Geometry and topology

Teo Banica

Department of Mathematics, University of Cergy-Pontoise, F-95000 Cergy-Pontoise, France. teo.banica@gmail.com

2010 *Mathematics Subject Classification.* 53C05

Key words and phrases. Algebraic manifold, Smooth manifold

Abstract. This is an introduction to geometry and topology, manifolds at large, with all the needed preliminaries included, and some applications included as well. We first discuss the conics, following the ancient Greeks, and then Kepler and Newton, followed by some commutative algebra, and an introduction to modern algebraic geometry. Then we discuss topology, mostly by focusing on the knots. Finally, we discuss the foundations of differential geometry, and its relations with multivariable calculus, and basic questions in physics, and we end with an introduction to Riemannian manifolds.

Preface

You certainly know some calculus, and that is good scientific knowledge, allowing you to deal with geometric questions. That is, no matter what problem you want to investigate in $\mathbb{R}^N$, be that in mathematics, physics, chemistry, engineering and so on, your variables $x, y, z, \ldots$ will be subject to some constraints, and will not evolve linearly, but rather on curved paths. And, multivariable calculus will allow you to study them.

But, what is geometry itself? According to the above, this is the struggle of mankind with curvature, and with you being part of that struggle, on the mankind camp. However, this is a bit loose, and for being more formal, geometry is the study of the beasts $X \subset \mathbb{R}^N$, called "manifolds", where your variables $x, y, z, \ldots$ are allowed to move. And with this point of view, we can see now, more clearly, that geometry falls into two flavors:

(1) First we have the general study of the manifolds $X \subset \mathbb{R}^N$, meaning understanding their shape, curvature and so on, not to forget their precise definition too, done without any precise motivation in mind. Which is the realm of pure mathematics.

(2) And then we have analysis on these manifolds $X \subset \mathbb{R}^N$, for solving your various calculus questions, in relation with the precise problems from mathematics, physics, chemistry and so on, that you are interested in. Which is applied mathematics.

With this understood, let us turn now to the manifolds X. What exactly are these? And here, things are quite complicated, and endlessly ramify, because various branches of mathematics, physics, chemistry and so on can lead to different types of manifolds X to be investigated. Here is a brief picture of the landscape, and judge yourself:

– Manifolds can be algebraic, given by polynomial equations $P_i(x) = 0$, which actually do not guarantee their smoothness, and allow for singularities, or differential, given by local equations $\varphi_i(x) = 0$, chosen as to guarantee their smoothness. Both are important, and this splits things, into algebraic geometry and differential geometry.

– Manifolds can be taken rigid, as they come, and studied in a metric sense, or up to deformations. The point indeed is that manifolds up to deformation are simpler to study, and their overall shape, that we can try to understand, is preserved by these deformations. This leads to another split, between traditional geometry, and topology.

– Manifolds can be taken continuous, as the usual manifolds $X \subset \mathbb{R}^N$, $X \subset \mathbb{C}^N$ that you are used to, from your previous practice of physics and calculus, or discrete, arising either via discretization, say as $X \subset (\varepsilon\mathbb{Z})^N$ with $\varepsilon > 0$ small, or via arithmetic, $X \subset F^N$, with F being an arbitrary field. So, another split, between continuous and discrete.

At this point, I can hear you thinking that this is madness, because taking into account as well the original split, between manifolds and analysis on them, we have a total of $2^4 = 16$ interesting branches of geometry, to be studied. But much more is true. Manifolds can be affine of projective, you can do your work on them locally or globally, you might be interested in smoothness or singularities, and so on. Also, differential geometry, which is the main branch of geometry, falls into several classes, such as general, Riemannian, symplectic, and so on. And finally, if you are brave enough and interested in quantum mechanics, some geometries there, called "noncommutative", are waiting for you.

Problem now, how to learn all this? With patience, I guess. Modern mathematics is more or less the same thing as geometry, but this should be not a source of scare, because depending on the precise questions that you are interested in, some branches of geometry are certainly more useful than other, and you will end up learning all that you need.

The present book is an introduction to geometry, at large. We will explore a bit the various branches of geometry, according to our scheme above, and with the aim of avoiding difficulties, rather of getting into them. That is, we will take one by one the various possible definitions for the manifolds X, somehow according to the our $2^4 = 16$ scheme, and have some easy math work done on them, all beautiful and useful things. With the policy of changing our definition of X, whenever getting into troubles.

The book will be mostly mathematical, and this not because I personally do not like physics, quite the opposite, but because geometry is so wide, and so many things to be learned. That is, my opinion is that, before getting into complicated physics and applications, it is worth reading 400 pages of geometry, done mostly mathematically. However, I am writing this now, at the start of my work, and knowing a bit myself, I am pretty much sure that I will end up in talking physics too, at least a little bit.

Many thanks go to my colleagues, most of the geometry I know, I learned it from them, over the time. With special thanks to the physicists, who always seem to have a trick for assuming that X is $\mathbb{R}^N$ itself. Finally, many thanks go to my cats, and tigers and other felines. Sitting in the savannah, relaxing, and from time to time hunting for this or that beast, all easy preys, is the main principle behind this book.

Contents

Part I

Algebraic manifolds

Rising up, back on the street
Did my time, took my chances
Went the distance, now I'm back on my feet
Just a man and his will to survive

CHAPTER 1

Plane curves

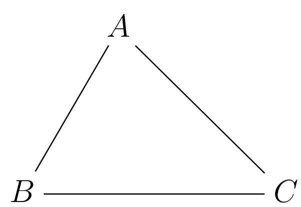
1a. Ellipses, conics

It all started with triangles. You probably know well triangle geometry from school, but always good to talk about this. Mainly I guess for myself, matter of checking if, after 30 plus years spent at the university, where the mathematics can be often highly abstract and conceptual, I still remember all that stuff. To start with, we have:

THEOREM 1.1. *Given a triangle ABC, the following happen:*

(1) *The angle bisectors cross, at a point called incenter.*
(2) *The medians cross, at a point called barycenter.*
(3) *The perpendicular bisectors cross, at a point called circumcenter.*
(4) *The altitudes cross, at a point called orthocenter.*

PROOF. Let us first draw our triangle, with this being always the first thing to be done in geometry, draw a picture, and then thinking and computations afterwards:



Allowing us the freedom to play with some tricks, as advanced mathematicians, both college students and professors, are allowed to, here is how the proof goes:

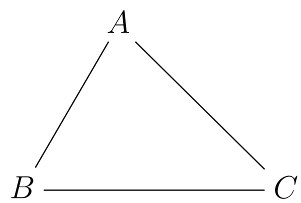
(1) Come with a small circle, inside ABC, and then inflate it, as to touch all 3 edges. The center of the circle will be then at equal distance from all 3 edges, so it will lie on all 3 angle bisectors. Thus, we have constructed the incenter, as required.

(2) This requires different techniques. Let us call $A, B, C \in \mathbb{C}$ the coordinates of A, B, C, and consider the average $P = (A + B + C)/3$. We have then:

$$P = \frac{1}{3} \cdot A + \frac{2}{3} \cdot \frac{B + C}{2}$$

Thus P lies on the median emanating from A, and a similar argument shows that P lies as well on the medians emanating from B, C. Thus, we have our barycenter.

(3) Time to draw a new triangle, for clarity, since we are now on page two:



Regarding our problem, we can use the same method as for (1). Indeed, come with a big circle, containing ABC, and then deflate it, as for it to pass through A, B, C. The center of the circle will be then at equal distance from all 3 vertices, so it will lie on all 3 perpendicular bisectors. Thus, we have constructed the circumcenter, as required.

(4) This is tougher, and I must admit that, when writing this book, I first struggled a bit with this, then ended looking it up on the internet. So, here is the trick. Draw a parallel to BC at A, and similarly, parallels to AB and AC at C and B. You will get in this way a bigger triangle, upside-down, $A'B'C'$. But then, the circumcenter of $A'B'C'$, that we know to exist from (3), will be the orthocenter of ABC, as desired. □

Along the same lines, but at a more advanced level now, we have:

Fact 1.2. *Besides the above 4 centers, many more remarkable points can be associated to a triangle ABC, and most of these lie on a line, called Euler line of ABC.*

And exercise for you of course to remember or figure out how all this works, both statement and proof. As bonus exercise, learn about the nine-point circle too.

Moving forward, all the above lies on paper, in fact originally on sand, where the ancients used to draw their math. So, what about looking up, towards the skies?

And here, things are quite fascinating. The first thing that you see is the Sun, seemingly moving around the Earth on a circle, but a more careful study reveals that this circle is rather a deformed circle, called ellipsis. As for the other stars and planets, these have all sort of weird trajectories, but a more careful study reveals that, with due attention to what the best "center" is, replacing our Earth, the trajectories are often ellipses:

(1) Indeed, this applies to all the planets in our Solar System, which move around the biggest object in the system, which is by far the Sun, on ellipses.

(2) The same trick applies to the trajectories of various distant stars, the rule being always the same, "small moves around big, on an ellipsis".

(3) However, there are counterexamples too, such as asteroids reaching our Solar system, but then travelling outwards, never to be seen again.

Summarizing, modulo some annoying asteroids that we will leave for later, we are led in this way to ellipses, and their mathematics. And good news, a full theory of ellipses is available, and this since the ancient Greeks, whose main findings were as follows:

THEOREM 1.3. *The ellipses, taken centered at the origin* 0, *and squarely oriented with respect to* Oxy, *can be defined in* 4 *possible ways, as follows:*

(1) *As the curves given by an equation as follows, with* $a, b > 0$*:*

$$\left(\frac{x}{a}\right)^2+\left(\frac{y}{b}\right)^2=1$$

(2) *Or given by an equation as follows, with* $q > 0$, $p = -q$, *and* $l \in (0, 2q)$*:*

$$d(z,p)+d(z,q)=l$$

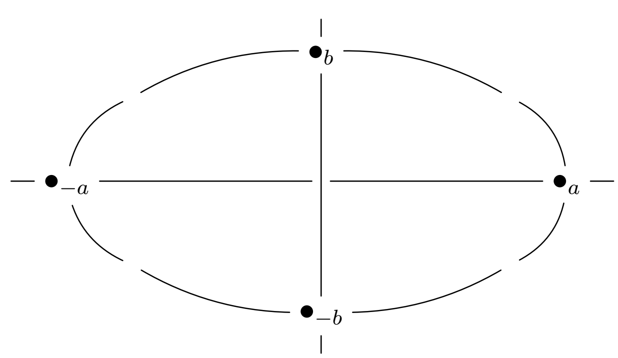
(3) *As the curves appearing when drawing a circle, from various perspectives:*

$$\bigcirc \quad \to \quad ?$$

(4) *As the closed non-degenerate curves appearing by cutting a cone with a plane.*

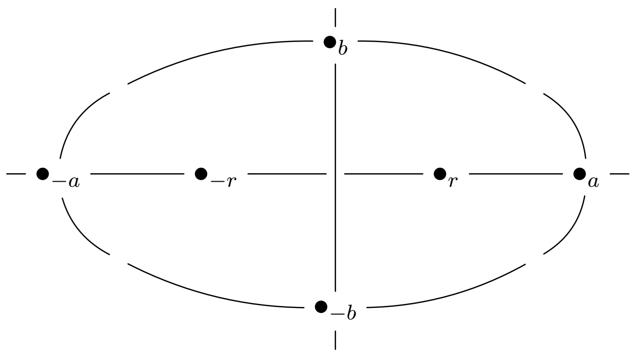
PROOF. This might look a bit confusing, and you might say, what exactly is to be proved here. Good point, and in answer, what is to be proved is that the above constructions (1-4) give rise to the same class of curves. And this can be done as follows:

(1) To start with, let us draw a picture from what comes out of (1), which will be our main definition for the ellipses, in what follows. Here that is, making it clear what the parameters $a, b > 0$ stand for, with $2a \times 2b$ being the gift box size for our ellipsis:



(2) Let us prove now that such an ellipsis has two focal points, as stated in (2). We must look for a number $r > 0$, and a number $l > 0$, such that our ellipsis appears as

$d(z,p)+d(z,q)=l$, with $p=(0,-r)$ and $q=(0,r)$, according to the following picture:



(3) Let us first compute these numbers $r,l>0$. Assuming that our result holds indeed as stated, by taking $z=(0,a)$, we see that the length l is:

$$l=(a-r)+(a+r)=2a$$

As for the parameter r, by taking $z=(b,0)$, we conclude that we must have:

$$2\sqrt{b^2+r^2}=2a\implies r=\sqrt{a^2-b^2}$$

(4) With these observations made, let us prove now the result. Given $l,r>0$, and setting $p=(0,-r)$ and $q=(0,r)$, we have the following computation, with $z=(x,y)$:

$$\begin{aligned}
& d(z,p)+d(z,q)=l\\
\iff\ & \sqrt{(x+r)^2+y^2}+\sqrt{(x-r)^2+y^2}=l\\
\iff\ & \sqrt{(x+r)^2+y^2}=l-\sqrt{(x-r)^2+y^2}\\
\iff\ & (x+r)^2+y^2=(x-r)^2+y^2+l^2-2l\sqrt{(x-r)^2+y^2}\\
\iff\ & 2l\sqrt{(x-r)^2+y^2}=l^2-4xr\\
\iff\ & 4l^2(x^2+r^2-2xr+y^2)=l^4+16x^2r^2-8l^2xr\\
\iff\ & 4l^2x^2+4l^2r^2+4l^2y^2=l^4+16x^2r^2\\
\iff\ & (4x^2-l^2)(4r^2-l^2)=4l^2y^2
\end{aligned}$$

(5) Now observe that we can further process the equation that we found as follows:

$$\begin{aligned}(4x^2-l^2)(4r^2-l^2)=4l^2y^2 &\iff \frac{4x^2-l^2}{l^2}=\frac{4y^2}{4r^2-l^2}\\ &\iff \frac{4x^2-l^2}{l^2}=\frac{y^2}{r^2-l^2/4}\\ &\iff \left(\frac{x}{2l}\right)^2-1=\left(\frac{y}{\sqrt{r^2-l^2/4}}\right)^2\\ &\iff \left(\frac{x}{2l}\right)^2+\left(\frac{y}{\sqrt{r^2-l^2/4}}\right)^2=1\end{aligned}$$

(6) Thus, our result holds indeed, and with the numbers $l,r>0$ appearing, and no surprise here, via the formulae $l=2a$ and $r=\sqrt{a^2-b^2}$, found in (3) above.

(7) Getting back now to our theorem, we have two other assertions there at the end, labelled (3,4). But, thinking a bit, these assertions are in fact equivalent, and in what concerns us, we will rather focus on (4), which looks more mathematical. And in what regards this assertion (4), this can be established indeed, by doing some 3D computations, that we will leave here as an instructive exercise, for you. And with the promise that we will come back to this in a moment, with a full proof, in a more general setting. □

All this is very nice, but before getting into physics, with some explanations for the fact that planets travel indeed on ellipses, which is something that we must surely understand, before going with some further math, let us settle as well the question of wandering asteroids. Observations show that these can travel on parabolas and hyperbolas, so what we need as mathematics is a unified theory of ellipses, parabolas and hyperbolas. And fortunately, this theory exists, also since the ancient Greeks, summarized as follows:

THEOREM 1.4. *The conics, which are the algebraic curves of degree 2 in the plane,*

$$C=\left\{(x,y)\in\mathbb{R}^2\Big|P(x,y)=0\right\}$$

with $\deg P\leq 2$*, appear modulo degeneration by cutting a 2-sided cone with a plane, and can be classified into ellipses, parabolas and hyperbolas.*

PROOF. This follows by further building on Theorem 1.3, as follows:

(1) Let us first classify the conics up to non-degenerate linear transformations of the plane, which are by definition transformations as follows, with $\det A\neq 0$:

$$\begin{pmatrix}x\\y\end{pmatrix}\to A\begin{pmatrix}x\\y\end{pmatrix}$$

Our claim is that as solutions we have the circles, parabolas, hyperbolas, along with some degenerate solutions, namely $\emptyset$, points, lines, pairs of lines, $\mathbb{R}^2$.

(2) As a first remark, it looks like we forgot precisely the ellipses, but via linear transformations these become circles, so things fine. As a second remark, all our claimed solutions can appear. Indeed, the circles, parabolas, hyperbolas can appear as follows:

$$x^2+y^2=1 \quad , \quad x^2=y \quad , \quad xy=1$$

As for $\emptyset$, points, lines, pairs of lines, $\mathbb{R}^2$, these can appear too, as follows, and with our polynomial P chosen, whenever possible, to be of degree exactly 2:

$$x^2=-1 \quad , \quad x^2+y^2=0 \quad , \quad x^2=0 \quad , \quad xy=0 \quad , \quad 0=0$$

Observe here that, when dealing with these degenerate cases, assuming $\deg P=2$ instead of $\deg P\leq 2$ would only rule out $\mathbb{R}^2$ itself, which is not worth it.

(3) Getting now to the proof of our claim in (1), classification up to linear transformations, consider an arbitrary conic, written as follows, with $a,b,c,d,e,f\in\mathbb{R}$:

$$ax^2+by^2+cxy+dx+ey+f=0$$

Assume first $a\neq 0$. By making a square out of ax^2, up to a linear transformation in (x,y), we can get rid of the term cxy, and we are left with:

$$ax^2+by^2+dx+ey+f=0$$

In the case $b\neq 0$ we can make two obvious squares, and again up to a linear transformation in (x,y), we are left with an equation as follows:

$$x^2\pm y^2=k$$

In the case of positive sign, $x^2+y^2=k$, the solutions are the circle, when $k\geq 0$, the point, when $k=0$, and $\emptyset$, when $k<0$. As for the case of negative sign, $x^2-y^2=k$, which reads $(x-y)(x+y)=k$, here once again by linearity our equation becomes $xy=l$, which is a hyperbola when $l\neq 0$, and two lines when $l=0$.

(4) In the case $b\neq 0$ the study is similar, with the same solutions, so we are left with the case $a=b=0$. Here our conic is as follows, with $c,d,e,f\in\mathbb{R}$:

$$cxy+dx+ey+f=0$$

If $c\neq 0$, by linearity our equation becomes $xy=l$, which produces a hyperbola or two lines, as explained before. As for the remaining case, $c=0$, here our equation is:

$$dx+ey+f=0$$

But this is generically the equation of a line, unless we are in the case $d=e=0$, where our equation is $f=0$, having as solutions $\emptyset$ when $f\neq 0$, and $\mathbb{R}^2$ when $f=0$.

(5) Thus, done with the classification, up to linear transformations as in (1). But this classification leads to the classification in general too, by applying now linear transformations to the solutions that we found. So, done with this, and very good.

(6) It remains to discuss the cone cutting. By suitably choosing our coordinate axes (x, y, z), we can assume that our cone is given by an equation as follows, with $k > 0$:

$$x^2 + y^2 = kz^2$$

In order to prove the result, we must in principle intersect this cone with an arbitrary plane, which has an equation as follows, with $(a, b, c) \neq (0, 0, 0)$:

$$ax + by + cz = d$$

(7) However, before getting into computations, observe that what we want to find is a certain degree 2 equation in the above plane, for the intersection. Thus, it is convenient to change the coordinates, as for our plane to be given by the following equation:

$$z = 0$$

(8) But with this done, what we have to do is to see how the cone equation $x^2+y^2 = kz^2$ changes, under this change of coordinates, and then set $z = 0$, as to get the (x, y) equation of the intersection. But this leads, via some thinking or computations, to the conclusion that the cone equation $x^2 + y^2 = kz^2$ becomes in this way a degree 2 equation in (x, y), which can be arbitrary, and so to the final conclusion in the statement. □

1b. Kepler and Newton

Ready for some physics? All we have so far is certainly nice, but a bit too mathematical, seemingly away from the real life, and its problems. To be more precise, browsing through what we did so far, we can basically count on two applications of that:

(1) First we have Theorem 1.3 (3), teaching us how to draw circles, from different perspectives. But that rather belongs to Art and Humanities.

(2) We have as well Theorem 1.3 (4), teaching us that when coming with a big Viking axe, and slashing a conical tree stump, we get an ellipsis. Interesting too.

In short, and hope you get my point, before going ahead with more math, let us make sure that what we're doing is relevant to physics. And here, good news, not only what we did is relevant, but is actually at the origin of modern physics, thanks to:

THEOREM 1.5. *Planets and other celestial bodies move around the Sun on conics,*

$$C = \left\{ (x, y) \in \mathbb{R}^2 \Big| P(x, y) = 0 \right\}$$

with $P \in \mathbb{R}[x, y]$ being of degree 2, which can be ellipses, parabolas or hyperbolas.

PROOF. This is something quite long, due to Kepler and Newton, but no fear, we know calculus, and threrefore what can resist us. The proof goes as follows:

(1) According to observations and calculations performed over the centuries, since the ancient times, and first formalized by Newton, following some groundbreaking work of Kepler, the force of attraction between two bodies of masses M,m is given by:

$$||F||=G\cdot\frac{Mm}{d^2}$$

Here d is the distance between the two bodies, and $G\simeq 6.674\times 10^{-11}$ is a constant. Now assuming that M is fixed at $0\in\mathbb{R}^3$, the force exterted on m positioned at $x\in\mathbb{R}^3$, regarded as a vector $F\in\mathbb{R}^3$, is given by the following formula:

$$\begin{aligned}F&=-||F||\cdot\frac{x}{||x||}\\&=-\frac{GMm}{||x||^2}\cdot\frac{x}{||x||}\\&=-\frac{GMmx}{||x||^3}\end{aligned}$$

But $F=ma=m\ddot{x}$, with $a=\ddot{x}$ being the acceleration, second derivative of the position, so the equation of motion of m, assuming that M is fixed at 0, is:

$$\ddot{x}=-\frac{GMx}{||x||^3}$$

Obviously, the problem happens in 2 dimensions, and you can even find, as an exercise, a formal proof of that, based on the above equation, if your really want to. Now here the most convenient is to use standard x,y coordinates, and denote our point as $z=(x,y)$. With this change made, and by setting $K=GM$, the equation of motion becomes:

$$\ddot{z}=-\frac{Kz}{||z||^3}$$

(2) The idea now is that the problem can be solved via some calculus. Let us write indeed our vector $z=(x,y)$ in polar coordinates, as follows:

$$x=r\cos\theta\quad,\quad y=r\sin\theta$$

We have then $||z||=r$, and our equation of motion becomes:

$$\ddot{z}=-\frac{Kz}{r^3}$$

Let us differentiate now x,y. By using the standard calculus rules, we have:

$$\dot{x}=\dot{r}\cos\theta-r\sin\theta\cdot\dot{\theta}$$

$$\dot{y}=\dot{r}\sin\theta+r\cos\theta\cdot\dot{\theta}$$

Differentiating one more time gives the following formulae:

$$\ddot{x} = \ddot{r}\cos\theta - 2\dot{r}\sin\theta \cdot \dot{\theta} - r\cos\theta \cdot \dot{\theta}^2 - r\sin\theta \cdot \ddot{\theta}$$

$$\ddot{y} = \ddot{r}\sin\theta + 2\dot{r}\cos\theta \cdot \dot{\theta} - r\sin\theta \cdot \dot{\theta}^2 + r\cos\theta \cdot \ddot{\theta}$$

Consider now the following two quantities, appearing as coefficients in the above:

$$a = \ddot{r} - r\dot{\theta}^2 \quad , \quad b = 2\dot{r}\dot{\theta} + r\ddot{\theta}$$

In terms of these quantities, our second derivative formulae read:

$$\ddot{x} = a\cos\theta - b\sin\theta$$

$$\ddot{y} = a\sin\theta + b\cos\theta$$

(3) We can now solve the equation of motion from (1). Indeed, with the formulae that we found for $\ddot{x}, \ddot{y}$, our equation of motion takes the following form:

$$a\cos\theta - b\sin\theta = -\frac{K}{r^2}\cos\theta$$

$$a\sin\theta + b\cos\theta = -\frac{K}{r^2}\sin\theta$$

But these two formulae can be written in the following way:

$$\left(a + \frac{K}{r^2}\right)\cos\theta = b\sin\theta \quad , \quad \left(a + \frac{K}{r^2}\right)\sin\theta = -b\cos\theta$$

By making now the product, and assuming that we are in a non-degenerate case, where the angle θ varies indeed, we obtain by positivity that we must have:

$$a + \frac{K}{r^2} = b = 0$$

(4) Let us first examine the second equation, $b = 0$. This can be solved as follows:

$$\begin{aligned} b = 0 \quad &\iff \quad 2\dot{r}\dot{\theta} + r\ddot{\theta} = 0 \\ &\iff \quad \frac{\ddot{\theta}}{\dot{\theta}} = -2\frac{\dot{r}}{r} \\ &\iff \quad (\log\dot{\theta})' = (-2\log r)' \\ &\iff \quad \log\dot{\theta} = -2\log r + c \\ &\iff \quad \dot{\theta} = \frac{\lambda}{r^2} \end{aligned}$$

As for the first equation the we found, namely $a + K/r^2 = 0$, this becomes:

$$\ddot{r} - \frac{\lambda^2}{r^3} + \frac{K}{r^2} = 0$$

As a conclusion to all this, in polar coordinates, $x = r\cos\theta$, $y = r\sin\theta$, our equations of motion are as follows, with λ being a constant, not depending on t:

$$\ddot{r} = \frac{\lambda^2}{r^3} - \frac{K}{r^2} \quad , \quad \dot{\theta} = \frac{\lambda}{r^2}$$

Even better now, by writing $K = \lambda^2/c$, these equations read:

$$\ddot{r} = \frac{\lambda^2}{r^2}\left(\frac{1}{r} - \frac{1}{c}\right) \quad , \quad \dot{\theta} = \frac{\lambda}{r^2}$$

(5) In order to study the first equation, we use a trick. Let us write:

$$r(t) = \frac{1}{f(\theta(t))}$$

Abbreviated, and by reminding that f takes $\theta = \theta(t)$ as variable, this reads:

$$r = \frac{1}{f}$$

With the convention that dots mean as usual derivatives with respect to t, and that the primes will denote derivatives with respect to $\theta = \theta(t)$, we have:

$$\dot{r} = -\frac{f'\dot{\theta}}{f^2} = -\frac{f'}{f^2} \cdot \frac{\lambda}{r^2} = -\lambda f'$$

By differentiating one more time with respect to t, we obtain:

$$\ddot{r} = -\lambda f''\dot{\theta} = -\lambda f'' \cdot \frac{\lambda}{r^2} = -\frac{\lambda^2}{r^2} f''$$

On the other hand, our equation for $\ddot{r}$ found in (4) above reads:

$$\ddot{r} = \frac{\lambda^2}{r^2}\left(\frac{1}{r} - \frac{1}{c}\right) = \frac{\lambda^2}{r^2}\left(f - \frac{1}{c}\right)$$

Thus, in terms of $f = 1/r$ as above, our equation for $\ddot{r}$ simply reads:

$$f'' + f = \frac{1}{c}$$

But this latter equation is elementary to solve. Indeed, both functions $\cos t, \sin t$ satisfy $g" + g = 0$, so any linear combination of them satisfies as well this equation. But the solutions of $f'' + f = 1/c$ being those of $g'' + g = 0$ shifted by $1/c$, we obtain:

$$f = \frac{1 + \varepsilon\cos\theta + \delta\sin\theta}{c}$$

Now by inverting, we obtain the following formula:

$$r = \frac{c}{1 + \varepsilon\cos\theta + \delta\sin\theta}$$

(6) But this leads to the conclusion that the trajectory is a conic. Indeed, in terms of the parameter θ, the formulae of the coordinates are:

$$x=\frac{c\cos\theta}{1+\varepsilon\cos\theta+\delta\sin\theta}\quad,\quad y=\frac{c\sin\theta}{1+\varepsilon\cos\theta+\delta\sin\theta}$$

Now observe that these two functions x,y satisfy the following formula:

$$x^2+y^2=\frac{c^2(\cos^2\theta+\sin^2\theta)}{(1+\varepsilon\cos\theta+\delta\sin\theta)^2}=\frac{c^2}{(1+\varepsilon\cos\theta+\delta\sin\theta)^2}$$

On the other hand, these two functions satisfy as well the following formula:

$$\begin{aligned}(\varepsilon x+\delta y-c)^2 &= \frac{c^2\big(\varepsilon\cos\theta+\delta\sin\theta-(1+\varepsilon\cos\theta+\delta\sin\theta)\big)^2}{(1+\varepsilon\cos\theta+\delta\sin\theta)^2}\\ &= \frac{c^2}{(1+\varepsilon\cos\theta+\delta\sin\theta)^2}\end{aligned}$$

We conclude that our coordinates x,y satisfy the following equation:

$$x^2+y^2=(\varepsilon x+\delta y-c)^2$$

But what we have here is an equation of a conic, and we are done. □

We have the following result, coming as a useful version of Theorem 1.5:

THEOREM 1.6. *In the context of a 2-body problem, with M fixed at 0, and m starting its movement from Ox, the equation of motion of m, namely*

$$\ddot{z}=-\frac{Kz}{||z||^3}$$

with $K=GM$, and $z=(x,y)$, becomes in polar coordinates, $x=r\cos\theta$, $y=r\sin\theta$,

$$\ddot{r}=\frac{\lambda^2}{r^2}\left(\frac{1}{r}-\frac{1}{c}\right)\quad,\quad \dot{\theta}=\frac{\lambda}{r^2}$$

for some $\lambda,c\in\mathbb{R}$, related by $\lambda^2=Kc$. The value of r in terms of θ is given by

$$r=\frac{c}{1+\varepsilon\cos\theta+\delta\sin\theta}$$

for some $\varepsilon,\delta\in\mathbb{R}$. At the level of the affine coordinates x,y, this means

$$x=\frac{c\cos\theta}{1+\varepsilon\cos\theta+\delta\sin\theta}\quad,\quad y=\frac{c\sin\theta}{1+\varepsilon\cos\theta+\delta\sin\theta}$$

with $\theta=\theta(t)$ being subject to $\dot{\theta}=\lambda^2/r$, as above. Finally, we have

$$x^2+y^2=(\varepsilon x+\delta y-c)^2$$

which is a degree 2 equation, and so the resulting trajectory is a conic.

PROOF. This is a sort of "best of" the formulae found in the proof of Theorem 1.5. And in the hope of course that we have not forgotten anything. □

There are of course many other things that can be said, as a continuation of the above. For instance, we would like to understand how the various motion parameters $\lambda, c, \varepsilon, \delta$ appear from the initial data. And the formulae here are as follows:

PROPOSITION 1.7. *In the context of Theorem 1.6, and in polar coordinates,* $x = r\cos\theta$, $y = r\sin\theta$, *the initial data is as follows, with* $R = r_0$*:*

$$r_0 = \frac{c}{1+\varepsilon} \quad , \quad \theta_0 = 0$$

$$\dot{r}_0 = -\frac{\delta\sqrt{K}}{\sqrt{c}} \quad , \quad \dot{\theta}_0 = \frac{\sqrt{Kc}}{R^2}$$

$$\ddot{r}_0 = \frac{\varepsilon K}{R^2} \quad , \quad \ddot{\theta}_0 = \frac{4\delta K}{R^2}$$

The corresponding formulae for the affine coordinates x, y *can be deduced from this. Also, the various motion parameters* c, ε, δ *and* $\lambda = \sqrt{Kc}$ *can be recovered from this data.*

PROOF. We have several assertions here, the idea being as follows:

(1) As mentioned in Theorem 1.6, the object m begins its movement on Ox. Thus we have $\theta_0 = 0$, and from this we get the formula of r_0 in the statement.

(2) Regarding now the initial speed, the formula of $\dot{\theta}_0$ follows from:

$$\dot{\theta} = \frac{\lambda}{r^2} = \frac{\sqrt{Kc}}{r^2}$$

Also, in what concerns the radial speed, the formula of $\dot{r}_0$ follows from:

$$\dot{r} = \frac{c(\varepsilon\sin\theta - \delta\cos\theta)\dot{\theta}}{(1+\varepsilon\cos\theta+\delta\sin\theta)^2} = \frac{\sqrt{K}(\varepsilon\sin\theta - \delta\cos\theta)}{\sqrt{c}}$$

(3) Regarding now the initial acceleration, by using $\dot{\theta} = \sqrt{Kc}/r^2$ we find:

$$\ddot{\theta} = -2\sqrt{Kc}\cdot\frac{2r\dot{r}}{r^3} = -\frac{4\sqrt{Kc}\cdot\dot{r}}{r^2}$$

In particular at $t = 0$ we obtain the formula in the statement, namely:

$$\ddot{\theta}_0 = -\frac{4\sqrt{Kc}\cdot\dot{r}_0}{R^2} = \frac{4\sqrt{Kc}}{R^2}\cdot\frac{\delta\sqrt{K}}{\sqrt{c}} = \frac{4\delta K}{R^2}$$

(4) Also regarding acceleration, with $\lambda = \sqrt{Kc}$ our main motion formula reads:

$$\ddot{r} = \frac{Kc}{r^2}\left(\frac{1}{r} - \frac{1}{c}\right)$$

In particular at $t = 0$ we obtain the formula in the statement, namely:

$$\ddot{r}_0 = \frac{Kc}{R^2}\left(\frac{1}{R} - \frac{1}{c}\right) = \frac{Kc}{R^2} \cdot \frac{\varepsilon}{c} = \frac{\varepsilon K}{R^2}$$

(5) Finally, the last assertion is clear, and since the formulae look better anyway in polar coordinates than in affine coordinates, we will not get into details here. □

With the above formulae in hand, we can work out how various inital speeds and accelerations lead to various types of conics. The computations here are many, and very interesting, and we will leave them as a long, pleasant and instructive exercise.

1c. Algebraic curves

As a conclusion to what we did so far, conics are at the core of everything, mathematics, physics, life. But, what is next? A natural answer to this question comes from:

Definition 1.8. *An algebraic curve in $\mathbb{R}^2$ is the vanishing set*

$$C = \left\{(x, y) \in \mathbb{R}^2 \Big| P(x, y) = 0\right\}$$

of a polynomial $P \in \mathbb{R}[X, Y]$ of arbitrary degree.

