Lecture 01 : Course outline and Fundamentals

So what is arithmetic geometry? So we will study equations, basically system of polynomial equations and specifically in this course it will be over finite fields. So I do not think we will be doing concepts beyond finite fields. so if you are not if you are not even aware of about this then you will be in trouble but since this is the first course first day so I will just define it so you take a prime you do arithmetic modulo the prime p. So, you can basically add integers, you can multiply them, you can also divide them. So, what you get is a object which is called field and its finite because its elements are only from 0 to p - 1. So, this is what is called a finite field, this is the first example and we will write it as f(p).

And then there are these constructions which you have to do as a homework from f(p) you can go to a field of size p 2. So, which we write f(p) 2 which is not the same as z mod p 2 with z mod p 2 is something very different for example, it is not even a field. So, f(p) 2 is definitely something else. In particular it is an object whose characteristic is p.

So, you multiply anything by p you get 0 and it has elements which are not integers. So, it has more abstract elements which are called polynomials over f(p) and you can keep doing this and if you do it for a long time which is infinite time then in the end you get a very big field which is called f(p) bar. So, this is the algebraic closure of F(p). So, this is just an introduction to this term finite field, what does it mean? It starts with a prime and then it moves to bigger fields maintaining the characteristic and containing F(p) inside. So, this is actually a tower.

So you have F(p) is contained in F(p) 2 is contained, so you cannot say that F(p) 2 is contained in F(p) 3, but F(p) is certainly contained and then all these are contained inside F(p) bar. So this course will actually be about F(p) bar. we will be mostly studying concepts to do with algebraic closure of the finite field F(p) which is why I am defining it right in the beginning. So, why should this be studied in a computer science department? So, the reason is that finite fields like F(P) are useful in many designs and constructions in computer science and specially in cryptography there are more complicated questions people study over F(P) which are to do with polynomial systems and that is why we need many of these concepts actually in practical algorithms. need some things from algebraic geometry, so this studies polynomial equations, so polynomial equations you can just think of either you can think of univariate like x 2 - So you are interested in finding solutions of x 2 - 2 equal to 0.

So those things for this course are pretty much solved. By solved I mean if you want to do computations with these univariates, there is a whole course where we draw this which is called computational algebra and number theory. So, there we study computational algorithms regarding these univariates. This course starts above this which is bivariates. So, for example y 2 - x 3 - x.

So, this course is actually interested in studying solutions of this. So, the equation y 2 equal

to x 3 + x modulo p for example, how many roots are there and then in f(p) 2 how many solutions are there and so on till f(p) bar and the solutions in f(p) bar, I mean f(p) bar is an first of all I did not say that but it is an infinite field. f(p) bar has infinitely many elements, so how do these roots of f(p), f(p) 2, f(p) 3, how do they fit inside f(p) bar, can we compute objects which are somehow universal, so that they contain the information of all these f(p) to the i. So, we will actually, one of the major achievements in the end of this course will be that we will identify a universal object and we will compute it. That object is called the zeta function of curves over finite fields.

So, believe it or not in this course in the end we will prove the Riemann hypothesis. But the caveat is that it will be Riemann hypothesis for curves over finite fields. So, you will still not win million dollars. may be few dollars worth. And then no reason to stop at this, so we can also look at higher degrees like this and so on.

So, starting from this second example, all these other examples are examples for curves. So, first this y 2 - x 3 - x is called an elliptic curve and these other ones will be called hyper elliptic curves and so on. So, these are directly used in cryptography for example. So, algebraic geometry studies polynomial equations of this type. from a geometric perspective.

Now this may not be clear what this geometric perspective So, we will make it painfully clear in the next 2-3 weeks, what is the meaning of geometric perspective because see this F(p) is such a highly discrete object that there is no geometry per say. So, in this course I will be drawing many pictures. but all these pictures will be to fool you because if the solutions are in F(P), these are discrete points, so how can I draw continuous lines and curves and so on. So, all these pictures will be just to deceive you, but this deception will actually give formal proofs. So, that deception is basically the geometric perspective.

