Bachelor's project

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Mathematical Sciences

Skiftestad, Tord

Projective spaces

An extension of affine spaces

Bachelor's project in Mathematical Studies
Supervisor: Smalø, Sverre Olaf
December 2020

NTNU
Norwegian University of Science and Technology

Skiftestad, Tord

Projective spaces

An extrension of affine spaces

Bachelor's project in Mathematical Studies
Supervisor: Smalø, Sverre Olaf
December 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Mathematical Sciences

NTNU
Norwegian University of
Science and Technology

Projective spaces

An extrension of affine spaces

Skiftestad, Tord

December 9, 2020

1 Introduction

Affine spaces are geometric structures where there is a notion of parallel lines. Parallel lines by definition do not intersect each other in any point. However, inspired by visual perspective in the real world, where parallel lines seem to converge to a point on the horizon, comes the idea of a projective space. In a projective space, we add certain "points at infinity", such that parallel lines actually do meet in these points. This introduces a slight problem, as we now have a space containing two different types of points, "regular points", and "points at infinity". This is cumbersome to work with, so we want to use another definition. In this text we will instead define a projective space by looking at the set of 1-dimensional subspaces of a vector space V, together with some additional structure. We will see that this does indeed reflect the above description of what a space with "points at infinity" should look like, while still just containing one type of points.

After defining what projective spaces are and looking at a couple of examples, we will take a look at finite projective spaces, polynomials in projective spaces, and maps between projective spaces. After that we will look at grassmannians, a sort of generalization of projective spaces. In the end, we will look at how grassmannians can be realized as structured subsets of projective spaces, through the use of the "Plücker embedding".

2 Projective Spaces

Let V be a finite dimensional vector space over a field F. We define the equivalence relation on the set $V\backslash\{0\}$:

$$a \sim b \Leftrightarrow \exists \lambda \in F\backslash\{0\}, \lambda a = b \tag{1}$$

In other words, two points in $V\backslash\{0\}$ are related if they belong to the same 1-dimensional subspace of V. The projective space of V, $P(V)$, is then defined as the equivalence classes of $V\backslash\{0\}$ under this equivalence relation:

$$P(V) = (V\backslash\{0\})/\sim \tag{2}$$

("Projective space", Wikipedia)

The elements, or "points", in $P(V)$ are therefore the 1-dimensional subspaces of V. Notice that if $V = \{0\}$, then $P(V) = \emptyset$, since it contains no 1-dimensional subspaces.

We define the map $p_V : V\backslash\{0\} \to P(V)$ given by $p_V(v) = [v]$, the map that maps a vector in $V\backslash\{0\}$ onto the unique 1-dimensional subspace that contains it. We also define a choice function $s_V : P(V) \to V\backslash\{0\}$ that will serve as a right inverse of p_V. Given a 1-dimensional subspace $a \in P(V)$, s_V will choose a vector $v \neq 0$ belonging to this subspace, and define $s_V(a) = v$. In other words we want s_V to satisfy: $p_V(s_V(a)) = a, \forall a \in P(V)$. While s_V does not work as a left inverse, it will atleast satisfy that given a $v \in V\backslash\{0\}$, $s_V(p_V(v)) = \lambda v$ for some $\lambda \in F\backslash\{0\}$.

We then give $P(V)$ a geometric structure by defining what a line in $P(V)$ is: Given two distinct points $a, b \in P(V)$, the line through these points consists of all points $c \in P(V)$ such that $s_V(c) \in \text{span}\{s_V(a), s_V(b)\}$. This means that all 1-dimensional subspaces that belong to the same 2-dimensional subspace of V lie on a line in $P(V)$. In other words a line in $P(V)$ corresponds to a 2-dimensional subspace of V. Generalizing this concept, a k-dimensional subspace U of V corresponds to a "subspace" in $P(V)$ of dimension $k-1$. If the whole space V has dimension $n+1$, we say that $P(V)$ has dimension n.

For any vector space V over F, if $\dim V = n+1$, we have $V \simeq F^{n+1}$ through the choice of a basis for V. In section 5 we will see that this implies

that their projective spaces are also isomorphic: $P(V) \simeq P(F^{n+1}) := P^n(F)$. This shows that since all $n+1$ dimensional F vector spaces are isomorphic, we can talk about the projective space of dimension n over F, $P^n(F)$, without needing to specify what the underlying vector space is.

How should we denote the elements of $P(V)$? For any point $a \neq 0$ in V, there is a unique 1-dimensional subspace of V containing a. Given an ordered basis of V, we can use the coordinates of a to denote this 1-dimensional subspace. This comes with a slight problem, since for any $\lambda \in F\backslash\{0\}$, a and λa denote the same 1-dimensional subspace. To counteract this we simply define the "homogeneous coordinates" of an element in $P(V)$ to be equal to the coordinates of any nonzero vector in the 1-dimensional subspace, together with the equivalence relation that two sets of homogeneous coordinates represent the same element if one can be scaled by some number $\lambda \in F\backslash\{0\}$ to get the the other one. If we want a unique representation for each 1-dimensional subspace of V, we can scale a in such a way that the first nonzero coordinate becomes 1. Geometrically, this corresponds to seeing where the line intersects a specific affine subspace of V. If $\dim(V) = n$, an element in $P(V)$ can then be uniquely identified by one element in the following set:

$$S = \{(1, a_{12}, \ldots, a_{1n})\} \cup \{(0, 1, a_{23}, \ldots, a_{2n})\} \cup \ldots \cup (0, \ldots, 1), a_{ij} \in F \quad (3)$$

Example: Let $V = \mathbb{R}^3$, and take any $v = (v_1, v_2, v_3) \in V$. We want to represent the 1-dimensional subspace U of V containing this vector uniquely. If $v_1 \neq 0$, we can represent U by $v/v_1 = (1, v_2/v_1, v_3/v_1) = (1, a, b)$, which geometrically corresponds to the intersection of U and the affine plane given by $x = 1$. So we can represent any 1-dimensional subspace U where $v_1 \neq 0$ uniquely by an element on the form $(1, a, b)$.

If $v_1 = 0$ and $v_2 \neq 0$, we can represent U by the element $v/v_2 = (0, 1, v_3/v_2) = (0, 1, c)$. Geometrically this corresponds to the point where U intersects the affine line given by $y = 1, x = 0$. Thus we can represent any of these elements by a point on the form $(0, 1, c)$.