We already know well the algebraic curves in degree 2, which are the conics, and a first problem is, what results from what we learned about conics have a chance to be relevant to the arbitrary algebraic curves. And normally none, because the ellipses, parabolas and hyperbolas are obviously very particular curves, having very particular properties.

Let us record however a useful statement here, as follows:

Proposition 1.9. *The conics can be written in cartesian, polar, parametric or complex coordinates, with the equations for the unit circle being*

$$x^2 + y^2 = 1 \quad , \quad r = 1 \quad , \quad x = \cos t \,,\, y = \sin t \quad , \quad |z| = 1$$

and with the equations for ellipses, parabolas and hyperbolas being similar.

Proof. The equations for the circle are clear, those for ellipses can be found in the above, and we will leave as an exercise those for parabolas and hyperbolas. □

As a true answer to our question now, coming this time from a very modest conic, namely $xy = 0$, that we dismissed in the above as being "degenerate", we have:

Theorem 1.10. *The following happen, for curves C defined by polynomials P:*

1. *In degree $d = 2$, curves can have singularities, such as $xy = 0$ at $(0, 0)$.*
2. *In general, assuming $P = P_1 \ldots P_k$, we have $C = C_1 \cup \ldots\ldots \cup C_k$.*
3. *A union of curves $C_i \cup C_j$ is generically non-smooth, unless disjoint.*
4. *Due to this, we say that C is non-degenerate when P is irreducible.*

PROOF. All this is self-explanatory, the details being as follows:

(1) This is something obvious, just the story of two lines crossing.

(2) This comes from the following trivial fact, with the notation $z = (x, y)$:

$$P_1 \ldots P_k(z) = 0 \iff P_1(z) = 0, \text{ or } P_2(z) = 0, \ \ldots \ , \text{ or } P_k(z) = 0$$

(3) This is something very intuitive, and it actually takes a bit of time to imagine a situation where $C_1 \cap C_2 \neq \emptyset$, $C_1 \not\subset C_2$, $C_2 \not\subset C_1$, but $C_1 \cup C_2$ is smooth. In practice now, "generically" has of course a mathematical meaning, in relation with probability, and our assertion does say something mathematical, that we are supposed to prove. But, we will not insist on this, and leave this as an instructive exercise, precise formulation of the claim, and its proof, in the case you are familiar with probability theory.

(4) This is just a definition, based on the above, that we will use in what follows. □

With degree 1 and 2 investigated, and our conclusions recorded, let us get now to degree 3, see what new phenomena appear here. And here, to start with, we have the following remarkable curve, well-known from calculus, because 0 is not a maximum or minimum of the function $x \to y$, despite the derivative vanishing there:

$$x^3 = y$$

Also, in relation with set theory and logic, and with the foundations of mathematics in general, we have the following curve, which looks like the empyset $\emptyset$:

$$(x - y)(x^2 + y^2 - 1) = 0$$

But, it is not about counterexamples to calculus, or about logic, that we want to talk about here. As a first truly remarkable degree 3 curve, or cubic, we have the cusp:

PROPOSITION 1.11. *The standard cusp, which is the cubic given by*

$$x^3 = y^2$$

has a singularity at $(0, 0)$*, with only* 1 *tangent line at that singularity.*

PROOF. The two branches of the cusp are indeed both tangent to Ox, because:

$$y' = \pm\frac{3}{2}\sqrt{x} \implies y'(0) = 0$$

Observe also that what happens for the cusp is different from what happens for $xy = 0$, precisely because we have 1 line tangent at the singularity, instead of 2. □

As a second remarkable cubic, which gets the crown, and the right to have a Theorem about it, we have the Tschirnhausen curve, which is as follows:

THEOREM 1.12. *The Tschirnhausen cubic, given by the following equation,*

$$x^3 = x^2 - 3y^2$$

makes the dream of $xy = 0$ *come true, by self-intersecting, and being non-degenerate.*

PROOF. This is something self-explanatory, by drawing a picture, but there are several other interesting things that can be said about this curve, and the family of curves containing it, depending on a parameter, and up to basic transformations, as follows:

(1) Let us start with the curve written in polar coordinates as follows:

$$r\cos^3\left(\frac{\theta}{3}\right)=a$$

With $t=\tan(\theta/3)$, the equations of the coordinates are as follows:

$$x=a(1-3t^2)\quad,\quad y=at(3-t^2)$$

Now by eliminating t, we reach to the following equation:

$$(a-x)(8a+x)^2=27ay^2$$

(2) By translating horizontally by $8a$, and changing signs of variables, we have:

$$x=3a(3-t^2)\quad,\quad y=at(3-t^2)$$

Now by eliminating t, we reach to the following equation:

$$x^3=9a(x^2-3y^2)$$

But with $a=1/9$ this is precisely the equation in the statement. □

In degree 4 now, quartics, we have enough dimensions for "improving" the cusp and the Tschirnhausen curve. First we have the cardioid, which is as follows:

PROPOSITION 1.13. *The cardioid, which is a quartic, given in polar coordinates by*

$$2r=a(1-\cos\theta)$$

makes the dream of $x^3=y^2$ come true, by being a closed curve, with a cusp.

PROOF. As before with the Tschirnhausen curve, this is something self-explanatory, by drawing a picture, but there are several things that must be said, as follows:

(1) The cardioid appears by definition by rolling a circle of radius $c>0$ around another circle of same radius $c>0$. With θ being the rolling angle, we have:

$$x=2c(1-\cos\theta)\cos\theta$$

$$y=2c(1-\cos\theta)\sin\theta$$

(2) Thus, in polar coordinates we get the equation in the statement, with $a=4c$:

$$r=2c(1-\cos\theta)$$

(3) Finally, in cartesian coordinates, the equation is as follows:

$$(x^2+y^2)^2+4cx(x^2+y^2)=4c^2y^2$$

Thus, what we have is indeed a degree 4 curve, as claimed. □

Still in degree 4, the crown gets to the Bernoulli lemniscate, which is as follows:

THEOREM 1.14. *The Bernoulli lemniscate, a quartic, which is given by*

$$r^2 = a^2 \cos 2\theta$$

makes the dream of $x^3 = x^2 - 3y^2$ *come true, by being closed, and self-intersecting.*

PROOF. As usual, this is something self-explanatory, by drawing a picture, which looks like ∞, but there are several other things that must be said, as follows:

(1) In cartesian coordinates, the equation is as follows, with $a^2 = 2c^2$:

$$(x^2 + y^2)^2 = c^2(x^2 - y^2)$$

(2) Also, we have the following nice complex reformulation of this equation:

$$|z + c| \cdot |z - c| = c^2$$

Thus, we are led to the conclusions in in the statement. □

In degree 5, in the lack of any spectacular quintic, let us record:

THEOREM 1.15. *Unlike in degree* $3, 4$*, where equations can be solved, by the Cardano formula, in degree* 5 *this generically does not happen, an example being*

$$x^5 - x - 1 = 0$$

having Galois group S_5*, not solvable. Geometrically, this tells us that the intersection of the quintic* $y = x^5 - x - 1$ *with the line* $y = 0$ *cannot be computed.*

PROOF. Obviously off-topic, but with no good quintic available, and still a few more minutes before the bell ringing, I had to improvise a bit, and tell you about this:

(1) As indicated, the degree 3 equations can be solved a bit like the degree 2 ones, but with the formula, due to Cardano, being more complicated. With some square making tricks, which are non-trivial either, the Cardano formula applies to degree 4 as well.

(2) In degree 5 or higher, none of this is possible. Long story here, the idea being that in order for $P = 0$ to be solvable, the group $Gal(P)$ must be solvable, in the sense of group theory. But, unlike S_3, S_4 which are solvable, S_5 and higher are not solvable. □

Back now to our usual business, in degree 6, sextics, we first have here:

PROPOSITION 1.16. *The trefoil sextic, or Kiepert curve, which is given by*

$$r^3 = a^3 \cos 3\theta$$

looks like a trefoil, closed curve, with a triple self-intersection.

PROOF. As before, drawing a picture is mandatory. With $z = re^{i\theta}$ we have:

$$\begin{aligned} r^3 = a^3\cos 3\theta \quad &\iff \quad r^3\cos 3\theta = \left(\frac{r^2}{a}\right)^3 \\ &\iff \quad z^3 + \bar{z}^3 = 2\left(\frac{z\bar{z}}{a}\right)^3 \\ &\iff \quad (x+iy)^3 + (x-iy)^3 = 2\left(\frac{x^2+y^2}{a}\right)^3 \\ &\iff \quad x^3 - 3xy^2 = \left(\frac{x^2+y^2}{a}\right)^3 \\ &\iff \quad (x^2+y^2)^3 = a^3(x^3-3xy^2) \end{aligned}$$

Thus, we have indeed a sextic, as claimed. □

We also have in degree 6 the most beautiful of curves them all, the Cayley sextic:

THEOREM 1.17. *The Cayley sextic, given in polar coordinates by*

$$r = a\cos^3\left(\frac{\theta}{3}\right)$$

makes the dream of everyone come true, by looking like a self-intersecting heart.

PROOF. As before, picture mandatory. With $z = re^{i\theta}$ and $u = z^{1/3}$ we have:

$$\begin{aligned} r = a\cos^3\left(\frac{\theta}{3}\right) \quad &\iff \quad ar\cos^3\left(\frac{\theta}{3}\right) = r^2 \\ &\iff \quad a\left(\frac{u+\bar{u}}{2}\right)^3 = r^2 \\ &\iff \quad a(u^3+\bar{u}^3+3u\bar{u}(u+\bar{u})) = 8r^2 \\ &\iff \quad 3au\bar{u}\cdot\frac{u+\bar{u}}{2} = 4r^2 - ax \\ &\iff \quad 27a^3r^6\cdot\frac{r^2}{a} = (4r^2-ax)^3 \\ &\iff \quad 27a^2(x^2+y^2)^2 = (4x^2+4y^2-ax)^3 \end{aligned}$$

Thus, we have indeed a sextic, as claimed. □

1d. Spirals, lemniscates

Quite remarkably, most of the above curves are sinusoidal spirals, in the following sense, and with actually the term "sinusoidal spiral" being a bit unfortunate:

THEOREM 1.18. *The sinusoidal spirals, which are as follows,*

$$r^n = a^n \cos n\theta$$

with $a \neq 0$ and $n \in \mathbb{Q} - \{0\}$, include the following curves:

(1) $n = -1$ *line.*
(2) $n = 1$ *circle,* $n = -1/2$ *parabola,* $n = -2$ *hyperbola.*
(3) $n = -3$ *Humbert cubic,* $n = -1/3$ *Tschirnhausen curve.*
(4) $n = 1/2$ *cardioid,* $n = 2$ *Bernoulli lemniscate.*
(5) $n = 3$ *Kiepert trefoil,* $n = 1/3$ *Cayley sextic.*

PROOF. We first have to prove that the sinusoidal spirals are indeed algebraic curves. But this is best done by using the complex coordinate $z = re^{i\theta}$, as follows:

$$\begin{aligned} r^n = a^n \cos n\theta \quad &\iff \quad r^n \cos n\theta = \left(\frac{r^2}{a}\right)^n \\ &\iff \quad z^n + \bar{z}^n = 2\left(\frac{z\bar{z}}{a}\right)^n \\ &\iff \quad (x+iy)^n + (x-iy)^n = 2\left(\frac{x^2+y^2}{a}\right)^n \end{aligned}$$

As a first observation now, in the case $n \in \mathbb{N}$ we can simply use the binomial formula, and we get an algebraic equation of degree $2n$, as follows:

$$\sum_{k=0}^{[n/2]} (-1)^k \binom{n}{2k} x^{n-2k} y^{2k} = \left(\frac{x^2+y^2}{a}\right)^n$$

In general, things are a bit more complicated, as shown for instance by our computation for the Cayley sextic. However, the same idea as there applies, and we are led in this way to the equation of an algebraic curve, as claimed. Regarding now the examples:

(1) At $n = -1$ the equation is as follows, producing a line:

$$r \cos\theta = a \iff x = a$$

(2) At $n = 1$ the equation is as follows, producing a circle:

$$r = a\cos\theta \iff r^2 = ax \iff x^2 + y^2 = ax$$

(3) At $n = -1/2$ the equation is as follows, producing a parabola:

$$a = r\cos^2(\theta/2) \iff r + x = 2a \iff y^2 = 4a(a - x)$$

(4) At $n = -2$ the equation is as follows, producing a hyperbola:

$$a^2 = r\cos^2 2\theta \iff a^2 = 2x^2 - r^2 \iff (x+y)(x-y) = a^2$$

(5) At $n=-3$ the equation is as follows, producing a curve with 3 components, which looks like some sort of "trivalent hyperbola", called Humbert cubic:

$$r^3\cos 3\theta = a^3 \iff z^3+\bar{z}^3 = 2a^3 \iff x^3-3xy^2 = a^3$$

(6) As for the other curves, this follows from our various formulae above. □

Let us study now more in detail the sinusoidal spirals. We first have:

PROPOSITION 1.19. *The sinusoidal spirals, which with $z=x+iy$ are*

$$z^n+\bar{z}^n = 2\left(\frac{z\bar{z}}{a}\right)^n$$

with $a\neq 0$ and $n\in\mathbb{Q}-\{0\}$, are as follows:

1. *With $n=-m$, $m\in\mathbb{N}$, the equation is $z^m+\bar{z}^m=2a^m$, degree m.*
2. *With $n=m$, $m\in\mathbb{N}$, the equation is $z^m+\bar{z}^m=2(z\bar{z}/a)^m$, degree $2m$.*
3. *With $n=-1/m$, $m\in\mathbb{N}$, the equation is $(z^{1/m}+\bar{z}^{1/m})^m=2^m a$.*
4. *With $n=1/m$, $m\in\mathbb{N}$, the equation is $(z^{1/m}+\bar{z}^{1/m})^m=2^m z\bar{z}/a$.*

PROOF. This is something self-explanatory, the details being as follows:

(1) With $n=-m$ and $m\in\mathbb{N}$ as in the statement, the equation is, as claimed:

$$z^{-m}+\bar{z}^{-m} = 2\left(\frac{z\bar{z}}{a}\right)^{-m} \iff z^m+\bar{z}^m = 2a^m$$

(2) This is an empty statement, just a matter of using the new variable $m=n$.

(3) With $n=-1/m$ and $m\in\mathbb{N}$ as in the statement, the equation is, as claimed:

$$\begin{aligned} z^{-1/m}+\bar{z}^{-1/m} = 2\left(\frac{z\bar{z}}{a}\right)^{-1/m} &\iff z^{1/m}+\bar{z}^{1/m} = 2a^{1/m} \\ &\iff (z^{1/m}+\bar{z}^{1/m})^m = 2^m a \end{aligned}$$

(4) With $n=1/m$ and $m\in\mathbb{N}$ as in the statement, the equation is, as claimed:

$$z^{1/m}+\bar{z}^{1/m} = 2\left(\frac{z\bar{z}}{a}\right)^{1/m} \iff (z^{1/m}+\bar{z}^{1/m})^m = 2^m\cdot\frac{z\bar{z}}{a}$$

Thus, we are led to the conclusions in the statement. □

Observe that in the fractionary cases, $n=\pm 1/m$, the equations in the above statement are not polynomial in x,y, unless at very small values of m. To be more precise:

(1) In the case $n=-1/m$, we certainly have at $m=1,2,3$ the $d=1$ line, $d=2$ parabola, and $d=3$ Tschirnhausen curve, but at $m=4$ things change, with the equation $(z^{1/4}+\bar{z}^{1/4})^4=16a$ being no longer polynomial in x,y, and requiring a further square operation to make it polynomials, and therefore leading to a curve of degree $d=8$.

(2) As for the case $n=1/m$, this is more complicated, with the data that we have at $m=1,2,3$, namely the $d=2$ circle, $d=3$ cardioid, and $d=6$ Cayley sextic, being not very good, and with things getting even more complicated at $m=4$ and higher.

In short, things quite complicated, and the general case, $n=\pm p/q$ with $p,q\in\mathbb{N}$, is certainly even more complicated. Instead of insisting on this, let us focus now on the simplest sinusoidal spirals that we have, namely those with $n=\pm m$, with $m\in\mathbb{N}$.

The point indeed is that the sinusoidal spirals with $n\in\mathbb{N}$ are also part of another remarkable family of plane algebraic curves, going back to Cassini, as follows:

THEOREM 1.20. *The polynomial lemniscates, which are as follows,*

$$|P(z)|=b^n$$

with $P\in\mathbb{C}[X]$ having n distinct roots, and $b>0$, include the following curves:

1. *The sinusoidal spirals with $n\in\mathbb{N}$, including the $n=1$ circle, $n=2$ Bernoulli lemniscate, and $n=3$ Kiepert trefoil.*
2. *The Cassini ovals, which are the quartics given by $|z+c|\cdot|z-c|=b^2$, covering too the Bernoulli lemniscate, appearing at $b=c$.*

PROOF. This is something quite self-explanatory, the details being as follows:

(1) Regarding the sinusoidal spirals with $n\in\mathbb{N}$, their equation is, with $a^n=2c^n$:

$$\begin{aligned}z^n+\bar{z}^n=2\left(\frac{z\bar{z}}{a}\right)^n &\iff c^n(z^n+\bar{z}^n)=(z\bar{z})^n\\ &\iff (z^n-c^n)(\bar{z}^n-c^n)=c^{2n}\\ &\iff |z^n-c^n|=c^n\end{aligned}$$

(2) Regarding the Cassini ovals, these correspond to the case where the polynomial $P\in\mathbb{C}[X]$ has degree 2, and we already know from the above that these cover the Bernoulli lemniscate. In general, the equation for the Cassini ovals is:

$$\begin{aligned}|z+c|\cdot|z-c|=b^2 &\iff |z^2-c^2|=b^2\\ &\iff (z^2-c^2)(\bar{z}^2-c^2)=b^4\\ &\iff (z\bar{z})^2-c^2(z^2+\bar{z}^2)+c^4=b^4\\ &\iff (x^2+y^2)^2-c^2(x^2-y^2)+c^4=b^4\\ &\iff (x^2+y^2)^2=c^2(x^2-y^2)+b^4-c^4\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

The polynomial lemniscates can be geometrically understood as follows:

THEOREM 1.21. *The equation $|P(z)| = b$ defining the polynomial lemniscates can be written as follows, in terms of the roots $c_1, \ldots, c_n$ of the polynomial P,*

$$\sqrt[n]{\prod_{k=1}^{n} |z - c_i|} = b$$

telling us that the geometric mean of the distances from z to the vertices of the polygon formed by $c_1, \ldots, c_n$ must be the constant $b > 0$.

PROOF. This is something self-explanatory, and as an illustration, let us work out the case of sinusoidal spirals with $n \in \mathbb{N}$. Here with $w = e^{2\pi i/n}$ we have:

$$z^n - c^n = \prod_{k=1}^{n} (z - cw^k)$$

Thus, the sinusoidal spiral equation reformulates as follows:

$$|z^n - c^n| = c^n \iff \prod_{k=1}^{n} |z - cw^k| = c^n$$

$$\iff \sqrt[n]{\prod_{k=1}^{n} |z - cw^k|} = c$$

Thus, for a sinusoidal spiral with positive integer parameter, the geometric mean of the distances to the vertices of a regular polygon must equal the radius of the polygon. □

Regarding now the sinusoidal spirals with $n \in -\mathbb{N}$, these are too part of another remarkable family of plane algebraic curves, constructed as follows:

THEOREM 1.22. *Given points in the plane $c_1, \ldots, c_n \in \mathbb{C}$ and a number $d \in \mathbb{R}$, construct the associated stelloid as being the set of points $z \in \mathbb{C}$ verifying*

$$\frac{1}{n} \sum_{k=1}^{n} \alpha_v (z - c_i) = d$$

with α_v denoting the angle with respect to a direction v. Then the stelloid is an algebraic curve, not depending on v, and at the level of examples we have the sinusoidal spirals with $n \in -\mathbb{N}$, including the $n = -1$ line, $n = -2$ hyperbola, and $n = -3$ Humbert cubic.

PROOF. All this is quite self-explanatory, and we will leave the verification of the various generalities regarding the stelloids, as well as the verification of the relation with the sinusoidal spirals with $n \in -\mathbb{N}$, as an instructive exercise. As a bonus exercise, try understanding the precise relation between stelloids, and polynomial lemniscates. □

So long for plane algebraic curves. Needless to say, all the above is old-style, first class mathematics, having countless applications. For instance when doing classical mechanics or electrodynamics, you will certainly meet polynomial lemniscates and stelloids, when looking at the field lines. Also, the image of any circle passing though 0 by $z \to z^2$ is a cardioid, and the famous Mandelbrot set is organized around such a cardioid.

And we will stop here our study of plane curves. The problem is that at the level of the general theory, without commutative algebra, and without projective geometry either, it is quite hard to say general things. But, we will be back to this, in due time.

1e. Exercises

We talked about many things in this opening chapter, and up to you to think what you want about this, depending on your previous knowledge. As exercises, we have:

Exercise 1.23. *Learn more triangle geometry, Euler line, and nine-point circle.*

Exercise 1.24. *Clarify the details for the cone cutting leading to conics.*

Exercise 1.25. *Write parabolas and hyperbolas in all types of coordinates.*

Exercise 1.26. *Do more computations, in relation with Kepler and Newton.*

Exercise 1.27. *Draw pictures for all the plane curves discussed in this chapter.*

Exercise 1.28. *Study the cardioid, from the perspective of classical mechanics.*

Exercise 1.29. *Have the Cayley sextic computations redone, by yourself.*

Exercise 1.30. *Further explore the sinusoidal spirals, and related curves.*

As bonus exercise, learn some theory for the smooth curves too, such as computing their lengths, or doing calculus on them. We will discuss this, but later in this book.

CHAPTER 2

Algebraic manifolds

2a. Surfaces, manifolds

Let us get now to $\mathbb{R}^3$. Here we are right away into a dillema, because the plane curves have two possible generalizations. First we have the algebraic curves in $\mathbb{R}^3$:

DEFINITION 2.1. *An algebraic curve in $\mathbb{R}^3$ is a curve as follows,*

$$C=\left\{(x,y,z)\in\mathbb{R}^3\Big|P(x,y,z)=0,\ Q(x,y,z)=0\right\}$$

appearing as the joint zeroes of two polynomials P,Q.

These curves look of course like the usual plane curves, and at the level of the phenomena that can appear, these are similar to those in the plane, involving singularities and so on, but also knotting, which is a new phenomenon. However, it is hard to say something with bare hands about knots. We will be back to this, later in this book.

On the other hand, as another natural generalization of the plane curves, and this might sound a bit surprising, we have the surfaces in $\mathbb{R}^3$, constructed as follows:

DEFINITION 2.2. *An algebraic surface in $\mathbb{R}^3$ is a surface as follows,*

$$S=\left\{(x,y,z)\in\mathbb{R}^3\Big|P(x,y,z)=0\right\}$$

appearing as the zeroes of a polynomial P.

The point indeed is that, as it was the case with the plane curves, what we have here is something defined by a single equation. And with respect to many questions, having a single equation matters a lot, and this is why surfaces in $\mathbb{R}^3$ are "simpler" than curves in $\mathbb{R}^3$. In fact, believe me, they are even the correct generalization of the curves in $\mathbb{R}^2$.

As an example of what can be done with surfaces, which is very similar to what we did with the conics $C\subset\mathbb{R}^2$, in the beginning of this chapter, we have:

THEOREM 2.3. *The degree 2 surfaces $S\subset\mathbb{R}^3$, called quadrics, are the ellipsoid*

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1$$

which is the only compact one, plus 16 more, which can be explicitely listed.

PROOF. We have two statements here, the idea being as follows:

(1) The equations for a quadric $S \subset \mathbb{R}^2$ are best written as follows, with $A \in M_3(\mathbb{R})$ being a matrix, $B \in M_{1\times 3}(\mathbb{R})$ being a row vector, and $C \in \mathbb{R}$ being a constant:

$$< Au, u > + Bu + C = 0$$

(2) By doing now the linear algebra, and we will come back to this in a moment, with details, or by invoking the theorem of Sylvester on quadratic forms, we are left, modulo degeneracy and linear transformations, with signed sums of squares, as follows:

$$\pm x^2 \pm y^2 \pm z^2 = 0, 1$$

(3) Thus the sphere is the only compact quadric, up to linear transformations, and by applying now linear transformations to it, we are led to the ellipsoids in the statement.

(4) As for the other quadrics, there are many of them, a bit similar to the parabolas and hyperbolas in 2 dimensions, and some work here leads to a 16 item list. $\square$

The above proof was of course quite short, but we will come back with details, at least on its first part, which is the main one, in a moment, in a more general setting.

More generally now, we have the following definition, in arbitrary N dimensions:

DEFINITION 2.4. *An algebraic hypersurface in $\mathbb{R}^N$ is a space of the form*

$$S = \left\{ (x_1, \ldots, x_N) \in \mathbb{R}^N \Big| P(x_1, \ldots, x_N) = 0, \forall i \right\}$$

appearing as the zeroes of a polynomial $P \in \mathbb{R}[x_1, \ldots, x_N]$.

In order to have now a full collection of beasts, in all possible dimensions $N \in \mathbb{N}$, and of all possible dimensions $k \in \mathbb{N}$, we must intersect such algebraic hypersurfaces. We are led in this way to the zeroes of families of polynomials, as follows:

DEFINITION 2.5. *An algebraic manifold in $\mathbb{R}^N$ is a space of the form*

$$X = \left\{ (x_1, \ldots, x_N) \in \mathbb{R}^N \Big| P_i(x_1, \ldots, x_N) = 0, \forall i \right\}$$

with $P_i \in \mathbb{R}[x_1, \ldots, x_N]$ being a family of polynomials.

And, good news, this is the good definition, and with the branch of mathematics studying such manifolds being called algebraic geometry. In what follows we will discuss a bit what can be done with this, as a continuation of our previous work on the plane curves, at the elementary level. All this will lead us into the conclusion that we must first develop commutative algebra, and come back to algebraic geometry afterwards.

Let us look now more in detail at the hypersurfaces. We have here:

Theorem 2.6. *The degree 2 hypersurfaces $S\subset\mathbb R^N$, called quadrics, are up to degeneracy and to linear transformations the hypersurfaces of the following form,*

$$\pm x_1^2\pm\ldots\pm x_N^2=0,1$$

and with the sphere being the only compact one.

Proof. We have two statements here, the idea being as follows:

(1) The equations for a quadric $S\subset\mathbb R^N$ are best written as follows, with $A\in M_N(\mathbb R)$ being a matrix, $B\in M_{1\times N}(\mathbb R)$ being a row vector, and $C\in\mathbb R$ being a constant:

$$<Ax,x>+Bx+C=0$$

(2) By doing the linear algebra, or by invoking the theorem of Sylvester on quadratic forms, we are left, modulo linear transformations, with signed sums of squares:

$$\pm x_1^2\pm\ldots\pm x_N^2=0,1$$

(3) To be more precise, with linear algebra, by evenly distributing the terms x_ix_j above and below the diagonal, we can assume that our matrix $A\in M_N(\mathbb R)$ is symmetric. Thus A must be diagonalizable, and by changing the basis of $\mathbb R^N$, as to have it diagonal, our equation becomes as follows, with $D\in M_N(\mathbb R)$ being now diagonal:

$$<Dx,x>+Ex+F=0$$

(4) But now, by making squares in the obvious way, which amounts in applying yet another linear transformation to our quadric, the equation takes the following form, with $G\in M_N(-1,0,1)$ being diagonal, and with $H\in\{0,1\}$ being a constant:

$$<Gx,x>=H$$

(5) Now barring the degenerate cases, we can further assume $G\in M_N(-1,1)$, and we are led in this way to the equation claimed in (2) above, namely:

$$\pm x_1^2\pm\ldots\pm x_N^2=0,1$$

(6) In particular we see that, up to some degenerate cases, namely emptyset and point, the only compact quadric, up to linear transformations, is the one given by:

$$x_1^2+\ldots+x_N^2=1$$

(7) But this is the unit sphere, so are led to the conclusions in the statement. □

As an interesting application now of all this, to linear algebra, we have:

Theorem 2.7. *We have the following results:*

(1) *The invertible matrices $A\in M_N(\mathbb R)$ are dense.*
(2) *The diagonalizable matrices $A\in M_N(\mathbb C)$ are dense.*

PROOF. These results are well-known, and can be proved with some linear algebra work, but we can recover them in a very simple way with geometry, as follows:

(1) We know from basic linear algebra that the non-invertible matrices $A \in M_N(\mathbb{R})$ are precisely those matrices satisfying the following equation:

$$\det(A) = 0$$

But this equation defines a hypersurface in $M_N(\mathbb{R})$, whose complement must be dense. Thus, the invertible matrices $A \in M_N(\mathbb{R})$ are dense, as stated.

(2) We also know from basic linear algebra that a complex matrix $A \in M_N(\mathbb{C})$ with distinct eigenvalues must be diagonalizable. But the complement of these matrices, namely the matrices $A \in M_N(\mathbb{C})$ having multiple eigenvalues, are given by the following equation, with P being the characteristic polynomial, and with Δ being the discriminant:

$$\Delta(P_A) = 0$$

As before, this equation defines a hypersurface in $M_N(\mathbb{C})$, whose complement must be dense. Thus, the diagonalizable matrices $A \in M_N(\mathbb{C})$ are dense, as stated. □

Getting back now to the basics, it is in fact possible to do even more generally, by looking at the algebraic manifolds defined over an arbitrary field F, as follows:

$$X = \left\{(x_1, \ldots, x_N) \in F^N \Big| P_i(x_1, \ldots, x_N) = 0, \forall i\right\}$$

Such ideas are very old, again going back to the ancient Greeks, and there are many things that can be said about algebraic geometry in its "arithmetic" version, over arbitrary fields F as above. In fact, this is a point where algebraic geometry really shines, with many known advanced results in number theory having been obtained in this way.

2b. Commutative algebra

As explained above, in order to better understand our algebraic manifolds, and go beyond what can be done at the elementary level, we are in need of a crash course in abstract algebra in general, and in commutative algebra in particular, with focus on ideals of polynomials. Hang on, many abstract things to follow. But this will be a good investment, useful for topology and for differential geometry too, later in this book.

First in abstract algebra came the groups, defined as follows:

DEFINITION 2.8. *A group is a set G with a multiplication operation $(g, h) \to gh$, which must satisfy the following conditions:*

1. *Associativity: we have $(gh)k = g(hk)$, for any $g, h, k \in G$.*
2. *Unit: there is an element $1 \in G$ such that $g1 = 1g = g$, for any $g \in G$.*
3. *Inverses: for any $g \in G$ there is $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$.*

When the multiplication is commutative, $gh = hg$, we say that G is abelian.

Let us first look at the abelian groups. Here as basic examples we have $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the addition operation $+$. However, we have as well as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and the unit circle $\mathbb{T}$, with the multiplication operation $\times$. In relation with this, observe that we made a choice in Definition 2.8, namely that of privileging the multiplicative notations $gh, 1, g^{-1}$ over of the additive ones $g+h, 0, -g$. More on this choice in a moment.

Still speaking abelian groups, let us look into the finite group case, $|G| < \infty$. Here as basic examples we have the cyclic groups, constructed as follows:

PROPOSITION 2.9. *The following constructions produce the same group, denoted $\mathbb{Z}_N$, which is finite and abelian, and is called cyclic group of order N:*

(1) *$\mathbb{Z}_N$ is the set of remainders modulo N, with operation $+$.*
(2) *$\mathbb{Z}_N \subset \mathbb{T}$ is the group of N-th roots of unity, with operation $\times$.*

PROOF. Here the equivalence between (1) and (2) is obvious. More complicated, however, is the question of finding the good philosophy and notation for this group. In what concerns us, we will be rather geometers, of course, and we will often prefer the interpretation (2). As for the notation, we will use $\mathbb{Z}_N$, which is very natural. □

As a basic thing to be known, about the abelian groups, still in the finite case, we can construct further examples of such groups by making products between various cyclic groups $\mathbb{Z}_N$. Quite remarkably, we obtain in this way all the finite abelian groups:

THEOREM 2.10. *The finite abelian groups are precisely the products of cyclic groups:*

$$G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$$

Moreover, there are technical extensions of this result, going beyond the finite case.

PROOF. This is something quite tricky, the idea being as follows:

(1) In order to prove our result, assume that G is finite and abelian. For any prime number $p \in \mathbb{N}$, let us define $G_p \subset G$ to be the subset of elements having as order a power of p. Equivalently, this subset $G_p \subset G$ can be defined as follows:

$$G_p = \left\{ g \in G \Big| \exists k \in \mathbb{N}, g^{p^k} = 1 \right\}$$

(2) It is then routine to check, based on definitions, that each G_p is a subgroup. Our claim now is that we have a direct product decomposition as follows:

$$G = \prod_p G_p$$

(3) Indeed, by using the fact that our group G is abelian, we have a morphism as follows, with the order of the factors when computing $\prod_p g_p$ being irrelevant:

$$\prod_p G_p \to G \quad , \quad (g_p) \to \prod_p g_p$$

Moreover, it is routine to check that this morphism is both injective and surjective, via some simple manipulations, so we have our group decomposition, as in (2).