We have to work hard to actually formalize all this, so that it gives you formal proofs. So that basically means studying those properties that one can visualize even over f(p). So even in a discrete setting, f(p) unlike reals, so in real it is actually you can draw a line and it every point on the line will make sense, in F(P) it will it would not make sense because there is nothing between 0 and 1, 0 and 1 you cannot, I mean all these things which are present in reals are missing between 0 and 1, but still we can draw a line and then we can make claims and we can formalize all that. So we will do that slowly, this is not very simple to do. So one goal will be to count points, so that is the goal of arithmetic geometry.

So this course is also about, I mean it is mainly about arithmetic geometry, so how is that different from algebraic geometry. So the goal of arithmetic geometry is just to count points of given equations. How many solutions are there and since we are in a finite field, so the solutions are only finitely many, unless you go to F(P) bar, but before F(P) bar everything is finite, so all the fields are finite, so you can talk about exact counts. So arithmetic geometry studies the counting questions. So for example, how many points are So points or solutions that is the same thing for me, which is also the same as roots, which is also the same as

zeros, all these terms will mean the same thing.

So you count points through solutions, roots or zeros, let us say on this y 2 equal x 3 mod p. So, you can do a heuristic estimate, so you can fix x anything from 0 to p - 1 and accordingly you may or may not find its 2 root, the 2 root of x 3. which actually reduces to 2 root of just x. So, you can substitute x, x takes p values and sometimes it is a 2, there is a 2 root, sometimes you do not find a 2 root and you can actually show that, this again is a question for you as a homework exercise, property of finite fields that 2 roots are exactly half many. So, in half(t)he cases there will be a 2 root which means there will be two y's.

So the number of solutions is, it's exactly p in this case, right? Because maybe I'm doing a + - one, but I think p + one is the number of solutions. So you exclude the zero zero point and then after that you have, yeah, something like that. So it's p exactly, right? So, which is basically 1 + 2 times p - 1 by 2. So, that is p. Yes, so there are two variables.

So, potentially there were p 2 points available in the space, but out of p 2 points you can see that it cannot be p 2 it has to be something much less because once you fix x there may not be a y. and when there is a y then there are two of them. So, whatever loss you are taking on the x side it is being covered by y and so overall you get p. So, it is a property of curves that what you are fighting against is around p points. So, here it is the maximum possible in general it may be smaller than p slightly smaller than p or slightly bigger than p.

So, you are always targeting p. And when I say arithmetic geometry is the study of counting points, it will be how far away from P are you and on which side. So, that kind of estimates we will be interested in. It may sound exotic at this point that why should you be interested in exact count around P, but hopefully it will clear during the course and as you see these theorems that it entails almost complete understanding of curves. It gives you algorithms and so on.

So these methods which estimate will be very powerful. They will not just stop at an estimate. So they will basically tell you everything you would want to know for curves and not just in finite fields but also in other fields. So these will be like fundamental constructions. So finally in this course we will be interested in algorithmic or computational questions Okay so that is the third part, so there is algebra, there is geometry, arithmetic and there will be algorithms.

So this algorithm part I have to see how much time remains, maybe you can present algorithms and I will present the math, but overall I mean the end goal is that you see some algorithms in this course and how they are applied in let us say cryptographic applications. or how they are applied in error correcting codes. So, here is a concrete question that motivates this general area. So, you are given polynomials.

over some finite field. So, this is the polynomial ring. I do not know your basic, so whether

you have seen these objects. If you have not seen, you have two options either you go home and read about it or you drop. is no third option because these things I will just assume that you are familiar with. So, f(p) is some finite field in this case it is a prime field and there are n variables.

So, you are looking at polynomials, m polynomials in n variables with coefficient 0 to p - 1 essentially. This is given to you in the input. Now, what you have to find is or you just have to test whether there exists a point P in the space f(p) to the n such that all these vanish. Okay, so in other words is there a 0 that is common to all these polynomials in the base field, base field space which is the f(p) to the n space. How hard is this question? What do you think? Algorithmically.

okay can you find an algorithm which will solve this in practice yes or no there are some people in the back who are experts in this is there an algorithm for this so this is what is called an NP-hard problem okay so you can show that if you can find a If you can even decide the existence of a common root or common zero, then you can solve all the problems which are NP complete, which contains many algebra and number theory questions and more importantly combinatorial optimization problems. So, all these optimization problems can be solved if this can be solved. So pessimistically people think that this cannot be solved. Practical algorithms will always be exponential time, which in this case just means that you go over the whole space f p to the n, which is of size p to the n. So if you take p to be 2, the space has size 2 raise to n.

