美国数学会经典影印系列

AMS
AMERICAN MATHEMATICAL SOCIETY

An Epsilon of Room, II

pages from year three
of a mathematical blog

ε空间，II 第三年的数学博客选文

Terence Tao

高等教育出版社

美国数学会经典影印系列
AMS
American Mathematical Society

An Epsilon of Room, II

pages from year three
of a mathematical blog

ε空间，II 第三年的数学博客选文

Terence Tao

高等教育出版社·北京

图字：01-2016-2519 号

ε 空间 . II
ε Kongjian. II

图书在版编目 (CIP) 数据

ε 空间 . II, 第三年的数学博客选文 = An Epsilon of Room, II: pages from year three of a mathematical blog : 英文 / (澳) 陶哲轩 (Terence Tao) 著 . —影印本. —北京 : 高等教育出版社 , 2017.1
ISBN 978-7-04-046899-1
Ⅰ. ① ε… Ⅱ. ①陶… Ⅲ. ①数学—文集—英文
Ⅳ. ①O1-53
中国版本图书馆 CIP 数据核字 (2016) 第 281729 号

策划编辑　赵天夫　　责任编辑　赵天夫
封面设计　张申申　　责任印制　毛斯璐

出版发行　高等教育出版社
社址　北京市西城区德外大街 4 号
邮政编码　100120
购书热线　010-58581118
咨询电话　400-810-0598
网址　http://www.hep.edu.cn
http://www.hep.com.cn
网上订购　http://www.hepmall.com.cn
http://www.hepmall.com
http://www.hepmall.cn
印刷　北京中科印刷有限公司

开本　787mm × 1092mm　1/16
印张　16.5
字数　380 千字
版次　2017 年 1 月第 1 版
印次　2017 年 1 月第 1 次印刷
定价　99.00 元

[物 料 号 46899-00]

To Garth Gaudry, who set me on the road;
To my family, for their constant support;
And to the readers of my blog, for their feedback and contributions.

Preface

In February of 2007, I converted my "What's new" web page of research updates into a blog at `terrytao.wordpress.com`. This blog has since grown and evolved to cover a wide variety of mathematical topics, ranging from my own research updates, to lectures and guest posts by other mathematicians, to open problems, to class lecture notes, to expository articles at both basic and advanced levels.

With the encouragement of my blog readers, and also of the American Mathematical Society, I published many of the mathematical articles from the first two years of the blog as [**Ta2008**] and [**Ta2009**], which will henceforth be referred to as *Structure and Randomness* and *Poincaré's Legacies Vols. I, II* throughout this book. This gave me the opportunity to improve and update these articles to a publishable (and citeable) standard, and also to record some of the substantive feedback I had received on these articles by the readers of the blog.

The current text contains many (though not all) of the posts for the third year (2009) of the blog, focusing primarily on those posts of a mathematical nature which were not contributed primarily by other authors, and which are not published elsewhere. It has been split into two volumes.

The first volume (referred to henceforth as *Volume 1*) consisted primarily of lecture notes from my graduate courses on real analysis that I taught at UCLA. The current volume consists instead of sundry articles on a variety of mathematical topics, which I have divided (somewhat arbitrarily) into expository articles (Chapter 1) which are introductory articles on topics of relatively broad interest, and more technical articles (Chapter 2) which are narrower in scope and often related to one of my current research interests.

These can be read in any order, although they often reference each other as well as articles from previous volumes in this series.

A remark on notation

For reasons of space, we will not be able to define every single mathematical term that we use in this book. If a term is italicised for reasons other than emphasis or for definition, then it denotes a standard mathematical object, result, or concept, which can be easily looked up in any number of references. (In the blog version of the book, many of these terms were linked to their Wikipedia pages, or other on-line reference pages.)

I will however mention a few notational conventions that I will use throughout. The cardinality of a finite set E will be denoted $|E|$. We will use the asymptotic notation $X = O(Y)$, $X \ll Y$, or $Y \gg X$ to denote the estimate $|X| \leq CY$ for some absolute constant $C > 0$. In some cases we will need this constant C to depend on a parameter (e.g., d), in which case we shall indicate this dependence by subscripts, e.g., $X = O_d(Y)$ or $X \ll_d Y$. We also sometimes use $X \sim Y$ as a synonym for $X \ll Y \ll X$.