The only remaining 1-dimensional subspace is the z-axis, which we can then represent by the point $(0, 0, 1)$. All in all, this gives us a way to denote each element in $P(V)$ with a unique element in the set:

$$S = \{(1, a, b)|a, b \in \mathbb{R}\} \cup \{(0, 1, c)|c \in \mathbb{R}\} \cup (0, 0, 1) \tag{4}$$

The points with first coordinate 0 are the ones corresponding to the "points at infinity" mentioned in the introduction. To see this, we take an element with nonzero first coordinate $v = (1, a, b)$. We want to see what happens to v when we get further out in this plane, as $(a^2 + b^2) \to \infty$. Since there are many ways this can approach infinity, we dont always get that v converges to a point in the projective space (for example by going out in a spiral). However, if we assume that $\lim_{(a^2+b^2)\to\infty} a \neq 0$, and $\lim_{(a^2+b^2)\to\infty} \frac{b}{a} = r$, then v converges. Since v is represented with homogeneous coordinates, we can scale v by $\frac{1}{a}$ to get $v = (\frac{1}{a}, 1, \frac{b}{a})$. Because of the assumptions above, we get that $|a| \to \infty$, so the frist coordinate will go to 0, and the third coordinate will go to r. The result is that v will converge to the point $(0, 1, r)$. If we instead assume that $\lim_{(a^2+b^2)\to\infty} a = 0$, then $|b| \to \infty$. Scaling the homogeneous coordinates by $\frac{1}{b}$, we get that $v = (\frac{1}{b}, \frac{a}{b}, 1)$, which converges to $(0, 0, 1)$ as $(a^2 + b^2) \to \infty$. Since $\frac{b}{a} = r = \frac{-b}{-a}$, $(1, a, b)$ and $(1, -a, -b)$ converge to the same point as $(a^2 + b^2) \to \infty$. This shows that there is a 180 degree rotational equivalence of the limit points. To picture this fact we can "glue" the set $\{(0, 1, c)|c \in \mathbb{R}\} \cup (0, 0, 1)$ twice around the affine part of the projective space, with $(0, 1, 0)$ at both infinities along the y axis, and $(0, 0, 1)$ at both infinities along the z axis. (see bottom of figure 1)

Another way to look at the elements of $P(\mathbb{R}^3)$ is to identify a 1-dimensional subspace of $\mathbb{R}^3$ with the two points in which they intersect the unit sphere. Specifically:

$$\begin{aligned} P(\mathbb{R}^3) &\simeq S^2/\sim \\ a \sim b &\Leftrightarrow a = b \vee a = -b \end{aligned} \tag{5}$$

This approach has the benefit of being indpendent of choice of coordinate system, as well as showing that all points are equivalent; there isn't technically anything "infinite" or special about some of the points. Since lines in $P(\mathbb{R}^3)$ correspond to 2-dimensional subspaces of $\mathbb{R}^3$, they will be represented by the intersection of a 2-dimensional subspace and the unit sphere, which is a great circle on the unit sphere. This representation also gives a way to define a distance between two points in $P(\mathbb{R}^3)$, as the shortest distance along the unit sphere between the representatives of the two points.

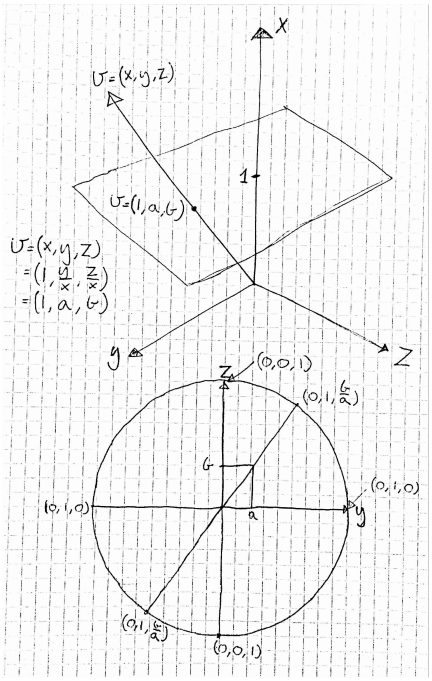


Figure 1:
Top picture shows how scaling the first coordinate of a vector to 1 is equivalent to see where it intersects the plane given by $x = 1$.

Bottom picture shows the plane given by $x = 1$ seen from above, and how the points with $x = 0$ can be seen as "points at infinity" on the edge of the plane.

3 Finite Projective Spaces

Let F_q be the finite field with q elements. We now look at the vector space $V = F_q^n$ over F_q. How many elements are there in $P(V)$? There are several approaches here. One option is to look at the set S we defined in section 2:

$$S = \{(1, a_{12}, \ldots, a_{1n})\} \cup \{(0, 1, a_{23}, \ldots, a_{2n})\} \cup \ldots \cup (0, \ldots, 1), a_{ij} \in F_q \quad (6)$$

We argued previously how there is a bijection between S and $P(V)$, so we just need to count the number of elements in S and we're done. Since $|F_q| = q$, we have: $|P(V)| = |S| = q^{n-1} + \ldots + 1 = \frac{q^n - 1}{q-1}$.

Another approach is to look at all the vectors in V, and what 1-dimensional subspaces those vectors generate. We know $|V| = |F_q^n| = |F_q|^n = q^n$. We remove 0, the only vector which does not genrerate a 1-dimensional subspace. We are left with $q^n - 1$ vectors, each generating a 1-dimensional subspace. But we are overcounting, because given a 1-dimensional subspace generated by v, it is also generated by the $q-2$ other elements $f_2 \cdot v, \ldots, f_{q-1} \cdot v, f_i \in F_q$, in total we have $q - 1$ generators for this subspace. This means we are overcounting each 1-dimensional subspace exactly $q - 1$ times too many, which

means we get: $|P(V)| = \frac{q^n-1}{q-1}$.