So you go over the whole space 2 raise to n and just do the trivial check. So there is nothing better certainly nothing better is known and also it is expected to be that hard. So, in the future also we do not expect any improvements. Even if you develop quantum computers, even then we do not expect any improvement. So, you have to come up with a radically different kind of computational device to solve this.

So, that is an exercise. well not the invention of a device but much simpler show that this is NP hard. In fact in this case it is NP complete, so any problem in NP reduces to this and this problem itself is in NP, it is NP hard and it is in NP, so it is an NP complete problem even when Degree of, even when F i's are quadratic and P is 2. So, the situation is that bad you can assume F i's to be just quadratic polynomials and you can take prime P to be 2, even then it is a NP hard problem. So, the issue is that this n is arbitrary, number of variables is arbitrary. So, when n grows then the problem becomes really hard, even for the smallest prime possible it is very hard.

So, in this course we will try to avoid this issue by fixing n to be 2. So, that case there is no NP hardness, curse of NP hardness is absent. and we will develop a whole theory for n equal to 2 which in this perspective looks like a trivial thing we are doing but you will see it is not. So efficient or even practical algorithms are unlikely here. however in this course we will restrict to curves over finite fields.

which is expected to be a much easier case, both in theory and practice. So, we will focus on this and curves already will generate enough theory that one day you will be able to generalize it to any n. So, the theory itself will scale well, but of course the corresponding algorithms you cannot hope them to work because of NP hardness curves as n grows. So, this is not an exaggeration to say that.

much of modern maths arose from this. Okay, so the objects which we will be studying while studying curves over finite fields, much of modern maths has been invented or discovered to generalize those things to harder cases. Yes. In the original problem, is there an exponential limitation only on the number of variables or on other parameters also? Yes, so you, well I mean.

.. Formally speaking for NP completeness or for the measure of practicality of an algorithm, you look at the full input. So, the input representation is, well these are polynomials, so they are given to you in certain representation which I have not specified, but at least you will need m things. So, m is in the input size. p you can represent in binary, so that will be log p and n again you will have to enumerate. So, you have m and n and log p and degree of the polynomials also will be needed like completely specified.

So, you can take degree and m and n and log p to the input size. So, formally you want polynomial time in that. No, no, so there are many algorithms with different features. Yeah, that you have to see as a homework. This problem has many, many algorithms and they are, they have different features.

But for this course I think. all that will not apply because we will just fix n to be 2. When n is 2 then there are essentially only two things which can trouble you which is how big the prime p is and how big is the degree of the polynomial. So, you want polynomial time in both log p and the degree. Other things will not concern us in this course. But in general, this is called the Null-Stellen-Satz problem.

So, you can see there are tons of articles on this and algorithms also solving the Null-Stellen-Satz problem in under various restrictions, but of course you do not expect them to work in general. In general, it is the NP hardness curse is there, so the first part of the course is This will only be about the algebraic geometric fundamentals of this machinery that we want to develop. so needed for counting zeros and the second part will be the algorithms which you can potentially derive from these fundamentals. We can do CS applications. Most probably we will not have enough time for this thing, so probably we have to do it in parallel.

So, students have to do the CS applications as extra talks. So, maybe I can sketch. just give an overview of what we will do in the fundamentals and in the applications. So, in the fundamentals we can we hope to cover curves in the modern language of algebraic

geometry. So, now for example, Madhavan here will not agree with this that it is modern, but I guarantee that it will be modern for the others, although it is 100 years old.

So, there are more modern things which mathematicians, which is the only thing which current mathematicians do, but it is too hard to do that here. and impossible to do in one semester, it will need many years. So, first we do this and then we will see how many students remain for the real modern development. But the starting point is this, so we will see the starting point which is quite advanced ideas in algebraic geometry, which you do not see in basic algebra courses, so which is which is varieties, morphisms between them. So varieties will basically be the core part of these equations.