In many situations there will be a large parameter n that goes off to infinity. When that occurs, we also use the notation $o_{n\to\infty}(X)$ or simply $o(X)$ to denote any quantity bounded in magnitude by $c(n)X$, where $c(n)$ is a function depending only on n that goes to zero as n goes to infinity. If we need $c(n)$ to depend on another parameter, e.g., d, we indicate this by further subscripts, e.g., $o_{n\to\infty;d}(X)$.

We will occasionally use the averaging notation $\mathbf{E}_{x\in X} f(x) := \frac{1}{|X|}\sum_{x\in X} f(x)$ to denote the average value of a function $f : X \to \mathbf{C}$ on a nonempty finite set X.

Acknowledgments

The author is supported by a grant from the MacArthur Foundation, by NSF grant DMS-0649473, and by the NSF Waterman Award.

Thanks to Konrad Swanepoel, Blake Stacey, and anonymous commenters for global corrections to the text, and to Edward Dunne at the AMS for encouragement and editing.

Contents

Preface vii

A remark on notation viii

Acknowledgments viii

Chapter 1. Expository articles 1

§1.1. An explicitly solvable nonlinear wave equation 2

§1.2. Infinite fields, finite fields, and the Ax-Grothendieck theorem 7

§1.3. Sailing into the wind or faster than the wind 12

§1.4. The completeness and compactness theorems of first-order logic 20

§1.5. Talagrand's concentration inequality 35

§1.6. The Szemerédi-Trotter theorem and the cell decomposition 42

§1.7. Benford's law, Zipf's law, and the Pareto distribution 48

§1.8. Selberg's limit theorem for the Riemann zeta function on the critical line 59

§1.9. $P = NP$, relativisation, and multiple-choice exams 68

§1.10. Moser's entropy compression argument 74

§1.11. The AKS primality test 82

§1.12. The prime number theorem in arithmetic progressions, and dueling conspiracies 87

§1.13. Mazur's swindle 105

§1.14. Grothendieck's definition of a group 108

§1.15. The "no self-defeating object" argument 116

§1.16. From Bose-Einstein condensates to the nonlinear Schrödinger equation 129

Chapter 2. Technical articles 141

§2.1. Polymath1 and three new proofs of the density Hales-Jewett theorem 142

§2.2. Szemerédi's regularity lemma via random partitions 154

§2.3. Szemerédi's regularity lemma via the correspondence principle 162

§2.4. The two-ends reduction for the Kakeya maximal conjecture 171

§2.5. The least quadratic nonresidue, and the square root barrier 177

§2.6. Determinantal processes 188

§2.7. The Cohen-Lenstra distribution 200

§2.8. An entropy Plünnecke-Ruzsa inequality 203

§2.9. An elementary noncommutative Freiman theorem 206

§2.10. Nonstandard analogues of energy and density increment arguments 209

§2.11. Approximate bases, sunflowers, and nonstandard analysis 212

§2.12. The double Duhamel trick and the in/out decomposition 230

§2.13. The free nilpotent group 233

Bibliography 241

Index 247

Chapter 1

Expository articles

1.1. An explicitly solvable nonlinear wave equation

As is well known, the linear one-dimensional wave equation

$$-\phi_{tt} + \phi_{xx} = 0, \tag{1.1}$$

where $\phi : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ is the unknown field (which, for simplicity, we assume to be smooth), can be solved explicitly; indeed, the general solution to (1.1) takes the form

$$\phi(t,x) = f(t+x) + g(t-x) \tag{1.2}$$

for some arbitrary (smooth) functions $f, g : \mathbf{R} \to \mathbf{R}$. (One can of course determine f and g once one specifies enough initial data or other boundary conditions, but this will not be the focus of this article.)