How do some of the simplest finite projective spaces look like? We take $V = F_2^3$, and look at $P(V)$. Given any vector $a \in V$, the 1-dimensional subspace containing a consists of exactly two points: a and 0. Therefore each 1-dimensional subspace of V is uniquely determined by the nonzero vector it contains. There are 7 nonzero vectors in V, each of which determine a 1-dimensional subspace. This means $P(V)$ consists of 7 points, which can be represented in homogeneous coordinates by the unique nonzero vector contained in each of the 1-dimensional subspace. Writing it out we get the set:

$$S = \{(a, b, c) \in F_2^3 | (a, b, c) \neq (0, 0, 0)\} \tag{7}$$

The lines in $P(V)$ can in this case be determined by the following: Given two points $a = (a_1, a_2, a_3), b = (b_1, b_2, b_3)$, a third point $c = (c_1, c_2, c_3)$ lie on the same line if $c = f_1 \cdot a + f_2 \cdot b$. Since the field is so small, the only such nonzero linear combinations are a, b and $a + b$. So the only point on this line distinct from a and b is $a + b$. We end up with the following picture consisting of 7 points and 7 lines, 3 point on each line, 3 lines through each point. This is called the "Fano plane". (Figure 2)

The case above where we use F_2 as the base field is a bit special, because the elements in $P(V)$ are in a 1 to 1 correspondence with the nonzero elements of V, since each 1-dimensional subspace only contain one nonzero element. What happens if we look at $V = F_3^3$ instead? By the formula at the start of this section, we know that $|P(V)| = \frac{3^3-1}{3-1} = 13$, but how are these points connected by lines?

We identify each line in $P(V)$ with the homogeneous coordinate where the first nonzero coordinate is 1. There are 9 points on the form $(1, a, b)$, 3 points on the form $(0, 1, c)$, and the last point represented by $(0, 0, 1)$. We start out by putting the 9 points with nonzero first coordinate in a 3×3 grid, such that any straight line or diagonal in this grid is a line in $P(V)$. After this is done, the points on the offset diagonals and the corner points farthest away from this diagonal also lie on a line in $P(V)$, so we draw this in. Now each line contains exactly 3 points. We get this picture (Figure 3):

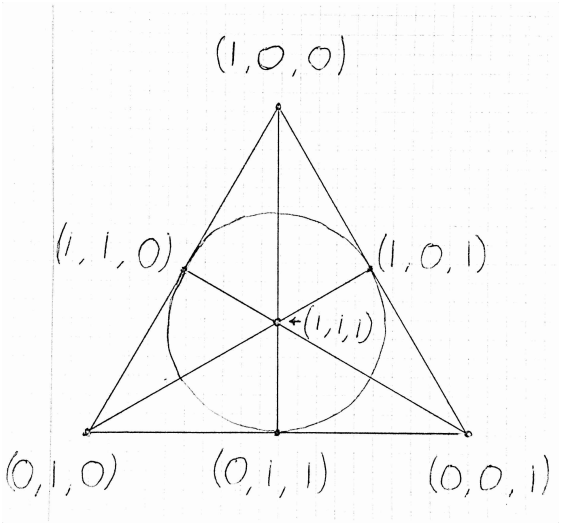
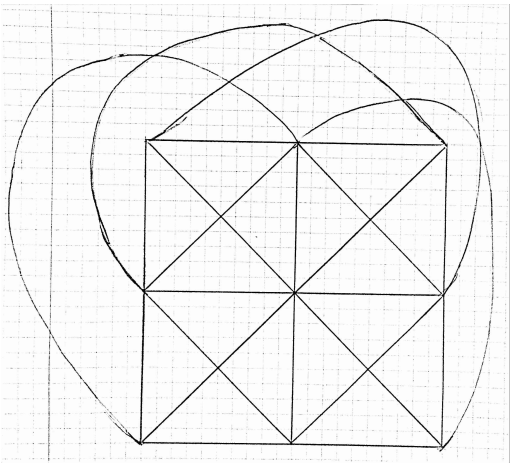
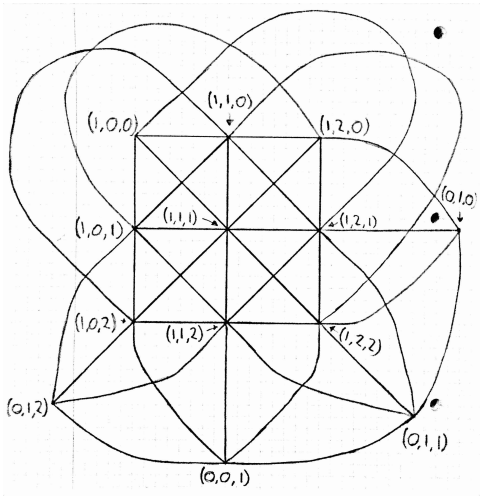


Figure 2:
$P(F_2^3)$, the "Fano plane".

Figure 3 (Below):
Shows the 9 points of $P(F_3^3)$ with nonzero first coordinates and the lines between them.



Adding the 4 remaining points (which all lie on a line), and drawing out the lines which contain them, we get:



We end up with 13 lines, each of which contain 4 points. We can also notice that each point is contained in 4 lines. Notice that in both of these examples there seems to be some sort of symmetry hiding, the number of points in $P(V)$ is equal to the number of lines in $P(V)$, and the number of lines through any point is the same as the number of points on any line. We will get back to why this happens.

Finite projective spaces are entirely symetrical in the following sense: Every line contains an equal number of points, and all points have an equal number of lines going through them. We can see this by looking at the underlying vector space:

Let $V = F_q^n$ over F_q. Given a 2-dimensional subspace U of V, we can write $U = span(v_1, v_2)$. Given any fixed 1-dimensional subspace W of U, W is generated by a single element w. Since W is a subspace of U, w can be written as a linear combination of v_1 and v_2. We claim that the spaces generated by each of the following vectors are distinct and are all the 1-dimensional subspaces of U: $S = \{v_1, v_2, v_1 + f_1 v_2, v_1 + f_2 v_2 \ldots, v_1 + f_{q-1} v_2\}$,

where $f_1 \dots f_{q-1}$ are the $q-1$ nonzero elements of F. Given any other element generating a 1-dimensional subspace $(f_i v_1 + f_j v_2)$, we can multiply it by f_i^{-1} to get $(v_1 + f_i^{-1} f_j v_2) \in S$ (If $f_i = 0$, then $f_i v_1 + f_j v_2 = f_j v_2$, so this generates the same space as $v_2 \in S$). Since $|S| = q+1$ independent on the choice of U, this shows that all 2-dimensional subspaces of V contain the same number of 1-dimensional subspaces.

