $A'_n = S_n \setminus A_n$ for the set of odd permutations (warning: this is non-standard notation). Then $\{A_n, A'_n\}$ is a partitition of S_n.

Aside. If X is a finite set of size n then the number of partitions of X is denoted by B_n and called the **n-th Bell number**. You might be interested in the Wikipedia page on Bell numbers. Here's an interesting random fact:

$$B_n = \frac{n!}{2\pi i e} \int_\gamma \frac{e^{e^z}}{z^{n+1}} dz$$

where γ is any closed simple anticlockwise path going around the origin in the complex plane. The proof of this requires Cauchy's integral formula which is one of the most beautiful and powerful tools in all of mathematics. You learn Cauchy's integral formula and how to wield it if you choose to do the 3rd year Complex Analysis module. It's a bit early to be giving you advice about third year modules, but I'll do it anyway as I probably won't get

another chance. You should choose the ones you enjoy, but my own personal favourites are Galois Theory, Algebraic Number Theory, Algebraic Topology, Complex Analysis, Groups & Representations, Functional Analysis. My least favourite is Rings & Modules. Avoid that one like the plague.

Theorem 16. *Let $\sim$ be an equivalence relation on X. Then the set of equivalence classes*

$$\{[x] \ : \ x \in X\}$$

is a partition of X.

Proof. Note that every element of the set $\{[x] \ : \ x \in X\}$ has the form $[x]$ and so is a subset of X. We'll show that conditions (I), (II), (III) of the proposition are satisfied. By reflexivity $x \sim x$ for all x. Thus $x \in [x]$ from the definition of the equivalence class $[x]$ in (1). Hence (I) is satisfied. Moreover, the union of all the classes will contain all the elements of X, and so (III) is satisfied.

Let's prove (II). So suppose x, y are elements of X such that $[x] \neq [y]$. We want to show that $[x] \cap [y] = \emptyset$. We do this by contradiction. Suppose $z \in [x] \cap [y]$. Then $z \in [x]$ and $z \in [y]$. Lemma 12 tells us that $[x] = [z]$ and $[y] = [z]$. Thus $[x] = [y]$, giving a contradiction and completing the proof. □

8. Cosets are Equivalence Classes

Exercise 8. Let G be a group and H a subgroup. We define a relation $\sim$ on G by the following rule:

$$g_1 \sim g_2 \quad \iff \quad g_1^{-1} g_2 \in H.$$

(i) Show that $\sim$ is an equivalence relation.
(ii) Let $g \in G$. Show that $[g] = gH$ where $[g]$ is the equivalnce class of g.
(iii) Deduce that the set of cosets $\{gH \ : \ g \in G\}$ is a partition of G.

Example 17. Let $m \geq 2$. The cosets of $m\mathbb{Z}$ in $\mathbb{Z}$ are congruence classes $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. The of congruence classes $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ forms a partition of $\mathbb{Z}$.

Example 18. Recall what we said earlier about the cosets of $\mathbb{S}$ in $\mathbb{C}^*$, "$\mathbb{S}$ is the circle centred at the origin of radius 1, and its cosets in $\mathbb{C}^*$ are the circles centred at the origin (of positive radius)". It should be clear that the cosets of $\mathbb{S}$ form a partition of $\mathbb{C}^*$.

Example 19. Let L be a line in $\mathbb{R}^2$ passing through the origin and parallel to a non-zero vector $\mathbf{v}$. At school you probably wrote the equation of the line like this:

$$L \ : \ \mathbf{x} = \lambda \mathbf{v}.$$

Here λ is the parameter. In set notation we can specify the same line by writing

$$L = \{\lambda \mathbf{v} \ : \ \lambda \in \mathbb{R}\}.$$

This is a 1-dimensional subspace of $\mathbb{R}^2$ with basis $\mathbf{v}$. It's also a subgroup of $\mathbb{R}^2$ (recall that every vector space is an additive group and every subspace is a subgroup). Now let $\mathbf{u} \in \mathbb{R}^2$. Let

$$L_{\mathbf{u}} \ : \ \mathbf{x} = \mathbf{u} + \lambda \mathbf{v}.$$

This is the line passing through $\mathbf{u}$ and parallel to $\mathbf{v}$. It is therefore a line parallel to L. In set notation,

$$L_{\mathbf{u}} = \{\mathbf{u} + \lambda \mathbf{v} \ : \ \lambda \in \mathbb{R}\}.$$

Thus $L_{\mathbf{u}} = \mathbf{u} + L$. See Figure 2

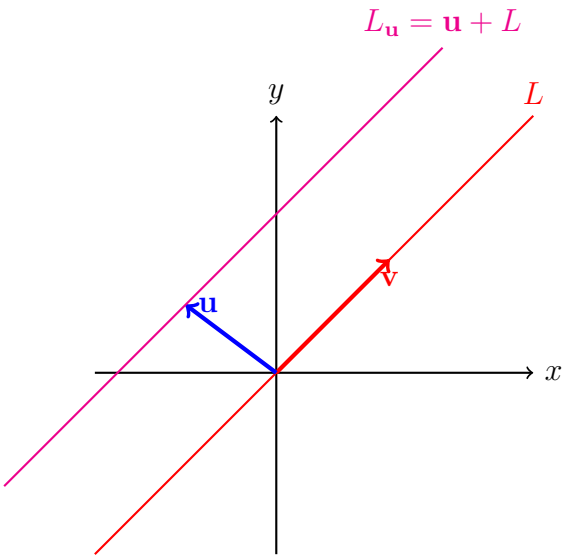

FIGURE 2. A line L defines a subgroup of $\mathbb{R}^2$ if and only if it passes through the origin. In that case, its cosets are the lines parallel to it. Also adding red to blue gives you magenta.