When one moves from linear wave equations to nonlinear wave equations, then in general one does not expect to have a closed-form solution such as (1.2). So I was pleasantly surprised recently while playing with the nonlinear wave equation

$$-\phi_{tt} + \phi_{xx} = e^{\phi} \tag{1.3}$$

to discover that this equation can also be explicitly solved in closed form. (For the reason why I was interested in this equation, see [**Ta2010**].)

A posteriori, I now know the reason for this explicit solvability: (1.3) is the limiting case $a = 0, b \to -\infty$ of the more general equation

$$-\phi_{tt} + \phi_{xx} = e^{\phi+a} - e^{-\phi+b}$$

which (after applying the simple transformation

$$\phi = \frac{b-a}{2} + \psi(\sqrt{2}e^{\frac{a+b}{4}}t, \sqrt{2}e^{\frac{a+b}{4}}x))$$

becomes the *sinh-Gordon equation*

$$-\psi_{tt} + \psi_{xx} = \sinh(\psi)$$

(a close cousin of the more famous *sine-Gordon equation* $-\phi_{tt} + \phi_{xx} = \sin(\phi)$), which is known to be completely integrable and exactly solvable. However, I only realised this after the fact and stumbled upon the explicit solution to (1.3) by much more classical and elementary means. I thought I might share the computations here, as I found them somewhat cute, and they seem to serve as an example of how one might go about finding explicit solutions to PDE in general; accordingly, I will take a rather pedestrian approach to describing the hunt for the solution, rather than presenting the shortest or slickest route to the answer.

After the initial publishing of this post, Patrick Dorey pointed out to me that (1.3) is extremely classical; it is known as *Liouville's equation* and was

solved by Liouville [**Li1853**], with essentially the same solution as presented here.

1.1.1. Symmetries. To simplify the discussion, let us ignore all issues of regularity, division by zero, taking square roots and logarithms of negative numbers, etc., and proceed for now in a purely formal fashion, pretending that all functions are smooth and lie in the domain of whatever algebraic operations are being performed. (It is not too difficult to go back after the fact and justify these formal computations, but I do not wish to focus on that aspect of the problem here.)

Although not strictly necessary for solving the equation (1.3), I find it convenient to bear in mind the various symmetries that (1.3) enjoys, as this provides a useful "reality check" to guard against errors (e.g., arriving at a class of solutions which is not invariant under the symmetries of the original equation). These symmetries are also useful to normalise various special families of solutions.

One easily sees that solutions to (1.3) are invariant under space-time translations

$$\phi(t,x) \mapsto \phi(t-t_0, x-x_0) \tag{1.4}$$

and also space-time reflections

$$\phi(t,x) \mapsto \phi(\pm t, \pm x). \tag{1.5}$$

Being relativistic, the equation is also invariant under Lorentz transformations

$$\phi(t,x) \mapsto \phi(\frac{t-vx}{\sqrt{1-v^2}}, \frac{x-vt}{\sqrt{1-v^2}}). \tag{1.6}$$

Finally, one has the scaling symmetry

$$\phi(t,x) \mapsto \phi(\lambda t, \lambda x) + 2\log\lambda. \tag{1.7}$$

1.1.2. Solution. Henceforth, ϕ will be a solution to (1.3). In view of the linear explicit solution (1.2), it is natural to move to null coordinates

$$u = t + x, v = t - x,$$

thus

$$\partial_u = \frac{1}{2}(\partial_t + \partial_x); \partial_v = \frac{1}{2}(\partial_t - \partial_x)$$

and (1.3) becomes

$$\phi_{uv} = -\frac{1}{4}e^{\phi}. \tag{1.8}$$

The various symmetries (1.4)–(1.7) can of course be rephrased in terms of null coordinates in a straightforward manner. The Lorentz symmetry (1.6) simplifies particularly nicely in null coordinates, to

$$\phi(u,v) \mapsto \phi(\lambda u, \lambda^{-1} v). \tag{1.9}$$

Motivated by the general theory of stress-energy tensors of relativistic wave equations (of which (1.3) is a very simple example), we now look at the null energy densities ϕ_u^2, ϕ_v^2. For the linear wave equation (1.1) (or equivalently $\phi_{uv} = 0$), these null energy densities are transported in null directions:

$$\partial_v \phi_u^2 = 0; \partial_u \phi_v^2 = 0. \tag{1.10}$$

(One can also see this from the explicit solution (1.2).)