The second part of the symmetry mentioned above corresponds to counting the number of 2-dimensional subspaces of V which contain a fixed 1-dimensional subspace of V.

Again let $V = F_q^n$ over F_q. Given a 1-dimensional subspace U of V, how many choices do we have for a second 1-dimensional subspace W of V such that $\dim(U+W) = 2$? There are $q^n - q$ ways to chose a vector $w \notin U$, which will then be a generator of W. There are $q-1$ generators of W, so we divide by this. We get that there are $\frac{q^n-q}{q-1}$ choices for W such that $\dim(U+W) = 2$. But can we chose $W_1 \neq W_2$ and get $U + W_1 = U + W_2$? Yes, but this is exactly when W_1 and W_2 lie on the same line as U in $P(V)$. Above we saw that each line in $P(V)$ contains $q+1$ points, so without counting U itself, there are q choices of W which result in the same 2-dimensional subspace $U+W$. Dividing by this we get: #2-dimensional subspaces containing $U = \frac{q^n-q}{(q-1)\cdot q} = \frac{q^{n-1}-1}{(q-1)}$. We see here that this is also independent of the choice of U, so its the same for any fixed 1-dimensional subspace of V.

The above explains parts of the symetries we noticed when looking at $P(F_2^3)$ and $P(F_3^3)$. In these examples the number of lines through any point and the number of points on any line were equal. We see now that this is not true in general, but just a consequence of that for $n = 3$, we have $\frac{q^{n-1}-1}{(q-1)} = \frac{q^2-1}{(q-1)} = \frac{(q+1)(q-1)}{(q-1)} = q+1$.

As a result of the symmetry of these finite projective spaces, we can look at the symmetry group of any of them, the set of permutations of the points in $P(V)$ which preserve the line structure through the points.

Example: We will look at the symmetry group of $P(F_2^3)$. We can find the size of the group by just counting. There are 7 choices for where to put the first point, and 6 choices for the choice of another point on the same line. To preserve colinearity, the choice for the last point on that line is forced.

Now we have 4 choices for the next point. After this however, the choices for the last 3 points are forced. So the size of the symmetry group is $7 \cdot 6 \cdot 4 = 168$.

4 Polynomials in projectives spaces

Given the projective space $P^{n-1}(F)$, elements can be represented by homogeneous coordinates, a set of n numbers as shown in section 2. Given a polynomial $f \in F[x_1, \ldots, x_n]$, can we evaluate it in a point in the projective space? In general, no, because we require the value of f to be independent of representative of the point in the projective space: $f(x_1, \ldots, x_n) = f(\lambda x_1, \ldots, \lambda x_n)\ \forall \lambda \neq 0$. If we limit ourselfs to homogeneous polynomials, the polynomials in which all terms are of the same degree k, we get: $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^k f(x_1, \ldots, x_n)$. So while $f(x)$ and $f(\lambda x)$ do not have the same values, the set of points in which they evaluate to zero are the same: $f(x) = 0 \Leftrightarrow f(\lambda x) = 0$. Because of this, in a projective space it is often interresting to study the zero set of a homogeneous polynomial. We therefore make the following definition:
Given a set S of homogeneous polynomials in n variables over a field F:

$$S = \{f \in F[x_1, \ldots x_n] | f \text{ homogeneous}\} \tag{8}$$

the projective variety $U_S \subseteq P^{n-1}(F)$ defined by S is the set of common zeroes for all these polynomials.

$$U_S = \{x \in P^{n-1}(F) | f(x) = 0\ \forall f \in S\} \tag{9}$$

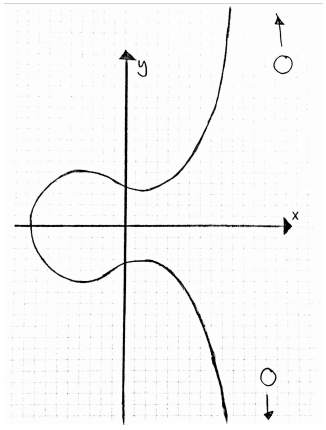
("Projective variety", Wikipedia)

If $|S| = \infty$, we know through hilberts basis theorem that there exists a finite set of homogeneous polynomials S' such that $U_S = U_{S'}$ ("Hilbert's basis theorem", Wikipedia).

If we have a polynomial $f \in F[x_1, \ldots, x_n]$ of degree k which is not homogeneous, we can homogenize it by introducing a new variable x_0, and multiplying each term by it enough times so that each term has degree k. We can now study it in a projective space, and setting $x_0 = 1$ will return back the original polynomial.

Why would we want to work with projective varieties compared to for example affine varieties? One example of how projective varieties behave nicely is a result known as Bézout's theorem. The statement of the theorem is as follows: Take the projective space $P^n(F)$, F algebraically closed, and n projective varieties, where each one is defined by a single homogeneous polynomial in $n+1$ variables. Then the number of common intersection points of all these projective varieties is either equal to the product of the degrees of their defining polynomials, or infinite. ("Bézout's theorem", Wikipedia)

We will now take a look at elliptic curves, an example of a projective variety that is used in cryptography and number theory among other things. An elliptic curve over a field F (with characteristic different from 2 and 3) is often defined as the points $(x, y) \in F^2$ that satisfies an equation on the form: $y^2 = x^3+ax+b$, where $4a^3+27b^2 \neq 0$, together with a unique point O at infinity. Because of this point at infinity, the curve really lies in a projective plane. If we homogenize the equation, we can find out exactly how the elliptic curve looks like. We add a variable z, and look at the projective variety defined by the equation $zy^2 = x^3 + az^2x + bz^3$ in homogenous coordinates (z, x, y). Putting $z = 1$ we get back the original equation, so that gives us all the points of the elliptic curve that lies on the affine part. If $z = 0$, we get that $0 = x^3$, which means $x = 0$. Thus we are left with the point $(0, 0, 1)$ in the projective space as the only solution outside of the affine part of the projective plane, this is the unique point at infinity O. If we look at a picture of an elliptic curve, this makes sense: As we look further out on the curve, it becomes more and more parallel to the y axis, and the homogeneous coordinate $(0, 0, 1)$ represents exactly this, the direction along the y axis. ("Elliptic curve", Wikipedia)



5 Homographies

A homography is an isomorphism of projective spaces. It is a bijection that is structure preserving in the sense that lines are mapped to lines. Given an isomorphism of vector spaces $G : V \to W$, there is an induced isomor-

phism of their projective spaces, $H : P(V) \to P(W),\ H(x) = p_W(G(s_V(x)))$. Here p_W and s_V are the functions defined in section 2. In words, given a 1-dimensional subspace x of V, $H(x)$ first chooses a vector contained in x, then maps that vector into W through the isomorphism G, then projects the result back onto the 1-dimensional subspace of W containing the result.