(4) Thus, we are left with proving that each component G_p decomposes as a product of cyclic groups, having as orders powers of p, as follows:

$$G_p = \mathbb{Z}_{p^{r_1}} \times \ldots \times \mathbb{Z}_{p^{r_s}}$$

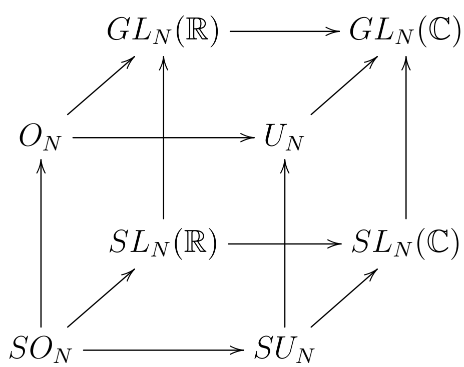
But this is something that can be checked by recurrence on $|G_p|$, via some routine computations, and we are led to the conclusion in the statement.

(5) Finally, for full details on all this, and for some technical extensions to the infinite groups as well, we recommend a solid algebra book, such as Lang [68]. □

Moving forward now, let us look as well into the general, non-abelian case. The first thought goes here to the $N \times N$ matrices with their multiplication, but these do not form a group, because we must assume $\det A \neq 0$ in order for our matrix to be invertible.

So, let us call $GL_N(\mathbb{C})$ the group formed by these latter matrices, with nonzero determinant, with GL standing here for "general linear". By further imposing the condition $\det A = 1$ we obtain a subgroup $SL_N(\mathbb{C})$, with SL standing for "special linear", and then we can talk as well about the real versions of these groups, and also intersect everything with the group of unitary matrices U_N. We obtain in this way 8 groups, as follows:

THEOREM 2.11. *We have groups of invertible matrices as follows,*



with S standing here for "special", meaning having determinant 1.

PROOF. This is clear indeed from the above discussion. As a comment, we can talk in fact about $GL_N(F)$ and $SL_N(F)$, once we have a ground field F, but in what regards the corresponding orthogonal and unitary groups, things here are more complicated. □

There are many other groups of matrices, besides the above ones, as for instance the symplectic groups $Sp_N \subset U_N$, appearing at $N \in 2\mathbb{N}$. Generally speaking, the theory of Lie groups and algebras is in charge with the classification of such beasts.

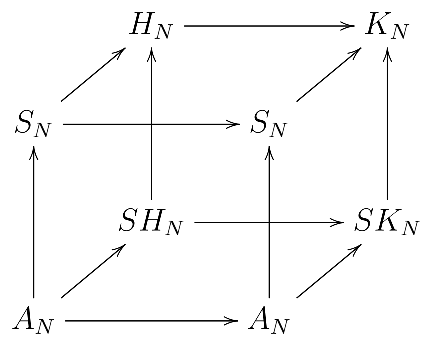
Finally, a word about the finite non-abelian groups. As basic example here you have the symmetric group S_N, and its various subgroups. Let us record here:

PROPOSITION 2.12. *We have finite non-abelian groups, as follows:*
(1) S_N*, the group of permutations of* $\{1,\ldots,N\}$.
(2) $A_N\subset S_N$*, the permutations having signature* 1.
(3) $D_N\subset S_N$*, the group of symmetries of the regular* N*-gon.*

PROOF. The fact that we have indeed groups is clear from definitions, and the non-abelianity of these groups is clear as well, provided of course that in each case N is chosen big enough, and with exercise for you to work out all this, with full details. □

For constructing further examples of finite non-abelian groups, the best is to "look up", by regarding S_N as being the permutation group of the N coordinate axes of $\mathbb R^N$. Indeed, this suggests looking at the symmetry groups of all sorts of geometric beasts inside $\mathbb R^N$, or even $\mathbb C^N$, and we end with a whole menagery of groups, as follows:

THEOREM 2.13. *We have groups of unitary matrices as follows,*



for the most finite, and non-abelian, called complex reflection groups.

PROOF. The above statement is of course something informal, and here are explanations on all this, including definitions for all the groups involved:

(1) To start with, S_N is the symmetric group S_N that we know, but regarded now as permutation group of the N coordinate axes of $\mathbb R^N$, and so as subgroup $S_N\subset O_N$.

(2) Similarly, A_N is the alternating group A_N that we know, but coming now geometrically, as $A_N=S_N\cap SO_N$, with the intersection being computed inside O_N.

(3) Regarding $H_N\subset O_N$, this is a famous group, called hyperoctahedral group, appearing as the symmetry group of the hypercube $\square_N\subset\mathbb R^N$.

(4) Regarding $K_N\subset U_N$, this is the complex analogue of H_N, consisting of the unitary matrices $U\in U_N$ having exactly one nonzero entry, on each row and each column.

(5) We have as well on our diagram the groups SH_N,SK_N, with S standing as usual for "special", that is, consisting of the matrices in H_N,K_N having determinant 1.

(6) In what regards now the diagram itself, sure I can see that S_N, A_N appear twice, but nothing can be done here, after thinking a bit, at how the diagram works.

(7) Let us mention too that the groups $\mathbb{Z}_N, D_N$ have their place here, in N-dimensional geometry, but not exactly on our diagram, as being the symmetry groups of the oriented cycle, and unoriented cycle, with vertices at the simplex $X_N = \{e_i\} \subset \mathbb{R}^N$.

(8) Finally, in what regards finiteness, non-abelianity, and also the name "complex reflection groups", many things to be checked here, left to you as an exercise. □

Very nice all this. Let us summarize this group theory discussion as follows:

Conclusion 2.14. *All groups, or almost, are best seen as being groups of matrices. And even as groups of unitary matrices, in most cases.*

Observe that this justifies our choice in Definition 2.8, for the group operation to be denoted multiplicatively, $\times$. Indeed, in most cases, that is a matrix multiplication.

Moving ahead with more general theory and notions, next in abstract algebra came the rings and ideals, which are more technical objects, defined as follows:

Definition 2.15. *We have notions of rings, modules and ideals, as follows:*

1. *A ring R is a set with operations $+$ and $\times$, satisfying the usual conditions for such operations, except for $ab = ba$, and for $a \neq 0 \implies \exists a^{-1}$.*
2. *A module V over a ring R is a vector space, but we will call it ring, and keep the name vector spaces for the modules over fields, $R = F$.*
3. *An ideal $I \subset R$ is a subgroup with the left ideal property $i \in I, r \in R \implies ir \in I$, or the right ideal property $i \in I, r \in R \implies ri \in I$, or both.*

This was a quite crowded statement, but you get the point, with (1) and (2) we are sort of trying to do field and vector space mathematics, over things which are not necessarily fields and vector spaces over them, and (3) is something technical, non-field specific. At the level of examples, these abound, and we have two important ones, as follows:

(1) The integers form a ring, $R = \mathbb{Z}$, which in addition is commutative, $ab = ba$. As obvious module over $\mathbb{Z}$, we have the lattice $V = \mathbb{Z}^N$. Finally, since $R = \mathbb{Z}$ is commutative, the 3 notions of ideals coincide, and these are the subsets $I = a\mathbb{Z}$, with $a \in \mathbb{Z}$.

(2) The matrices over the integers form a ring, $R = M_N(\mathbb{Z})$, which is noncommutative at $N \geq 1$. As obvious module over $M_N(\mathbb{Z})$, we have the lattice $V = \mathbb{Z}^N$. As for the ideals, things here are a bit more complicated, but since at $N = 2$ the matrices of type $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ form a left ideal which is not a right ideal, and the matrices of type $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ form a right ideal which is not a left ideal, at least we know that our 3 types of ideals make sense.

The question that you surely have in mind is, what are ideals good for? Answer:

PROPOSITION 2.16. *For a subgroup $I \subset R$, the following are equivalent:*

1. *I is a two-sided ideal.*
2. *R/I is a ring.*

PROOF. This is something which requires some thinking, as follows:

(1) Since the additive group $(R, +)$ is abelian, given an additive subgroup $I \subset R$ we can form the quotient group R/I, which is abelian too, with addition as follows:

$$(a + I) + (b + I) = (a + b + I)$$

Observe that the unit is $(0 + I) = I$, and that inverses are given by $(-a + I)$.

(2) The question is now, can we turn this abelian group R/I into a ring? Normally the multiplication can only be as follows, and with this clarifying our statement, with the condition "R/I is a ring" there meaning, with respect to this precise multiplication:

$$(a + I)(b + I) = (ab + I)$$

(3) But, will this work. As a first observation, there is a bit of analogy here with group theory, where $H \subset G$ must be normal in order for G/H to be a group. Thus, our claim is that the ideal condition is somehow the "analogue of normality, in the ring setting".

(4) In practice now, it is quite clear, exactly as in the group theory setting, that everything will be fine, provided that our multiplication is well-defined. And for this multiplication to be well-defined, the following condition must be satisfied:

$$(a + I) = (a' + I)\ ,\ (b + I) = (b' + I) \quad \Longrightarrow \quad (ab + I) = (a'b' + I)$$

But this amounts in the following condition to be satisfied:

$$a - a' \in I\ ,\ b - b' \in I \quad \Longrightarrow \quad ab - a'b' \in I$$

(5) Now comes the math. We have the following identity, which shows that if $I \subset R$ is a two-sided ideal, then the above condition is satisfied, and so done:

$$ab - a'b' = a(b - b') + (a - a')b'$$

(6) Conversely now, if the condition in (4) is satisfied, we have in particular:

$$i - 0 \in I\ ,\ r - r \in I \quad \Longrightarrow \quad ir - 0r \in I$$

$$r - r \in I\ ,\ i - 0 \in I \quad \Longrightarrow \quad ri - r0 \in I$$

Thus $I \subset R$ must be a two-sided ideal, and this finishes the proof. □

Many things can be said about rings, modules and ideals, and we will be back to this soon. For formulating however a theorem on the subject, we have:

THEOREM 2.17. *Assuming that R is commutative and $I \subset R$ is a maximal ideal, in the sense that it is a proper ideal, $I \neq R$, and there is no bigger proper ideal*

$$I \subset J \subset R$$

the quotient ring $F = R/I$ is a field.

PROOF. This is something very standard, the idea being as follows:

(1) Before starting, a quick example. We know that over $R = \mathbb{Z}$, the ideals are the subsets $I = p\mathbb{Z}$ with $p \in \mathbb{N}$. But such an ideal is maximal precisely when p is prime, and this is the same as asking for the quotient ring $R/I = \mathbb{Z}_p$ to be a field.

(2) In general now, assume first that R/I is a field. This means that any nonzero element of R/I is invertible, and with our usual conventions for R/I, this reads:

$$\forall a \notin I \ , \ \exists b \in R \ , \ (ab + I) = (1 + I)$$

Now assume by contradiction that $I \subset R$ is not maximal, so that we have a bigger ideal $I \subset J \subset R$. If we pick $a \in J - I$, we obtain, by the above, the following:

$$a \in J - I \ , \ b \in R \ , \ ab = 1 + i \ , \ i \in I$$

But this is contradictory, because since J is an ideal, containing I, we must have $ab, i \in J$, so we conclude that we have $1 \in J$, and so $J = R$, contradiction.

(3) Conversely, assume now that I is maximal, and assume too, by contradiction, that R/I is not a field. Then we can find a zero divisor in R/I, which reads:

$$(a + I)(b + I) = (I) \ , \ a, b \notin I$$

In other words, we can find $ab \in I$ with $a, b \notin I$. But then, let us look at:

$$I \subset I + aR \subset R$$

(4) What we have in the middle is an ideal, and it is also clear, from $a \notin I$, that the inclusion on the left is proper. As for the inclusion on the right, our claim is that this is proper too. Indeed, assuming otherwise, we would have a formula as follows:

$$i + ac = 1 \ , \ i \in I$$

Now by multiplying everything by b, we obtain from this:

$$ib + acb = b \ , \ i \in I$$

But this is contradictory, because on the left we have $ib \in I$ and $acb = (ab)c \in I$, which gives $b \in I$, contradicting the condition $b \notin I$. Thus, our claim is proved.

(5) But this is the end of the story, because what we just proved is that what we have in (3) is indeed a proper ideal, contradicting the maximality of I, as desired. $\square$

As already mentioned, more on all this in a moment. Going ahead now with our general abstract algebra program, as a third and last batch of objects, we have:

Definition 2.18. *We have notions of fields, vector spaces and algebras, as follows:*

(1) *A field F is a field F as we know them, with in algebra parlance these being the commutative rings R with each nonzero element being invertible.*
(2) *A vector space V over a field F is a vector space as we know them, in algebra parlance these being the modules V over a field F.*
(3) *An algebra A over a field F is a vector space over F, with a ring multiplication operation $\times$, compatible with the vector space structure.*

As previously mentioned, we already know of course about fields, and in what regards the vector spaces, we know about them since ever, and finally, regarding algebras, we know many algebras of functions from analysis. But, thinking well, from a purely algebraic perspective, all these objects have many operations, and this is why they come at last.

As basic examples now, passed the fields F and the vector spaces V that we know well, we are left with finding interesting examples of algebras A. And here the examples abound, with this being actually easy to believe, due to the name "algebras" that algebraists chose for these beasts, and among them, we have two main examples, as follows:

(1) The algebra of polynomials $A = F[X]$. This is a very nice and important algebra, with the extra feature that it is commutative, $PQ = QP$.

(2) The algebra of matrices $A = M_N(F)$. Again this is a very basic example, that we know well, which this time is not commutative, $PQ \neq QP$.

As an illustration for all this, providing us with a third basic class of algebras, and bringing some light too on Theorem 2.17, we have the following basic result:

Theorem 2.19. *Given a compact space X, the following happen:*

(1) *The continuous functions $f : X \to \mathbb{C}$ form a complex algebra $C(X)$.*
(2) *Given $x \in X$, the functions satisfying $f(x) = 0$, form an ideal $I \subset C(X)$.*
(3) *This ideal is maximal, and any maximal ideal $I \subset C(X)$ appears in this way.*
(4) *In this picture, the fact that the quotient is a field, $C(X)/I = \mathbb{C}$, is clear.*

Proof. All this is self-explanatory, the idea being as follows:

(1) This is clear. Observe that our algebra is commutative, $fg = gf$.

(2) This is again clear, because $f(x) = 0$ implies $(fg)(x) = 0$.

(3) This follows from basic topology, via a suitable open cover for X.

(4) This is clear, because $C(X) \to C(X)/I$ maps $f \to f(x) \in \mathbb{C}$. □

2c. Algebraic geometry

Algebraic geometry.

2d. Regular functions

Regular functions.

2e. Exercises

Exercises:

EXERCISE 2.20.

EXERCISE 2.21.

EXERCISE 2.22.

EXERCISE 2.23.

EXERCISE 2.24.

EXERCISE 2.25.

EXERCISE 2.26.

EXERCISE 2.27.

Bonus exercise.

CHAPTER 3

Polynomials, roots

3a. Resultant, discriminant

We have seen that many questions lead us into computing roots of polynomials. Let us start with something that we know well, but is always good to remember:

PROPOSITION 3.1. *The solutions of $ax^2+bx+c=0$ with $a,b,c\in\mathbb C$ are*

$$x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

with the square root of complex numbers being defined as $\sqrt{re^{it}}=\sqrt{r}e^{it/2}$.

PROOF. We can indeed write our equation in the following way:

$$\begin{aligned}ax^2+bx+c=0 &\iff x^2+\frac{b}{a}x+\frac{c}{a}=0\\ &\iff \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}\\ &\iff x+\frac{b}{2a}=\pm\frac{\sqrt{b^2-4ac}}{2a}\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In degree 3 and higher, we would first like to understand what the analogue of the discriminant $\Delta=b^2-4ac$ is. In order to discuss this question, let us start with:

THEOREM 3.2. *Given a monic polynomial $P\in\mathbb C[X]$, factorized as*

$$P=(X-a_1)\ldots(X-a_k)$$

the following happen:

1. *The coefficients of P are symmetric functions in $a_1,\ldots,a_k$.*
2. *The symmetric functions in $a_1,\ldots,a_k$ are polynomials in the coefficients of P.*

PROOF. This is something standard, the idea being as follows:

(1) By expanding our polynomial, we have the following formula:

$$P=\sum_{r=0}^k(-1)^r\sum_{i_1<\ldots<i_r}a_{i_1}\ldots a_{i_r}\cdot X^{k-r}$$

Thus the coefficients of P are, up to some signs, the following functions:

$$f_r = \sum_{i_1<\ldots<i_r} a_{i_1}\ldots a_{i_r}$$

But these are indeed symmetric functions in $a_1,\ldots,a_k$, as claimed.

(2) Conversely now, let us look at the symmetric functions in the roots $a_1,\ldots,a_k$. These appear as linear combinations of the basic symmetric functions, given by:

$$S_r = \sum_i a_i^r$$

Moreover, when allowing polynomials instead of linear combinations, we need in fact only the first k such sums, namely $S_1,\ldots,S_k$. That is, the symmetric functions $\mathcal{F}$ in our variables $a_1,\ldots,a_k$, with integer coefficients, appear as follows:

$$\mathcal{F} = \mathbb{Z}[S_1,\ldots,S_k]$$

(3) The point now is that, alternatively, the symmetric functions in our variables $a_1,\ldots,a_k$ appear as well as linear combinations of the functions f_r that we found in (1), and that when allowing polynomials instead of linear combinations, we need in fact only the first k functions, namely $f_1,\ldots,f_k$. That is, we have as well:

$$\mathcal{F} = \mathbb{Z}[f_1,\ldots,f_k]$$

But this gives the result, because we can pass from $\{S_r\}$ to $\{f_r\}$, and vice versa.

(4) This was for the idea, and in practice now up to you to clarify all the details. In fact, we will also need in what follows the extension of all this to the case where P is no longer assumed to be monic, and with this being, again, exercise for you. $\square$

Getting back now to our original question, namely that of deciding whether two polynomials $P,Q\in\mathbb{C}[X]$ have a common root or not, this has the following nice answer:

THEOREM 3.3. *Given two polynomials $P,Q\in\mathbb{C}[X]$, written as*

$$P = c(X-a_1)\ldots(X-a_k)\quad,\quad Q = d(X-b_1)\ldots(X-b_l)$$

the following quantity, which is called resultant of P,Q,

$$R(P,Q) = c^l d^k \prod_{ij}(a_i-b_j)$$

is a certain polynomial in the coefficients of P,Q, with integer coefficients, and we have $R(P,Q)=0$ precisely when P,Q have a common root.

PROOF. This is something quite tricky, the idea being as follows:

(1) Given two polynomials $P, Q \in \mathbb{C}[X]$, we can certainly construct the quantity $R(P,Q)$ in the statement, with the role of the normalization factor $c^l d^k$ to become clear later on, and then we have $R(P,Q) = 0$ precisely when P, Q have a common root:

$$R(P,Q) = 0 \iff \exists i, j, a_i = b_j$$

(2) As bad news, however, this quantity $R(P,Q)$, defined in this way, is a priori not very useful in practice, because it depends on the roots a_i, b_j of our polynomials P, Q, that we cannot compute in general. However, and here comes our point, as we will prove below, it turns out that $R(P,Q)$ is in fact a polynomial in the coefficients of P, Q, with integer coefficients, and this is where the power of $R(P,Q)$ comes from.

(3) You might perhaps say, nice, but why not doing things the other way around, that is, formulating our theorem with the explicit formula of $R(P,Q)$, in terms of the coefficients of P, Q, and then proving that we have $R(P,Q) = 0$, via roots and everything. Good point, but this is not exactly obvious, the formula of $R(P,Q)$ in terms of the coefficients of P, Q being something terribly complicated. In short, trust me, let us prove our theorem as stated, and for alternative formulae of $R(P,Q)$, we will see later.

(4) Getting started now, let us expand the formula of $R(P,Q)$, by making all the multiplications there, abstractly, in our head. Everything being symmetric in $a_1, \ldots, a_k$, we obtain in this way certain symmetric functions in these variables, which will be therefore certain polynomials in the coefficients of P. Moreover, due to our normalization factor c^l, these polynomials in the coefficients of P will have integer coefficients.

(5) With this done, let us look now what happens with respect to the remaining variables $b_1, \ldots, b_l$, which are the roots of Q. Once again what we have here are certain symmetric functions in these variables $b_1, \ldots, b_l$, and these symmetric functions must be certain polynomials in the coefficients of Q. Moreover, due to our normalization factor d^k, these polynomials in the coefficients of Q will have integer coefficients.

(6) Thus, we are led to the conclusion in the statement, that $R(P,Q)$ is a polynomial in the coefficients of P, Q, with integer coefficients, and with the remark that the $c^l d^k$ factor is there for these latter coefficients to be indeed integers, instead of rationals. □

All the above might seem a bit complicated, so as an illustration, let us work out an example. Consider the case of a polynomial of degree 2, and a polynomial of degree 1:

$$P = ax^2 + bx + c \quad , \quad Q = dx + e$$

In order to compute the resultant, let us factorize our polynomials:

$$P = a(x-p)(x-q) \quad , \quad Q = d(x-r)$$

The resultant can be then computed as follows, by using the method above:

$$\begin{aligned} R(P,Q) &= ad^2(p-r)(q-r) \\ &= ad^2(pq-(p+q)r+r^2) \\ &= cd^2+bd^2r+ad^2r^2 \\ &= cd^2-bde+ae^2 \end{aligned}$$

Finally, observe that $R(P,Q)=0$ corresponds indeed to the fact that P,Q have a common root. Indeed, the root of Q is $r=-e/d$, and we have:

$$P(r)=\frac{ae^2}{d^2}-\frac{be}{d}+c=\frac{R(P,Q)}{d^2}$$

Regarding now the explicit formula of the resultant $R(P,Q)$, this is something quite complicated, and there are several methods for dealing with this problem. We have:

Theorem 3.4. *The resultant of two polynomials, written as*

$$P=p_kX^k+\ldots+p_1X+p_0\quad,\quad Q=q_lX^l+\ldots+q_1X+q_0$$

appears as the determinant of an associated matrix, as follows,

$$R(P,Q)=\begin{vmatrix} p_k & & & q_l & & \\ \vdots & \ddots & & \vdots & \ddots & \\ p_0 & & p_k & q_0 & & q_k \\ & \ddots & \vdots & & \ddots & \vdots \\ & & p_0 & & & q_0 \end{vmatrix}$$

with the matrix having size $k+l$, and having 0 coefficients at the blank spaces.

Proof. This is something clever, due to Sylvester, as follows:

(1) Consider the vector space $\mathbb{C}_k[X]$ formed by the polynomials of degree $<k$:

$$\mathbb{C}_k[X]=\left\{P\in\mathbb{C}[X]\Big|\deg P<k\right\}$$

This is a vector space of dimension k, having as basis the monomials $1,X,\ldots,X^{k-1}$. Now given polynomials P,Q as in the statement, consider the following linear map:

$$\Phi:\mathbb{C}_l[X]\times\mathbb{C}_k[X]\to\mathbb{C}_{k+l}[X]\quad,\quad(A,B)\to AP+BQ$$

(2) Our first claim is that with respect to the standard bases for all the vector spaces involved, namely those consisting of the monomials $1,X,X^2,\ldots$, the matrix of Φ is the matrix in the statement. But this is something which is clear from definitions.

(3) Our second claim is that $\det\Phi=0$ happens precisely when P,Q have a common root. Indeed, our polynomials P,Q having a common root means that we can find A,B such that $AP+BQ=0$, and so that $(A,B)\in\ker\Phi$, which reads $\det\Phi=0$.

(4) Finally, our claim is that we have $\det\Phi = R(P,Q)$. But this follows from the uniqueness of the resultant, up to a scalar, and with this uniqueness property being elementary to establish, along the lines of the proofs of Theorems 3.2 and 3.3. □

In what follows we will not really need the above formula, so let us just check now that this formula works indeed. Consider our favorite polynomials, as before:

$$P = ax^2 + bx + c \quad , \quad Q = dx + e$$

According to the above result, the resultant should be then, as it should:

$$R(P,Q) = \begin{vmatrix} a & d & 0 \\ b & e & d \\ c & 0 & e \end{vmatrix} = ae^2 - bde + cd^2$$

We can go back now to our original question, and we have:

THEOREM 3.5. *Given a polynomial $P \in \mathbb{C}[X]$, written as*

$$P(X) = aX^N + bX^{N-1} + cX^{N-2} + \ldots$$

its discriminant, defined as being the following quantity,

$$\Delta(P) = \frac{(-1)^{\binom{N}{2}}}{a} R(P,P')$$

is a polynomial in the coefficients of P, with integer coefficients, and $\Delta(P) = 0$ happens precisely when P has a double root.

PROOF. The fact that the discriminant $\Delta(P)$ is a polynomial in the coefficients of P, with integer coefficients, comes from Theorem 3.3, coupled with the fact that the division by the leading coefficient a is indeed possible, under $\mathbb{Z}$, as being shown by the following formula, which is written of course a bit informally, coming from Theorem 3.4:

$$R(P,P') = \begin{vmatrix} a & & & Na & & \\ \vdots & \ddots & & \vdots & \ddots & \\ z & & a & y & & Na \\ & \ddots & \vdots & & \ddots & \vdots \\ & & z & & & y \end{vmatrix}$$

Also, the fact that we have $\Delta(P) = 0$ precisely when P has a double root is clear from Theorem 3.3. Finally, let us mention that the sign $(-1)^{\binom{N}{2}}$ is there for various reasons, including the compatibility with some well-known formulae, at small values of $N \in \mathbb{N}$, such as $\Delta(P) = b^2 - 4ac$ in degree 2, that we will discuss in a moment. □

As already mentioned, by using Theorem 3.4, we have an explicit formula for the discriminant, as the determinant of a certain matrix. There is a lot of theory here, and in order to get into this, let us first see what happens in degree 2. Here we have:

$$P = aX^2 + bX + c \quad , \quad P' = 2aX + b$$

Thus, the resultant is given by the following formula:

$$\begin{aligned} R(P, P') &= ab^2 - b(2a)b + c(2a)^2 \\ &= 4a^2c - ab^2 \\ &= -a(b^2 - 4ac) \end{aligned}$$

It follows that the discriminant of our polynomial is, as it should:

$$\Delta(P) = b^2 - 4ac$$

Alternatively, we can use the formula in Theorem 3.4, and we obtain:

$$\begin{aligned} \Delta(P) = &= -\frac{1}{a}\begin{vmatrix} a & 2a & \\ b & b & 2a \\ c & & b \end{vmatrix} \\ &= -\begin{vmatrix} 1 & 2 & \\ b & b & 2a \\ c & & b \end{vmatrix} \\ &= -b^2 + 2(b^2 - 2ac) \\ &= b^2 - 4ac \end{aligned}$$

We will be back later to such formulae, in degree 3, and in degree 4 as well, with the comment however, coming in advance, that these formulae are not very beautiful.

At the theoretical level now, we have the following result, which is not trivial:

THEOREM 3.6. *The discriminant of a polynomial P is given by the formula*

$$\Delta(P) = a^{2N-2} \prod_{i<j} (r_i - r_j)^2$$

where a is the leading coefficient, and $r_1, \ldots, r_N$ are the roots.

PROOF. This is something quite tricky, the idea being as follows:

(1) The first thought goes to the formula in Theorem 3.3, so let us see what that formula teaches us, in the case $Q = P'$. Let us write P, P' as follows:

$$P = a(x - r_1) \ldots (x - r_N)$$

$$P' = Na(x - p_1) \ldots (x - p_{N-1})$$

According to Theorem 3.3, the resultant of P,P' is then given by:

$$R(P,P')=a^{N-1}(Na)^N\prod_{ij}(r_i-p_j)$$

And bad news, this is not exactly what we wished for, namely the formula in the statement. That is, we are on the good way, but certainly have to work some more.

(2) Obviously, we must get rid of the roots $p_1,\ldots,p_{N-1}$ of the polynomial P'. In order to do this, let us rewrite the formula that we found in (1) in the following way:

$$\begin{aligned}R(P,P') &= N^Na^{2N-1}\prod_i\left(\prod_j(r_i-p_j)\right)\\ &= N^Na^{2N-1}\prod_i\frac{P'(r_i)}{Na}\\ &= a^{N-1}\prod_iP'(r_i)\end{aligned}$$

(3) In order to compute now P', and more specifically the values $P'(r_i)$ that we are interested in, we can use the Leibnitz rule. So, consider our polynomial:

$$P(x)=a(x-r_1)\ldots(x-r_N)$$

The Leibnitz rule for derivatives tells us that $(fg)'=f'g+fg'$, but then also that $(fgh)'=f'gh+fg'h+fgh'$, and so on. Thus, for our polynomial, we obtain:

$$P'(x)=a\sum_i(x-r_1)\ldots\underbrace{(x-r_i)}_{missing}\ldots(x-r_N)$$

Now when applying this formula to one of the roots r_i, we obtain:

$$P'(r_i)=a(r_i-r_1)\ldots\underbrace{(r_i-r_i)}_{missing}\ldots(r_i-r_N)$$

By making now the product over all indices i, this gives the following formula:

$$\prod_iP'(r_i)=a^N\prod_{i\neq j}(r_i-r_j)$$

(4) Time now to put everything together. By taking the formula in (2), making the normalizations in Theorem 3.5, and then using the formula found in (3), we obtain:

$$\begin{aligned}\Delta(P) &= (-1)^{\binom{N}{2}}a^{N-2}\prod_iP'(r_i)\\ &= (-1)^{\binom{N}{2}}a^{2N-2}\prod_{i\neq j}(r_i-r_j)\end{aligned}$$

(5) This is already a nice formula, which is very useful in practice, and that we can safely keep as a conclusion, to our computations. However, we can do slightly better, by grouping opposite terms. Indeed, this gives the following formula:

$$\begin{aligned}\Delta(P) &= (-1)^{\binom{N}{2}} a^{2N-2} \prod_{i\neq j}(r_i - r_j)\\ &= (-1)^{\binom{N}{2}} a^{2N-2} \prod_{i<j}(r_i - r_j) \cdot \prod_{i>j}(r_i - r_j)\\ &= (-1)^{\binom{N}{2}} a^{2N-2} \prod_{i<j}(r_i - r_j) \cdot (-1)^{\binom{N}{2}} \prod_{i<j}(r_i - r_j)\\ &= a^{2N-2} \prod_{i<j}(r_i - r_j)^2\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

As applications now, the formula in Theorem 3.6 is quite useful for the real polynomials $P \in \mathbb{R}[X]$ in small degree, because it allows to say when the roots are real, or complex, or at least have some partial information about this. For instance, we have:

PROPOSITION 3.7. *Consider a polynomial with real coefficients, $P \in \mathbb{R}[X]$, assumed for simplicity to have nonzero discriminant, $\Delta \neq 0$.*

(1) *In degree 2, the roots are real when $\Delta > 0$, and complex when $\Delta < 0$.*
(2) *In degree 3, all roots are real precisely when $\Delta > 0$.*

PROOF. This is very standard, the idea being as follows:

(1) The first assertion is something that we certainly know, coming from Proposition 3.1, but let us see how this comes via the formula in Theorem 3.6, namely:

$$\Delta(P) = a^{2N-2} \prod_{i<j}(r_i - r_j)^2$$

In degree $N = 2$, this formula looks as follows, with r_1, r_2 being the roots:

$$\Delta(P) = a^2(r_1 - r_2)^2$$

Thus $\Delta > 0$ amounts in saying that we have $(r_1 - r_2)^2 > 0$. Now since r_1, r_2 are conjugate, and with this being something trivial, meaning no need here for the computations in Proposition 3.1, we conclude that $\Delta > 0$ means that r_1, r_2 are real, as stated.

(2) In degree $N = 3$ now, we know from analysis that P has at least one real root, and the problem is whether the remaining 2 roots are real, or complex conjugate. For this purpose, we can use the formula in Theorem 3.6, which in degree 3 reads:

$$\Delta(P) = a^4(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$$

We can see that in the case $r_1, r_2, r_3 \in \mathbb{R}$, we have $\Delta(P) > 0$. Conversely now, assume that $r_1 = r$ is the real root, coming from analysis, and that the other roots are $r_2 = z$ and $r_3 = \bar{z}$, with z being a complex number, which is not real. We have then:

$$\begin{aligned}\Delta(P) &= a^4(r-z)^2(r-\bar{z})^2(z-\bar{z})^2\\ &= a^4|r-z|^4(2iIm(z))^2\\ &= -4a^4|r-z|^4Im(z)^2\\ &< 0\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In relation with the above, for our result to be truly useful, we must of course compute the discriminant in degree 3. We will do this in the next section.

Finally, as another application of all this, worth mentioning, we have:

THEOREM 3.8. *The diagonalizable matrices are dense.*

PROOF. As a first observation, this is something extremely useful, more or less allowing you in practice to assume that any matrix $A \in M_N(\mathbb{C})$ is diagonalizable, but of course do not try this at home, unless you know what you're doing. As for the proof, this is non-trivial, and there are actually two standard proofs, both non-trivial, as follows:

(1) Via the pedestrian way, by using the Jordan form. Here you have to learn well the Jordan form, and good luck with that, and once that done, you can argue that by perturbing the Jordan blocks, in the obvious way, you can arrange up to epsilon as for your matrix to have distinct eigenvalues, and so to be diagonalizable.

(2) As a geometry king, using the discriminant. Indeed, for a matrix $A \in M_N(\mathbb{C})$, with characteristic polynomial P_A, having distinct eigenvalues means:

$$\Delta(P_A) \neq 0$$

But this is the complement of a hypersurface, which is dense, and since all these matrices are diagonalizable, the diagonalizable matrices are dense too. Just like that. □

3b. Cardano formula

Let us work out now what happens in degree 3. Here the result is as follows:

THEOREM 3.9. *The discriminant of a degree 3 polynomial,*

$$P = aX^3 + bX^2 + cX + d$$

is the number $\Delta(P) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$.