The above transport law is not quite true for the nonlinear wave equation, of course, but we can hope to get some usable substitute. Let us just look at the first null energy ϕ_u^2 for now. By two applications of (1.10), this density obeys the transport equation

$$\begin{aligned} \partial_v \phi_u^2 &= 2\phi_u \phi_{uv} \\ &= -\frac{1}{2}\phi_u e^{\phi} \\ &= -\frac{1}{2}\partial_u(e^{\phi}) \\ &= 2\partial_u \phi_{uv} \\ &= \partial_v(2\phi_{uu}), \end{aligned}$$

and thus we have the pointwise conservation law

$$\partial_v(\phi_u^2 - 2\phi_{uu}) = 0,$$

which implies that

$$-\frac{1}{2}\phi_{uu} + \frac{1}{4}\phi_u^2 = U(u) \tag{1.11}$$

for some function $U : \mathbf{R} \to \mathbf{R}$ depending only on u. Similarly we have

$$-\frac{1}{2}\phi_{vv} + \frac{1}{4}\phi_v^2 = V(v)$$

for some function $V : \mathbf{R} \to \mathbf{R}$ depending only on v.

For any fixed v, (1.11) is a nonlinear ODE in u. To solve it, we can first look at the homogeneous ODE

$$-\frac{1}{2}\phi_{uu} + \frac{1}{4}\phi_u^2 = 0. \tag{1.12}$$

Undergraduate ODE methods (e.g., separation of variables after substituting $\psi := \phi_u$) soon reveal that the general solution to this ODE is given by $\phi(u) = -2\log(u + C) + D$ for arbitrary constants C, D (ignoring the issue of singularities or degeneracies for now). Equivalently, (1.12) is obeyed if

and only if $e^{-\phi/2}$ is linear in u. Motivated by this, we become tempted to rewrite (1.11) in terms of $\Phi := e^{-\phi/2}$. One soon realises that

$$\partial_{uu}\Phi = (-\frac{1}{2}\phi_{uu} + \frac{1}{4}\phi_u^2)\Phi,$$

and hence (1.11) becomes

$$(-\partial_{uu} + U(u))\Phi = 0, \tag{1.13}$$

thus Φ is a null (generalised) eigenfunction of the Schrodinger operator (or Hill operator) $-\partial_{uu} + U(u)$. If we let $a(u)$ and $b(u)$ be two linearly independent solutions to the ODE

$$-f_{uu} + Uf = 0, \tag{1.14}$$

we thus have

$$\Phi = a(u)c(v) + b(u)d(v) \tag{1.15}$$

for some functions c, d (which one easily verifies to be smooth, since ϕ, a, b are smooth and a, b are linearly independent). Meanwhile, by playing around with the second null energy density, we have the counterpart to (1.14),

$$(-\partial_{vv} + V(v))\Phi = 0,$$

and hence (by linear independence of a, b) c, d must be solutions to the ODE

$$-g_{vv} + Vg = 0.$$

This would be a good time to pause and see whether our implications are reversible, i.e., whether any ϕ that obeys the relation (1.15) will solve (1.3) or (1.10). It is of course natural to first write (1.10) in terms of Φ. Since

$$\Phi_u = -\frac{1}{2}\phi_u\Phi; \Phi_v = -\frac{1}{2}\phi_v\Phi; \Phi_{uv} = (\frac{1}{4}\phi_u\phi_v - \frac{1}{2}\phi_{uv})\Phi,$$

one soon sees that (1.10) is equivalent to

$$\Phi\Phi_{uv} = \Phi_u\Phi_v + \frac{1}{8}. \tag{1.16}$$

If we then insert the ansatz (1.15), we soon reformulate the above equation as

$$(a(u)b'(u) - b(u)a'(u))(c(v)d'(v) - d(v)c'(v)) = \frac{1}{8}.$$

It is at this time that one should remember the classical fact that if a, u are two solutions to the ODE (1.11), then the *Wronskian* $ab' - ba'$ is constant; similarly $cd' - dc'$ is constant. Putting this all together, we see that