We show that H is in fact an isomorphism. Its inverse is doing almost the same as H, just going opposite way through the use of G^{-1}, $H^{-1}(y) = p_V(G^{-1}(s_W(y)))$, $H(H^{-1}(y)) = p_W(G(s_V(p_V(G^{-1}(s_W(y))))))) =$ $p_W(G(\lambda G^{-1}(s_W(y)))) = p_W(\lambda G(G^{-1}(s_W(y)))) = p_W(\lambda s_W(y)) = p_W(s_W(y)) = y$, calculating that $H^{-1}(H(x)) = x$ is exactly the same argument.

Is it structure preserving, in that lines in P(V) are mapped to lines in P(W)? Since G is an isomorphism, a 2-dimensional subspace of V is mapped surjectively onto a 2-dimensional subspace of W. This is exactly what it means for lines to be mapped to lines in the projective spaces, so yes it is structure preserving.

We also need to show that the isomorphism H is independent of the choice function s_V used: Let s_V and $\overline{s_V}$ be two different choice functions as defined in section 2, with $s_V(x) = v$ and $\overline{s_V}(x) = u$. Since u and v are both nonzero and belong to the same 1-dimensional subspace of V, we can write $v = \lambda u$ for some $\lambda \neq 0$. We get: $H(x) = p_W(G(s_V(x))) = p_W(G(v)) = p_W(G(\lambda u)) = p_W(\lambda G(u)) = p_W(G(u)) = p_W(G(\overline{s_V}(x)))$. This works because G is linear and $p_W(a) = p_W(\lambda a)\ \forall \lambda \in F \backslash \{0\}$.

This verifies the statement in section 2 that we can identify a projective space $P^n(F)$ without knowing or specifying what the underlying vector space is: Given any $V \simeq F^{n+1}$, we get by the induced isomorphism above that: $P(V) \simeq P(F^{n+1}) := P^n(F)$.

An example of a homography, and maybe the classical reason why people started studying projective spaces, is that of visual perspective. Let $P^3(F)$ be a projective space. We define a central projection C as such: Fix a point $O \in P^3(F)$, called the center of the projection, and a plane $S \subset P^3(F)$ that does not contain O. Given a point $A \in P^3(F) \backslash \{O\}$, let AO denote the line in $P^3(F)$ going through A and O. Then define $C(A) := AO \cap S$. Now given another plane $Q \subset P^3(F)$ not containing O, we can make a bijection between

the two planes S and Q by restricting the domain of the central projection to Q. This type of bijection is called perspectivity, and is a type of homography. ("Homography", Wikipedia)

Perspectivities can also be generalized to projective spaces of higher dimensions, and form the basis for all homographies. In fact, the "Fundamental theorem of projective geometry" states that all homographies are the composition of a finite number of perspectivities. ("Homography", Wikipedia)

6 Grassmannians

Grassmannians generalize the idea introduced with projective spaces. Whereas the elements in a projective space $P(V)$ are the 1-dimensional subspaces of V, the elements in the grassmannian $Gr(k, V)$, are the k-dimensional subspaces of V ("Grassmannian", Wikipedia). $Gr(k, V)$ is also denoted as $Gr(k, n)$ for an unspecified n-dimensional vector space V. When a basis of V is chosen, we can represent an element U in $Gr(k, V)$ by a $k \times n$ matrix:

$$M = \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{k1} & \dots & m_{kn} \end{pmatrix} = \begin{pmatrix} M_1 \\ \vdots \\ M_k \end{pmatrix}, M_i \text{ row vectors} \tag{10}$$

where $span\{M_1, ..., M_k\} = U$

Note here that like we had with projectve spaces this representation isn't unique. If we multiply this matrix from the left with an invertible $k \times k$ matrix, we get a new matrix where the row vectors still span U, so the matrix represents the same element in $Gr(k, V)$. In other words, two $k \times n$ matrices A, B represent the same element in $Gr(k, V)$ if $\exists\ C \in GL(k, F)$ such that $CA = B$

If $V = F_q^n$ over F_q, how many elements are there in $Gr(k, V)$? The idea here is that any k-dimensional subspace can be mapped onto any other k-dimensional subspace through an invertible $n \times n$ matrix. If we can find how many such matrices there are, and how many of these which map a k-dimensional space onto itself, we will get what we're looking for by using

the orbit-stabilizer theorem.

Let's first look at the general linear group $GL(n, V)$, the set of invertible $n \times n$ matrices with the group operation being matrix multiplication. To find $|GL(n, V)|$, we consider how many choices we have for the column vectors. The first column can be any nonzero vector, so we have $q^n - 1$ choices. For the next column, we have to chose something linearly independent of the first, so we are left with $q^n - q$ choices. Next we have $q^n - q^2$, and so on. In the end $|GL(n, V)| = (q^n - 1) \cdot (q^n - q) \cdot \ldots \cdot (q^n - q^{n-1})$.

We can now look at $GL(n, V)$ as a group action acting on $Gr(k, V)$. The reason that this is useful, is because a matrix in $GL(n, V)$ can map any element in $Gr(k, V)$ onto any other. In other words, this is a transitive group action. We are interested in the number of matrices in $GL(n, V)$ that maps a k-dimensional subspace onto itself. We choose an element U in $Gr(k, V)$. If we pick an ordered basis for V where the first k basis elements span out U, then an invertible matrix mapping U onto itself is on the form:

$$M = \begin{pmatrix} GL(k) & A \\ 0 & GL(n-k) \end{pmatrix} \tag{11}$$

where A is any $k \times (n-k)$ matrix. There are in total $|GL(k)| \cdot |GL(n-k)| \cdot q^{k(n-k)}$ such matrices.