PROOF. We have two methods available, based on Theorem 3.3 and Theorem 3.4, and both being instructive, we will try them both. The computations are as follows:

(1) Let us first go the pedestrian way, based on the definition of the resultant, from Theorem 3.3. Consider two polynomials, of degree 3 and degree 2, written as follows:

$$P = aX^3 + bX^2 + cX + d$$

$$Q = eX^2 + fX + g = e(X-s)(X-t)$$

The resultant of these two polynomials is then given by:

$$\begin{aligned} R(P,Q) &= a^2e^3(p-s)(p-t)(q-s)(q-t)(r-s)(r-t) \\ &= a^2 \cdot e(p-s)(p-t) \cdot e(q-s)(q-t) \cdot e(r-s)(r-t) \\ &= a^2Q(p)Q(q)Q(r) \\ &= a^2(ep^2+fp+g)(eq^2+fq+g)(er^2+fr+g) \end{aligned}$$

By expanding, we obtain the following formula for this resultant:

$$\begin{aligned} \frac{R(P,Q)}{a^2} &= e^3p^2q^2r^2 + e^2f(p^2q^2r + p^2qr^2 + pq^2r^2) \\ &+ e^2g(p^2q^2 + p^2r^2 + q^2r^2) + ef^2(p^2qr + pq^2r + pqr^2) \\ &+ efg(p^2q + pq^2 + p^2r + pr^2 + q^2r + qr^2) + f^3pqr \\ &+ eg^2(p^2 + q^2 + r^2) + f^2g(pq + pr + qr) \\ &+ fg^2(p + q + r) + g^3 \end{aligned}$$

Note in passing that we have 27 terms on the right, as we should, and with this kind of check being mandatory, when doing such computations. Next, we have:

$$p+q+r = -\frac{b}{a} \quad , \quad pq+pr+qr = \frac{c}{a} \quad , \quad pqr = -\frac{d}{a}$$

By using these formulae, we can produce some more, as follows:

$$p^2+q^2+r^2 = (p+q+r)^2 - 2(pq+pr+qr) = \frac{b^2}{a^2} - \frac{2c}{a}$$

$$p^2q + pq^2 + p^2r + pr^2 + q^2r + qr^2 = (p+q+r)(pq+pr+qr) - 3pqr = -\frac{bc}{a^2} + \frac{3d}{a}$$

$$p^2q^2 + p^2r^2 + q^2r^2 = (pq+pr+qr)^2 - 2pqr(p+q+r) = \frac{c^2}{a^2} - \frac{2bd}{a^2}$$

By plugging now this data into the formula of $R(P,Q)$, we obtain:

$$\begin{aligned}R(P,Q) &= a^2e^3\cdot\frac{d^2}{a^2}-a^2e^2f\cdot\frac{cd}{a^2}+a^2e^2g\left(\frac{c^2}{a^2}-\frac{2bd}{a^2}\right)+a^2ef^2\cdot\frac{bd}{a^2}\\ &+ a^2efg\left(-\frac{bc}{a^2}+\frac{3d}{a}\right)-a^2f^3\cdot\frac{d}{a}\\ &+ a^2eg^2\left(\frac{b^2}{a^2}-\frac{2c}{a}\right)+a^2f^2g\cdot\frac{c}{a}-a^2fg^2\cdot\frac{b}{a}+a^2g^3\end{aligned}$$

Thus, we have the following formula for the resultant:

$$\begin{aligned}R(P,Q) &= d^2e^3-cde^2f+c^2e^2g-2bde^2g+bdef^2-bcefg+3adefg\\ &- adf^3+b^2eg^2-2aceg^2+acf^2g-abfg^2+a^2g^3\end{aligned}$$

Getting back now to our discriminant problem, with $Q=P'$, which corresponds to $e=3a$, $f=2b$, $g=c$, we obtain the following formula:

$$\begin{aligned}R(P,P') &= 27a^3d^2-18a^2bcd+9a^2c^3-18a^2bcd+12ab^3d-6ab^2c^2+18a^2bcd\\ &- 8ab^3d+3ab^2c^2-6a^2c^3+4ab^2c^2-2ab^2c^2+a^2c^3\end{aligned}$$

By simplifying terms, and dividing by a, we obtain the following formula:

$$-\Delta(P)=27a^2d^2-18abcd+4ac^3+4b^3d-b^2c^2$$

But this gives the formula in the statement, namely:

$$\Delta(P)=b^2c^2-4ac^3-4b^3d-27a^2d^2+18abcd$$

(2) Let us see as well how the computation does, by using Theorem 3.4, which is our most advanced tool, so far. Consider a polynomial of degree 3, and its derivative:

$$P=aX^3+bX^2+cX+d$$

$$P'=3aX^2+2bX+c$$

By using now Theorem 3.4 and computing the determinant, we obtain:

$$\begin{aligned}
R(P,P') &= \begin{vmatrix} a & & 3a & & \\ b & a & 2b & 3a & \\ c & b & c & 2b & 3a \\ d & c & & c & 2b \\ & d & & & c \end{vmatrix} \\
&= \begin{vmatrix} a & & & & \\ b & a & -b & 3a & \\ c & b & -2c & 2b & 3a \\ d & c & -3d & c & 2b \\ & d & & & c \end{vmatrix} \\
&= a\begin{vmatrix} a & -b & 3a & \\ b & -2c & 2b & 3a \\ c & -3d & c & 2b \\ d & & & c \end{vmatrix} \\
&= -ad\begin{vmatrix} -b & 3a & \\ -2c & 2b & 3a \\ -3d & c & 2b \end{vmatrix} + ac\begin{vmatrix} a & -b & 3a \\ b & -2c & 2b \\ c & -3d & c \end{vmatrix} \\
&= -ad(-4b^3-27a^2d+12abc+3abc) \\
&\quad +ac(-2ac^2-2b^2c-9abd+6ac^2+b^2c+6abd) \\
&= a(4b^3d+27a^2d^2-15abcd+4ac^3-b^2c^2-3abcd) \\
&= a(4b^3d+27a^2d^2-18abcd+4ac^3-b^2c^2)
\end{aligned}$$

Now according to Theorem 3.5, the discriminant of our polynomial is given by:

$$\begin{aligned}
\Delta(P) &= -\frac{R(P,P')}{a} \\
&= -4b^3d-27a^2d^2+18abcd-4ac^3+b^2c^2 \\
&= b^2c^2-4ac^3-4b^3d-27a^2d^2+18abcd
\end{aligned}$$

Thus, we have again obtained the formula in the statement. □

Still talking degree 3 equations, let us try now to solve such an equation $P=0$, with $P=aX^3+bX^2+cX+d$ as above. By linear transformations we can assume $a=1,b=0$, and then it is convenient to write $c=3p,d=2q$. Thus, our equation becomes:

$$x^3+3px+2q=0$$

Regarding such equations, many things can be said, and to start with, we have the following famous result, dealing with real roots, due to Cardano:

Theorem 3.10. *For a normalized degree* 3 *equation, namely*

$$x^3 + 3px + 2q = 0$$

the discriminant is $\Delta = -108(p^3 + q^2)$. *Assuming* $p, q \in \mathbb{R}$ *and* $\Delta < 0$, *the number*

$$x = \sqrt[3]{-q + \sqrt{p^3 + q^2}} + \sqrt[3]{-q - \sqrt{p^3 + q^2}}$$

is a real solution of our equation.

Proof. The formula of Δ is clear from definitions, and with $108 = 4 \times 27$. Now with x as in the statement, by using $(a+b)^3 = a^3 + b^3 + 3ab(a+b)$, we have:

$$\begin{aligned} x^3 &= \left(\sqrt[3]{-q + \sqrt{p^3 + q^2}} + \sqrt[3]{-q - \sqrt{p^3 + q^2}}\right)^3 \\ &= -2q + 3\sqrt[3]{-q + \sqrt{p^3 + q^2}} \cdot \sqrt[3]{-q - \sqrt{p^3 + q^2}} \cdot x \\ &= -2q + 3\sqrt[3]{q^2 - p^3 - q^2} \cdot x \\ &= -2q - 3px \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Regarding the other roots, we know from Proposition 3.7 that these are both real when $\Delta < 0$, and complex conjugate when $\Delta < 0$. Thus, in the context of Theorem 3.10, the other two roots are complex conjugate, the formula for them being as follows:

Proposition 3.11. *For a normalized degree* 3 *equation, namely*

$$x^3 + 3px + 2q = 0$$

with $p, q \in \mathbb{R}$ *and discriminant* $\Delta = -108(p^3 + q^2)$ *negative,* $\Delta < 0$, *the numbers*

$$z = w\sqrt[3]{-q + \sqrt{p^3 + q^2}} + w^2\sqrt[3]{-q - \sqrt{p^3 + q^2}}$$

$$\bar{z} = w^2\sqrt[3]{-q + \sqrt{p^3 + q^2}} + w\sqrt[3]{-q - \sqrt{p^3 + q^2}}$$

with $w = e^{2\pi i/3}$ *are the complex conjugate solutions of our equation.*

Proof. As before, by using $(a+b)^3 = a^3 + b^3 + 3ab(a+b)$, we have:

$$\begin{aligned} z^3 &= \left(w\sqrt[3]{-q + \sqrt{p^3 + q^2}} + w^2\sqrt[3]{-q - \sqrt{p^3 + q^2}}\right)^3 \\ &= -2q + 3\sqrt[3]{-q + \sqrt{p^3 + q^2}} \cdot \sqrt[3]{-q - \sqrt{p^3 + q^2}} \cdot z \\ &= -2q + 3\sqrt[3]{q^2 - p^3 - q^2} \cdot z \\ &= -2q - 3pz \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

As a conclusion, we have the following statement, unifying the above:

THEOREM 3.12. *For a normalized degree* 3 *equation, namely*

$$x^3 + 3px + 2q = 0$$

the discriminant is $\Delta = -108(p^3 + q^2)$. *Assuming* $p, q \in \mathbb{R}$ *and* $\Delta < 0$, *the numbers*

$$x = w\sqrt[3]{-q + \sqrt{p^3 + q^2}} + w^2\sqrt[3]{-q - \sqrt{p^3 + q^2}}$$

with $w = 1, e^{2\pi i/3}, e^{4\pi i/3}$ *are the solutions of our equation.*

PROOF. This follows indeed from Theorem 3.10 and Proposition 3.11. Alternatively, we can redo the computation in their proof, which was nearly identical anyway, in the present setting, with x being given by the above formula, by using $w^3 = 1$. $\square$

As a comment here, the formula in Theorem 3.12 holds of course in the case $\Delta > 0$ too, and also when the coefficients are complex numbers, $p, q \in \mathbb{C}$, and this due to the fact that the proof rests on the nearly trivial computation from the proof of Theorem 3.10, or of Proposition 3.11. However, these extensions are quite often not very useful, because when it comes to extract all the above square and cubic roots, for complex numbers, you can well end up with the initial question, the one that you started with.

Thus, as a conclusion to this, Theorem 3.12 as formulated above is what can be best said about the degree 3 equations. There are of course many versions of it, and slight generalizations, but in practice, Theorem 3.12 is what mostly matters.

3c. Higher degree

In higher degree things become quite complicated. In degree 4, to start with, we first have the following result, dealing with the discriminant and its applications:

THEOREM 3.13. *The discriminant of* $P = ax^4 + bx^3 + cx^2 + dx + e$ *is given by the following formula:*

$$\begin{aligned}\Delta &= 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e - 27a^2d^4\\ &\quad +144ab^2ce^2 - 6ab^2d^2e - 80abc^2de + 18abcd^3 + 16ac^4e\\ &\quad -4ac^3d^2 - 27b^4e^2 + 18b^3cde - 4b^3d^3 - 4b^2c^3e + b^2c^2d^2\end{aligned}$$

In the case $\Delta < 0$ *we have* 2 *real roots and* 2 *complex conjugate roots, and in the case* $\Delta > 0$ *the roots are either all real or all complex.*

PROOF. The formula of Δ follows from the definition of the discriminant, from Theorem 3.5, with the resultant computed via Theorem 3.4, as follows:

$$\Delta=\frac{1}{a}\begin{vmatrix} a&&&4a&&&\\ b&a&&3b&4a&&\\ c&b&a&2c&3b&4a&\\ d&c&b&d&2c&3b&4a\\ e&d&c&&d&2c&3b\\ &e&d&&&d&2c\\ &&e&&&&d \end{vmatrix}$$

As for the last assertion, the study here is routine, a bit as in degree 3. □

In practice, as in degree 3, we can do first some manipulations on our polynomials, as to have them in simpler form, and we have the following version of Theorem 3.13:

PROPOSITION 3.14. *The discriminant of $P=x^4+cx^2+dx+e$, normalized degree 4 polynomial, is given by the following formula:*

$$\Delta=16c^4e-4c^3d^2-128c^2e^2+144cd^2e-27d^4+256e^3$$

As before, if $\Delta<0$ we have 2 real roots and 2 complex conjugate roots, and if $\Delta>0$ the roots are either all real or all complex.

PROOF. This is a consequence of Theorem 3.13, with $a=1,b=0$, but we can deduce this as well directly. Indeed, the formula of Δ follows, quite easily, from:

$$\Delta=\begin{vmatrix} 1&&&4&&&\\ &1&&&4&&\\ c&&1&2c&&4&\\ d&c&&d&2c&&4\\ e&d&c&&d&2c&\\ &e&d&&&d&2c\\ &&e&&&&d \end{vmatrix}$$

As for the last assertion, this is something that we know, from Theorem 3.13. □

We still have some work to do. Indeed, looking back at what we did in degree 3, the passage there from Theorem 3.9 to Theorem 3.10 was made of two operations, namely "depressing" the equation, that is, getting rid of the next-to-highest term, and then rescaling the coefficients, as for the formula of Δ to become as simple as possible.

In our present setting now, degree 4, with the depressing done as above, in Proposition 3.14, it remains to rescale the coefficients, as for the formula of Δ to become as simple as possible. And here, a bit of formula hunting, in relation with $2,3$ powers, leads to:

THEOREM 3.15. *The discriminant of a normalized degree 4 polynomial, written as*

$$P = x^4 + 6px^2 + 4qx + 3r$$

is given by the following formula:

$$\Delta = 256 \times 27 \times \left(9p^4r - 2p^3q^2 - 6p^2r^2 + 6pq^2r - q^4 + r^3\right)$$

In the case $\Delta < 0$ we have 2 real roots and 2 complex conjugate roots, and in the case $\Delta > 0$ the roots are either all real or all complex.

PROOF. This follows from Proposition 3.14, with $c = 6p, d = 4q, e = 3r$, but we can deduce this as well directly. Indeed, the formula of Δ follows, quite easily, from:

$$\Delta = \begin{vmatrix} 1 & & & 4 & & & \\ & 1 & & & 4 & & \\ 6p & & 1 & 12p & & 4 & \\ 4q & 6p & & 4q & 12p & & 4 \\ 3r & 4q & 6p & & 4q & 12p & \\ & 3r & 4q & & & 4q & 12p \\ & & 3r & & & & 4q \end{vmatrix}$$

As for the last assertion, this is something that we know from Theorem 3.13. □

Time now to get to the real thing, solving the equation. We have here:

THEOREM 3.16. *The roots of a normalized degree 4 equation, written as*

$$x^4 + 6px^2 + 4qx + 3r = 0$$

are as follows, with y satisfying the equation $(y^2 - 3r)(y - 3p) = 2q^2$,

$$x_1 = \frac{1}{\sqrt{2}}\left(-\sqrt{y - 3p} + \sqrt{-y - 3p + \frac{4q}{\sqrt{2y - 6p}}}\right)$$

$$x_2 = \frac{1}{\sqrt{2}}\left(-\sqrt{y - 3p} - \sqrt{-y - 3p + \frac{4q}{\sqrt{2y - 6p}}}\right)$$

$$x_3 = \frac{1}{\sqrt{2}}\left(\sqrt{y - 3p} + \sqrt{-y - 3p - \frac{4q}{\sqrt{2y - 6p}}}\right)$$

$$x_4 = \frac{1}{\sqrt{2}}\left(\sqrt{y - 3p} - \sqrt{-y - 3p - \frac{4q}{\sqrt{2y - 6p}}}\right)$$

and with y being computable via the Cardano formula.

Proof. This is something quite tricky, the idea being as follows:

(1) To start with, let us write our equation in the following form:

$$x^4 = -6px^2 - 4qx - 3r$$

The idea will be that of adding a suitable common term, to both sides, as to make square on both sides, as to eventually end with a sort of double quadratic equation. For this purpose, our claim is that what we need is a number y satisfying:

$$(y^2 - 3r)(y - 3p) = 2q^2$$

Indeed, assuming that we have this number y, our equation becomes:

$$\begin{aligned}
(x^2+y)^2 &= x^4 + 2x^2y + y^2\\
&= -6px^2 - 4qx - 3r + 2x^2y + y^2\\
&= (2y-6p)x^2 - 4qx + y^2 - 3r\\
&= (2y-6p)x^2 - 4qx + \frac{2q^2}{y-3p}\\
&= \left(\sqrt{2y-6p}\cdot x - \frac{2q}{\sqrt{2y-6p}}\right)^2
\end{aligned}$$

(2) Which looks very good, leading us to the following degree 2 equations:

$$x^2 + y + \sqrt{2y-6p}\cdot x - \frac{2q}{\sqrt{2y-6p}} = 0$$

$$x^2 + y - \sqrt{2y-6p}\cdot x + \frac{2q}{\sqrt{2y-6p}} = 0$$

Now let us write these two degree 2 equations in standard form, as follows:

$$x^2 + \sqrt{2y-6p}\cdot x + \left(y - \frac{2q}{\sqrt{2y-6p}}\right) = 0$$

$$x^2 - \sqrt{2y-6p}\cdot x + \left(y + \frac{2q}{\sqrt{2y-6p}}\right) = 0$$

(3) Regarding the first equation, the solutions there are as follows:

$$x_1 = \frac{1}{2}\left(-\sqrt{2y-6p} + \sqrt{-2y - 6p + \frac{8q}{\sqrt{2y-6p}}}\right)$$

$$x_2 = \frac{1}{2}\left(-\sqrt{2y-6p} - \sqrt{-2y - 6p + \frac{8q}{\sqrt{2y-6p}}}\right)$$

As for the second equation, the solutions there are as follows:

$$x_3 = \frac{1}{2}\left(\sqrt{2y-6p} + \sqrt{-2y-6p-\frac{8q}{\sqrt{2y-6p}}}\right)$$

$$x_4 = \frac{1}{2}\left(\sqrt{2y-6p} - \sqrt{-2y-6p-\frac{8q}{\sqrt{2y-6p}}}\right)$$

(4) Now by cutting a $\sqrt{2}$ factor from everything, this gives the formulae in the statement. As for the last claim, regarding the nature of y, this comes from Cardano. □

We still have to compute the number y appearing in the above via Cardano, and the result here, adding to what we already have in Theorem 3.16, is as follows:

THEOREM 3.17 (continuation). *The value of y in the previous theorem is*

$$y = t + p + \frac{a}{t}$$

where the number t is given by the formula

$$t = \sqrt[3]{b + \sqrt{b^2 - a^3}}$$

with $a = p^2 + r$ and $b = 2p^2 - 3pr + q^2$.

PROOF. The legend goes that this is what comes from Cardano, but depressing and normalizing and solving $(y^2-3r)(y-3p) = 2q^2$ makes it for too many operations, so the most pragmatic is to simply check this equation. With y as above, we have:

$$\begin{aligned} y^2 - 3r &= t^2 + 2pt + (p^2 + 2a) + \frac{2pa}{t} + \frac{a^2}{t^2} - 3r \\ &= t^2 + 2pt + (3p^2 - r) + \frac{2pa}{t} + \frac{a^2}{t^2} \end{aligned}$$

With this in hand, we have the following computation:

$$\begin{aligned} (y^2-3r)(y-3p) &= \left(t^2 + 2pt + (3p^2 - r) + \frac{2pa}{t} + \frac{a^2}{t^2}\right)\left(t - 2p + \frac{a}{t}\right) \\ &= t^3 + (a - 4p^2 + 3p^2 - r)t + (2pa - 6p^3 + 2pr + 2pa) \\ &\quad + (3p^2a - ra - 4p^2a + a^2)\frac{1}{t} + \frac{a^3}{t^3} \\ &= t^3 + (a - p^2 - r)t + 2p(2a - 3p^2 + r) + a(a - p^2 - r)\frac{1}{t} + \frac{a^3}{t^3} \\ &= t^3 + 2p(-p^2 + 3r) + \frac{a^3}{t^3} \end{aligned}$$

Now by using the formula of t in the statement, this gives:

$$\begin{aligned}(y^2-3r)(y-3p) &= b+\sqrt{b^2-a^3}-4p^2+6pr+\frac{a^3}{b+\sqrt{b^2-a^3}}\\ &= b+\sqrt{b^2-a^3}-4p^2+6pr+b-\sqrt{b^2-a^3}\\ &= 2b-4p^2+6pr\\ &= 2(2p^2-3pr+q^2)-4p^2+6pr\\ &= 2q^2\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In degree 5 and more, things become complicated. However, we have some arithmetic tricks here, for computing the integer or rational roots of polynomials having integer of rational coefficients. There are a lot of analytic tricks too, both real and complex.

3d. Galois theory

We discuss here Galois theory, and its applications to degree 5 equations. Let us start with a basic result regarding the arbitrary fields F and their structure, as follows:

THEOREM 3.18. *Given a field F, define its characteristic $p=char(F)$ as being the smallest $p\in\mathbb{N}$ such that the following happens, and as $p=0$, if this never happens:*

$$\underbrace{1+\ldots+1}_{p\ times}=0$$

Then, assuming $p>0$, this number p must be prime, we have a field embedding $\mathbb{F}_p\subset F$, and $q=|F|$ must be of the form $q=p^k$, with $k\in\mathbb{N}$. Also, we have the formulae

$$(a+b)^p=a^p+b^p\quad,\quad a^q=a$$

valid for any $a,b\in F$, and the Fermat poynomial X^q-X factorizes as:

$$X^q-X=\prod_{a\in F}(X-a)$$

Also, regardless of p, any finite multiplicative subgroup $G\subset F-\{0\}$ must be cyclic.

PROOF. This is a very crowded statement, the idea being as follows:

(1) The fact that $p>0$ must be prime comes by contradiction, by using:

$$(\underbrace{1+\ldots+1}_{a\ times})\times(\underbrace{1+\ldots+1}_{b\ times})=\underbrace{1+\ldots+1}_{ab\ times}$$

Indeed, assuming that we have $p=ab$ with $a,b>1$, the above formula corresponds to an equality of type $AB=0$ with $A,B\neq0$ inside F, which is impossible.

(2) Back to the general case, F has a smallest subfield $E\subset F$, called prime field, consisting of the various sums $1+\ldots+1$, and their quotients. In the case $p=0$ we

obviously have $E=\mathbb{Q}$. In the case $p>0$ now, the multiplication formula in (1) shows that the set $S=\{1+\ldots+1\}$ is stable under taking quotients, and so $E=S$.

(3) Now with $E=S$ in hand, we obviously have $(E,+)=\mathbb{Z}_p$, and since the multiplication is given by the formula in (1), we conclude that we have $E=\mathbb{F}_p$, as a field. Thus, in the case $p>0$, we have constructed an embedding $\mathbb{F}_p\subset F$, as claimed.

(4) In the context of the above embedding $\mathbb{F}_p\subset F$, we can say that F is a vector space over $\mathbb{F}_p$, and so we have $|F|=p^k$, with $k\in\mathbb{N}$ being the dimension of this space.

(5) The baby Fermat formula $(a+b)^p=a^p+b^p$, which reminds the Fermat little theorem, $a^p=a(p)$ over $\mathbb{Z}$, follows in the same way, namely from the binomial formula, because all the non-trivial binomial coefficients $\binom{p}{s}$ are multiples of p:

$$(a+b)^p=\sum_{k=0}^p\binom{p}{k}a^kb^{p-k}=a^p+b^p$$

(6) As for the Fermat formula $a^q=a$ itself, which implies the assertion about X^q-X, this follows from the last assertion, which can be proved via some basic arithmetic inside F, and which for $G=F-\{0\}$ itself, with $|F|=q$, gives $a^{q-1}=1$, for any $a\neq 0$.

(7) Let us pick indeed an element $g\in G$ of highest order, $n=ord(g)$. Our claim, which will prove the results, is that the order $m=ord(h)$ of any $h\in G$ satisfies $m|n$.

(8) In order to prove this claim, let $d=(m,n)$, write $d=am+bn$ with $a,b\in\mathbb{Z}$, and set $k=g^ah^b$. We have then the following computations:

$$k^m=g^{am}h^{bm}=g^{am}=g^{d-bn}=g^d$$

$$k^n=g^{an}h^{bn}=h^{bn}=h^{d-am}=h^d$$

By using either of these formulae, say the first one, we obtain:

$$k^{[m,n]}=k^{mn/d}=(k^m)^{n/d}=(g^d)^{n/d}=g^n=1$$

Thus $ord(k)|[m,n]$, and our claim is that we have in fact $ord(k)=[m,n]$.

(9) In order to prove this latter claim, assume first that we are in the case $d=1$. But here the result is clear, because the formulae in (8) read $g=k^m,h=g^n$, and since $n=ord(g),m=ord(g)$ are prime to each other, we conclude that we have $ord(k)=mn$, as desired. As for the general case, where d is arbitrary, this follows from this.

(10) Summarizing, we have proved our claim in (8). Now since the order $n=ord(g)$ was assumed to be maximal, we must have $[m,n]|n$, and so $m|n$. Thus, we have proved our claim in (7), namely that the order $m=ord(h)$ of any $h\in G$ satisfies $m|n$.

(11) But with this claim in hand, the result follows. Indeed, since the polynomial x^n-1 has all the elements $h\in G$ as roots, its degree must satisfy $n\geq|G|$. On the other hand, from $n=ord(g)$ with $g\in G$, we have $n||G|$. We therefore conclude that we have $n=|G|$, which shows that G is indeed cyclic, generated by the element $g\in G$.

(12) Finally, assuming $|F| = q < \infty$, we know that the multiplicative group $F - \{0\}$ is cyclic, of order $q - 1$. Thus, the following formula is satisfied, for any $a \in F - \{0\}$:

$$a^{q-1} = 1$$

Now by multiplying by a, this gives the Fermat formula $a^q = a$, with of course the remark that this formula trivially holds as well for $a = 0$. $\square$

The above result raises many questions. Since most of these questions seem to have something to do with field extensions, let us start by discussing this. We first have:

THEOREM 3.19. *Given a field extension $E \subset F$, we can talk about its Galois group G, as the group of automorphisms of F fixing E. The intermediate fields*

$$E \subset K \subset F$$

are then in correspondence with the subgroups $H \subset G$, with such a field K corresponding to the subgroup H consisting of automorphisms $g \in G$ fixing K.

PROOF. This is something self-explanatory, and follows indeed from some algebra, under suitable assumptions, in order for that algebra to properly apply. $\square$

Getting now towards polynomials and their roots, we have here:

THEOREM 3.20. *Given a field F and a polynomial $P \in F[X]$, we can talk about the abstract splitting field of P, where this polynomial decomposes as:*

$$P(X) = c\prod_i (X - a_i)$$

In particular, any field F has a certain algebraic closure $\bar{F}$, where all the polynomials $P \in F[X]$, and in fact all polynomials $P \in \bar{F}[X]$ too, have roots.

PROOF. This is again something self-explanatory, which follows from Theorem 3.19 and from some extra algebra, under suitable assumptions, in order for that extra algebra to properly apply. Regarding the construction at the end, as main example here we have $\bar{\mathbb{R}} = \mathbb{C}$. However, as an interesting fact, $\bar{\mathbb{Q}} \subset \mathbb{C}$ is a proper subfield. $\square$

Good news, with this in hand, we can now elucidate the structure of finite fields:

THEOREM 3.21. *For any prime power $q = p^k$ there is a unique field $\mathbb{F}_q$ having q elements. At $k = 1$ this is the usual $\mathbb{F}_p$. In general, this is the splitting field of:*

$$P = X^q - X$$

Moreover, we can construct an explicit model for $\mathbb{F}_q$, at $q = p^2$ or higher, as

$$\mathbb{F}_q = \mathbb{F}_p[X]/(Q)$$

with $Q \in \mathbb{F}_p[X]$ being a suitable irreducible polynomial, of degree k.

Proof. There are several assertions here, the idea being as follows:

(1) The first assertion, regarding the existence and uniqueness of $\mathbb{F}_q$, follows from Theorem 3.18 and Theorem 3.20. Indeed, we know from Theorem 3.18 that given a finite field, $|F| = q$ with $k \in \mathbb{N}$, the Fermat polynomial $P = X^q - X$ factorizes as follows:

$$X^q - X = \prod_{a \in F}(X - a)$$

But this shows, via the general theory from Theorem 3.20, that our field F must be the splitting field of P, and so is unique. As for the existence, this follows again from Theorem 3.20, telling us that the splitting field always exists.

(2) In what regards now the modeling of $\mathbb{F}_q$, at $q = p$ there is nothing to do, because we have our usual $\mathbb{F}_p$ here. At $q = p^2$ and higher, we know from commutative algebra that we have an isomorphism as follows, whenever $Q \in \mathbb{F}_p[X]$ is taken irreducible:

$$\mathbb{F}_q = \mathbb{F}_p[X]/(Q)$$

(3) Regarding now the best choice of the irreducible polynomial $Q \in \mathbb{F}_p[X]$, providing us with a good model for the finite field $\mathbb{F}_q$, that we can use in practice, this question depends on the value of $q = p^k$, and many things can be said here. All in all, our models are quite similar to $\mathbb{C} = \mathbb{R}[i]$, with i being a formal number satisfying $i^2 = -1$.

(4) To be more precise, at the simplest exponent, $q = 4$, to start with, we can use $Q = X^2 + X + 1$, with this being actually the unique possible choice of a degree 2 irreducible polynomial $Q \in \mathbb{F}_2[X]$, and this leads to a model as follows:

$$\mathbb{F}_4 = \left\{0, 1, a, a + 1 \,\middle|\, a^2 = a + 1\right\}$$

To be more precise here, we assume of course that the characteristic of our model is $p = 2$, which reads $x + x = 0$ for any x, and so determines the addition table. As for the multiplication table, this is uniquely determined by $a^2 = -a - 1 = a + 1$.

(5) Next, at exponents of type $q = p^2$ with $p \geq 3$ prime, we can use $Q = X^2 - r$, with r being a non-square modulo p, and with $(p - 1)/2$ choices here. We are led to:

$$\mathbb{F}_{p^2} = \left\{a + b\gamma \,\middle|\, \gamma^2 = r\right\}$$

Here, as before with $\mathbb{F}_4$, our formula is something self-explanatory. Observe the analogy with $\mathbb{C} = \mathbb{R}[i]$, with i being a formal number satisfying $i^2 = -1$.

(6) Finally, at $q = p^k$ with $k \geq 3$ things become more complicated, but the main idea remains the same. We have for instance models for $\mathbb{F}_8$, $\mathbb{F}_{27}$ using $Q = X^3 - X - 1$, and a model for $\mathbb{F}_{16}$ using $Q = X^4 + X + 1$. Many other things can be said here. □

As another application of the above, which motivated Galois, we have:

THEOREM 3.22. *Unlike in degree $N \leq 4$, there is no formula for the roots of polynomials of degree $N = 5$ and higher, with the reason for this, coming from Galois theory, being that S_5 is not solvable. The simplest numeric example is $P = X^5 - X - 1$.*

PROOF. This is something quite tricky, the idea being as follows:

(1) The first assertion, for generic polynomials, is due to Abel-Ruffini, but Galois theory helps in better understanding this, and comes with a number of bonus points too, namely the possibility of formulating a finer result, with Abel-Ruffini's original "generic", which was something algebraic, being now replaced by an analytic "generic", and also with the possibility of dealing with concrete polynomials, such as $P = X^5 - X - 1$.

(2) Regarding now the details of the Galois proof of the Abel-Ruffini theorem, assume that the roots of a polynomial $P \in F[X]$ can be computed by using iterated roots, a bit as for the degree 2 equation, or for the degree 3 and 4 equations, via Cardano. Then, algebrically speaking, this gives rise to a tower of fields as folows, with $F_0 = F$, and each F_{i+1} being obtained from F_i by adding a root, $F_{i+1} = F_i(x_i)$, with $x_i^{n_i} \in F_i$:

$$F_0 \subset F_1 \subset \ldots \subset F_k$$

(3) In order for Galois theory to apply well to this situation, we must make all the extensions normal, which amounts in replacing each $F_{i+1} = F_i(x_i)$ by its extension $K_i(x_i)$, with K_i extending F_i by adding a n_i-th root of unity. Thus, with this replacement, we can assume that the tower in (2) in normal, meaning that all Galois groups are cyclic.

(4) Now by Galois theory, at the level of the corresponding Galois groups we obtain a tower of groups as follows as follows, which is a resolution of the last group G_k, the Galois group of P, in the sense of group theory, in the sense that all quotients are cyclic:

$$G_1 \subset G_2 \subset \ldots \subset G_k$$

As a conclusion, Galois theory tells us that if the roots of a polynomial $P \in F[X]$ can be computed by using iterated roots, then its Galois group $G = G_k$ must be solvable.

(5) In the generic case, the conclusion is that Galois theory tells us that, in order for all polynomials of degree 5 to be solvable, via square roots, the group S_5, which appears there as Galois group, must be solvable, in the sense of group theory. But this is wrong, because the alternating subgroup $A_5 \subset S_5$ is simple, and therefore not solvable.

(6) Finally, regarding the polynomial $P = X^5 - X - 1$, some elementary computations here, based on arithmetic over $\mathbb{F}_2, \mathbb{F}_3$, and involving various cycles of length $2, 3, 5$, show that its Galois group is S_5. Thus, we have our counterexample.

(7) To be more precise, our polynomial factorizes over $\mathbb{F}_2$ as follows:

$$X^5 - X - 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$$

We deduce from this the existence of an element $\tau\sigma \in G \subset S_5$, with $\tau \in S_5$ being a transposition, and with $\sigma \in S_5$ being a 3-cycle, disjoint from it. Thus, we have:

$$\tau = (\tau\sigma)^3 \in G$$

(8) On the other hand since $P = X^5 - X - 1$ is irreducible over $\mathbb{F}_5$, we have as well available a certain 5-cycle $\rho \in G$. Now since $< \tau, \rho >= S_5$, we conclude that the Galois group of P is full, $G = S_5$, and by (4) and (5) we have our counterexample.