Theorem 1.1.1. *A smooth function ϕ solves* (1.3) *if and only if we have the relation* (1.13) *for some functions a, b, c, d obeying the Wronskian conditions $ab' - ba' = \alpha$, $cd' - dc' = \beta$ for some constants α, β multiplying to $\frac{1}{8}$.*

Note that one can generate solutions to the Wronskian equation $ab' - ba' = \alpha$ by a variety of means, for instance by first choosing a arbitrarily and then rewriting the equation as $(b/a)' = \alpha/a^2$ to recover b. (This does not quite work at the locations when a vanishes, but there are a variety of ways to resolve that; as I said above, we are ignoring this issue for the purposes of this discussion.)

This is not the only way to express solutions. Factoring $a(u)d(v)$ (say) from (1.13), we see that Φ is the product of a solution $c(v)/d(v)+b(u)/a(u)$ to the linear wave equation, plus the exponential of a solution $\log a(u)+\log d(u)$ to the linear wave equation. Thus we may write $\phi = F - 2\log G$, where F and G solve the linear wave equation. Inserting this back ansatz into (1.1), we obtain

$$2(-G_t^2 + G_x^2)/G^2 = e^F/G^2$$

and so we see that

$$\phi = \log \frac{2(-G_t^2 + G_x^2)}{G^2} = \log \frac{-8G_u G_v}{G^2}, \tag{1.17}$$

for some solution G to the free wave equation, and conversely every expression of the form (1.17) can be verified to solve (1.1) (since $\log 2(-G_t^2 + G_x^2)$ does indeed solve the free wave equation, thanks to (1.2)). Inserting (1.2) into (1.17), we thus obtain the explicit solution

$$\phi = \log \frac{-8f'(t+x)g'(t-x)}{(f(t+x)+g(t-x))^2} \tag{1.18}$$

to (1.1), where f and g are arbitrary functions (recall that we are neglecting issues such as whether the quotient and the logarithm are well defined).

I, for one, would not have expected the solution to take this form. But it is instructive to check that (1.18) does at least respect all the symmetries (1.4)–(1.7).

1.1.3. Some special solutions. If we set $U = V = 0$, then a, b, c, d are linear functions, and so Φ is affine linear in u, v. One also checks that the uv term in Φ cannot vanish. After translating in u and v, we end up with the ansatz $\Phi(u,v) = c_1 + c_2 uv$ for some constants c_1, c_2; applying (1.16), we see that $c_1 c_2 = 1/8$, and by using the scaling symmetry (1.7), we may normalise e.g., $c_1 = 8, c_2 = 1$, and so we arrive at the (singular) solution

$$\phi = -2\log(8+uv) = \log \frac{1}{(8+t^2-x^2)^2}. \tag{1.19}$$

To express this solution in the form (1.18), one can take $f(u) = \frac{8}{u}$ and $g(v) = v$; some other choices of f, g are also possible. (Determining the extent to which f, g are uniquely determined by ϕ in general can be established from a closer inspection of the previous arguments; this is left as an exercise.)

We can also look at what happens when ϕ is constant in space, i.e., it solves the ODE $-\phi_{tt} = e^{\phi}$. It is not hard to see that U and V must be constant in this case, leading to a, b, c, d which are either trigonometric or exponential functions. This soon leads to the ansatz $\Phi = c_1 e^{\alpha t} + c_2 e^{-\alpha t}$ for some (possibly complex) constants c_1, c_2, α, thus $\phi = -2\log(c_1 e^{\alpha t} + c_2 e^{-\alpha t})$. By using the symmetries (1.4), (1.7) we can make $c_1 = c_2$ and specify α to be whatever we please, thus leading to the solutions $\phi = -2\log\cosh \alpha t + c_3$. Applying (1.1) we see that this is a solution as long as $e^{c_3} = 2\alpha^2$. For instance, we may fix $c_3 = 0$ and $\alpha = 1/\sqrt{2}$, leading to the solution

$$\phi = -2\log\cosh\frac{t}{\sqrt{2}}. \tag{1.20}$$

To express this solution in the form (1.18), one can take for instance $f(u) = e^{u/\sqrt{2}}$ and $g(v) = e^{-v/\sqrt{2}}$.