From the orbit stabilizer theorem we know that $|G \cdot x| = \frac{|G|}{|G_x|}$ ("Group action", Wikipedia). In our case this corresponds to: $|Gr(k, V)| = \frac{|GL(n)|}{\#M}$, where $\#M$ is the number of matrices on form above. Putting it all together we get:

$$
\begin{aligned}
|G \cdot x| = \frac{|G|}{|G_x|} &= \frac{|GL(n)|}{|GL(k)| \cdot |GL(n-k)| \cdot q^{k(n-k)}} \\
&= \frac{(q^n-1)\cdot(q^n-q)\cdot\ldots\cdot(q^n-q^{n-1})}{(q^k-1)\cdot\ldots\cdot(q^k-q^{k-1})\cdot(q^{n-k}-1)\cdot\ldots\cdot(q^{n-k}-q^{n-k-1})\cdot q^{k(n-k)}} \\
&= \frac{(q^n-1)\cdot(q^{n-1}-1)\cdot\ldots\cdot(q-1)}{(q^k-1)\cdot(q^{k-1}-1)\cdot\ldots\cdot(q-1)\cdot(q^{n-k}-1)\cdot(q^{n-k-1}-1)\cdot\ldots\cdot(q-1)} \\
&= \frac{(q^n-1)\cdot(q^{n-1}-1)\cdot\ldots\cdot(q^{n-k+1}-1)}{(q^k-1)\cdot(q^{k-1}-1)\cdot\ldots\cdot(q-1)}
\end{aligned} \tag{12}
$$

On second to last line we factored out $q^{\frac{(n-1)n}{2}}$ in numerator and denominator. It's worth noting the symmetry of this expression, if we replace k with $n-k$ we get the same number. It's the same type of symmetry that we see in binomial coefficients, that $\binom{n}{k} = \binom{n}{n-k}$. To make it more clear, we define $f(q,n) = (q^n-1)\cdot(q^{n-1})\cdot\cdots\cdot(q-1)$, we get the familiar looking equation:

$$
|Gr(k,V)| = \frac{f(q,n)}{f(q,k)\cdot f(q,n-k)} \tag{13}
$$

This equation is on the same form that the formula for calculating binomial coefficients are, just that $x!$ is replaced by $f(q,x)$, so it makes sense that it has the same type of symetry. This also explains the symmetry we saw in section 3, that we had the same number of points and lines in $P(F_2^3)$ and $P(F_3^3)$. This is because points in these spaces corresponds to 1-dimensional subspaces of a 3-dimensional space, and lines are 2-dimensional subspaces of a 3-dimensional space. Since $3-1=2$ this satisfies the $(n-k) \sim k$ symetry.

7 The Plücker Embedding

Any grassmannian can be embedded as a projective variety into a projective space through Plücker embedding ("Plücker embedding", Wikipedia). Take an element $M = (M_1, \ldots, M_n) \in Gr(k,n)$. Choose k numbers $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, and form the $k \times k$ matrix $(M_{i_1}, M_{i_2}, \ldots, M_{i_k})$. Since there are $\binom{n}{k}$ ways to choose the numbers i_j, there are $\binom{n}{k}$ such matrices. After some ordering of these matrices are made, we label them D_i. We can then define the Plücker embedding $f : Gr(k,n) \to P^{\binom{n}{k}-1}$ as:

$$\begin{aligned} f(M) &= (v_1, \ldots, v_{\binom{n}{k}}), \\ v_i &= det(D_i) \end{aligned} \tag{14}$$

The resulting v_i-s here in the result are called the Plücker coordinates of the matrix M.
Note that since mutltiplying M by an invertible $k \times k$ matrix A doesn't change the element it represents, it shouldnt change its Plücker coordinates either. We have:

$$\begin{aligned} f(A \cdot M) &= (v_1, \ldots, v_{\binom{n}{k}}), \\ v_i = \det(A \cdot D_i) &= \det(A) \cdot \det(D_i) \end{aligned} \tag{15}$$

So each coordinate is scaled by the same constant $\det(A)$, so it still represents the same point in the projective space.

What is the image of the embedding? It turns out that it is a projective variety of $P^{\binom{n}{k}-1}$, we will get back to which polynomial equations define this variety and how to find them later.

Example: We look at the finite vector space $V = F_q^4$ over F_q, and want to look at the Plücker embedding $Gr(2, V) \to P^5(V)$. It turns out the image are exactly the points $(a_1, \ldots, a_6) \in P^5(V)$ which satisfy $a_1 \cdot a_6 - a_2 \cdot a_5 + a_3 \cdot a_4 = 0$. It is easily verifiable that the image of the embedding satisfies this equation. Are there any points which satisfy the equation, but are not in the image of the embedding? To answer this we rewrite the equation:

$$\begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_6 \\ a_5 \\ a_4 \end{pmatrix} = 0 \tag{16}$$

If we now fix $(a_1, a_2, a_3) \neq 0$, and multiply the row vector with the matrix, we end up with a new nonzero row vector (r_1, r_2, r_3), and get the equation:

$$\begin{pmatrix} r_1 & r_2 & r_3 \end{pmatrix} \begin{pmatrix} a_6 \\ a_5 \\ a_4 \end{pmatrix} = 0 \tag{17}$$

Since (r_1, r_2, r_3) is nonzero, it is a full rank 1×3 matrix. The rank-nullity theorem then gives us that the null space has dimension 2. Hence, for any fixed $(a_1, a_2, a_3) \neq 0$, there are q^2 choices of (a_4, a_5, a_6) such that eq.(17) holds. There are $q^3 - 1$ nonzero choices for (a_1, a_2, a_3). When these 3 are zero, we have to chose nonzero (a_4, a_5, a_6), this gives another $q^3 - 1$ choices. Since the image of the Plücker embedding is in a projective space, several of the solutions we get here represent the same element. In fact if $v = (v_1, \ldots, v_6)$ satisfies the equation, $f_i \cdot v, f_i \in F \backslash \{0\}$ also satisfies the equation, since it is a homogeneous polynomial. So we have counted all the $q - 1$ multiples of a solution, but all these represent the same element in the projective space. Thus we have to divide what we counted by $q - 1$. All in all we get:

$$\#\text{Solutions} = \frac{(q^3-1)\cdot q^2 + (q^3-1)}{q-1} = \frac{(q^3-1)\cdot(q^2+1)}{q-1} = \frac{(q^4-1)\cdot(q^3-1)}{(q^2-1)\cdot(q-1)} \tag{18}$$

We see that this is the same formula that we derived in section 6 if we put $n = 4$ and $k = 2$. In other words the number of solutions is the same as the number of 2-dimensional subspaces of V, and since we know that the image of the Plücker embeding satisfies this equation, the image must be exactly the solution set of the equation.