(9) Finally, as mentioned in (1), all this shows as well that a random polynomial of degree 5 or higher is not solvable by square roots, and with this being an elementary consequence of the main result from (5), via some standard analysis arguments. □

3e. Exercises

Here are some exercises, in relation with what we did in this chapter, for the most regarding the further clarification of certain results, that we did quite quickly:

Exercise 3.23. *Clarify the symmetric function theory needed for resultants.*

Exercise 3.24. *Rewrite the theory of resultants, with Sylvester coming first.*

Exercise 3.25. *Learn further degree 3 formulae, and more degree 4 too.*

Exercise 3.26. *Learn some arithmetic tricks for roots of polynomials.*

Exercise 3.27. *Learn complex analysis tricks for roots of polynomials.*

Exercise 3.28. *Clarify under which exact assumptions Galois theory works.*

Exercise 3.29. *Clarify all details for splitting fields, and algebraic closures.*

Exercise 3.30. *Have some fun with finite fields, and what can be done with them.*

As bonus exercise, learn full Galois theory, the hard way, from an old book of your choice, with all theorems read, details understood, and a lot of exercises done too.

CHAPTER 4

Projective manifolds

4a. Projective spaces

Instead of pursuing with usual, affine geometry, which can quickly escalate into fairly complicated things, let us take a look at projective geometry too, which is something fun, and interesting, and quite often more fun and interesting than affine geometry itself.

You might have heard of not of projective geometry. In case you didn't yet, the general principle is that "this is the wonderland where parallel lines cross". Which might sound a bit crazy, and not very realistic, but take a picture of some railroad tracks, and look at that picture. Do these parallel railroad tracks cross, on the picture? Sure they do. So, we are certainly not into abstractions here, but rather into serious science. QED.

Mathematically now, here are some axioms, to start with:

Definition 4.1. *A projective space is a space consisting of points and lines, subject to the following conditions:*

(1) *Each 2 points determine a line.*
(2) *Each 2 lines cross, on a point.*

As a basic example we have the usual projective plane $P^2_\mathbb{R}$, which is best seen as being the space of lines in $\mathbb{R}^3$ passing through the origin. To be more precise, let us call each of these lines in $\mathbb{R}^3$ passing through the origin a "point" of $P^2_\mathbb{R}$, and let us also call each plane in $\mathbb{R}^3$ passing through the origin a "line" of $P^2_\mathbb{R}$. Now observe the following:

(1) Each 2 points determine a line. Indeed, 2 points in our sense means 2 lines in $\mathbb{R}^3$ passing through the origin, and these 2 lines obviously determine a plane in $\mathbb{R}^3$ passing through the origin, namely the plane they belong to, which is a line in our sense.

(2) Each 2 lines cross, on a point. Indeed, 2 lines in our sense means 2 planes in $\mathbb{R}^3$ passing through the origin, and these 2 planes obviously determine a line in $\mathbb{R}^3$ passing through the origin, namely their intersection, which is a point in our sense.

Thus, what we have is a projective space in the sense of Definition 4.1. More generally, we have the following construction, in arbitrary dimensions:

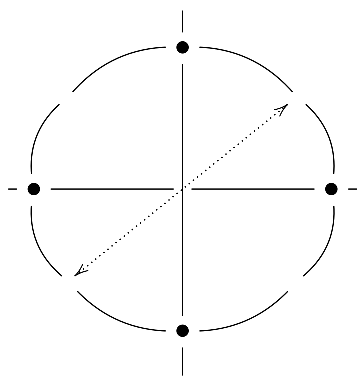
THEOREM 4.2. *We can define the projective space $P^{N-1}_\mathbb{R}$ as being the space of lines in $\mathbb{R}^N$ passing through the origin, and in small dimensions:*

(1) *$P^1_\mathbb{R}$ is the usual circle.*
(2) *$P^2_\mathbb{R}$ is some sort of twisted sphere.*

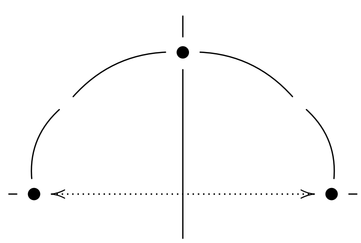
PROOF. We have several assertions here, with all this being of course a bit informal, and self-explanatory, the idea and some further details being as follows:

(1) To start with, the fact that the space $P^{N-1}_\mathbb{R}$ constructed in the statement is indeed a projective space in the sense of Definition 4.1 follows from definitions, exactly as in the discussion preceding the statement, regarding the case $N=3$.

(2) At $N=2$ now, a line in $\mathbb{R}^2$ passing through the origin corresponds to 2 opposite points on the unit circle $\mathbb{T}\subset\mathbb{R}^2$, according to the following scheme:

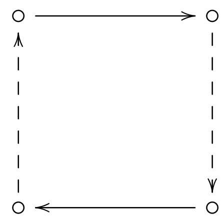


Thus, $P^1_\mathbb{R}$ corresponds to the upper semicircle of $\mathbb{T}$, with the endpoints identified, and so we obtain a circle, $P^1_\mathbb{R}=\mathbb{T}$, according to the following scheme:

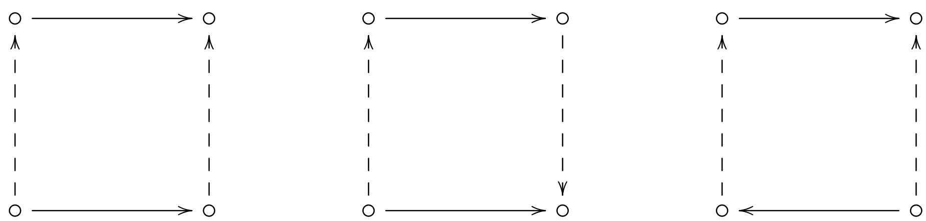


(3) At $N=3$, the space $P^2_\mathbb{R}$ corresponds to the upper hemisphere of the sphere $S^2_\mathbb{R}\subset\mathbb{R}^3$, with the points on the equator identified via $x=-x$. Topologically speaking, we can deform if we want the hemisphere into a square, with the equator becoming the boundary of this square, and in this picture, the $x=-x$ identification corresponds to a

"identify opposite edges, with opposite orientations" folding method for the square:



(4) Thus, we have our space. In order to understand now what this beast is, let us look first at the other 3 possible methods of folding the square, which are as follows:



Regarding the first space, the one on the left, things here are quite simple. Indeed, when identifying the solid edges we get a cylinder, and then when further identifying the dotted edges, what we get is some sort of closed cylinder, which is a torus.

(5) Regarding the second space, the one in the middle, things here are more tricky. Indeed, when identifying the solid edges we get again a cylinder, but then when further identifying the dotted edges, we obtain some sort of "impossible" closed cylinder, called Klein bottle. This Klein bottle obviously cannot be drawn in 3 dimensions, but with a bit of imagination, you can see it, in its full splendor, in 4 dimensions.

(6) Finally, regarding the third space, the one on the right, we know by symmetry that this must be the Klein bottle too. But we can see this as well via our standard folding method, namely identifying solid edges first, and dotted edges afterwards. Indeed, we first obtain in this way a Möbius strip, and then, well, the Klein bottle.

(7) With these preliminaries made, and getting back now to the projective space $P^2_{\mathbb{R}}$, we can see that this is something more complicated, of the same type, reminding the torus and the Klein bottle. So, we will call it "sort of twisted sphere", as in the statement, and exercise for you to imagine how this beast looks like, in 4 dimensions. $\square$

All this is quite exciting, and reminds childhood and primary school, but is however a bit tiring for our neurons, guess that is pure mathematics. It is possible to come up with some explicit formulae for the embedding $P^2_{\mathbb{R}} \subset \mathbb{R}^4$, which are useful in practice, allowing us to do some analysis over $P^2_{\mathbb{R}}$, and we will leave this as an instructive exercise.

There is some linear algebra to be done here too, by identifying the lines in $\mathbb{R}^N$ with the corresponding rank 1 projections, along with many other things, and we have:

THEOREM 4.3. *The projective space $P^{N-1}_\mathbb{R}$ can be thought of as being the space of rank 1 projections in the matrix algebra $M_N(\mathbb{R})$, given by*

$$P_x = \frac{1}{||x||^2}(x_i x_j)_{ij}$$

by identifying the lines in $\mathbb{R}^N$ passing through the origin with the corresponding rank 1 projections in $M_N(\mathbb{R})$, in the obvious way.

PROOF. There are several things going on here, the idea being as follows:

(1) The main assertion is more or less clear from definitions, the point being that the lines in $\mathbb{R}^N$ passing through the origin are obviously in bijection with the corresponding rank 1 projections. Thus, we obtain the interpretation of $P^{N-1}_\mathbb{R}$ in the statement.

(2) Regarding now the formula of the rank 1 projections, which is a must-know, for this, and in everyday life, consider a vector $y \in \mathbb{R}^N$. Its projection on $\mathbb{R}x$ must be a certain multiple of x, and we are led in this way to the following formula:

$$P_x y = \frac{< y, x >}{< x, x >} x = \frac{1}{||x||^2} < y, x > x$$

(3) But with this in hand, we can now compute the entries of P_x, as follows:

$$\begin{aligned}
(P_x)_{ij} &= < P_x e_j, e_i > \\
&= \frac{1}{||x||^2} < e_j, x >< x, e_i > \\
&= \frac{x_j x_i}{||x||^2}
\end{aligned}$$

Thus, we are led to the formula in the statement. □

Regarding now embeddings of $P^{N-1}_\mathbb{R}$ into Euclidean spaces $\mathbb{R}^n$, many things can be said, with a straightforward construction here being as follows:

THEOREM 4.4. *The projective space $P^{N-1}_\mathbb{R}$ is a smooth manifold, with charts*

$$(x_1, \ldots, x_N) \to \left(\frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_N}{x_i}\right)$$

where $x_i \neq 0$. This manifold is compact, and of dimension $N-1$.

PROOF. We know that $P^{N-1}_\mathbb{R}$ appears as the space of lines in $\mathbb{R}^N$ passing through the origin, so we have the following formula, with $\sim$ being the proportionality of vectors, given as usual by $x \sim y$ when $x = \lambda y$, for some scalar $\lambda \neq 0$:

$$P^{N-1}_\mathbb{R} = \mathbb{R}^N - \{0\} / \sim$$

Alternatively, we can restrict if we want the attention to the vectors on the unit sphere $S^{N-1}_\mathbb{R} \subset \mathbb{R}^N$, and this because any line in $\mathbb{R}^N$ passing through the origin will certainly cross this sphere. Moreover, it is clear that our line will cross the sphere in exactly two points $\pm x$, and we conclude that we have the following formula, with $\sim$ being now the proportionality of vectors on the sphere, given by $x \sim y$ when $x = \pm y$:

$$P^{N-1}_{\mathbb{R}} = S^{N-1}_{\mathbb{R}} / \sim$$

With this discussion made, let us get now to what is to be proved. Obviously, once we fix an index $i \in \{1, \ldots, N\}$, the condition $x_i \neq 0$ on the vectors $x \in \mathbb{R}^N - \{0\}$ defines an open subset $U_i \subset P^{N-1}_{\mathbb{R}}$, and the open subsets that we get in this way cover $P^{N-1}_{\mathbb{R}}$:

$$P^{N-1}_{\mathbb{R}} = U_1 \cup \ldots \cup U_N$$

Moreover, the map in the statement is injective $U_i \to \mathbb{R}^{N-1}$, and it is clear too that the changes of charts are C^∞. Thus, we have our smooth manifold, as claimed. □

Many other things can be said about $P^{N-1}_{\mathbb{R}}$, and we will be back to this. Importantly, most of the above results extend to the complex setting, and we have:

THEOREM 4.5. *We can define the complex projective space $P^{N-1}_{\mathbb{C}}$ as being the space of complex lines in $\mathbb{C}^N$ passing through the origin. Alternatively, we can say that $P^{N-1}_{\mathbb{C}}$ is the space of rank 1 projections in the matrix algebra $M_N(\mathbb{C})$, given by*

$$P_x = \frac{1}{||x||^2}(x_i \bar{x}_j)_{ij}$$

by identifying the lines in $\mathbb{C}^N$ passing through the origin with the corresponding rank 1 projections in $M_N(\mathbb{C})$, in the obvious way. The complex projective space $P^{N-1}_{\mathbb{C}}$ is a smooth compact manifold, having complex dimension $N-1$.

PROOF. All this follows indeed via the same arguments as in the real case. □

All this is very interesting, but we will pause our study here, because we still have many other things to say. Getting now to finite fields, we have:

THEOREM 4.6. *Given a field F, we can talk about the projective space P^2_F, as being the space of lines in F^3 passing through the origin, having cardinality*

$$|P^2_F| = q^2 + q + 1$$

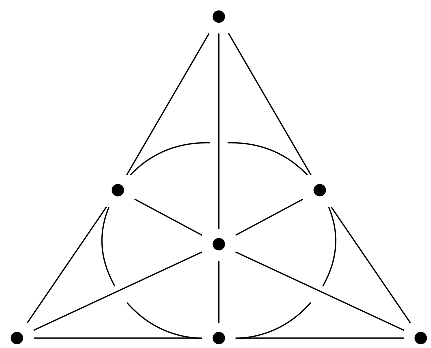
where $q = |F|$, in the case where our field F is finite.

PROOF. This is indeed clear from definitions, with the cardinality coming from:

$$|P^2_F| = \frac{|F^3 - \{0\}|}{|F - \{0\}|} = \frac{q^3 - 1}{q - 1} = q^2 + q + 1$$

Thus, we are led to the conclusions in the statement. □

As an example, let us see what happens for the simplest finite field that we know, namely $F = \mathbb{F}_2$. Here our projective plane, having $4+2+1=7$ points, and 7 lines, is a famous combinatorial object, called Fano plane, which is depicted as follows:



Here the circle in the middle is by definition a line, and with this convention, the basic axioms in Definition 4.1 are satisfied, in the sense that any two points determine a line, and any two lines determine a point. And isn't this beautiful.

4b. Bézout theorem

Bézout theorem.

4c. Projective manifolds

Projective manifolds.

4d. Grassmannians and more

Grassmannians and more.

4e. Exercises

Exercises:

Exercise 4.7.

Exercise 4.8.

Exercise 4.9.

Exercise 4.10.

Exercise 4.11.

Exercise 4.12.

Exercise 4.13.

Exercise 4.14.

Bonus exercise.

Part II

Topology, knots

Mississippi in the middle of a dry spell
Jimmie Rodgers on the Victrola up high
Mama's dancing with a baby on her shoulder
The sun is setting like molasses in the sky

CHAPTER 5

Homotopy groups

5a. Topological spaces

Welcome to topology. Before getting started with our mathematics, we need spaces. We will use here a very general definition, as folllows:

Definition 5.1. *A topological space is a set X, along with a collection of subsets $U \subset X$ called open sets, satisfying what we can expect from the open sets.*

In practice, for analysis, we will mostly need the case where X is a metric space, with the remark however that abstract topological spaces as above are something quite interesting, for instance in relation with the number theory considerations from chapter 2. So, getting now to metric spaces, the definition that we will need here is as follows:

Definition 5.2. *Let X be a metric space.*

1. *The open balls are the sets $B_x(r) = \{y \in X | d(x,y) < r\}$.*
2. *The closed balls are the sets $\bar{B}_x(r) = \{y \in X | d(x,y) \leq r\}$.*
3. *$E \subset X$ is called open if for any $x \in E$ we have a ball $B_x(r) \subset E$.*
4. *$E \subset X$ is called closed if its complement $E^c \subset X$ is open.*

At the level of examples, you can quickly convince yourself, by working out a few of them, that our notions above coincide with the usual ones, that we know well, in the case $X = \mathbb{R}, \mathbb{C}$. We will be back to this later, with some general results in this sense, confirming all this. But for the moment, let us work out the basics. We first have the following result, clarifying some terminology issues from Definition 5.2:

Proposition 5.3. *The open balls are open, and the closed balls are closed.*

Proof. This might sound a bit as a joke, but it is not one, because this is the kind of thing that we have to check. Fortunately, all this is elementary, as follows:

(1) Given an open ball $B_x(r)$ and a point $y \in B_x(r)$, by using the triangle inequality we have $B_y(r') \subset B_x(r)$, with $r' = r - d(x,y)$. Thus, $B_x(r)$ is indeed open.

(2) Given a closed ball $\bar{B}_x(r)$ and a point $y \in B_x(r)^c$, by using the triangle inequality we have $B_y(r') \subset B_x(r)^c$, with $r' = d(x,y) - r$. Thus, $\bar{B}_x(r)$ is indeed closed. □

Here is now something more interesting, making the link with our intuitive understanding of the notion of closedness, coming from our experience so far with analysis:

PROPOSITION 5.4. *For a set $E \in X$, the following are equivalent:*

(1) *E is closed in our sense, meaning that E^c is open.*
(2) *We have $x_n \to x, x_n \in E \implies x \in E$.*

PROOF. We can prove this by double implication, as follows:

(1) $\implies$ (2) Assume by contradiction $x_n \to x, x_n \in E$ with $x \notin E$. Since we have $x \in E^c$, which is open, we can pick a ball $B_x(r) \subset E^c$. But this contradicts our convergence assumption $x_n \to x$, so we are done with this implication.

(2) $\implies$ (1) Assume by contradiction that E is not closed in our sense, meaning that E^c is not open. Thus, we can find $x \in E^c$ such that there is no ball $B_x(r) \subset E^c$. But with $r = 1/n$ this provides us with a point $x_n \in B_x(1/n) \cap E$, and since we have $x_n \to x$, this contradicts our assumption (2). Thus, we are done with this implication too. □

Here is a now key result, making the link with the axioms in Definition 5.1:

THEOREM 5.5. *Let X be a metric space.*

(1) *If E_i are open, then $\cup_i E_i$ is open.*
(2) *If F_i are closed, then $\cap_i F_i$ is closed.*
(3) *If $E_1, \ldots, E_n$ are open, then $\cap_i E_i$ is open.*
(4) *If $F_1, \ldots, F_n$ are closed, then $\cup_i F_i$ is closed.*

Moreover, both (3) and (4) can fail for infinite intersections and unions.

PROOF. We have several things to be proved, the idea being as follows:

(1) This is clear from definitions, because any point $x \in \cup_i E_i$ must satisfy $x \in E_i$ for some i, and so has a ball around it belonging to E_i, and so to $\cup_i E_i$.

(2) This follows from (1), by using the following well-known set theory formula:

$$\left(\bigcup_i E_i\right)^c = \bigcap_i E_i^c$$

(3) Given an arbitrary point $x \in \cap_i E_i$, we have $x \in E_i$ for any i, and so we have a ball $B_x(r_i) \subset E_i$ for any i. Now with this in hand, let us set:

$$B = B_x(r_1) \cap \ldots \cap B_x(r_n)$$

As a first observation, this is a ball around x, $B = B_x(r)$, of radius given by:

$$r = \min(r_1, \ldots, r_n)$$

But this ball belongs to all the E_i, and so belongs to their intersection $\cap_i E_i$. We conclude that the intersection $\cap_i E_i$ is open, as desired.

(4) This follows from (3), by using the following well-known set theory formula:

$$\left(\bigcap_i E_i\right)^c=\bigcup_i E_i^c$$

(5) Finally, in what regards the counterexamples at the end, we will leave their construction, which is something very elementary, as an instructive exercise. □

Finally, still in relation with open and closed sets, we have as well:

DEFINITION 5.6. *Let X be a metric space, and $E\subset X$ be a subset.*

(1) *The interior $E^\circ\subset E$ is the set of points $x\in E$ which admit around them open balls $B_x(r)\subset E$.*
(2) *The closure $E\subset\bar{E}$ is the set of points $x\in X$ which appear as limits of sequences $x_n\to x$, with $x\in E$.*

These notions are quite interesting, because they make sense for any set E. That is, when E is open, that is open and end of the story, and when E is closed, that is closed and end of the story. In general, however, a set $E\subset X$ is not open or closed, and what we can best do to it, in order to study with our tools, is to "squeeze" it, as follows:

$$E^\circ\subset E\subset\bar{E}$$

In practice now, in order to use the above notions, we need to know a number of things, including that fact that E open implies $E^\circ=E$, the fact that E closed implies $\bar{E}=E$, and many more such results, not to forget the fact that the closures of the open balls $B_r(x)$ are the closed balls $\bar{B}_x(r)$, clarifying an obvious notational issue which appears with respect to Definition 5.2. But all this can be done, and the useful statement here, summarizing all that we need to know about interiors and closures, is as follows:

THEOREM 5.7. *Let X be a metric space, and $E\subset X$ be a subset.*

(1) *The interior $E^\circ\subset E$ is the biggest open set contained in E.*
(2) *The closure $E\subset\bar{E}$ is the smallest closed set containing E.*

PROOF. We have several things to be proved, the idea being as follows:

(1) Let us first prove that the interior E° is open. For this purpose, pick $x\in E^\circ$. We know that we have a ball $B_x(r)\subset E$, and since this ball is open, it follows that we have $B_x(r)\subset E^\circ$. Thus, the interior E° is open, as claimed.

(2) Let us prove now that the closure $\bar{E}$ is closed. For this purpose, we will prove that the complement $\bar{E}^c$ is open. So, pick $x\in\bar{E}^c$. Then x cannot appear as a limit of a sequence $x_n\to x$ with $x_n\in E$, so we have a ball $B_x(r)\subset\bar{E}^c$, as desired.

(3) Finally, the maximality and minimality assertions regarding E° and $\bar{E}$ are both routine too, coming from definitions, and we will leave them as exercises. □

As an application of the theory developed above, and more specifically of the notion of closure from Definition 5.6, we can talk as well about density, as follows:

DEFINITION 5.8. *We say that a subset $E \subset X$ is dense when:*

$$\bar{E} = X$$

That is, any point of X must appear as a limit of points of E.

Obviously, this is something which is in tune with what we know so far from this book, and with the intuitive notion of density. As a basic example, we have $\bar{\mathbb{Q}} = \mathbb{R}$, that we know well from the beginning of this book, and more specifically, from chapter 2.

Moving ahead now, at a more subtle level, again in analogy with what we know about $X = \mathbb{R}, \mathbb{C}$, we can talk about compact sets, and about connected sets. Again things here are quite tricky, in the general metric space framework, actually substantially deviating from what we know, and we will do this in detail. Let us start with:

DEFINITION 5.9. *A set $K \subset X$ is called compact if any cover with open sets*

$$K \subset \bigcup_i E_i$$

has a finite subcover, $K \subset (E_{i_1} \cup \ldots \cup E_{i_n})$.

This definition might seem overly abstract, and perhaps even sound like a joke, but our claim is that this is the correct definition, and that there is no way of doing otherwise. The point indeed is that we have the following counterexample:

PROPOSITION 5.10. *Given an infinite set X with the discrete distance on it, namely $d(p,q) = 1 - \delta_{pq}$, which can be modelled as the basis of a suitable Hilbert space,*

$$X = \{e_x\}_{x \in X} \subset l^2(X)$$

this set is closed and bounded, but not compact.

PROOF. Here the first part, regarding the modelling of X, that we will actually not really need, is something that we already know. Regarding now the second part:

(1) X being the total space, it is by definition closed. As a remark here, that we will need later, since the points of X are obviously open, any subset $E \subset X$ is open, and by taking complements, any set $E \subset X$ is closed as well.

(2) X is also bounded, because all distances are smaller than 1.

(3) However, our set X is not compact, because its points being open, as noted above, $X = \cup_{x \in X} \{x\}$ is an open cover, having no finite subcover. □

Let us develop now the theory of compact sets, as axiomatized above, and see what we get. We first have the following result, confirming that we are on the good track:

Proposition 5.11. *The following hold:*

(1) *Compact implies closed.*
(2) *Closed inside compact is compact.*
(3) *Compact intersected with closed is compact.*

Proof. These assertions are all clear from definitions, as follows:

(1) Assume that $K\subset X$ is compact, and let us prove that K is closed. For this purpose, we will prove that K^c is open. So, pick $p\in K^c$. For any $q\in K$ we set $r=d(p,q)/3$, and we consider the following balls, separating p and q:

$$U_q=B_p(r)\quad,\quad V_q=B_q(r)$$

We have then $K\subset\cup_{q\in K}V_q$, so we can pick a finite subcover, as follows:

$$K\subset(V_{q_1}\cup\ldots\cup V_{q_n})$$

With this done, consider the following intersection:

$$U=U_{q_1}\cap\ldots\cap U_{q_n}$$

This intersection is then a ball around p, and since this ball avoids $V_{q_1},\ldots,V_{q_n}$, it avoids the whole K. Thus, we have proved that K^c is open at p, as desired.

(2) Assume that $F\subset K$ is closed, with $K\subset X$ being compact. For proving our result, we can assume, by replacing X with K, that we have $X=K$. In order to prove now that F is compact, consider an open cover of it, as follows:

$$F\subset\bigcup_i E_i$$

By adding the set F^c, which is open, to this cover, we obtain a cover of K. Now since K is compact, we can extract from this a finite subcover Ω, and there are two cases:

– If $F^c\in\Omega$, by removing F^c from Ω we obtain a finite cover of F, as desired.

– If $F^c\notin\Omega$, we are done too, because in this case Ω is a finite cover of F.

(3) This follows from (1) and (2), because if $K\subset X$ is compact, and $F\subset X$ is closed, then $K\cap F\subset K$ is closed inside a compact, so it is compact. □

As a second batch of results, which are useful as well, we have:

Proposition 5.12. *The following hold:*

(1) *If $K_i\subset X$ are compact, satisfying $K_{i_1}\cap\ldots\cap K_{i_n}\neq\emptyset$, then $\cap_iK_i\neq\emptyset$.*
(2) *If $K_1\supset K_2\supset K_3\supset\ldots$ are non-empty compacts, then $\cap_iK_i\neq\emptyset$.*
(3) *If K is compact, and $E\subset K$ is infinite, then E has a limit point in K.*
(4) *If K is compact, any sequence $\{x_n\}\subset K$ has a limit point in K.*
(5) *If K is compact, any $\{x_n\}\subset K$ has a subsequence which converges in K.*

PROOF. Again, these are elementary results, which can be proved as follows:

(1) Assume by contradiction $\cap_i K_i = \emptyset$, and let us pick $K_1 \in \{K_i\}$. Since any $x \in K_1$ is not in $\cap_i K_i$, there is an index i such that $x \in K_i^c$, and we conclude that we have:

$$K_1 \subset \bigcup_{i \neq 1} K_i^c$$

But this can be regarded as being an open cover of K_1, that we know to be compact, so we can extract from it a finite subcover, as follows:

$$K_1 \subset \left(K_{i_1}^c \cup \ldots \cup K_{i_n}^c\right)$$

Now observe that this latter subcover tells us that we have:

$$K_1 \cap K_{i_1} \cap \ldots \cap K_{i_n} = \emptyset$$

But this contradicts our intersection assumption in the statement, and we are done.

(2) This is a particular case of (1), proved above.

(3) We prove this by contradiction. So, assume that E has no limit point in K. This means that any $p \in K$ can be isolated from the rest of E by a certain open ball $V_p = B_p(r)$, and in both the cases that can appear, $p \in E$ or $p \notin E$, we have:

$$|V_p \cap E| = 0, 1$$

Now observe that these sets V_p form an open cover of K, and so of E. But due to $|V_p \cap E| = 0, 1$ and to $|E| = \infty$, this open cover of E has no finite subcover. Thus the same cover, regarded now as cover of K, has no finite subcover either, contradiction.

(4) This follows from (3) that we just proved, with $E = \{x_n\}$.

(5) This is a reformulation of (4), that we just proved. □

Getting now to some more exciting theory, here is a key result about compactness, which is less trivial, and that we will need on a regular basis, in what follows:

THEOREM 5.13. *For a subset $K \subset \mathbb{R}^N$, the following are equivalent:*

1. *K is closed and bounded.*
2. *K is compact.*
3. *Any infinite subset $E \subset K$ has a limiting point in K.*

PROOF. This is something quite tricky, the idea being as follows:

(1) $\implies$ (2) As a first task, in order to establish this implication, let us prove that any product of closed intervals, as follows, is indeed compact:

$$J = \prod_{i=1}^{N} [a_i, b_i] \subset \mathbb{R}^N$$

We can assume by linearity that we are dealing with the unit cube:

$$C_1=\prod_{i=1}^N[0,1]\subset\mathbb R^N$$

In order to prove that C_1 is compact, we proceed by contradiction. So, assume that we have an open cover as follows, having no finite subcover:

$$C_1\subset\bigcup_iE_i$$

Now let us cut C_1 into 2^N small cubes, in the obvious way, over the N coordinate axes. Then at least one of these small cubes, which are all covered by $\cup_iE_i$ too, has no finite subcover. So, let us call $C_2\subset C_1$ one of these small cubes, having no finite subcover:

$$C_2\subset\bigcup_iE_i$$

We can then cut C_2 into 2^N small cubes, and by the same reasoning, we obtain a smaller cube $C_3\subset C_2$ having no finite subcover. And so on by recurrence, and we end up with a decreasing sequence of cubes, as follows, having no finite subcover:

$$C_1\supset C_2\supset C_3\supset\ldots$$

Now since these decreasing cubes have edge size $1,1/2,1/4,\ldots$, their intersection must be a point. So, let us call p this point, defined by the following formula:

$$\{p\}=\bigcap_kC_k$$

But this point p must be covered by $\cup_iE_i$, so we can find an index i such that:

$$p\in E_i$$

Now observe that E_i must contain a whole ball around p, and so starting from a certain $K\in\mathbb N$, all the cubes C_k will be contained in this ball, and so in E_i:

$$C_k\subset E_i\quad,\quad\forall k\geq K$$

But this is a contradiction, because C_K, and in fact the smaller cubes C_k with $k>K$ as well, were assumed to have no finite subcover. Thus, we have proved our claim.

(1) $\implies$ (2), continuation. But with this claim in hand, the result is now clear. Indeed, assume that $K\subset\mathbb R^N$ is closed and bounded. Then, since K is bounded, we can view it as a subset as a suitable big cube, of the following form:

$$K\subset\prod_{i=1}^N[-M,M]\subset\mathbb R^N$$

But, what we have here is a closed subset inside a compact set, that follows to be compact, as desired.

(2) $\implies$ (3) This is something that we already know, not needing $K \subset \mathbb{R}^N$.

(3) $\implies$ (1) We have to prove that K as in the statement is both closed and bounded, and we will do both these things by contradiction, as follows:

– Assume first that K is not closed. But this means that we can find a point $x \notin K$ which is a limiting point of K. Now let us pick $x_n \in K$, with $x_n \to x$, and consider the set $E = \{x_n\}$. According to our assumption, E must have a limiting point in K. But this limiting point can only be x, which is not in K, contradiction.

– Assume now that K is not bounded. But this means that we can find points $x_n \in K$ satisfying $||x_n|| \to \infty$, and if we consider the set $E = \{x_n\}$, then again this set must have a limiting point in K, which is impossible, so we have our contradiction, as desired. □

So long for compactness. As a last piece of general topology, in our metric space framework, we can talk as well about connectedness, as follows:

Definition 5.14. *We can talk about connected sets $E \subset X$, as follows:*

1. *We say that E is connected if it cannot be separated as $E = E_1 \cup E_2$, with the components E_1, E_2 satisfying $E_1 \cap \bar{E}_2 = \bar{E}_1 \cap E_2 = \emptyset$.*
2. *We say that E is path connected if any two points $p, q \in E$ can be joined by a path, meaning a continuous $f : [0.1] \to X$, with $f(0) = p$, $f(1) = q$.*

All this looks a bit technical, and indeed it is. To start with, (1) is something quite natural, but the separation condition there $E_1 \cap \bar{E}_2 = \bar{E}_1 \cap E_2 = \emptyset$ can be weakened into $E_1 \cap E_2 = \emptyset$, or strengthened into $\bar{E}_1 \cap \bar{E}_2 = \emptyset$, depeding on purposes, and with our (1) as formulated being the good compromise, for most purposes. As for (2), this condition is obviously something stronger, and we have in fact the following implications:

$$\text{convex} \implies \text{path connected} \implies \text{connected}$$

The problem, however, is that connected does not imply path connected, and there are as well various counterexamples in relation with the various versions of (1) that can be formulated, as explained above. In any case, once these questions clarified, the idea is that any set E can be written as a disjoint union of connected components, as follows:

$$E = \bigsqcup_i E_i$$

Getting back now to more concrete things, that is, calculus, we have:

Theorem 5.15. *Assuming that $f : X \to Y$ is continuous, the following happen:*

1. *If O is open, then $f^{-1}(O)$ is open.*
2. *If C is closed, then $f^{-1}(C)$ is closed.*
3. *If K is compact, then $f(K)$ is compact.*
4. *If E is connected, then $f(E)$ is connected.*

PROOF. This is something fundamental, which can be proved as follows:

(1) This is clear from the definition of continuity, written with ε, δ. In fact, the converse holds too, in the sense that if $f^{-1}(\text{open}) = \text{open}$, then f must be continuous.

(2) This follows from (1), by taking complements. And again, the converse holds too, in the sense that if $f^{-1}(\text{closed}) = \text{closed}$, then f must be continuous.

(3) Given an open cover $f(K) \subset \cup_i E_i$, we have by using (1) an open cover $K \subset \cup_i f^{-1}(E_i)$, and so by compactness of K, a finite subcover $K \subset f^{-1}(E_{i_1}) \cup \ldots \cup f^{-1}(E_{i_n})$, and so finally a finite subcover $f(K) \subset E_{i_1} \cup \ldots \cup E_{i_n}$, as desired.