So when you are given a polynomial system, a system of polynomial equations, it can be divided into smaller parts and the core of that is called a variety. And between varieties, so somehow although you wanted to compute with only one variety, to have a meaningful theory built on this, you need a way to compare two different varieties. So, for this comparison, you need a comparison mechanism which is called morphisms. So, we have to define morphisms. The reason for this is, although I promised before that I will take n to be 2.

As many times in this course, I will not follow that promise. I will actually take n to be 100 or whatever arbitrary and I will still call it a curve. So, the reason is that we will define a notion of dimension of a variety. So, as long as the dimension is 1, we will call it a curve.

It does not matter what you are given in the input. So, to do these things. fairly or formally we have to define things in a more general way and in particular we need the ability to compare two varieties. So, for example, when can you compare a given variety with a curve, when can you say that variety is a curve even though n is very big. So, you need some kind of basically you need the idea of homomorphism, isomorphism and so on. So we will define possibilities of morphisms between varieties and we will define something which is extremely important which is called function fields.

So basically on top of a variety we can define, we can ask what are the functions which are defined in a local neighborhood. and that will give the idea of function fields. So, they somehow sit above a variety not inside and many things related to this which I do not want to mention now. So, the guiding intuition is always the following in this business or guiding intuition. is that geometric properties of a variety or in our case a curve are manifested in the functions over it.

So, you want to study properties of a curve which means that you want to study points in the curve. So, this is something that you want to study inside the curve, but that will never be possible. What algebraic geometry will do is that it will actually study things above it which is functions that are defined. Now these functions may be defined everywhere on the curve which is the usual thing that you are used to, but in the deeper theory here we will

define notions of neighborhood and then functions defined on the neighborhood, but may not be defined everywhere on the curve. So, that is the part which is interesting and which allows many other.

we can say invariants about the curve which ultimately help in achieving whatever we want to achieve in particular counting points. So that is philosophically the most interesting thing in this theory that you study things locally and above and not directly the points. So basically these are, the dictionary that we will be using is the first thing, the geometric properties of a curve, this we will call geometric perspective and the functions over it we will call the algebraic perspective. So we will, from the next class what we will start is the geometric perspective. So we will define these geometric terms and after that we will do the algebraic perspective which is we will define the algebraic terms.

So algebra will always live above the geometric objects and then there will always be a dictionary when we move from one word to the next and back and there will be enough pitfalls in that. So just as an example to study the roots of. y 2 equal to x 3 or let us make an elliptic curve equal to x 3 + x, we should study the ring F(p) modulo this elliptic curve. Now, this is not, it is not very clear that, first of all again if you are not aware of this notation you have to practice it. So, what this is saying is that you have the polynomial ring in two variables over f(p) and this y 2 - x 3 - x is an ideal.

So, it is not a single polynomial, but it is actually all the polynomials which are multiples of this. and we are quotienting out by it. So, this is the quotient ring. So, instead of studying the roots as points in F(p) whole 2, you should study this quotient ring.

So, that is the again the transition from geometry to algebra. It is not clear at this point how this helps and It will probably be a long time before you accept this fact that it helps. So, it will be towards the end of the course that you will see results of this shift in viewpoint. So, a highlight of this. So, people who have done some complex analysis, they would know the term genus, what is the meaning of genus.

So how do you count number of holes in a surface or in a curve or so on. So the definitions you may or may not have seen are all very loop based, so you actually draw things and then you measure by drawing which is possible, I mean this continuous loops can be drawn for example in the real space, but since we are not in the real space we are in F(p). all those things actually break down. So how do you recover those things in this discrete world? So that recovery will be done through this ring. And a high point of that will be the Riemann-Roch theorem.

that defines the genus of a curve. Now, this is not needed for you to know because we will actually do it essentially from scratch. So, you do not need the meaning of the term genus beforehand, but many people in this business they like to compare finite fields with complex analysis. So, if you also want to do that, you can do that, but we will not do that formally,

officially in the course. So, once we have developed this geometric perspective and the algebraic perspective enough, then we will start, we will state the Riemann-Roch theorem and we will prove it and that theorem statement will actually define genus.