As we saw in the example above, the image of the Plücker embedding satisfied a quadratic homogeneous equation. In general, the image of any grassmannian under the Plücker embedding satisfies a set of quadratic homogeneous equations, called the "Grassmann-Plücker relations" ("Plücker embedding", Wikipedia). We will now see how these equations look like.

Given $Gr(k, n)$, we first start by making two ordered sequences, one of length $k - 1$, and one of $k + 1$:

$$\begin{aligned} 1 \leq i_1 < i_2 < \cdots < i_{k-1} \leq n \\ 1 \leq j_1 < j_2 < \cdots < j_{k+1} \leq n \end{aligned} \tag{19}$$

Now for each fixed j_s in the second sequence, we can transform these sequences into two sequences of equal length k:

$$\begin{aligned} i_1, i_2, \ldots i_{k-1}, j_s \\ j_1, j_2, \ldots \overline{j_s} \ldots, j_{k+1} \end{aligned} \tag{20}$$

Where $\overline{j_s}$ denotes the sequence where j_s is removed. Using the matrix representation of the elements in the grassmannian: $(M_1, \ldots, M_n)$, we pick out the columns according to the sequences generated above to create two $k \times k$ matrices. We then take their determinants:

$$\begin{aligned} D_{i_1,\ldots i_{k-1},j_s} &= \det(M_{i_1}, M_{i_2}, \ldots M_{i_{k-1}}, M_{j_s}) \\ D_{j_1,\ldots \overline{j_s} \ldots,j_{k+1}} &= \det(M_{j_1} M_{j_2}, \ldots, M_{j_{k+1}}) \end{aligned} \tag{21}$$

Notice here, that if $j_s = i_t$ for some t, then $D_{i_1,\ldots i_{k-1},j_s} = 0$, since two of its columns are the same. Now we can create the equation:

$$\sum_{s=1}^{k+1} (-1)^{(s-1)} D_{i_1,\ldots i_{k-1},j_s} D_{j_1,\ldots \overline{j_s} \ldots,j_{k+1}} = 0 \tag{22}$$

So going through all the $k+1$ choices of j_s, gives us one quadratic equation in Plücker coordinates with $k+1$ terms. Now going through all the possible starting sequences on the form:

$$\begin{aligned} 1 \leq i_1 < i_2 < \cdots < i_{k-1} \leq n \\ 1 \leq j_1 < j_2 < \cdots < j_{k+1} \leq n \end{aligned} \tag{23}$$

and do the same process as described above, we end up with a set of homogeneous quadratic equations in Plücker coordinates which define a projective variety, the image of the Plücker embedding of $Gr(k, n)$.

Does this method generate too many equations? Is there a subset of these equations that define the same projective variety? Yes, and its related to when the two starting sequences contain the same number. We can look at $Gr(2, 4)$ which we saw in the example to illustrate this.

Chosing the starting sequences 1, and $2 < 3 < 4$ of lengths $2 - 1 = 1$ and $2 + 1 = 3$, we get 3 sets of transformed sequences:

$$\begin{aligned} &1, 2 \mid 3, 4 \\ &1, 3 \mid 2, 4 \\ &1, 4 \mid 2, 3 \end{aligned} \tag{24}$$

which gives the equation:

$$D_{12} \cdot D_{34} - D_{13} \cdot D_{24} + D_{14} \cdot D_{23} = 0 \tag{25}$$

which is the equation that describes the Plücker embedding of $Gr(2,4)$. However if we choose the starting sequences to be: 1 and $1 < 2 < 3$, we get the sets of transformed sequences:

$$\begin{aligned} &1,1 \mid 2,3 \\ &1,2 \mid 1,3 \\ &1,3 \mid 1,2 \end{aligned} \tag{26}$$

which gives the equation:

$$D_{11} \cdot D_{23} - D_{12} \cdot D_{13} + D_{13} \cdot D_{12} = 0 \tag{27}$$

$D_{11} = 0$ because two of its columns are equal, which means the whole equation is always zero. Thus this equation gives us no information. Another way this method generates redundant equations, is by starting with the sequences 2, and $1 < 3 < 4$. The transformed sequences are:

$$\begin{aligned} &2,1 \mid 3,4 \\ &2,3 \mid 1,4 \\ &2,4 \mid 1,3 \end{aligned} \tag{28}$$

This gives the equation:

$$\begin{aligned} D_{21} \cdot D_{34} - D_{23} \cdot D_{14} + D_{24} \cdot D_{13} = \\ -D_{12} \cdot D_{34} + D_{24} \cdot D_{13} - D_{23} \cdot D_{14} = \\ (-1) \cdot (D_{12} \cdot D_{34} - D_{13} \cdot D_{24} + D_{14} \cdot D_{23}) = 0 \end{aligned} \tag{29}$$

Above the fact that the determinant is alternating is used: $D_{21} = -D_{12}$. The equation we get is the same as if we were using the first ordering (multiplying the equation by (-1) still gives the same zero set). While its not useless information, its redundant information, which means we still get the same projective variety if we include this in the set of defining equations.