(4) This can be proved via the same trick as for (3). Indeed, any separation of $f(E)$ into two parts can be returned via f^{-1} into a separation of E into two parts, contradiction. □

As a comment here, Theorem 5.15 generalizes, and in a clever way, many things that we know from one-variable calculus. Of particular interest is (3), which shows in particular that any continuous function on a compact space $f : X \to \mathbb{R}$ attains its minimum and its maximum, and then (4), which can be regarded as being a general mean value theorem. As for (1) and (2), these are useful in everyday life, and we will see examples of this.

5b. Homotopy groups

Time now to start investigating the shape of our topological spaces. Let us start with something that we know from the above, namely:

DEFINITION 5.16. *A topological space X is called connected when any two points $x, y \in X$ can be connected by a path. That is, given any two points $x, y \in X$, we can find a continuous function $f : [0, 1] \to X$ such that $f(0) = x$ and $f(1) = y$.*

The problem is now, given a connected space X, how to count its “holes”. And this is quite subtle problem, because as examples of such spaces we have:

(1) The sphere, the donut, the double-holed donut, the triple-holed donut, and so on. These spaces are quite simple, and intuition suggests to declare that the number of holes of the N-holed donut is, and you guessed right, N.

(2) However, we have as well as example the empty sphere, I mean just the crust of the sphere, and while this obviously falls into the class of “one-holed spaces”, this is not the same thing as a donut, its hole being of different nature.

(3) As another example, consider again the sphere, but this time with two tunnels drilled into it, in the shape of a cross. Whether that missing cross should account for 1 hole, or for 2 holes, or for something in between, I will leave it up to you.

Summarizing, things are quite tricky, suggesting that the "number of holes" of a topological space X is not an actual number, but rather something more complicated. Now with this in mind, let us formulate the following definition:

Definition 5.17. *The homotopy group $\pi_1(X)$ of a connected space X is the group of loops based at a given point $* \in X$, with the following conventions,*

1. *Two such loops are identified when one can pass continuously from one loop to the other, via a family of loops indexed by $t \in [0,1]$,*
2. *The composition of two such loops is the obvious one, namely is the loop obtaining by following the first loop, then the second loop,*
3. *The unit loop is the null loop at $*$, which stays there, and the inverse of a given loop is the loop itself, followed backwards,*

with the remark that the group $\pi_1(X)$ defined in this way does not depend on the choice of the given point $* \in X$, where the loops are based.

Here the fact that $\pi_1(X)$ defined in this way is indeed a group is obvious, and obvious as well is the fact that, since X is assumed to be connected, this group does not depend on the choice of the given point $* \in X$, where the loops are based.

As basic examples, for spaces having "no holes", such as $\mathbb{R}$ itself, or $\mathbb{R}^N$, and so on, we have $\pi_1 = \{1\}$. In fact, having no holes can only mean, by definition, that $\pi_1 = \{1\}$. As further illustrations, here are now a few basic computations:

Theorem 5.18. *We have the following computations of homotopy groups:*

1. *For the circle, we obtain $\pi_1 = \mathbb{Z}$.*
2. *For the torus, we obtain $\pi_1 = \mathbb{Z} \times \mathbb{Z}$.*
3. *For the disk minus 2 points, we have $\pi_1 = F_2$.*
4. *In fact, for the disk minus N points, we have $\pi_1 = F_N$.*

Proof. These results are all standard, as follows:

(1) The first assertion is clear, because a loop on the circle must wind $n \in \mathbb{Z}$ times around the center, and this parameter $n \in \mathbb{Z}$ uniquely determines the loop, up to the identification in Definition 5.17. Thus, the homotopy group of the circle is the group of such parameters $n \in \mathbb{Z}$, which is of course the group $\mathbb{Z}$ itself.

(2) In what regards now the second assertion, the torus being a product of two circles, we are led to the conclusion that its homotopy group must be some kind of product of $\mathbb{Z}$ with itself. But pictures show that the two standard generators of $\mathbb{Z}$, and so the two copies of $\mathbb{Z}$ themselves, commute, $gh = hg$, and so we obtain the product of $\mathbb{Z}$ with itself, subject to commutation, which is the usual product $\mathbb{Z} \times \mathbb{Z}$.

(3) This is quite clear, because the homotopy group is generated by the 2 loops around the 2 missing points, which are obviously free, algebrically speaking. Thus, we obtain a free product of the group $\mathbb{Z}$ with itself, which is the free group on 2 generators F_2.

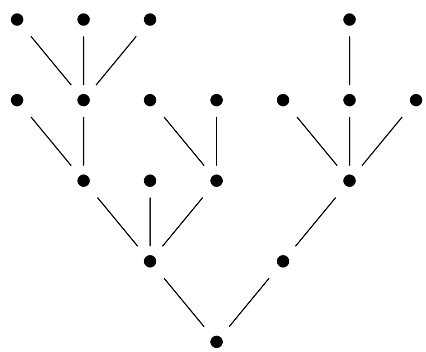
(4) This is again clear, because the homotopy group is generated by the N loops around the N missing points, which are free, algebrically speaking. Thus, we obtain a N-fold free product of $\mathbb{Z}$ with itself, which is the free group on N generators F_N. □

There are many other interesting things that can be said about the homotopy groups, notably about their behavior with respect to all sorts of product and gluing operations for the topological spaces, in the spirit of those that we met in Theorem 5.18.

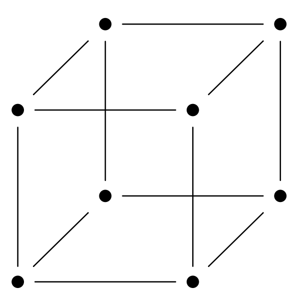
5c. Surfaces, genus

We can talk about the genus of a surface, $g \in \mathbb{N}$, as being its number of holes. In order to be rigorous here, there are many possible approaches, ranging from elementary to advanced, depending on how much geometric you want to be. The best answer, which is a bit complicated, involves complex analysis, and the notion of Riemann surface.

But this leads us into many things, mostly from discrete mathematics, via triangulations, and in particular, into graphs. Some graphs can be drawn without crossings in the plane, and we call them planar. For instance the fact that trees are planar is obvious, and as an illustration, here is some sort of "random" tree, which is clearly planar:

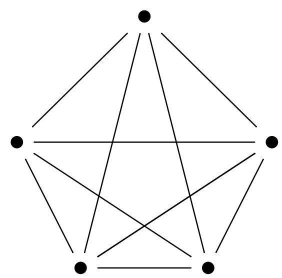


Of course, there are many other interesting examples of planar graphs, as for instance the cube graph, and up to you to tell me why this graph is planar:



However, not all graphs are planar. In order to find basic examples of non-planar graphs, we can look at simplices, and we are led to the following result:

PROPOSITION 5.19. *When looking at simplices, the segment K_2, the triangle K_3 and the tetrahedron K_4 are planar. However, the next simplex K_5, namely*

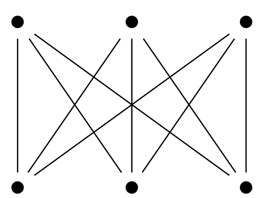


is not planar. Nor are the higher simplices, K_N with $N \geq 6$, planar.

PROOF. Here the planarity of K_2, K_3, K_4 is clear from definitions, and the non-planarity of K_5 and of higher K_N graphs is clear too, by thinking a bit. We will leave the formal proof of this latter fact as an instructive exercise, and of course, we will come back in a moment to such questions, with some tools for dealing with them. $\square$

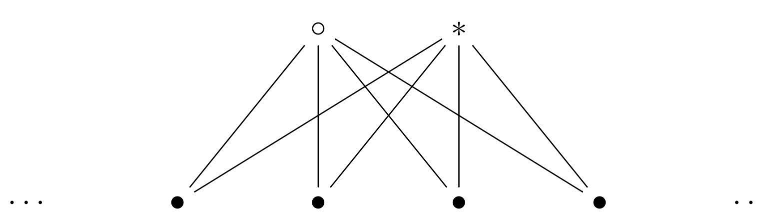
In order to find some further examples of non-planar graphs, we can look as well at the bipartite simplices, and we are led to the following result:

PROPOSITION 5.20. *When looking at bipartite simplices, the square $K_{2,2}$ is planar, and so are all the graphs $K_{2,N}$. However, the next such graph, namely $K_{3,3}$,*



called "utility graph" is not planar. Nor are planar the graphs $K_{M,N}$, for any $M, N \geq 3$.

PROOF. In what regards the first assertion, the bipartite simplex $K_{2,N}$ looks at follows, making it clear that at $N = 2$ we obtain a square, and also that at any $N \in \mathbb{N}$ we have something planar, by pulling the vertex $*$ downwards, in the obvious way:



As for the second assertion, since $K_{M,N}$ with $M, N \geq 3$ contains $K_{3,3}$, it is enough to prove that this latter graph is not planar. But here, as before with K_5, the result is quite clear by thinking a bit, and we will leave the formal proof of this as an instructive exercise, with of course the promise to come back to this, with appropriate tools. □

As a first result now about the planar graphs, which is something famous, we have:

THEOREM 5.21. *For a connected planar graph we have the Euler formula*

$$v - e + f = 2$$

with v, e, f being the number of vertices, edges and faces.

PROOF. As already mentioned, this is something famous, the precise details of the statement, and the idea of the proof, being as follows:

(1) First of all, the original Euler formula, $v - e + f = 2$, was something regarding a convex polyhedron, with v, e, f being as above the number of vertices, edges and faces. As an exercise here for you, check in practice that this formula holds indeed, for all the convex polyhedra that you know, and also that this fails, with $\chi = v - e + f$ being now allowed to take other values $\chi \in \mathbb{Z}$, when removing the convexity assumption.

(2) In what regards now our graph statement, this is something to be taken in a similar sense, that of graphs regarded as polyhedra. As a first exercise here, try making some sense of $v - e + f = 2$ for a tree, where the original quantities $e = v - 1$ and $f = 0$ must be certainly modified, in order for $v - e + f = 2$ to work. And as a second exercise, once this done, that is, once the formula $v - e + f = 2$ starts making sense, at least for trees and other simple graphs, prove this formula, by recurrence on the number of faces f.

(3) Finally, as bonus exercise, learn more about all this, and about the Euler characteristic $\chi = v - e + f$ in general, and also about the genus g, given by $v - e + f = 2 - 2g$. But, in the case of the graphs, we will be back to the genus g, in a moment. □

Speaking theorems coming without proofs, as a second main result about planar graphs, making the connection with the graphs K_5 and $K_{3,3}$ found before, we have:

THEOREM 5.22. *The fact that a graph X is non-planar can be checked as follows:*

1. *Kuratowski criterion: X contains a subdivision of K_5 or $K_{3,3}$.*
2. *Wagner criterion: X has a minor of type K_5 or $K_{3,3}$.*

PROOF. This is obviously something quite powerful, when thinking at the potential applications, and non-trivial to prove as well, the idea being as follows:

(1) Regarding the Kuratowski criterion, the convention is that "subdivision" means graph obtained by inserting vertices into edges, e.g. replacing $\circ - \circ$ with $\circ - \circ - \circ$.

(2) Regarding the Wagner criterion, the convention there is that "minor" means graph obtained by contracting certain edges into vertices.

(3) Finally, regarding the proofs, the Kuratowski and Wagner criteria are more or less equivalent, and their proof is via standard recurrence methods, exercise for you. □

Moving ahead in higher genus, we have here:

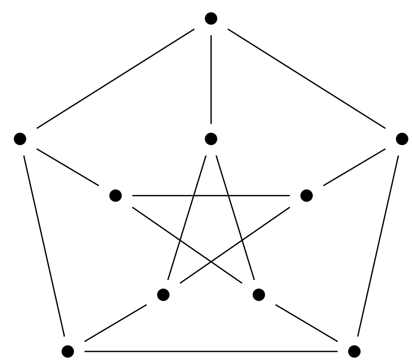
THEOREM 5.23. *For a connected graph of genus $g \in \mathbb{N}$ we have the Euler formula*

$$v - e + f = 2 - 2g$$

with v, e, f being the number of vertices, edges and faces.

PROOF. This comes as a continuation of Theorem 5.21, dealing with the case $g = 0$, and assuming that you have read in detail the proof there, to put it in this way, you will certainly have no troubles now in understanding the present extension, to genus $g \in \mathbb{N}$. ☐

As a basic example of toral graph, $g = 1$, we have the Petersen graph, as follows:



Many things can be said about this graph, and about toral graphs in general.

5d. Further results

Further results.

5e. Exercises

Exercises:

EXERCISE 5.24.

EXERCISE 5.25.

EXERCISE 5.26.

EXERCISE 5.27.

EXERCISE 5.28.

EXERCISE 5.29.

EXERCISE 5.30.

EXERCISE 5.31.

Bonus exercise.

CHAPTER 6

K-theory

6a. Vector bundles

Genrally speaking, you cannot do much geometry with an arbitrary compact space X. However, you can do some, and we have, for instance:

DEFINITION 6.1. *Given a compact space X, its first K-theory group $K_0(X)$ is the group of formal differences of complex vector bundles over X.*

This notion is quite interesting, and we can talk in fact about higher K-theory groups $K_n(X)$ as well, and all this is related to the homotopy groups $\pi_n(X)$ too. There are many non-trivial results on the subject, the end of the game being of course that of understanding the "shape" of X, in the case where X happens to be a manifold.

Getting started now, we can in fact talk about the first K-theory group $K_0(A)$ of an arbitrary C^*-algebra A. We will need the following simple fact:

PROPOSITION 6.2. *Given a C^*-algebra A, the finitely generated projective A-modules E appear via quotient maps $f : A^n \to E$, so are of the form*

$$E = pA^n$$

with $p \in M_n(A)$ being an idempotent. In the commutative case, $A = C(X)$ with X classical, these A-modules consist of sections of the complex vector bundles over X.

PROOF. Here the first assertion is clear from definitions, via some standard algebra, and the second assertion is clear from definitions too, again via some algebra. □

Given a compact space X, it is now clear that $K_0(X)$ can be recaptured from the knowledge of the C^*-algebra $A = C(X)$, and to be more precise we have $K_0(X) = K_0(A)$, when the K-theory group of a C^*-algebra is constructed as follows:

DEFINITION 6.3. *The first K-theory group of A is the group of formal differences*

$$K_0(A) = \{p - q\}$$

of equivalence classes of projections $p \in M_n(A)$, with the equivalence being given by

$$p \sim q \iff \exists u, uu^* = p, u^*u = q$$

and with the additive structure being the obvious one, by diagonal concatenation.

This is very nice, and as a first example, we have $K_0(\mathbb{C}) = \mathbb{Z}$. More generally, as already mentioned above, it follows from Proposition 6.2 that in the commutative case, where $A = C(X)$ with X being a compact space, we have $K_0(A) = K_0(X)$. Observe also that we have, by definition, the following formula, valid for any $n \in \mathbb{N}$:

$$K_0(A) = K_0(M_n(A))$$

Some further elementary observations include the fact that K_0 behaves well with respect to direct sums and with inductive limits, and also that K_0 is a homotopy invariant, and for details here, we refer to any introductory book on the subject.

6b. Higher groups

In what concerns us, we need more examples. However, these examples are not easy to find, and for getting them, we need more theory. We have:

Definition 6.4. *The second K-theory group of a C^*-algebra A is the group of connected components of the unitary group of $GL_\infty(A)$, with*

$$GL_n(A) \subset GL_{n+1}(A) \quad , \quad a \to \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

being the embeddings producing the inductive limit $GL_\infty(A)$.

Again, for a basic example we can take $A = \mathbb{C}$, and we have here $K_1(\mathbb{C}) = \{1\}$, trivially. In fact, in the commutative case, where $A = C(X)$, with X being a usual compact space, it is possible to establish a formula of type $K_1(A) = K_1(X)$. Further elementary observations include the fact that K_1 behaves well with respect to direct sums and with inductive limits, and also that K_1 is a homotopy invariant.

6c. Bott periodicity

Importantly, the first and second K-theory groups are related, as follows:

Theorem 6.5. *Given a C^*-algebra A, we have isomorphisms as follows, with*

$$SA = \left\{ f \in C([0,1], A) \Big| f(0) = 0 \right\}$$

standing for the suspension operation for the C^*-algebras:

(1) $K_1(A) = K_0(SA)$.
(2) $K_0(A) = K_1(SA)$.

Proof. Here the isomorphism in (1) is something rather elementary, and the isomorphism in (2) is something more complicated. In both cases, the idea is to start first with the commutative case, where $A = C(X)$ with X being a compact space, and understand there the isomorphisms (1,2), called Bott periodicity isomorphisms. Then, with this understood, the extension to the general C^*-algebra case is straightforward. □

The above result is quite interesting, making it clear that the groups K_0, K_1 are of the same nature. In fact, it is possible to be a bit more abstract here, and talk in various clever ways about the higher K-theory groups, $K_n(A)$ with $n \in \mathbb{N}$, of an arbitrary C^*-algebra, with the result that these higher K-theory groups are subject to Bott periodicity:

$$K_n(A) = K_{n+2}(A)$$

However, in practice, this leads us back to Definition 6.3, Definition 6.4 and Theorem 6.5, with these statements containing in fact all we need to know.

6d. Some applications

We discuss here some applications of the algebraic topology that we know, to an interesting and seemingly unrelated question from algebra, namely:

QUESTION 6.6. *We know that $\mathbb{R}$ is a field, and so is $\mathbb{R}^2 = \mathbb{C}$, with the usual multiplication of complex numbers. What about $\mathbb{R}^3, \mathbb{R}^4, \mathbb{R}^5, \mathbb{R}^6, \ldots$?*

This is something quite tricky, and to start with, you can play a bit with this, in order to see that the problem is non-trivial. However, the problem can be solved, following a long string of remarkable discoveries, in both mathematics and physics.

The answer to the question, formulated informally, is as follows:

THEOREM 6.7. *In contrast with $\mathbb{R}$, and with $\mathbb{R}^2 = \mathbb{C}$, which are fields:*
(1) *The vector space $\mathbb{R}^3$ does not have a multiplication, making it a field.*
(2) *For $\mathbb{R}^4$ however, something can be done, of rather physics flavor.*
(3) *Also, something can be done for $\mathbb{R}^8$, and that is all.*

PROOF. This is something tricky, the idea being as follows:

(1) Still staying a bit informal, let us first examine the field structures on $\mathbb{R}^N$, with $N \in \mathbb{N}$. A first idea, which is very natural, is that any multiplication on $\mathbb{R}^N$ must come by linearity from a multiplication on the unit sphere $S^{N-1}_\mathbb{R} \subset \mathbb{R}^N$. That is, once we know how to multiply the norm one vectors $x, y \in S^{N-1}_\mathbb{R}$, we can set, by linearity:

$$(\lambda x) * (\mu y) = (\lambda\mu)(x * y)$$

At the level of examples, this is certainly what happens at $N = 1, 2$, where the corresponding unit spheres are as follows, and with the multiplication on $\mathbb{R}^N$ itself appearing as above, from the obvious multiplication on these unit spheres, by linearity:

$$S^0_\mathbb{R} = \{-1, 1\} \quad , \quad S^1_\mathbb{R} = \mathbb{T}$$

(2) In practice now, such ideas require first proving that $||x|| = ||y|| = 1$ implies $||x * y|| = 1$, with $||x|| = \sqrt{\sum x_i^2}$ being the usual norm, and while not exactly obvious, this can be done indeed. As another remark, getting back now to $N = 1, 2$, while the

possible multiplication on $S^0_\mathbb{R}=\{-1,1\}$ is unique, $(-1)^2=1$, in what regards the possible multiplications on $S^1_\mathbb{R}=\mathbb{T}$ things are more complicated, of topology flavor. So, as conclusion, it is pretty much clear that all this leads us into geometry, and topology.

(3) Moving now to $\mathbb{R}^3$, you would say that the vector product $x\times y$ does the job, but this is wrong, because $x\sim y$ implies $x\times y=0$, so definitely wrong way. However, thinking well, a multiplication on $\mathbb{R}^3$ would induce a multiplication on the unit sphere $S^2_\mathbb{R}\subset\mathbb{R}^3$, as explained above, and the point is that there is a topological obstruction to this. And, with our algebraic topology knowledge, we can understand this.

(4) Getting now to $\mathbb{R}^4$, as a good surprise here, the unit sphere $S^3_\mathbb{R}\subset\mathbb{R}^4$ is naturally a group, $S^3_\mathbb{R}=SU_2$. Indeed, solving $U^*=U^{-1}$ under the assumption $\det U=1$ gives:

$$SU_2=\left\{\begin{pmatrix}a&b\\-\bar{b}&a\end{pmatrix}\Big||a|^2+|b|^2=1\right\}$$

Here we use complex numbers, and in real number notation, the result is:

$$SU_2=\left\{\begin{pmatrix}x+iy&z+it\\-z+it&x-iy\end{pmatrix}\Big|x^2+y^2+z^2+t^2=1\right\}$$

(5) But this is obviously good news, we more or less solved our problem, and it remains to work out the details. So, consider the following matrices:

$$c_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad,\quad c_2=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\quad,\quad c_3=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\quad,\quad c_4=\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

In terms of these matrices, which by the way are called Pauli spin matrices, discovered by Pauli in relation with quantum mechanics, but let us not get into this here, maybe later, towards the end of the present book, our result above reads:

$$SU_2=\left\{c_1x+c_2y+c_3z+c_4t\Big|x^2+y^2+z^2+t^2=1\right\}$$

In order to figure out how the resulting multiplication on $\mathbb{R}^4$ looks like, we must first multiply the Pauli matrices. Their products are given by the following formulae:

$$c_2^2=c_3^2=c_4^2=-1$$

$$c_2c_3=-c_3c_2=c_4$$

$$c_3c_4=-c_4c_3=c_2$$

$$c_4c_2=-c_2c_4=c_3$$

Thus, we are led in this way to a multiplication on $\mathbb{R}^4$, as stated.

(6) Alternatively, we have the following real matrices, multiplying quite similarly:

$$1=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\quad,\quad i=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

$$j=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\quad,\quad k=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$$

Thus, one way or another, we are led to the conclusion in the statement.

(7) There is as well a purely algebraic approach to this, using formal numbers $1,i,j,k$, called quaternions, with $1,i$ being the $1,i$ that we know, and with j,k being constructed similarly, a bit like i was, formally via $i^2=-1$, when introducing $\mathbb{C}$. To be more precise, the multiplication rules for i,j,k, found by Hamilton, are as follows:

$$i^2=j^2=k^2=ijk=-1$$

Observe that these are precisely the multiplication rules for the Pauli matrices, from (5) above. Thus, we are again led to the conclusion in the statement.

(8) Finally, along the same lines, the negative result in (3), and more specifically the topological obstruction discussed there, extends in fact to higher dimensions $N\geq 5$, except for the special value $N=8$. And here, at $N=8$, some beasts a bit similar to the quaternions, called octonions, can be constructed, and provide us with some sort of field structure on $\mathbb{R}^8$, missing however many of the field axioms. □

All this way very nice, but was probably more confusing than enlightening, as interesting physics is supposed to be. Adding to the plot, some of the above discoveries were followed by euphoria, first with Hamilton who discovered (7) when walking on a street of Dublin, and was so happy that he carved that i,j,k formula into the nearest stone bridge, then with Pauli who, well, was Pauli and did nothing spectacular when finding (5), and then later with Dirac, who came upon a key version of the Pauli matrices, related to (6), and claimed that he found these by watching logs burning in the fireplace.

Getiting back now to math, let us record, as a conclusion to the above discussion, and as a formal replacement of Theorem 6.7, featuring more math and less physics:

THEOREM 6.8. *In analogy with $\mathbb{R}^2=\mathbb{R}[i]$, with $i^2=-1$, which is a field, we can talk about $\mathbb{R}^4=\mathbb{R}[i,j,k]$, with the following multiplication rules for i,j,k,*

$$i^2=j^2=k^2=ijk=-1$$

called quaternion multiplication rules, and with this being a noncommutative field, in the sense that all the field axioms are satisfied, except for $ab=ba$.

PROOF. This follows indeed from the discussion in the proof of Theorem 6.7, and with the comment of course that, for proper understanding, all that discussion is needed. □

6e. Exercises

Exercises:

EXERCISE 6.9.

EXERCISE 6.10.

EXERCISE 6.11.

EXERCISE 6.12.

EXERCISE 6.13.

EXERCISE 6.14.

EXERCISE 6.15.

EXERCISE 6.16.

Bonus exercise.

CHAPTER 7

Knots

7a. Knots and links

Leaving the general manifolds aside, let us focus now on the simplest objects of topology, namely the knots, with this meaning the smooth closed curves in $\mathbb{R}^3$:

Definition 7.1. *A knot is a smooth closed curve in $\mathbb{R}^3$, regarded modulo smooth transformations.*

And isn't this a beautiful definition. We are here at the core of everything that can be called "geometry", and in fact, thinking a bit on how knots can be knotted, in so many fascinating ways, we are led to the following philosophical conclusion:

Conclusion 7.2. *Knots are to geometry and topology what prime numbers are to number theory.*

At the level of questions now, once we have a closed curve, say given via its algebraic equations, can we decide if is tied or not, and if tied, how complicated is it tied, how to untie it, and so on? But these are, obviously, quite difficult questions. Perhaps simpler now, experience with cables and ropes shows that a random closed curve is usually tied. But can we really prove this? Once again, difficult question.

Fortunately, graph theory comes to the rescue, due to the following fact:

Fact 7.3. *The plane projection of a knot is something similar to a graph with 4-valent vertices, except for the fact that we have some extra data at the vertices, telling us, about the 2 strings crossing there, which goes up and which goes down.*

Based on this, let us try to construct some knot invariants. A natural idea is that of defining the invariant on the 2D picture of the knot, that is, on a plane projection of the knot, and then proving that the invariant is indeed independent on the chosen plane. This method rests on the following technical result, which is well-known:

Theorem 7.4. *Two pictures correspond to plane projections of the same knot precisely when they differ by a sequence of Reidemeister moves.*

Proof. This is somewhat clear from definitions, and in practice, this can be done by some sort of cut and paste procedure, or recurrence if you prefer. □

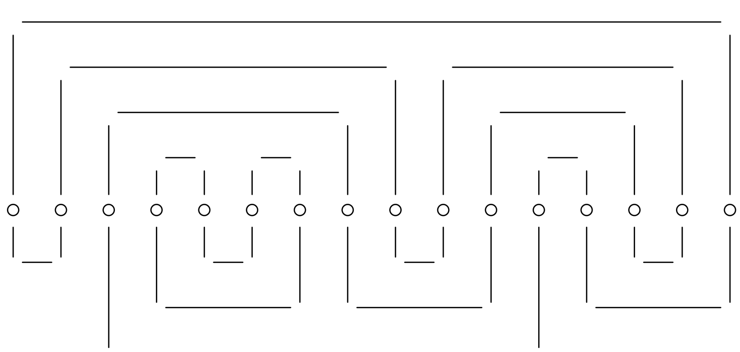
In order to construct now knot invariants, we will need:

THEOREM 7.5. *Any knot can be thought of as being the closure of a braid, with the braids forming a group, called braid group.*

PROOF. Again, this is somewhat clear from definitions, and in practice, this can be done by some sort of cut and paste procedure, or recurrence if you prefer. □

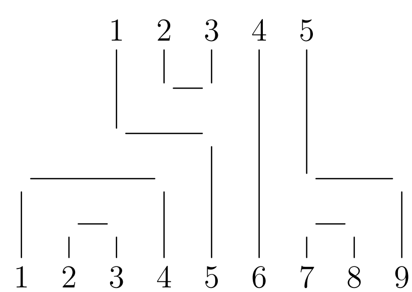
7b. Temperley-Lieb

In order to further advance, the idea is to use the obvious algebraic operation on the pairings in $NC_2(k)$, obtained by superposing such pairings. This leads to some interesting diagrams, known as "meanders", and here is an illustrating example:



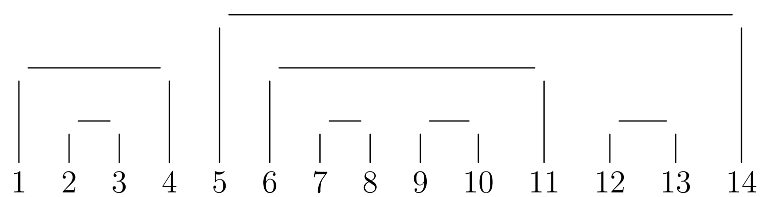
However, we can in fact do better than this. Remember category theory, telling us that for conceptual mathematics, we need objects, and arrows between them? We can do this in our context, by formulating first the following definition:

DEFINITION 7.6. *We denote by $NC_2(k,l)$ the set of noncrossing pairings between an upper row of k points, and a lower row of l points, with for instance*



being an element of $NC_2(5,9)$. With the remark that at $k=0$ we obtain the former $NC_2(l)$, and that at $l=0$ we obtain the former $NC_2(k)$, written upside down.

Observe that we have $NC_2(k,l)=\emptyset$ when $k+l$ is odd. As another key remark, the above definition brings in fact nothing new, combinatorially speaking, because we can always rotate the upper legs, say via $\curvearrowright$, as to reach to a diagram in $NC_2(k+l)$. As an illustration, the rotated version of the pairing in Definition 7.6 looks as follows:



Thus, no need for new counting results of anything, we are ready to go with more algebra. Now with the above definition in hand, we can formulate:

Definition 7.7. *The Temperley-Lieb category TL°_N has the positive integers $\mathbb{N}$ as objects, with the space of arrows $k \to l$ being the formal span*

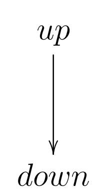
$$TL^\circ_N(k,l) = span(NC_2(k,l))$$

and with the composition of arrows appearing by composing the pairings, in the obvious way, with the rule $\bigcirc = N$, for the closed loops that might appear.

This definition is something quite subtle, hiding several non-trivial things, and is worth a detailed discussion, our comments about it being as follows:

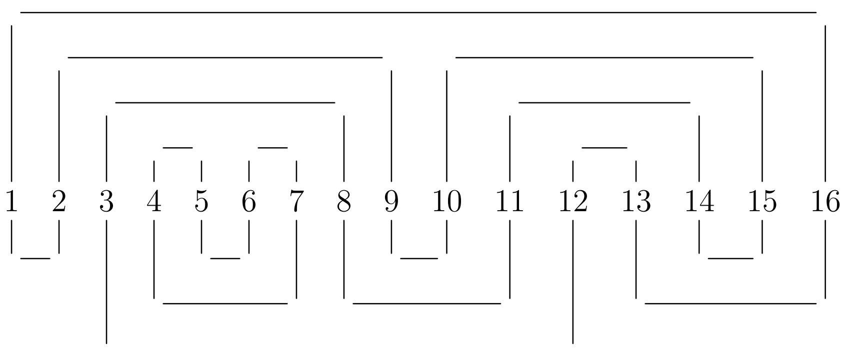
(1) First of all, our scalars in this book will be complex numbers, $\lambda \in \mathbb{C}$, and the "formal span" in the above must be understood in this sense, namely abstract complex vector space spanned by the elements of $NC_2(k,l)$. Of course it is possible to use an arbitrary field, at least at this stage of things, but remember that we are interested in quantum mechanics, and related mathematics, where the field of scalars is $\mathbb{C}$.

(2) Regarding the composition of arrows, this is by obvious vertical concatenation, with the convention, for here and for the rest of this book, that things go "from up to down". And with this convention coming from pure laziness, why pushing things from left to right, when we can have gravity work for us, pulling them from up to down:



(3) Less poetically, this "from up to down" convention is also useful for purely mathematical purposes, because the left-right direction will be reserved for the intervention of sums Σ and scalars $\lambda \in \mathbb{C}$, while the up-down direction will be reserved for "action". But of course, you might argue that this is a bit poetical, too. To which I will answer, give up with your cool and poetry, and your math will soon become some total garbage.

(4) More seriously now, let us discuss what happens with the closed circles, when concatenating. As an example here, let us consider the meander pictured before:



According to our conventions, this meander appears as the product $\pi\sigma \in NC_2(0,0)$ between the upper pairing $\sigma \in NC_2(0,16)$ and the lower pairing $\pi \in NC_2(16,0)$. But, what is the value of this product? We have two loops appearing, namely:

$$1-2-9-10-15-14-11-8-3-12-13-16$$

$$4-5-6-7$$

Thus, according to Definition 7.7, the value of this meander is N^2, with one N for each of the above loops, and with these two values of N multiplying each other.

(5) The same discussion applies to an arbitrary composition $\pi\sigma \in NC_2(k,m)$ between an upper pairing $\sigma \in NC_2(k,l)$ and a lower pairing $\pi \in NC_2(l,m)$, with a certain number of loops appearing in this way, each contributing with a multiplicative factor N.

(6) Finally, in Definition 7.7 the value of the circle $N = \bigcirc$ can be pretty much anything, but due to some positivity reasons to become clear later, we will assume in what follows $N \in [1,\infty)$. Also, we will call this parameter N the "index", with the precise reasons for calling this index to become clear later, too, as this book develops.