So, genus will be something to do with the degree of the curve. So, for example, this x 3 + x degree is 3 and Riemann-Roch theorem will say that the genus of this curve is 1 and we had an example of x to the 11 + x. So, in that case the genus will be 5 and so on. Okay but what is the geometric meaning of genus we will see that via functions which is this quotient ring. Yeah so that we will see when we reach that point genus of a curve in any field. So, we will give a algebraic definition of genus and then it will be available for you to use in any field, it will now become independent of complex and reals and so on.

And the final thing where we will stop in the course is the Riemann hypothesis, where this development up to Riemann-Roch theorem will be used. So we will prove and estimate for the number of points or number of roots on a curve over a finite field. So this is called, maybe I should give you some idea what this estimate will be. So for example, you have this y 2 equal to x 3 + x.

Now here, so say it is mod p, p is a prime. Here the heuristic is not very simple because when you fix x to a number between 0 to p - 1, it is hard to predict how many times x 3 + x is a 2. Because x 3 + x is kind of a random looking function and we do not have a good theorem how many times it is 2 or non-2. x 3 was very different because x 3 reduced to x. and for x we have a theorem I mean we have a basic property of finite fields which says that x is half the time 2 half the time non 2 the same thing cannot be said for this x 3 + x which is basically x 2 + 1.

So, x 2 + 1 is kind of arbitrary enough that we do not have general theorems. So, in fact this the last thing which where we will stop that is the only theorem the best theorem to understand which tells you when is x 2 + 1 a 2, how many times is it a 2 and overall it will give you an estimate now for the number of points to be something like p with the deviation of 2 root p. So, the number of points on y 2 equal to x 3 + x is somewhere between p - 2 root p and p + 2 root p and we will make it more precise. So, the deviation is coming out to be 2 root p that is the Riemann hypothesis for elliptic curves, but in the end of the course we will prove it for all curves. Even for elliptic curves it is highly non-trivial and then to generalize it to all curves it requires all this language which we are going to develop. As an exercise you may want to see the proof for elliptic curve of the Riemann hypothesis, it is not easy.

So, but if you are interested you can see that proof as an exercise, obviously in the end we would have subsumed it, we will go much far from that proof. So, this is called the Riemann hypothesis. for curves. Now, surely media articles you must have heard the term Riemann hypothesis.

I do not know how many of you actually know it. I myself do not know it very well. So, I will

not even attempt in this course to compare this theorem with the actual Riemann hypothesis. So, that is another exercise for you if you want to compare this with actual Riemann hypothesis which is an open question. for now around 200 years, you are welcome to do that, obviously there is no theorem, so Riemann hypothesis is a conjecture which is open and this Riemann hypothesis for curves over finite fields is a theorem that we will prove, in fact this is the main theorem we want to prove in this course, everything we will do will be towards it. and I promise you that will not contaminate this with anything else, will not do anything which doesn't in the end help in proving the Riemann hypothesis.

So, everything will be towards this. The statement is in fact exactly the same, you want to say the roots of the zeta function are real part of, this is the same statement. Yeah, but. It is analogous, the main Riemann hypothesis and the Riemann hypothesis work over columns, No, the Riemann hypothesis which Riemann stated which is for the Riemann zeta function, I mean yeah in what sense is it analogous even that requires work. Because the functional equations are there.

They are completely different objects, yeah so the analogy is not. I mean even if you know that definitions it is not immediate, but of course there is this common thing as Madhavan is saying 0.5.

So, in Riemann hypothesis there is a 0.5 and in the end of our course also there will be a 0.5. So, the analogy is there, but in what place it appears that is very different and what objects, the objects are also very different. But of course, all this work here was done to mirror Riemann hypothesis in algebra. The original Riemann hypothesis which is still open is a number theory question. It basically counts the number of primes in the best way possible.

The best counting for primes will be given if Riemann hypothesis is true. It is actually if and only if. So, the algebraic version is something to do with this quotient ring. In particular the prime ideals which divide this ideal, but as I said it is not easy. So, we say this to capture your interest, but if you actually want to see it mathematically you have to do a homework. Okay so that is for the fundamentals, we will do these keywords and in applications which you can pick to present because I don't think I will have the time to do this, so we can do this in extra classes.