We will now look at $Gr(2,5)$, and see what the Plücker relations tell us here about the image of the Plücker embedding. Since $k = 2$ just like above,

we still have to chose our starting sequences to have 1 and 3 elements. We start out with the sequences we know will not be redundant, namely the ones where there is no overlap between the sequences, and the elements of the first sequence are all smaller than any in the second sequence. This gives the 5 starting sequences:

$$\begin{aligned} 1 \mid 2,3,4 \\ 1 \mid 2,3,5 \\ 1 \mid 2,4,5 \\ 1 \mid 3,4,5 \\ 2 \mid 3,4,5 \end{aligned} \tag{30}$$

Which gives the 5 equations:

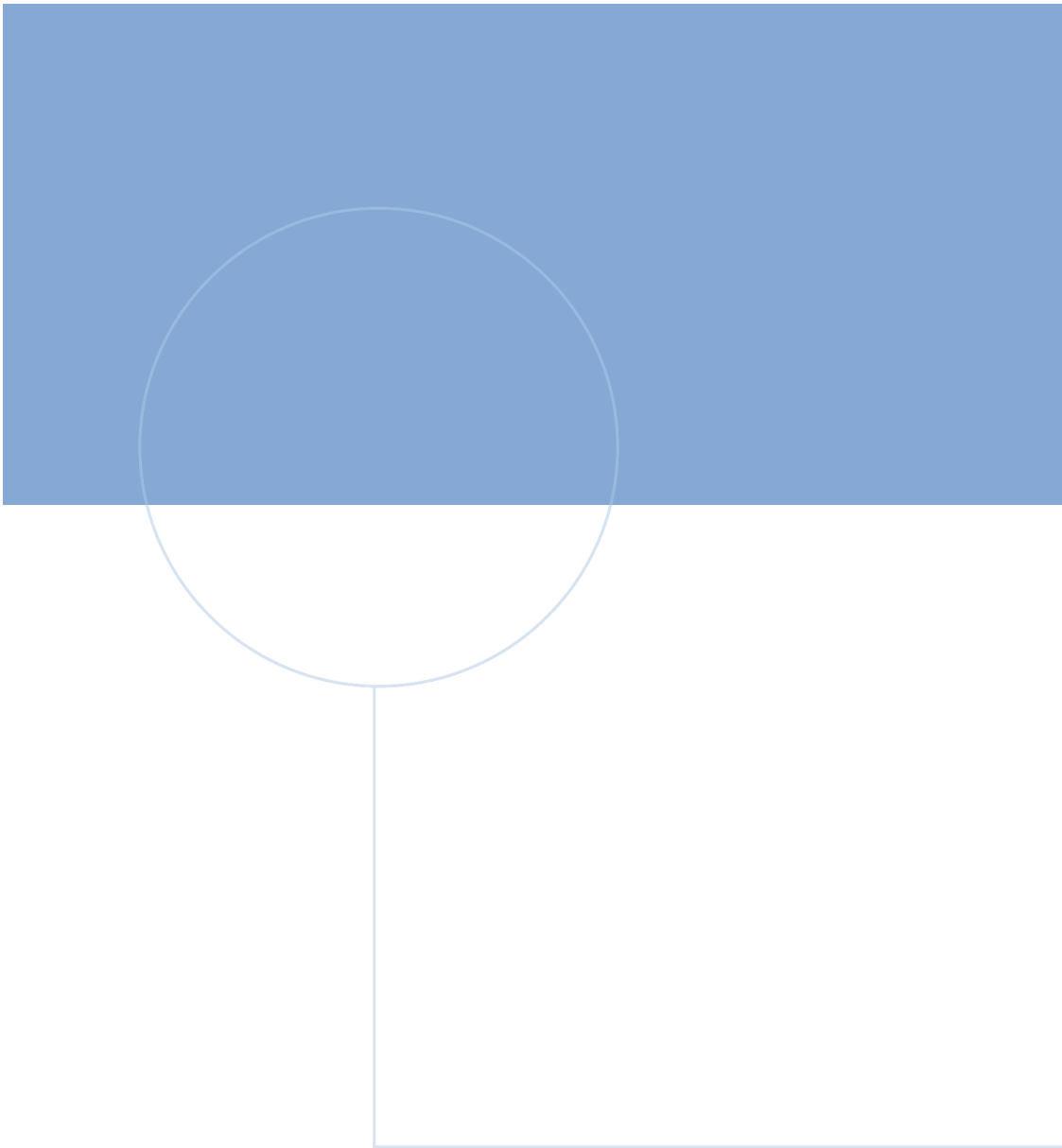
$$\begin{aligned} D_{12} \cdot D_{34} - D_{13} \cdot D_{24} + D_{14} \cdot D_{23} = 0 \\ D_{12} \cdot D_{35} - D_{13} \cdot D_{25} + D_{15} \cdot D_{23} = 0 \\ D_{12} \cdot D_{45} - D_{14} \cdot D_{25} + D_{15} \cdot D_{24} = 0 \\ D_{13} \cdot D_{45} - D_{14} \cdot D_{35} + D_{15} \cdot D_{34} = 0 \\ D_{23} \cdot D_{45} - D_{24} \cdot D_{35} + D_{25} \cdot D_{34} = 0 \end{aligned} \tag{31}$$

If we use any pairs of starting sequences where there are overlaping terms, this just will result in some terms being zero. This gives a less strict equation than what we already have, so it won't affect the projective variety which the equations define. Thus these equations define the image of the Plücker embedding of $Gr(2,5)$.

8 References

"Projective space", (Wikipedia), 29.11.20, `https://en.wikipedia.org/wiki/Projective_space`
"Projective variety", (Wikipedia), 03.12.20, `https://en.wikipedia.org/wiki/Projective_variety`
"Elliptic curve", (Wikipedia), 03.12.20, `https://en.wikipedia.org/wiki/Elliptic_curve`
"Homography", (Wikipedia), 29.11.20, `https://en.wikipedia.org/wiki/Homography`

"Grassmannian", (Wikipedia), 03.12.20, https://en.wikipedia.org/wiki/Grassmannian
"Plücker embedding", (Wikipedia), 29.11.20, https://en.wikipedia.org/wiki/Pl%C3%BCcker_embedding
"Hilbert's basis theorem", (Wikipedia), 03.12.20, https://en.wikipedia.org/wiki/Hilbert%27s_basis_theorem
"Bézout's theorem", (Wikipedia), 03.12.20, https://en.wikipedia.org/wiki/B%C3%A9zout%27s_theorem "Group action", (Wikipedia), 03.12.20, https://en.wikipedia.org/wiki/Group_action#Orbit-stabilizer_theorem
"Rank-nullity theorem", (Wikipedia), 03.12.20, https://en.wikipedia.org/wiki/Rank%E2%80%93nullity_theorem



NTNU

Norwegian University of
Science and Technology