With all this discussed, what is next? More category theory I guess, and matter of having a theorem formulated too, instead of definitions only, let us formulate:

Theorem 7.8. *The Temperley-Lieb category TL_N° is a tensor $*$-category, with:*

(1) *Composition of arrows: by vertical concatenation.*
(2) *Tensoring of arrows: by horizontal concatenation.*
(3) *Star operation: by turning the arrows upside-down.*

Proof. This is more of a definition, disguised as a theorem. To be more precise, we already know about (1), from Definition 7.7, and we can talk as well about (2) and (3), constructed as above, with (2) using of course multiplicativity with respect to the scalars, and with (3) using antimultiplicativity with respect to the scalars:

$$\left(\sum_i \lambda_i \pi_i\right) \otimes \left(\sum_j \mu_j \sigma_j\right) = \sum_{ij} \lambda_i \mu_j \pi_i \otimes \sigma_j$$

$$\left(\sum_i \lambda_i \pi_i\right)^* = \sum_i \bar{\lambda}_i \pi_i^*$$

And the point now is that our three operations are compatible with each other via all sorts of compatibility formulae, which are all clear from definitions, with the conclusion being that what we have a tensor $*$-category, as stated. We will leave the details here, basically amounting in figuring out what a tensor $*$-category exactly is, as an exercise. □

In order to further understand the category TL_N°, let us focus on its diagonal part, formed by the End spaces of various objects. With the convention that these End spaces embed into each other by adding bars at right, this is a graded algebra, as follows:

$$TL_N = \bigcup_{k \geq 0} TL_N^\circ(k,k)$$

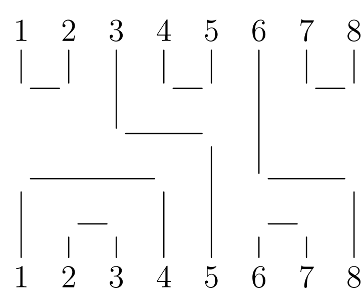
Moreover, for further fine-tuning our study, let us actually focus on the individual components of this graded algebra. These components will play a key role in what follows, and they are worth a dedicated definition, and new notation and name, as follows:

Definition 7.9. *The Temperley-Lieb algebra $TL_N(k)$ is the formal span*

$$TL_N(k) = span(NC_2(k,k))$$

with multiplication coming by concatenating, with the rule $\bigcirc = N$.

In other words, $TL_N(k)$ appears as the formal span of the noncrossing pairings between an upper row of k points, and a lower row of k points, with multiplication coming by concatenating, with $\bigcirc = N$. As an example, here is a basis element of $TL_N(8)$:



Getting back now to what we know about TL_N°, from Theorem 7.8, the tensor product operation makes sense in the context of the diagonal algebra TL_N, but does not apply to its individual components $TL_N(k)$. However, the involution is useful, and we have:

Theorem 7.10. *The Temperley-Lieb algebra $TL_N(k)$ is a $*$-algebra, with involution coming by turning the diagrams upside-down.*

Proof. This is something trivial, which follows from Theorem 7.8, and can be verified as well directly, and we will leave this as an instructive exercise. □

And good news, we have here all the needed definitions, in our bag.

7c. Knot invariants

With these tools, we can now construct some interesting knot invariants.

7d. Further invariants

Further invariants, basically constructed via the same method.

7e. Exercises

Exercises:

Exercise 7.11.

Exercise 7.12.

Exercise 7.13.

Exercise 7.14.

Exercise 7.15.

Exercise 7.16.

Exercise 7.17.

Exercise 7.18.

Bonus exercise.

CHAPTER 8

Mechanical aspects

8a. Ising model

We discuss here some interpretations of the knot invariants constructed in the previous chapter, and notably of the Jones polynomial, in relation with advanced theoretical physics, or if you prefer, in relation with advanced mathematics. The subject is deep and fascinating, lying at the core of what mathematics, physics, and life in general is, and there are two main discoveries to be discussed, due to Jones and Witten, as follows:

(1) After constructing his polynomial, as explained in the previous chapter, Jones further built on this, with a remarkable statistical mechanical interpretation of his invariant, and of other similar invariants. The idea is very simple, namely that on the 2D projection on the knot, "interactions happen at crossings", and it is these interactions which produce the knot invariant, as a kind of partition function. By the way, all this was originally motivated by the presence of the Temperley-Lieb algebra in the invariant constructions, because this algebra first appeared, guess where, in statistical mechanics.

(2) The Jones theory, namely construction of his invariant, of some related invariants, and subsequent statistical mechanics interpretation, can be completed with many other things, such as relation with quantum groups, planar algebras, subfactors and more, and is somehow a complete theory. However, this theory remains something 2D, somewhat missing the true 3D nature of the knot. Based on ideas from quantum field theory, Witten fixed this, by finding a 3D formula for the Jones polynomial, and other knot invariants. With this being, again, related to a lot of further modern mathematics and physics.

Excited by all this? We will explain here these key discoveries of Jones and Witten, from the late 80s, or rather provide an introduction to the subject, and its ramifications in various key branches of math and physics. Hang on, tough math to come.

8b. Knot projections

Knot projections.

8c. Further constructions

Further constructions.

8d. Three dimensions

Three dimensions.

8e. Exercises

Exercises:

Exercise 8.1.

Exercise 8.2.

Exercise 8.3.

Exercise 8.4.

Exercise 8.5.

Exercise 8.6.

Exercise 8.7.

Exercise 8.8.

Bonus exercise.

Part III

Differential geometry

Hey porter, hey porter
Would you tell me the time
How much longer will it be
Till we cross that Mason-Dixon line

CHAPTER 9

Calculus on spheres

9a. Cartography

Welcome to geometry, take two. We have learned to far many interesting things, but with most of them being however of rather algebraic nature. In this second half of the present book we go for the real thing, namely calculus, more calculus, and even more calculus, on suitable classes of manifolds, design to support our calculus desires.

So, let us go back to the basics. Although many interesting algebraic manifolds appear at the advanced level, making algebraic geometry a key tool in advanced physics, in what concerns the basics, here we are mostly in need of a different definition, as follows:

Definition 9.1. *A smooth manifold is a space X which is locally isomorphic to $\mathbb{R}^N$. To be more precise, this space X must be covered by charts, bijectively mapping open pieces of it to open pieces of $\mathbb{R}^N$, with the changes of charts being C^∞ functions.*

As a basic example, we have $\mathbb{R}^N$ itself, or any open subset $X \subset \mathbb{R}^N$. We also have the circles, or curves like ellipses and so on, as shown by the following result:

Theorem 9.2. *The following are smooth manifolds, in the plane:*

1. *The circles.*
2. *The ellipses.*
3. *The non-degenerate conics.*
4. *Smooth deformations of these.*

Proof. All this is quite intuitive, the idea being as follows:

(1) Consider the unit circle, $x^2 + y^2 = 1$. We can write then $x = \cos t$, $y = \sin t$, with $t \in [0, 2\pi)$, and we seem to have here the solution to our problem, just using 1 chart. But this is of course wrong, because $[0, 2\pi)$ is not open, and we have a problem at 0. In practice we need to use 2 such charts, say with the first one being with $t \in (0, 3\pi/2)$, and the second one being with $t \in (\pi, 5\pi/2)$. As for the fact that the change of charts is indeed smooth, this comes by writing down the formulae, or just thinking a bit, and arguing that this change of chart being actually a translation, it is automatically linear.

(2) This follows from (1), by pulling the circle in both the Ox and Oy directions, and the formulae here, based on the formulae from chapter 1, are left to you reader.

(3) We already have the ellipses, and the case of the parabolas and hyperbolas is elementary as well, and in fact simpler than the case of the ellipses. Indeed, a parablola is clearly homeomorphic to $\mathbb{R}$, and a hyperbola, to two copies of $\mathbb{R}$.

(4) This is something which is clear too, depending of course on what exactly we mean by "smooth deformation", and by using a bit of multivariable calculus if needed. □

In higher dimensions now, as basic examples here, we have the unit sphere in $\mathbb{R}^N$, and smooth deformations of it, once again, somehow by obvious reasons. In case you are wondering on how to construct explicit charts for the sphere, the answer comes from:

Theorem 9.3. *We have spherical coordinates in N dimensions,*

$$\begin{cases}x_1&=\ r\cos t_1\\ x_2&=\ r\sin t_1\cos t_2\\ \vdots\\ x_{N-1}&=\ r\sin t_1\sin t_2\ldots\sin t_{N-2}\cos t_{N-1}\\ x_N&=\ r\sin t_1\sin t_2\ldots\sin t_{N-2}\sin t_{N-1}\end{cases}$$

with the corresponding Jacobian being given by the following formula,

$$J(r,t)=r^{N-1}\sin^{N-2}t_1\sin^{N-3}t_2\,\ldots\,\sin^2 t_{N-3}\sin t_{N-2}$$

and with this guaranteeing that the sphere is indeed a smooth manifold.

Proof. There are several things going on here, the idea being as follows:

(1) Let us start with something that you know well, and use all the time in your computations, namely polar coordinates in 2 dimensions. These are as follows:

$$\begin{cases}x&=\ r\cos t\\ y&=\ r\sin t\end{cases}$$

As for the corresponding Jacobian, this can be computed as follows:

$$\begin{aligned}J&=\begin{vmatrix}\frac{d(r\cos t)}{dr}&\frac{d(r\cos t)}{dt}\\ \\ \frac{d(r\sin t)}{dr}&\frac{d(r\sin t)}{dt}\end{vmatrix}\\ &=\begin{vmatrix}\cos t&-r\sin t\\ \sin t&r\cos t\end{vmatrix}\\ &=r\cos^2 t+r\sin^2 t\\ &=r\end{aligned}$$

(2) You know too that we have spherical coordinates in 3 dimensions, as follows:

$$\begin{cases} x &= r\cos s\\ y &= r\sin s\cos t\\ z &= r\sin s\sin t\end{cases}$$

The corresponding Jacobian is a bit tougher to compute, as follows:

$$\begin{aligned}
&J(r,s,t)\\
=&\begin{vmatrix}\cos s & -r\sin s & 0\\ \sin s\cos t & r\cos s\cos t & -r\sin s\sin t\\ \sin s\sin t & r\cos s\sin t & r\sin s\cos t\end{vmatrix}\\
=&\ r^2\sin s\sin t\begin{vmatrix}\cos s & -r\sin s\\ \sin s\sin t & r\cos s\sin t\end{vmatrix}+r\sin s\cos t\begin{vmatrix}\cos s & -r\sin s\\ \sin s\cos t & r\cos s\cos t\end{vmatrix}\\
=&\ r\sin s\sin^2 t\begin{vmatrix}\cos s & -r\sin s\\ \sin s & r\cos s\end{vmatrix}+r\sin s\cos^2 t\begin{vmatrix}\cos s & -r\sin s\\ \sin s & r\cos s\end{vmatrix}\\
=&\ r\sin s(\sin^2 t+\cos^2 t)\begin{vmatrix}\cos s & -r\sin s\\ \sin s & r\cos s\end{vmatrix}\\
=&\ r\sin s\times 1\times r\\
=&\ r^2\sin s
\end{aligned}$$

(3) Moving now to arbitrary N dimensions, the fact that we have indeed spherical coordinates is clear, as before, with the only point to be clarified being the identification of the precise ranges of the angles, which follows from some geometric thinking, first at $N=2,3$, and then in general, and that we will leave as an instructive exercise.

(4) With the remark that we use here mathematicians' convention for the angles, which works nicely in N arbitrary dimensions, as opposed to physicists' convention, which works best at $N=3$. And with this being something quite subjective, because mathematicians' convention is based on physicists' finding that the more dimensions, the better.

(5) Regarding the Jacobian, as before, by developing over the last column, we have:

$$\begin{aligned}
J_N &= r\sin t_1\ldots\sin t_{N-2}\sin t_{N-1}\times\sin t_{N-1}J_{N-1}\\
&+ r\sin t_1\ldots\sin t_{N-2}\cos t_{N-1}\times\cos t_{N-1}J_{N-1}\\
&= r\sin t_1\ldots\sin t_{N-2}(\sin^2 t_{N-1}+\cos^2 t_{N-1})J_{N-1}\\
&= r\sin t_1\ldots\sin t_{N-2}J_{N-1}
\end{aligned}$$

Thus, we obtain the formula in the statement, by recurrence.

(6) Finally, in what regards the last assertion, smooth manifold, this can proved a bit like for the circle, as we did in the proof of Theorem 9.2 (1), basically by cutting the sphere into 2^N parts, and we will leave the details here as an instructive exercise. □

The above formulae are all extremely useful, and we will use them on a daily basis in what follows, at breakfast, lunch and dinner. As a first application, we can now compute the Gauss integral, which is the best calculus formula ever, as follows:

THEOREM 9.4. *We have the following formula,*

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

called Gauss integral formula.

PROOF. Let I be the above integral. By using polar coordinates, we obtain:

$$\begin{aligned} I^2 &= \int_{\mathbb{R}}\int_{\mathbb{R}} e^{-x^2-y^2} dxdy \\ &= \int_0^{2\pi}\int_0^{\infty} e^{-r^2} rdrdt \\ &= 2\pi \int_0^{\infty} \left(-\frac{e^{-r^2}}{2}\right)' dr \\ &= 2\pi \left[0 - \left(-\frac{1}{2}\right)\right] \\ &= \pi \end{aligned}$$

Thus, we are led to the formula in the statement. □

More applications of spherical coordinates, along the same lines, in a moment. Getting back now to our original problem, namely parametrizing the spheres, we have the stereographic projection as well, which was an operation dear to Riemann, the founding father of modern geometry, and which works more directly, as follows:

THEOREM 9.5. *The stereographic projection is given by inverse maps*

$$\Phi : \mathbb{R}^N \to S^N_{\mathbb{R}} - \{\infty\} \quad , \quad \Psi : S^N_{\mathbb{R}} - \{\infty\} \to \mathbb{R}^N$$

given by the following formulae,

$$\Phi(v) = (1,0) + \frac{2}{1+||v||^2}(-1,v) \quad , \quad \Psi(c,x) = \frac{x}{1-c}$$

with the convention $\mathbb{R}^{N+1} = \mathbb{R} \times \mathbb{R}^N$, and with the coordinate of $\mathbb{R}$ denoted x_0, and with the coordinates of $\mathbb{R}^N$ denoted $x_1, \ldots, x_N$.

PROOF. We are looking for the formulae of the isomorphism $\mathbb{R}^N \simeq S^N_{\mathbb{R}} - \{\infty\}$, obtained by identifying $\mathbb{R}^N = \mathbb{R}^N \times \{0\} \subset \mathbb{R}^{N+1}$ with the unit sphere $S^N_{\mathbb{R}} \subset \mathbb{R}^{N+1}$, with the convention that the point which is added is $\infty = (1, 0, \ldots, 0)$, via the stereographic projection. That is, we need the precise formulae of two inverse maps, as follows:

$$\Phi : \mathbb{R}^N \to S^N_{\mathbb{R}} - \{\infty\} \quad , \quad \Psi : S^N_{\mathbb{R}} - \{\infty\} \to \mathbb{R}^N$$

In one sense, according to our conventions above, we must have a formula as follows for our map Φ, with the parameter $t \in (0,1)$ being such that $||\Phi(v)|| = 1$:

$$\Phi(v) = t(0, v) + (1-t)(1, 0)$$

The equation for the parameter $t \in (0,1)$ can be solved as follows:

$$\begin{aligned}(1-t)^2 + t^2||v||^2 = 1 \quad &\iff \quad t^2(1+||v||^2) = 2t \\ &\iff \quad t = \frac{2}{1+||v||^2}\end{aligned}$$

We conclude that the formula of the map Φ is as follows:

$$\Phi(v) = (1,0) + \frac{2}{1+||v||^2}(-1, v)$$

In the other sense now we must have, for a certain $\alpha \in \mathbb{R}$:

$$(0, \Psi(c,x)) = \alpha(c,x) + (1-\alpha)(1,0)$$

But from $\alpha c + 1 - \alpha = 0$ we get the following formula for the parameter α:

$$\alpha = \frac{1}{1-c}$$

We conclude that the formula of the map Ψ is as follows:

$$\Psi(c,x) = \frac{x}{1-c}$$

Here, as before, we use the convention in the statement, namely $\mathbb{R}^{N+1} = \mathbb{R} \times \mathbb{R}^N$, with the coordinate of $\mathbb{R}$ denoted x_0, and with the coordinates of $\mathbb{R}^N$ denoted $x_1, \ldots, x_N$. □

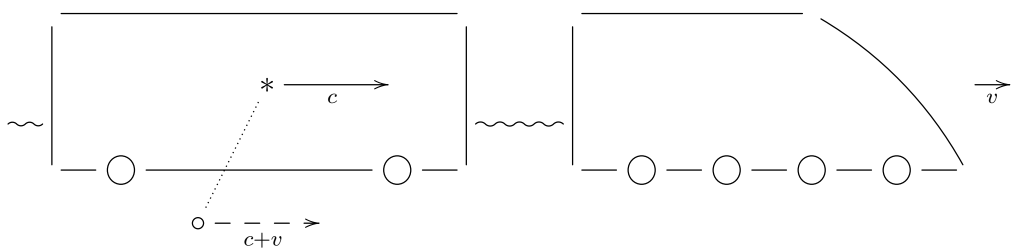
Many interesting things can be said about the stereograophic projection, following Riemann and others, and we will discuss this later, after learning some more abstract geometry, needed in order to formulate our results. In the meantime, however, we can have some fun with relativity, following Einstein, in relation with all this.

Based on experiments by Fizeau, then Michelson-Morley and others, and some physics by Maxwell and Lorentz too, Einstein came upon the following principles:

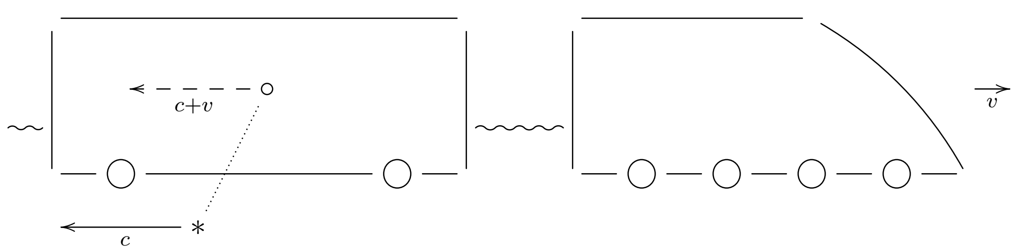
Fact 9.6 (Einstein principles). *The following happen:*

(1) *Light travels in vacuum at a finite speed, $c < \infty$.*
(2) *This speed c is the same for all inertial observers.*
(3) *In non-vacuum, the light speed is lower, $v < c$.*
(4) *Nothing can travel faster than light, $v \not> c$.*

The point now is that, obviously, something is wrong here. Indeed, assuming for instance that we have a train, running in vacuum at speed $v>0$, and someone on board lights a flashlight $*$ towards the locomotive, then an observer $\circ$ on the ground will see the light travelling at speed $c+v>c$, which is a contradiction:



Equivalently, with the same train running, in vacuum at speed $v>0$, if the observer on the ground lights a flashlight $*$ towards the back of the train, then viewed from the train, that light will travel at speed $c+v>c$, which is a contradiction again:



Summarizing, Fact 9.6 implies $c+v=c$, so contradicts classical mechanics, which therefore needs a fix. By dividing all speeds by c, as to have $c=1$, and by restricting the attention to the 1D case, to start with, we are led to the following puzzle:

PUZZLE 9.7. *How to define speed addition on the space of* 1D *speeds, which is*

$$I=[-1,1]$$

with our $c=1$ *convention, as to have* $1+c=1$*, as required by physics?*

In view of our geometric knowledge so far, a natural idea here would be that of wrapping $[-1,1]$ into a circle, and then stereographically projecting on $\mathbb{R}$. Indeed, we can then "import" to $[-,1,1]$ the usual addition on $\mathbb{R}$, via the inverse of this map.

So, let us see where all this leads us. First, the formula of our map is as follows:

PROPOSITION 9.8. *The map wrapping* $[-1,1]$ *into the unit circle, and then stereographically projecting on* $\mathbb{R}$ *is given by the formula*

$$\varphi(u)=\tan\left(\frac{\pi u}{2}\right)$$

with the convention that our wrapping is the most straightforward one, making correspond $\pm 1\to i$*, with negatives on the left, and positives on the right.*

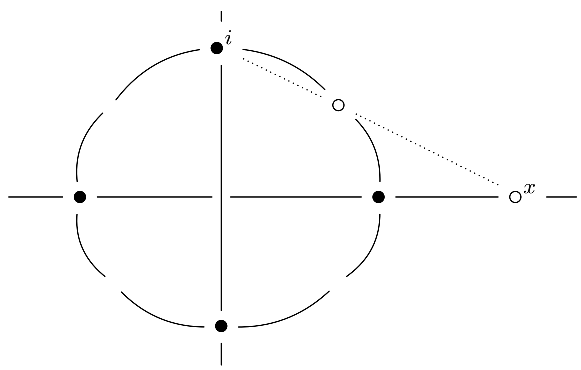
PROOF. Regarding the wrapping, as indicated, this is given by:

$$u \to e^{it} \quad , \quad t = \pi u - \frac{\pi}{2}$$

Indeed, this correspondence wraps $[-1, 1]$ as above, the basic instances of our correspondence being as follows, and with everything being fine modulo 2π:

$$-1 \to \frac{\pi}{2} \quad , \quad -\frac{1}{2} \to -\pi \quad , \quad 0 \to -\frac{\pi}{2} \quad , \quad \frac{1}{2} \to 0 \quad , \quad 1 \to \frac{\pi}{2}$$

Regarding now the stereographic projection, the picture here is as follows:



Thus, by Thales, the formula of the stereographic projection is as follows:

$$\frac{\cos t}{x} = \frac{1 - \sin t}{1} \implies x = \frac{\cos t}{1 - \sin t}$$

Now if we compose our wrapping operation above with the stereographic projection, what we get is, via the above Thales formula, and some trigonometry:

$$\begin{aligned}
x &= \frac{\cos t}{1 - \sin t} \\
&= \frac{\cos\left(\pi u - \frac{\pi}{2}\right)}{1 - \sin\left(\pi u - \frac{\pi}{2}\right)} \\
&= \frac{\cos\left(\frac{\pi}{2} - \pi u\right)}{1 + \sin\left(\frac{\pi}{2} - \pi u\right)} \\
&= \frac{\sin(\pi u)}{1 + \cos(\pi u)} \\
&= \frac{2 \sin\left(\frac{\pi u}{2}\right) \cos\left(\frac{\pi u}{2}\right)}{2 \cos^2\left(\frac{\pi u}{2}\right)} \\
&= \tan\left(\frac{\pi u}{2}\right)
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

The above result is very nice, but when it comes to physics, things do not work, for instance because of the wrong slope of the function $\varphi(u) = \tan\left(\frac{\pi u}{2}\right)$ at the origin, which makes our summing on $[-1,1]$ not compatible with the Galileo addition, at low speeds.

So, what to do? Obviously, trash Proposition 9.8, and start all over again. Getting back now to Puzzle 9.7, this has in fact a simpler solution, based this time on algebra, and which in addition is the good, physically correct solution, as follows:

THEOREM 9.9. *If we sum the speeds according to the Einstein formula*

$$u +_e v = \frac{u+v}{1+uv}$$

then the Galileo formula still holds, approximately, for low speeds

$$u +_e v \simeq u + v$$

and if we have $u = 1$ or $v = 1$, the resulting sum is $u +_e v = 1$.

PROOF. All this is self-explanatory, and clear from definitions, and with the Einstein formula of $u +_e v$ itself being just an obvious solution to Puzzle 9.7, provided that, importantly, we know 0 geometry, and rely on very basic algebra only. □

So, very nice, problem solved, at least in 1D. But, shall we give up with geometry, and the stereographic projection? Certainly not, let us try to recycle that material. In order to do this, let us recall that the usual trigonometric functions are given by:

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i} \quad , \quad \cos x = \frac{e^{ix} + e^{-ix}}{2} \quad , \quad \tan x = \frac{e^{ix} - e^{-ix}}{i(e^{ix} + e^{-ix})}$$

The point now is that, and you might know this from calculus, the above functions have some natural "hyperbolic" or "imaginary" analogues, constructed as follows:

$$\sinh x = \frac{e^{x} - e^{-x}}{2} \quad , \quad \cosh x = \frac{e^{x} + e^{-x}}{2} \quad , \quad \tanh x = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}}$$

But the function on the right, tanh, starts reminding the formula of Einstein addition, from Theorem 9.9. So, we have our idea, and we are led to the following result:

THEOREM 9.10. *The Einstein speed summation in 1D is given by*

$$\tanh x +_e \tanh y = \tanh(x+y)$$

with $\tanh : [-\infty, \infty] \to [-1, 1]$ *being the hyperbolic tangent function.*

PROOF. This follows by putting together our various formulae above, but it is perhaps better, for clarity, to prove this directly. Our claim is that we have:

$$\tanh(x+y) = \frac{\tanh x + \tanh y}{1 + \tanh x \tanh y}$$

But this can be checked via direct computation, from the definitions, as follows:

$$\begin{aligned}
&\frac{\tanh x+\tanh y}{1+\tanh x\tanh y}\\
&= \left(\frac{e^x-e^{-x}}{e^x+e^{-x}}+\frac{e^y-e^{-y}}{e^y+e^{-y}}\right)\Big/\left(1+\frac{e^x-e^{-x}}{e^x+e^{-x}}\cdot\frac{e^y-e^{-y}}{e^y+e^{-y}}\right)\\
&= \frac{(e^x-e^{-x})(e^y+e^{-y})+(e^x+e^{-x})(e^y-e^{-y})}{(e^x+e^{-x})(e^y+e^{-y})+(e^x-e^{-x})(e^y+e^{-y})}\\
&= \frac{2(e^{x+y}-e^{-x-y})}{2(e^{x+y}+e^{-x-y})}\\
&= \tanh(x+y)
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Very nice all this, hope you agree. As a conclusion, passing from the Riemann stereographic projection sum to the Einstein summation basically amounts in replacing:

$$\tan\to\tanh$$

Let us formulate as well this finding more philosophically, as follows:

CONCLUSION 9.11. *The Einstein speed summation in 1D is the imaginary analogue of the summation on* $[-1,1]$ *obtained via Riemann's stereographic projection.*

Which looks quite deep, and we will stop here. More on this later, in chapter 16 below, when discussing curved spacetime, and Lorentz geometry.

9b. Spherical integrals

Getting back now to calculus on the spheres, in a general, all-purpose sense, let us attemps to compute the volumes of spheres. For this purpose, we must understand how the products of coordinates integrate over spheres. Let us start with the case $N=2$. Here the sphere is the unit circle $\mathbb{T}$, and with $z=e^{it}$ the coordinates are $\cos t,\sin t$. We can first integrate arbitrary powers of these coordinates, as follows:

PROPOSITION 9.12. *We have the following formulae,*

$$\int_0^{\pi/2}\cos^p t\,dt=\int_0^{\pi/2}\sin^p t\,dt=\left(\frac{\pi}{2}\right)^{\varepsilon(p)}\frac{p!!}{(p+1)!!}$$

where $\varepsilon(p)=1$ *if* p *is even, and* $\varepsilon(p)=0$ *if* p *is odd, and where*

$$m!!=(m-1)(m-3)(m-5)\ldots$$

with the product ending at 2 *if* m *is odd, and ending at* 1 *if* m *is even.*

PROOF. Let us first compute the integral on the left in the statement:

$$I_p=\int_0^{\pi/2}\cos^pt\,dt$$

We do this by partial integration. We have the following formula:

$$\begin{aligned}(\cos^pt\sin t)' &= p\cos^{p-1}t(-\sin t)\sin t+\cos^pt\cos t\\ &= p\cos^{p+1}t-p\cos^{p-1}t+\cos^{p+1}t\\ &= (p+1)\cos^{p+1}t-p\cos^{p-1}t\end{aligned}$$

By integrating between 0 and $\pi/2$, we obtain the following formula:

$$(p+1)I_{p+1}=pI_{p-1}$$

Thus we can compute I_p by recurrence, and we obtain:

$$\begin{aligned}I_p &= \frac{p-1}{p}\,I_{p-2}\\ &= \frac{p-1}{p}\cdot\frac{p-3}{p-2}\,I_{p-4}\\ &= \frac{p-1}{p}\cdot\frac{p-3}{p-2}\cdot\frac{p-5}{p-4}\,I_{p-6}\\ &\ \vdots\\ &= \frac{p!!}{(p+1)!!}\,I_{1-\varepsilon(p)}\end{aligned}$$

But $I_0=\frac{\pi}{2}$ and $I_1=1$, so we get the result. As for the second formula, this follows from the first one, with $t=\frac{\pi}{2}-s$. Thus, we have proved both formulae in the statement. $\square$

We can now compute the volume of the sphere, as follows:

THEOREM 9.13. *The volume of the unit sphere in $\mathbb{R}^N$ is given by*

$$V=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{2^N}{(N+1)!!}$$

with our usual convention $N!!=(N-1)(N-3)(N-5)\ldots$

PROOF. Let us denote by B^+ the positive part of the unit sphere, or rather unit ball B, obtained by cutting this unit ball in 2^N parts. At the level of volumes, we have:

$$V=2^NV^+$$

We have the following computation, using spherical coordinates, and Fubini:

$$\begin{aligned}
V^+ &= \int_{B^+} 1 \\
&= \int_0^1 \int_0^{\pi/2} \ldots \int_0^{\pi/2} r^{N-1} \sin^{N-2} t_1 \ldots \sin t_{N-2}\, dr dt_1 \ldots dt_{N-1} \\
&= \int_0^1 r^{N-1}\, dr \int_0^{\pi/2} \sin^{N-2} t_1\, dt_1 \ldots \int_0^{\pi/2} \sin t_{N-2} dt_{N-2} \int_0^{\pi/2} 1 dt_{N-1} \\
&= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{(N-2)!!}{(N-1)!!} \cdot \frac{(N-3)!!}{(N-2)!!} \ldots \frac{2!!}{3!!} \cdot \frac{1!!}{2!!} \cdot 1 \\
&= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{1}{(N-1)!!} \\
&= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{1}{(N+1)!!}
\end{aligned}$$

Here we have used the following formula, for computing the exponent of $\pi/2$:

$$\begin{aligned}
\varepsilon(0) + \varepsilon(1) + \varepsilon(2) + \ldots + \varepsilon(N-2) &= 1 + 0 + 1 + \ldots + \varepsilon(N-2) \\
&= \left[\frac{N-2}{2}\right] + 1 \\
&= \left[\frac{N}{2}\right]
\end{aligned}$$

Thus, we obtain the formula in the statement. □

As main particular cases of the above formula, we have:

Theorem 9.14. *The volumes of the low-dimensional spheres are as follows:*

(1) *At $N = 1$, the length of the unit interval is $V = 2$.*
(2) *At $N = 2$, the area of the unit disk is $V = \pi$.*
(3) *At $N = 3$, the volume of the unit sphere is $V = \frac{4\pi}{3}$*
(4) *At $N = 4$, the volume of the corresponding unit sphere is $V = \frac{\pi^2}{2}$.*

Proof. Some of these results are well-known, but we can obtain all of them as particular cases of the general formula in Theorem 9.13, as follows:

(1) At $N = 1$ we obtain $V = 1 \cdot \frac{2}{1} = 2$.

(2) At $N = 2$ we obtain $V = \frac{\pi}{2} \cdot \frac{4}{2} = \pi$.

(3) At $N = 3$ we obtain $V = \frac{\pi}{2} \cdot \frac{8}{3} = \frac{4\pi}{3}$.

(4) At $N = 4$ we obtain $V = \frac{\pi^2}{4} \cdot \frac{16}{8} = \frac{\pi^2}{2}$. □

Let us discuss now the computation of the arbitrary integrals over the sphere. We will need a technical result extending Proposition 9.12, as follows:

THEOREM 9.15. *We have the following formula,*

$$\int_0^{\pi/2}\cos^p t\sin^q t\,dt=\left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)}\frac{p!!q!!}{(p+q+1)!!}$$

where $\varepsilon(p)=1$ if p is even, and $\varepsilon(p)=0$ if p is odd, and where

$$m!!=(m-1)(m-3)(m-5)\ldots$$

with the product ending at 2 if m is odd, and ending at 1 if m is even.

PROOF. We use the same idea as in Proposition 9.12. Let I_{pq} be the integral in the statement. In order to do the partial integration, observe that we have:

$$\begin{aligned}(\cos^p t\sin^q t)' &= p\cos^{p-1}t(-\sin t)\sin^q t\\ &+ \cos^p t\cdot q\sin^{q-1}t\cos t\\ &= -p\cos^{p-1}t\sin^{q+1}t+q\cos^{p+1}t\sin^{q-1}t\end{aligned}$$

By integrating between 0 and $\pi/2$, we obtain, for $p,q>0$:

$$pI_{p-1,q+1}=qI_{p+1,q-1}$$

Thus, we can compute I_{pq} by recurrence. When q is even we have:

$$\begin{aligned}I_{pq} &= \frac{q-1}{p+1}\,I_{p+2,q-2}\\ &= \frac{q-1}{p+1}\cdot\frac{q-3}{p+3}\,I_{p+4,q-4}\\ &= \frac{q-1}{p+1}\cdot\frac{q-3}{p+3}\cdot\frac{q-5}{p+5}\,I_{p+6,q-6}\\ &= \vdots\\ &= \frac{p!!q!!}{(p+q)!!}\,I_{p+q}\end{aligned}$$

But the last term comes from Proposition 9.12, and we obtain the result:

$$\begin{aligned}I_{pq} &= \frac{p!!q!!}{(p+q)!!}\,I_{p+q}\\ &= \frac{p!!q!!}{(p+q)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(p+q)}\frac{(p+q)!!}{(p+q+1)!!}\\ &= \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)}\frac{p!!q!!}{(p+q+1)!!}\end{aligned}$$

Observe that this gives the result for p even as well, by symmetry. Indeed, we have $I_{pq} = I_{qp}$, by using the following change of variables:

$$t = \frac{\pi}{2} - s$$

In the remaining case now, where both p, q are odd, we can use once again the formula $pI_{p-1,q+1} = qI_{p+1,q-1}$ established above, and the recurrence goes as follows:

$$\begin{aligned}
I_{pq} &= \frac{q-1}{p+1}\, I_{p+2,q-2} \\
&= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3}\, I_{p+4,q-4} \\
&= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} \cdot \frac{q-5}{p+5}\, I_{p+6,q-6} \\
&= \vdots \\
&= \frac{p!!q!!}{(p+q-1)!!}\, I_{p+q-1,1}
\end{aligned}$$

In order to compute the last term, observe that we have:

$$\begin{aligned}
I_{p1} &= \int_0^{\pi/2} \cos^p t \sin t\, dt \\
&= -\frac{1}{p+1} \int_0^{\pi/2} (\cos^{p+1} t)'\, dt \\
&= \frac{1}{p+1}
\end{aligned}$$

Thus, we can finish our computation in the case p, q odd, as follows:

$$\begin{aligned}
I_{pq} &= \frac{p!!q!!}{(p+q-1)!!}\, I_{p+q-1,1} \\
&= \frac{p!!q!!}{(p+q-1)!!} \cdot \frac{1}{p+q} \\
&= \frac{p!!q!!}{(p+q+1)!!}
\end{aligned}$$

Thus, we obtain the formula in the statement, the exponent of $\pi/2$ appearing there being $\varepsilon(p)\varepsilon(q) = 0 \cdot 0 = 0$ in the present case, and this finishes the proof. $\square$

We can now compute the arbitrary polynomial integrals over spheres, as follows:

THEOREM 9.16. *The polynomial integrals over the unit sphere $S^{N-1}_\mathbb{R}\subset\mathbb{R}^N$, with respect to the normalized, mass 1 measure, are given by the following formula,*

$$\int_{S^{N-1}_\mathbb{R}} x_1^{k_1}\ldots x_N^{k_N}\,dx=\frac{(N-1)!!k_1!!\ldots k_N!!}{(N+\Sigma k_i-1)!!}$$

valid when all exponents k_i are even. If an exponent is odd, the integral vanishes.