So there are many algorithms based on the theory to count points. Now this is an amazing thing and may be completely unclear at this point that the Riemann hypothesis once we have proved it will say for the elliptic curve that number of points is not p but it is deviated, it's p + - 2 root p, that's only an estimate. So that still doesn't tell you directly how many points there are and is there an algorithm. But it's the beauty of the method that is used to prove Riemann hypothesis that it actually gives you an algorithm. So there is a fast algorithm, practical algorithm to do the counting on elliptic curves. So, similar thing you want to do for other curves, which is basically the degree is higher, it is not a cubic, it may be degree 5, degree 7 and so on.

So, there are multiple, I mean at least three algorithms I know, which use very different theories and work in different special cases. I should say that this question is open in general. So for curves we do not have a fast algorithm. So Riemann hypothesis we will show in the course but that does not mean that we have a fast algorithm that works for all cases. So that's an open question for research, but it will work for many cases that are useful in cryptology and other applications.

Based on this theory, there are also integer factoring algorithms. So you can, again there are two or three minimum algorithms. that fundamentally use this theory of Riemann hypothesis to factor numbers to attack RSA, which again is an open question. So, in general it is open. So, what you can do is for some special cases and there are many other questions like one computing 2 roots of a number or computing rth roots of unity in finite fields.

So, there are also these curve based algorithms which are used to factor univariate. So, this 2 root a is essentially you are factoring x 2 - a, it is a univariate There are algorithms which use curves to do this and similarly rth root of a primitive rth root of unity computation is again essentially a univariate factoring question. You are factoring essentially x to the r - 1. So, those things those connections you can present then there are cryptosystems based on these theories.

and there are error correcting codes, coding theory based on this. So these are the applications. The course will not be focused on this because we will not have enough time but you can do this. Say you give a 45 minute talk each of you. So I think Let's just give the policy then of the course.

So we can have assignments. We can have mid-sem and sem exams. These will be take home, so everything will be take home, assignments, mid sim, end sim. So, you do not have to be fast, I just want you to be deep. Here in this business speed will not matter and finally you can give a talk. I suspect not many of you will be finishing the course. So assuming that numbers are small of the students, I think we can afford to have one talk per student, let's say on the weekends towards third, fourth month.

So they can cover the applications. Yeah, of course, if we have 10 + students, then it will be hard to schedule that. But I'm hoping that you will get afraid and drop. So textbook is essentially one which I am using by Carlos Moreno. Algebraic curves over finite fields. But if you cannot access it, it will hardly matter because all these things which are present, there are hundreds if not thousands of references available on the net.

Again, most of these references will be too modern for you. So you will not even be able to understand what I am saying and what they are saying is the same thing. For that, you will always have to contact Madhavan. Since we are only interested in curves, you will be able to find references which match very close to what we are doing in the class. You do not have to

look at very general things that are available in the books.

You can find for example courses and lecture notes and even books which do these things that we are doing exactly. Yes, I don't think this textbook will be a problem. You have many options to study this material.

OK, so we have 20 more minutes. Do you have any questions? Till now. So we have a TA, Tiptojit will be your TA. So you can contact him not just for the grading of the assignments but also you can ask questions about the lectures. He will be able to help you with almost anything in this. Okay, so no questions then we can start with the first topic. which is affine varieties, so as I said we will start the geometric perspective, so that will be things about affine varieties.

So, we will start with a field k, but if you have trouble imagining general fields, you should just think of f(p) bar. okay if that is too complicated then you just think of f(p) okay so in this course we will only be interested in these fields yeah sometimes thinking of complex may also help but you won't need anything else other than these three okay i take p to be two or three or five and then think of f(p) or the algebraic closure of that. Difference is that f(p) will be finite, f(p) bar will be infinite. So, you have to take care of this infinity being involved everywhere if you are thinking of f(p) bar. So, before thinking of f(p) bar maybe you can think of complex because complex is somewhat I mean it has more physical interpretation.

But that is something we will be avoiding in this course. We do not want physical interpretation because Ultimately our application case is F(P) and that has no physical interpretation, that has no geometry in a true way. So, we will just be mimicking it. So, the affine space is the following. it just a set, we will write it like this, but what it means is simply all the n tuples, so that is the affine n space.