We see that the cosets of the line L in $\mathbb{R}^2$ are the lines parallel to L. It should be geometrically clear that these lines form a partition of $\mathbb{R}^2$.

9. Lagrange's Theorem

Before we prove Lagrange's theorem we need a fact which you have seen before in Introduction to Abstract Algebra.

Exercise 9. Let G be a group and H a finite subgroup. Let $g \in G$. Show that

$$\#gH = \#H. \tag{2}$$

Don't look up the proof. Try to do it yourself first. I'll remind you that the proof starts by enunciating a profound philosophical precept of tremendous utilitarian import,

> "The best way to show that two sets have the same number of elements is to set up a bijection between them".

Let

$$\phi \ : \ H \to gH, \qquad \phi(h) = gh.$$

Prove (2) by showing that ϕ is a bijection.

Theorem 20 (Lagrange's Theorem)**.** *Let G be a finite group and H a subgroup. Then*

$$\#G = [G : H] \cdot \#H.$$

Proof. Let $g_1H, \ldots, g_rH$ be the **distinct** cosets of H in G. Here $r = [G : H]$ is the index. These cosets form a partition of G (see Exercise 8 if you've already forgotten). In particular, they are pairwise disjoint and their union is G. Hence

$$\begin{aligned} \#G &= \#g_1H + \#g_2H + \cdots + \#g_rH \\ &= r \cdot \#H \qquad \text{(by (2))} \\ &= [G : H] \cdot \#H. \end{aligned}$$

□

Exercise 10. Let $n \geq 1$. Write

$$U_n = \{z \in \mathbb{C} \ : \ z^n = 1\}$$

for the set of n-th roots of 1.

(i) Show that U_n is a subgroup of $\mathbb{C}^*$. What's $\#U_n$? What do the n-th roots of 1 sum to?

(ii) Let m, $n \geq 1$. Under what condition on the pair m, n would U_m be a subgroup of U_n. In that case, what would the index be?

(iii) Let $\alpha \in \mathbb{C}^*$. Let

$$W = \{w \in \mathbb{C} \ : \ w^n = \alpha\}$$

be the set of n-th roots of α. Show that W is a coset of U_n inside $\mathbb{C}^*$.

10. $\mathrm{GL}_2(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$ (Optional)

This section is a little tougher than the previous sections, so I'll leave it as optional. Recall that for any field K we defined

$$\mathrm{GL}_n(K) = \{A \in M_n(K) \ : \ \det(A) \neq 0\}$$

and

$$\mathrm{SL}_n(K) = \{A \in M_n(K) \ : \ \det(A) = 1\}.$$

We checked that $\mathrm{GL}_2(K)$ is a group and $\mathrm{SL}_n(K)$ is a subgroup. Of course if K is infinite (e.g. $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) then so these two matrix groups are infinite

too. But if K is finite then they are finite. In fact they fit inside $M_n(K)$ which has to be finite itself.

Exercise 11. Let $\mathbb{F}_q$ be the field with q elements. Show that $\#M_n(\mathbb{F}_q) = q^{n^2}$. **Hint:** how many entries does an $n \times n$ matrix have, and how many possibilities are there for each entry?

Exercise 12. For $\alpha \in \mathbb{F}_q^*$ let

$$\mathcal{D}_\alpha = \{A \in \mathrm{GL}_n(\mathbb{F}_q) \ : \ \det(A) = \alpha\}.$$

(i) Show that $\{\mathcal{D}_\alpha \ : \ \alpha \in \mathbb{F}_q^*\}$ is a partition of $\mathrm{GL}_n(\mathbb{F}_q)$.
(ii) Show that $\mathcal{D}_\alpha$ is a coset of $\mathrm{SL}_n(\mathbb{F}_q)$, and also that every coset of $\mathrm{SL}_n(\mathbb{F}_q)$ is of this form.
(iii) Deduce that

$$[\mathrm{GL}_n(\mathbb{F}_q) \ : \ \mathrm{SL}_n(\mathbb{F}_q)] \ = \ q - 1.$$

To work out the order of $\mathrm{SL}_n(\mathbb{F}_q)$ it's enough to work out the order of $\mathrm{GL}_n(\mathbb{F}_q)$. To work out the latter order, we need to do some linear algebra.

Exercise 13. Let V be an $\mathbb{F}_q$-vector space. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ be a linearly independent subset of V. Show that the span of $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ has q^r elements. **Hint.** At first sight this looks easy. The elements of the span have the form

$$\alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_r \mathbf{v}_r,$$

with $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{F}_q$. There are q possibilities for α_1, q possibilities for α_2, and so on. But where do we use the linear independence hypothesis?

Exercise 14. Let V be a vector space, and let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be vectors in V. Show $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly independent if and only if the following simultaneously hold.

- $\mathbf{v}_1 \neq \mathbf{0}$;
- $\mathbf{v}_2$ is not a linear combination of $\{\mathbf{v}_1\}$;
- $\mathbf{v}_3$ is not a linear combination of $\{\mathbf{v}_1, \mathbf{v}_2\}$;

  $\vdots$

- $\mathbf{v}_n$ is not a linear combination of $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{n-1}\}$.

Exercise 15. Show that

$$\#\,\mathrm{GL}_n(\mathbb{F}_q) \ = \ (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Hint: a square matrix is non-singular (i.e. has non-zero determinant) if and only if its columns are linearly independent.