PROOF. The integral in the statement can be written in spherical coordinates, as follows, with A being the area of the sphere, J the Jacobian, and the 2^N factor coming from the restriction to the $1/2^N$ part of the sphere where all coordinates are positive:

$$I=\frac{2^N}{A}\int_0^{\pi/2}\ldots\int_0^{\pi/2}x_1^{k_1}\ldots x_N^{k_N}\,J\,dt_1\ldots dt_{N-1}$$

The normalization constant in front of the integral is easy to compute, given by:

$$\frac{2^N}{A}=\left(\frac{2}{\pi}\right)^{[N/2]}(N-1)!!$$

As for the unnormalized integral, this is given by:

$$\begin{aligned}I'=\int_0^{\pi/2}\ldots\int_0^{\pi/2}\quad&(\cos t_1)^{k_1}(\sin t_1\cos t_2)^{k_2}\\&\vdots\\&(\sin t_1\sin t_2\ldots\sin t_{N-2}\cos t_{N-1})^{k_{N-1}}\\&(\sin t_1\sin t_2\ldots\sin t_{N-2}\sin t_{N-1})^{k_N}\\&\sin^{N-2}t_1\sin^{N-3}t_2\ldots\sin^2 t_{N-3}\sin t_{N-2}\\&dt_1\ldots dt_{N-1}\end{aligned}$$

By rearranging the terms, we obtain the following formula:

$$\begin{aligned}I'&=\int_0^{\pi/2}\cos^{k_1}t_1\sin^{k_2+\ldots+k_N+N-2}t_1\,dt_1\\&\quad\int_0^{\pi/2}\cos^{k_2}t_2\sin^{k_3+\ldots+k_N+N-3}t_2\,dt_2\\&\quad\vdots\\&\quad\int_0^{\pi/2}\cos^{k_{N-2}}t_{N-2}\sin^{k_{N-1}+k_N+1}t_{N-2}\,dt_{N-2}\\&\quad\int_0^{\pi/2}\cos^{k_{N-1}}t_{N-1}\sin^{k_N}t_{N-1}\,dt_{N-1}\end{aligned}$$

Now by using the Wallis formula from Theorem 9.15, this gives:

$$\begin{aligned} I' &= \frac{k_1!!(k_2+\ldots+k_N+N-2)!!}{(k_1+\ldots+k_N+N-1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-2)} \\ &\quad \frac{k_2!!(k_3+\ldots+k_N+N-3)!!}{(k_2+\ldots+k_N+N-2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-3)} \\ &\quad \vdots \\ &\quad \frac{k_{N-2}!!(k_{N-1}+k_N+1)!!}{(k_{N-2}+k_{N-1}+l_N+2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(1)} \\ &\quad \frac{k_{N-1}!!k_N!!}{(k_{N-1}+k_N+1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(0)} \end{aligned}$$

Now let F be the part involving the double factorials, and P be the part involving the powers of $\pi/2$, so that $I' = F \cdot P$. Regarding F, by cancelling terms we have:

$$F = \frac{k_1!!\ldots k_N!!}{(\Sigma k_i + N - 1)!!}$$

As in what regards P, by summing the exponents, we obtain $P = \left(\frac{\pi}{2}\right)^{[N/2]}$. We can now put everything together, and we obtain the formula in the statement. □

As a key application of the above result, we have:

THEOREM 9.17. *The moments of the hyperspherical variables are*

$$\int_{S^{N-1}_\mathbb{R}} x_i^p dx = \frac{(N-1)!!p!!}{(N+p-1)!!}$$

and the rescaled variables $y_i = \sqrt{N}x_i$ become normal and independent with $N \to \infty$.

PROOF. The moment formula in the statement follows from the general formula in Theorem 9.16. As a consequence, with $N \to \infty$ we have the following estimate:

$$\begin{aligned} \int_{S^{N-1}_\mathbb{R}} x_i^p dx &\simeq N^{-p/2} \times p!! \\ &= N^{-p/2} M_p(g_1) \end{aligned}$$

Thus, the rescaled variables $\sqrt{N}x_i$ become normal with $N \to \infty$, as claimed. As for the proof of the asymptotic independence, this is standard too, once again by using the formula in Theorem 9.16. Indeed, the joint moments of $x_1, \ldots, x_N$ are given by:

$$\begin{aligned} \int_{S^{N-1}_\mathbb{R}} x_1^{k_1} \ldots x_N^{k_N}\, dx &= \frac{(N-1)!!k_1!!\ldots k_N!!}{(N+\Sigma k_i - 1)!!} \\ &\simeq N^{-\Sigma k_i} \times k_1!!\ldots k_N!! \end{aligned}$$

By rescaling, the joint moments of the variables $y_i = \sqrt{N}x_i$ are given by:

$$\int_{S^{N-1}_\mathbb{R}} y_1^{k_1}\ldots y_N^{k_N}\,dx \simeq k_1!!\ldots k_N!!$$

Thus, we have multiplicativity, and so independence with $N\to\infty$, as claimed. □

We can recover the normal laws as well in connection with the rotation groups:

THEOREM 9.18. *We have the integration formula*

$$\int_{O_N} U_{ij}^p\,dU = \frac{(N-1)!!p!!}{(N+p-1)!!}$$

and the rescaled variables $V_{ij} = \sqrt{N}U_{ij}$ become normal and independent with $N\to\infty$.

PROOF. We use the basic fact that the rotations $U\in O_N$ act on the points of the real sphere $z\in S^{N-1}_\mathbb{R}$, with the stabilizer of $z=(1,0,\ldots,0)$ being the subgroup $O_{N-1}\subset O_N$. In algebraic terms, this gives an identification as follows:

$$S^{N-1}_\mathbb{R} = O_N/O_{N-1}$$

In functional analytic terms, this result provides us with an embedding as follows, for any i, which makes correspond the respective integration functionals:

$$C(S^{N-1}_\mathbb{R})\subset C(O_N)\quad,\quad x_i\to U_{1i}$$

With this identification made, the result follows from Theorem 9.17. □

Many other things can be said, along these lines. We will be back to this.

9c. Laplace operator

Let us do now something tough, with our spheres. You have certainly heard about the heat equation $\dot{\varphi} = \alpha\Delta\varphi$, or about the wave equation $\ddot{\varphi} = v^2\Delta\varphi$, both involving the Laplace operator for the functions $\varphi:\mathbb{R}^N\to\mathbb{C}$, given by the following formula:

$$\Delta\varphi = \sum_{i=1}^N \frac{d^2\varphi}{dx_i^2}$$

Thinking a bit, it is pretty much clear that, once we will get into serious physics, be that heat or waves or other, we will need the formula of Δ in spherical coordinates. So, let us do this, as a quick calculus exercise. The result, and its proof, are as follows:

THEOREM 9.19. *The Laplace operator in spherical coordinates is*

$$\Delta = \frac{1}{r^2}\cdot\frac{d}{dr}\left(r^2\cdot\frac{d}{dr}\right) + \frac{1}{r^2\sin s}\cdot\frac{d}{ds}\left(\sin s\cdot\frac{d}{ds}\right) + \frac{1}{r^2\sin^2 s}\cdot\frac{d^2}{dt^2}$$

with our standard conventions for these coordinates, in 3D.

PROOF. There are several proofs here, a short, elementary one being as follows:

(1) Let us first see how Δ behaves under a change of coordinates $\{x_i\} \to \{y_i\}$, in arbitrary N dimensions. Our starting point is the chain rule for derivatives:

$$\frac{d}{dx_i} = \sum_j \frac{d}{dy_j} \cdot \frac{dy_j}{dx_i}$$

By using this rule, then Leibnitz for products, then again this rule, we obtain:

$$\begin{aligned}
\frac{d^2 f}{dx_i^2} &= \sum_j \frac{d}{dx_i}\left(\frac{df}{dy_j} \cdot \frac{dy_j}{dx_i}\right) \\
&= \sum_j \frac{d}{dx_i}\left(\frac{df}{dy_j}\right) \cdot \frac{dy_j}{dx_i} + \frac{df}{dy_j} \cdot \frac{d}{dx_i}\left(\frac{dy_j}{dx_i}\right) \\
&= \sum_j \left(\sum_k \frac{d}{dy_k} \cdot \frac{dy_k}{dx_i}\right)\left(\frac{df}{dy_j}\right) \cdot \frac{dy_j}{dx_i} + \frac{df}{dy_j} \cdot \frac{d^2 y_j}{dx_i^2} \\
&= \sum_{jk} \frac{d^2 f}{dy_k dy_j} \cdot \frac{dy_k}{dx_i} \cdot \frac{dy_j}{dx_i} + \sum_j \frac{df}{dy_j} \cdot \frac{d^2 y_j}{dx_i^2}
\end{aligned}$$

(2) Now by summing over i, we obtain the following formula, with A being the derivative of $x \to y$, that is to say, the matrix of partial derivatives dy_i/dx_j:

$$\begin{aligned}
\Delta f &= \sum_{ijk} \frac{d^2 f}{dy_k dy_j} \cdot \frac{dy_k}{dx_i} \cdot \frac{dy_j}{dx_i} + \sum_{ij} \frac{df}{dy_j} \cdot \frac{d^2 y_j}{dx_i^2} \\
&= \sum_{ijk} A_{ki} A_{ji} \frac{d^2 f}{dy_k dy_j} + \sum_{ij} \frac{d^2 y_j}{dx_i^2} \cdot \frac{df}{dy_j} \\
&= \sum_{jk} (AA^t)_{jk} \frac{d^2 f}{dy_k dy_j} + \sum_j \Delta(y_j) \frac{df}{dy_j}
\end{aligned}$$

(3) So, this will be the formula that we will need. Observe that this formula can be further compacted as follows, with all the notations being self-explanatory:

$$\Delta f = Tr(AA^t H_y(f)) + < \Delta(y), \nabla_y(f) >$$

(4) Getting now to spherical coordinates, $(x, y, z) \to (r, s, t)$, the derivative of the inverse, obtained by differentiating x, y, z with respect to r, s, t, is given by:

$$A^{-1} = \begin{pmatrix} \cos s & -r \sin s & 0 \\ \sin s \cos t & r \cos s \cos t & -r \sin s \sin t \\ \sin s \sin t & r \cos s \sin t & r \sin s \cos t \end{pmatrix}$$

The product $(A^{-1})^tA^{-1}$ of the transpose of this matrix with itself is then:

$$\begin{pmatrix}\cos s&\sin s\cos t&\sin s\sin t\\-r\sin s&r\cos s\cos t&r\cos s\sin t\\0&-r\sin s\sin t&r\sin s\cos t\end{pmatrix}\begin{pmatrix}\cos s&-r\sin s&0\\\sin s\cos t&r\cos s\cos t&-r\sin s\sin t\\\sin s\sin t&r\cos s\sin t&r\sin s\cos t\end{pmatrix}$$

But everything simplifies here, and we have the following remarkable formula, which by the way is something very useful, worth to be memorized:

$$(A^{-1})^tA^{-1}=\begin{pmatrix}1&0&0\\0&r^2&0\\0&0&r^2\sin^2 s\end{pmatrix}$$

Now by inverting, we obtain the following formula, in relation with the above:

$$AA^t=\begin{pmatrix}1&0&0\\0&1/r^2&0\\0&0&1/(r^2\sin^2 s)\end{pmatrix}$$

(5) Let us compute now the Laplacian of r,s,t. We first have the following formula, that we will use many times in what follows, and is worth to be memorized:

$$\begin{aligned}\frac{dr}{dx}&=\frac{d}{dx}\sqrt{x^2+y^2+z^2}\\&=\frac{1}{2}\cdot\frac{2x}{\sqrt{x^2+y^2+z^2}}\\&=\frac{x}{r}\end{aligned}$$

Of course the same computation works for y,z too, and we therefore have:

$$\frac{dr}{dx}=\frac{x}{r}\quad,\quad\frac{dr}{dy}=\frac{y}{r}\quad,\quad\frac{dr}{dz}=\frac{z}{r}$$

(6) By using the above formulae, twice, we can compute the Laplacian of r:

$$\begin{aligned}\Delta(r)&=\Delta\left(\sqrt{x^2+y^2+z^2}\right)\\&=\frac{d}{dx}\left(\frac{x}{r}\right)+\frac{d}{dy}\left(\frac{y}{r}\right)+\frac{d}{dz}\left(\frac{z}{r}\right)\\&=\frac{r^2-x^2}{r^3}+\frac{r^2-y^2}{r^3}+\frac{r^2-z^2}{r^3}\\&=\frac{2}{r}\end{aligned}$$

(7) In what regards now s, the computation here goes as follows:

$$\begin{aligned}
\Delta(s) &= \Delta\left(\arccos\left(\frac{x}{r}\right)\right)\\
&= \frac{d}{dx}\left(-\frac{\sqrt{r^2-x^2}}{r^2}\right)+\frac{d}{dy}\left(\frac{xy}{r^2\sqrt{r^2-x^2}}\right)+\frac{d}{dz}\left(\frac{xz}{r^2\sqrt{r^2-x^2}}\right)\\
&= \frac{2x\sqrt{r^2-x^2}}{r^4}+\frac{r^2(z^2-2y^2)+2x^2y^2}{r^4\sqrt{r^2-x^2}}+\frac{r^2(y^2-2z^2)+2x^2z^2}{r^4\sqrt{r^2-x^2}}\\
&= \frac{2x\sqrt{r^2-x^2}}{r^4}+\frac{x(2x^2-r^2)}{r^4\sqrt{r^2-x^2}}\\
&= \frac{x}{r^2\sqrt{r^2-x^2}}\\
&= \frac{\cos s}{r^2\sin s}
\end{aligned}$$

(8) Finally, in what regards t, the computation here goes as follows:

$$\begin{aligned}
\Delta(t) &= \Delta\left(\arctan\left(\frac{z}{y}\right)\right)\\
&= \frac{d}{dx}(0)+\frac{d}{dy}\left(-\frac{z}{y^2+z^2}\right)+\frac{d}{dz}\left(\frac{y}{y^2+z^2}\right)\\
&= 0-\frac{2yz}{(y^2+z^2)^2}+\frac{2yz}{(y^2+z^2)^2}\\
&= 0
\end{aligned}$$

(9) We can now plug the data from (4) and (6,7,8) in the general formula that we found in (2) above, and we obtain in this way:

$$\begin{aligned}
\Delta f &= \frac{d^2f}{dr^2}+\frac{1}{r^2}\cdot\frac{d^2f}{ds^2}+\frac{1}{r^2\sin^2 s}\cdot\frac{d^2f}{dt^2}+\frac{2}{r}\cdot\frac{df}{dr}+\frac{\cos s}{r^2\sin s}\cdot\frac{df}{ds}\\
&= \frac{2}{r}\cdot\frac{df}{dr}+\frac{d^2f}{dr^2}+\frac{\cos s}{r^2\sin s}\cdot\frac{df}{ds}+\frac{1}{r^2}\cdot\frac{d^2f}{ds^2}+\frac{1}{r^2\sin^2 s}\cdot\frac{d^2f}{dt^2}\\
&= \frac{1}{r^2}\cdot\frac{d}{dr}\left(r^2\cdot\frac{df}{dr}\right)+\frac{1}{r^2\sin s}\cdot\frac{d}{ds}\left(\sin s\cdot\frac{df}{ds}\right)+\frac{1}{r^2\sin^2 s}\cdot\frac{d^2f}{dt^2}
\end{aligned}$$

Thus, we are led to the formula in the statement. □

Still with me, I hope. We will get back later to physics, using our formula above. We will get back as well to the Laplace operator Δ, with some alternative definitions for it.

9d. Low dimensions

Many interesting things can be said about the low-dimensional spheres, and we have already met in fact some of them, in chapter 6, when talking about multiplications on $\mathbb{R}^4$. As a joint continuation of that material, and of what we did here, we have:

THEOREM 9.20. *The main character of SU_2 follows the following law,*

$$\gamma_1=\frac{1}{2\pi}\sqrt{4-x^2}dx$$

which is the Wigner law of parameter 1.

PROOF. There are several things going on here, the idea being as follows:

(1) In order to prove the result, our first claim is that we have the following formula, which makes SU_2 isomorphic to the unit sphere $S^1_\mathbb{C}\subset\mathbb{C}^2$:

$$SU_2=\left\{\begin{pmatrix}a&b\\-\bar{b}&\bar{b}\end{pmatrix}\Big|\,|a|^2+|b|^2=1\right\}$$

Indeed, consider an arbitrary 2×2 matrix, written as follows:

$$U=\begin{pmatrix}a&b\\c&d\end{pmatrix}$$

Assuming $\det U=1$, the inverse is then given by the following formula:

$$U^{-1}=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$$

On the other hand, assuming $U\in U_2$, the inverse must be the adjoint:

$$U^{-1}=\begin{pmatrix}\bar{a}&\bar{c}\\\bar{b}&\bar{d}\end{pmatrix}$$

We conclude that our matrix must be of the following special form:

$$U=\begin{pmatrix}a&b\\-\bar{b}&\bar{a}\end{pmatrix}$$

Since the determinant is 1, we must have $|\alpha|^2+|\beta|^2=1$, so we are done with one direction. As for the converse, this is clear too. Finally, we have, as claimed too:

$$S^1_\mathbb{C}=\left\{(a,b)\in\mathbb{C}^2\,\Big|\,|a|^2+|b|^2=1\right\}$$

(2) Our second claim is that we have the following formula, which makes this time SU_2 isomorphic to the unit real sphere $S^3_\mathbb{R}\subset\mathbb{R}^3$:

$$SU_2=\left\{\begin{pmatrix}p+iq&r+is\\-r+is&p-iq\end{pmatrix}\Big|\,p^2+q^2+r^2+s^2=1\right\}$$

Indeed, let us write our parameters $a,b\in\mathbb{C}$, which belong to the complex unit sphere $S^1_\mathbb{C}\subset\mathbb{C}^2$, in terms of their real and imaginary parts, as follows:

$$a=p+iq\quad,\quad b=r+is$$

In terms of these new parameters $p,q,r,s\in\mathbb{R}$, our formula for a generic matrix $U\in SU_2$, that we established before, reads:

$$U=\begin{pmatrix}p+iq&r+is\\-r+is&p-iq\end{pmatrix}$$

As for the condition to be satisfied by the parameters $p,q,r,s\in\mathbb{R}$, this comes the condition $|a|^2+|b|^2=1$ to be satisfied by $\alpha,\beta\in\mathbb{C}$, which reads:

$$p^2+q^2+r^2+s^2=1$$

Thus, we have proved the first part of pur claim. Regarding now the last assertion of our claim, this follows from the fact that the unit sphere $S^3_\mathbb{R}\subset\mathbb{R}^4$ is given by:

$$S^3_\mathbb{R}=\left\{(p,q,r,s)\Big|p^2+q^2+r^2+s^2=1\right\}$$

(3) Getting now to computations, in the geometric picture of $SU_2\simeq S^3_\mathbb{R}$ explained above, the main character of SU_2 is given by the following formula:

$$\chi\begin{pmatrix}a+ib&c+id\\-c+id&a-ib\end{pmatrix}=2a$$

We are therefore left with computing the law of the variable $a\in C(S^3_\mathbb{R})$. But this variable is something very familiar, namely a hyperspherical variable at $N=4$, so we can use here Theorem 9.17. We obtain the following moment formula:

$$\begin{aligned}\int_{S^3_\mathbb{R}}a^{2k}&=\frac{3!!(2k)!!}{(2k+3)!!}\\&=2\cdot\frac{(2k)!}{2^kk!2^{k+1}(k+1)!}\\&=\frac{1}{4^k}\cdot\frac{1}{k+1}\binom{2k}{k}\\&=\frac{C_k}{4^k}\end{aligned}$$

(4) Our claim now is that the variable $2a\in C(S^3_\mathbb{R})$ follows the Wigner semicircle law γ_1. Indeed, the even moments of the Wigner law can be computed with the change of

variable $x = 2\cos t$, and we are led to the following formula:

$$\begin{aligned}
M_{2k} &= \frac{1}{\pi}\int_0^2 \sqrt{4-x^2}x^{2k}\,dx \\
&= \frac{1}{\pi}\int_0^{\pi/2} \sqrt{4-4\cos^2 t}\,(2\cos t)^{2k} 2\sin t\,dt \\
&= \frac{4^{k+1}}{\pi}\int_0^{\pi/2} \cos^{2k} t \sin^2 t\,dt \\
&= \frac{4^{k+1}}{\pi}\cdot\frac{\pi}{2}\cdot\frac{(2k)!!2!!}{(2k+3)!!} \\
&= 2\cdot 4^k\cdot\frac{(2k)!/2^k k!}{2^{k+1}(k+1)!} \\
&= C_k
\end{aligned}$$

As for the odd moments, these all vanish, because the density of γ_1 is an even function. Thus, we are led to the conclusion in the statement. □

9e. Exercises

We had a lot of computations in this chapter, which are all important, the sphere $S^{N-1}_{\mathbb{R}}$ coming just below $\mathbb{R}^N$, in the hierarchy of manifolds. As exercises, we have:

EXERCISE 9.21. *Clarify the range of angles, in the spherical coordinate formula.*

EXERCISE 9.22. *Find other proofs of the Gauss integral formula.*

EXERCISE 9.23. *Learn more about Einstein and relativity, including $E = mc^2$.*

EXERCISE 9.24. *Try to find the speed addition formula in 2D, and in 3D.*

EXERCISE 9.25. *Work out asymptotics for the volume of the sphere in $\mathbb{R}^N$.*

EXERCISE 9.26. *Work out the asymptotics of the hyperspherical laws.*

EXERCISE 9.27. *Apply our formula for Δ to various questions from physics.*

EXERCISE 9.28. *Learn more about the group SU_2, and about SO_3 too.*

As bonus exercise, have some fun with cartography. What is the best possible method, accurately reflecting distances, angles and so on? Once find, patent it.

CHAPTER 10

Smooth manifolds

10a.

10b.

10c.

10d.

10e. Exercises

Exercises:

EXERCISE 10.1.

EXERCISE 10.2.

EXERCISE 10.3.

EXERCISE 10.4.

EXERCISE 10.5.

EXERCISE 10.6.

EXERCISE 10.7.

EXERCISE 10.8.

Bonus exercise.

CHAPTER 11

Embedded manifolds

11a.

11b.

11c.

11d.

11e. Exercises

Exercises:

EXERCISE 11.1.

EXERCISE 11.2.

EXERCISE 11.3.

EXERCISE 11.4.

EXERCISE 11.5.

EXERCISE 11.6.

EXERCISE 11.7.

EXERCISE 11.8.

Bonus exercise.

CHAPTER 12

Stokes, applications

12a.

12b.

12c.

12d.

12e. Exercises

Exercises:

Exercise 12.1.

Exercise 12.2.

Exercise 12.3.

Exercise 12.4.

Exercise 12.5.

Exercise 12.6.

Exercise 12.7.

Exercise 12.8.

Bonus exercise.

Part IV

Riemannian manifolds

There's not a problem that I can't fix
Cause I can do it in the mix
And if your man gives you trouble
Just you move out on the double

CHAPTER 13

Length, area, volume

13a.

13b.

13c.

13d.

13e. Exercises

Exercises:

Exercise 13.1.

Exercise 13.2.

Exercise 13.3.

Exercise 13.4.

Exercise 13.5.

Exercise 13.6.

Exercise 13.7.

Exercise 13.8.

Bonus exercise.

CHAPTER 14

Riemannian manifolds

14a.

14b.

14c.

14d.

14e. Exercises

Exercises:

Exercise 14.1.

Exercise 14.2.

Exercise 14.3.

Exercise 14.4.

Exercise 14.5.

Exercise 14.6.

Exercise 14.7.

Exercise 14.8.

Bonus exercise.

CHAPTER 15

Nash embedding

15a.

15b.

15c.

15d.

15e. Exercises

Exercises:

EXERCISE 15.1.

EXERCISE 15.2.

EXERCISE 15.3.

EXERCISE 15.4.

EXERCISE 15.5.

EXERCISE 15.6.

EXERCISE 15.7.

EXERCISE 15.8.

Bonus exercise.

CHAPTER 16

Curved spacetime

16a.

16b.

16c.

16d.

16e. Exercises

Congratulations for having read this book, and no exercises for this final chapter.

Bibliography

[1] T.M. Apostol, Introduction to analytic number theory, Springer (1976).

[2] V.I. Arnold, Ordinary differential equations, Springer (1973).

[3] V.I. Arnold, Mathematical methods of classical mechanics, Springer (1974).

[4] V.I. Arnold, Lectures on partial differential equations, Springer (1997).

[5] V.I. Arnold, Catastrophe theory, Springer (1974).

[6] V.I. Arnold and B.A. Khesin, Topological methods in hydrodynamics, Springer (1998).

[7] M.F. Atiyah, K-theory, CRC Press (1964).

[8] M.F. Atiyah, The geometry and physics of knots, Cambridge Univ. Press (1990).

[9] M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Addison-Wesley (1969).

[10] T. Banica, Calculus and applications (2024).

[11] T. Banica, Basic number theory (2024).

[12] T. Banica, The joys of relativity theory (2024).

[13] R.J. Baxter, Exactly solved models in statistical mechanics, Academic Press (1982).

[14] N. Berline, E. Getzler and M. Vergne, Heat kernels and Dirac operators, Springer (2004).

[15] B. Blackadar, K-theory for operator algebras, Cambridge Univ. Press (1986).

[16] S.J. Blundell and K.M. Blundell, Concepts in thermal physics, Oxford Univ. Press (2006).

[17] S.M. Carroll, Spacetime and geometry, Cambridge Univ. Press (2004).

[18] A.R. Choudhuri, Astrophysics for physicists, Cambridge Univ. Press (2012).

[19] T.H. Colding and W.P. Minicozzi, A course in minimal surfaces, AMS (2011).

[20] A. Connes, Noncommutative geometry, Academic Press (1994).

[21] A. Connes and M. Marcolli, Noncommutative geometry, quantum fields and motives, AMS (2008).

[22] W.N. Cottingham and D.A. Greenwood, An introduction to the standard model of particle physics, Cambridge Univ. Press (2012).

[23] H.S.M. Coxeter, Regular polytopes, Dover (1948).

[24] P.A. Davidson, Introduction to magnetohydrodynamics, Cambridge Univ. Press (2001).

[25] P.A.M. Dirac, Principles of quantum mechanics, Oxford Univ. Press (1930).

[26] M.P. do Carmo, Differential geometry of curves and surfaces, Dover (1976).

[27] M.P. do Carmo, Riemannian geometry, Birkhäuser (1992).

[28] S. Dodelson, Modern cosmology, Academic Press (2003).

[29] S.K. Donaldson, Riemann surfaces, Oxford Univ. Press (2004).

[30] R. Durrett, Probability: theory and examples, Cambridge Univ. Press (1990).

[31] A. Einstein, Relativity: the special and the general theory, Dover (1916).

[32] L.C. Evans, Partial differential equations, AMS (1998).

[33] W. Feller, An introduction to probability theory and its applications, Wiley (1950).

[34] E. Fermi, Thermodynamics, Dover (1937).

[35] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics, Caltech (1963).

[36] R.P. Feynman and A.R. Hibbs, Quantum mechanics and path integrals, Dover (1965).

[37] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge Univ. Press (2009).

[38] A.P. French, Special relativity, Taylor and Francis (1968).

[39] W. Fulton, Algebraic topology, Springer (1995).

[40] W. Fulton and J. Harris, Representation theory, Springer (1991).

[41] C. Godsil and G. Royle, Algebraic graph theory, Springer (2001).

[42] H. Goldstein, C. Safko and J. Poole, Classical mechanics, Addison-Wesley (1980).

[43] M.B. Green, J.H. Schwarz and E. Witten, Superstring theory, Cambridge Univ. Press (2012).

[44] D.J. Griffiths, Introduction to electrodynamics, Cambridge Univ. Press (2017).

[45] D.J. Griffiths and D.F. Schroeter, Introduction to quantum mechanics, Cambridge Univ. Press (2018).

[46] D.J. Griffiths, Introduction to elementary particles, Wiley (2020).

[47] P. Griffiths and J. Harris, Principles of algebraic geometry, Wiley (1994).

[48] A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique, IHES (1967).

[49] A. Grothendieck et al., Séminaire de géométrie algébrique, IHES (1972).

[50] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford Univ. Press (1938).

[51] J. Harris, Algebraic geometry, Springer (1992).

[52] R. Hartshorne, Algebraic geometry, Springer (1977).

[53] A. Hatcher, Algebraic topology, Cambridge Univ. Press (2002).

[54] H. Hofer and E. Zehnder, Symplectic invariants and Hamiltonian dynamics, Birkhäuser (1994).

[55] L. Hörmander, The analysis of linear partial differential operators, Springer (1983).

[56] R.A. Horn and C.R. Johnson, Matrix analysis, Cambridge Univ. Press (1985).

[57] K. Huang, Introduction to statistical physics, CRC Press (2001).

[58] J.E. Humphreys, Introduction to Lie algebras and representation theory, Springer (1972).

[59] J.E. Humphreys, Linear algebraic groups, Springer (1975).

[60] K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer (1982).

[61] N. Jacobson, Basic algebra, Dover (1974).

[62] V.F.R. Jones, Subfactors and knots, AMS (1991).

[63] V.F.R. Jones and V.S Sunder, Introduction to subfactors, Cambridge Univ. Press (1997).

[64] M. Karoubi, K-theory: an introduction, Springer (1978).

[65] T. Kibble and F.H. Berkshire, Classical mechanics, Imperial College Press (1966).

[66] T. Lancaster and K.M. Blundell, Quantum field theory for the gifted amateur, Oxford Univ. Press (2014).

[67] L.D. Landau and E.M. Lifshitz, Course of theoretical physics, Pergamon Press (1960).

[68] S. Lang, Algebra, Addison-Wesley (1993).

[69] S. Lang, Abelian varieties, Dover (1959).

[70] P. Lax, Linear algebra and its applications, Wiley (2007).

[71] P. Lax, Functional analysis, Wiley (2002).

[72] J.M. Lee, Introduction to topological manifolds, Springer (2011).

[73] J.M. Lee, Introduction to smooth manifolds, Springer (2012).

[74] J.M. Lee, Introduction to Riemannian manifolds, Springer (2019).

[75] D. McDuff and D. Salamon, Introduction to symplectic topology, Oxford Univ. Press (2017).

[76] P. Petersen, Linear algebra, Springer (2012).

[77] P. Petersen, Riemannian geometry, Springer (2006).

[78] B.M. Peterson and B. Ryden, Foundations of astrophysics, Cambridge Univ. Press (2010).

[79] W. Rudin, Principles of mathematical analysis, McGraw-Hill (1964).

[80] W. Rudin, Real and complex analysis, McGraw-Hill (1966).

[81] W. Rudin, Fourier analysis on groups, Dover (1974).

[82] B. Ryden, Introduction to cosmology, Cambridge Univ. Press (2002).

[83] W. Schlag, A course in complex analysis and Riemann surfaces, AMS (2014).

[84] D.V. Schroeder, An introduction to thermal physics, Oxford Univ. Press (1999).

[85] J.P. Serre, A course in arithmetic, Springer (1973).

[86] J.P. Serre, Linear representations of finite groups, Springer (1977).

[87] I.R. Shafarevich, Basic algebraic geometry, Springer (1974).

[88] J.H. Silverman, The arithmetic of elliptic curves, Springer (1986).

[89] J.H. Silverman and J.T. Tate, Rational points on elliptic curves, Springer (2015).

[90] B. Singh, Basic commutative algebra, World Scientific (2011).

[91] C.H. Taubes, Differential geometry, Oxford Univ. Press (2011).

[92] J.R. Taylor, Classical mechanics, Univ. Science Books (2003).

[93] J. von Neumann, Mathematical foundations of quantum mechanics, Princeton Univ. Press (1955).

[94] S. Weinberg, Foundations of modern physics, Cambridge Univ. Press (2011).

[95] S. Weinberg, Lectures on quantum mechanics, Cambridge Univ. Press (2012).

[96] S. Weinberg, Lectures on astrophysics, Cambridge Univ. Press (2019).

[97] H. Weyl, The theory of groups and quantum mechanics, Princeton Univ. Press (1931).

[98] H. Weyl, The classical groups: their invariants and representations, Princeton Univ. Press (1939).

[99] H. Weyl, Space, time, matter, Princeton Univ. Press (1918).

[100] B. Zwiebach, A first course in string theory, Cambridge Univ. Press (2004).

Index