Now the critiques amongst you may ask if it is just k to the n why did we define such a complicated notation and a name. So the reason is that it is true that as a set it is k to the n but affine n space will have other interrelationships and its own geometry which we will soon define. What you should compare this with is R to the n. So, the Euclidean n space when you think of it, you do not think of just n tuples of reals discreetly. You have a immediate understanding of length of a vector, vectors which are close in length, vectors which are close to 0 and so on.

So, there is also you have this idea of metric also. So that kind of a thing we want to simulate which is why we have defined this affine n space although as a set it is just n doubles. So just bear with that till we actually define the topological structure. Yes so its elements are just points. so since it is an n tuple you have these coordinates, so then ai is the ith coordinate of the point and there is the polynomial ring So, whenever we define a geometric object, we will also define its ring, the coordinate ring, the so called coordinate

ring. So, in this case we have the affine n space over k and we have the corresponding polynomial ring, we have the corresponding ring which in this case happens to be the polynomial ring.

The way these two connect is the following. So any f defines any element f in that ring A, it defines a function from the affine space to the base field. So what does the function do? It takes a point. and it does what? Just evaluates the point, just say evaluation map. So, that is the meaning of the coordinate ring of your geometric space. So, this coordinate ring of which in this case is A, big A, it collects all the functions that map the geometric space to the base field.

It is the collection of all functions. Yes, but when we will define a general variety then we will say that this is the coordinate ring. In this case it is just it happens to be the polynomial ring. But I am trying to define or just suggest the association between the geometric space and the algebra.

So, maybe I should write that. So, it is also the coordinate ring of the affine space. okay but it's a bit simpler to just say to just call it the polynomial ring because that's what polynomial rings are and so the connection between the two is the is is as follows that from the affine space if you wanted to map to the base field these are all the maps a has all these maps okay yeah so the the viewpoint is as follows you have a to the n that you wanted to study these points and instead what you will study is something that surrounds these points and is more algebraic. So, you have for example, you have F, you have G which are elements in this ring A and when you take a point. a geometric point P, then what F is doing is it is evaluating it, right and what G is doing is it is evaluating it. So, you have this green geometric object and the orange thing is which sits outside.

So, these are the functions defined on top of this. So this is a picture which will make more and more complicated as we go along in the theory. So right now these are kind of global functions because they are defined everywhere in your space. And slowly we'll make it more and more local and maybe not in this course, but ultimately you may also be, you may also want to study things which are not even functions, but I think in this course we will restrict to functions, probably I think in this course we will restrict to functions, but this intuition can be extended even to objects which are not even functions in this way. So make it more abstract, which by the way are called sheaves, in case you have heard the term.

So F associates a value to each point in the space. So, we have not said anything particularly deep or of any use. We are just defining terms. So, let us continue to define more terms, since we have time to fill. So, the zeros of F. So, now we are interested in for this f how many points actually gives 0 right so f(p) equal to 0 so those are zeros of f and we define this notation z of f is the set of those points such that f(p) is So, at this point I should ask, is there a function f which is 0 on the whole space, whole green space? 0, but other than 0 is there a non-zero function which is 0 everywhere? Yes, so in finite field they are, that is a

good point, but say over complex or over So show as a homework exercise that a function f assuming that the field k was complex or f(p) bar, the points on which it vanishes is always a very sparse part of the whole space, it is a very small part.

So this z of f is actually a very small part of the whole space. So, which is why we will always work with the complex field in complex analysis, but in our case f(p) bar because in f(p) bar there is this property that the zeros are few. So, these are kind of the interesting subsets of your space which you should focus on and patching them together hopefully you can understand the information about the whole space. So it is kind of a crazy induction. So just let me generalize this and then we can stop. So similarly for a subset of A, we can define Z of T to be those points in your green space such that for all f in T, each of these f they vanish.

So, in other words for a subset T of the coordinate ring or the polynomial ring in this case, Z of T are the points which are common zeros of T. So these sets will be very special, our whole topological space will actually build on these things as atoms. These will be the smallest building structures, based on this we can build bigger structures which we will do next time.