One can of course push around (1.19), (1.20) by the symmetries (1.4)–(1.7) to generate a few more special solutions.

Notes. This article first appeared at

`terrytao.wordpress.com/2009/01/22`.

Thanks to Jake K. for corrections.

There was some interesting discussion online regarding whether the heat equation had a natural relativistic counterpart, and more generally whether it was profitable to study nonrelativistic equations via relativistic approximations.

1.2. Infinite fields, finite fields, and the Ax-Grothendieck theorem

Jean-Pierre Serre (whose papers are, of course, always worth reading) recently wrote a lovely article [**Se2009**] in which he describes several ways in which algebraic statements over fields of zero characteristic, such as $\mathbf{C}$, can be deduced from their positive characteristic counterparts such as F_{p^m}, despite the fact that there is no nontrivial field homomorphism between the two types of fields. In particular, finitary tools, including such basic concepts as cardinality, can now be deployed to establish infinitary results. This leads to some simple and elegant proofs of nontrivial algebraic results which are not easy to establish by other means.

One deduction of this type is based on the idea that positive characteristic fields can partially *model* zero characteristic fields, and it proceeds like this: If a certain algebraic statement failed over (say) $\mathbf{C}$, then there should be a "finitary algebraic" obstruction that "witnesses" this failure over $\mathbf{C}$.

Because this obstruction is both finitary and algebraic, it must also be definable in some (large) finite characteristic, thus leading to a comparable failure over a finite characteristic field. Taking contrapositives, one obtains the claim.

Algebra is definitely not my field of expertise, but it is interesting to note that similar themes have also come up in my own area of additive combinatorics (and more generally arithmetic combinatorics), because the combinatorics of addition and multiplication on finite sets is definitely of a "finitary algebraic" nature. For instance, a recent paper of Vu, Wood, and Wood [**VuWoWo2010**] establishes a finitary "Freiman-type" homomorphism from (finite subsets of) the complex numbers to large finite fields that allows them to pull back many results in arithmetic combinatorics in finite fields (e.g., the sum-product theorem) to the complex plane; Van Vu and I also used a similar trick in [**TaVu2007**] to control the singularity property of random sign matrices by first mapping them into finite fields in which cardinality arguments became available). And I have a particular fondness for correspondences between finitary and infinitary mathematics; the correspondence Serre discusses is slightly different from the one I discuss, for instance in Section 1.3 of *Structure and Randomness*, although there seems to be a common theme of "compactness" (or of model theory) tying these correspondences together.

As one of his examples, Serre cites one of my favourite results in algebra, discovered independently by Ax [**Ax1968**] and by Grothendieck [**Gr1966**] (and then rediscovered many times since). Here is a special case of that theorem:

Theorem 1.2.1 (Ax-Grothendieck theorem, special case). *Let $P : \mathbf{C}^n \to \mathbf{C}^n$ be a polynomial map from a complex vector space to itself. If P is injective, then P is bijective.*

The full version of the theorem allows one to replace $\mathbf{C}^n$ by an algebraic variety X over any algebraically closed field, and it allows for P to be an morphism from the algebraic variety X to itself. But for simplicity I will just discuss the above special case. This theorem is not at all obvious; it is not too difficult (see Lemma 1.2.6 below) to show that the *Jacobian* of P is nondegenerate, but this does not come close to solving the problem since one would then be faced with the notorious *Jacobian conjecture*. Also, the claim fails if "polynomial" is replaced by "holomorphic", due to the existence of *Fatou-Bieberbach domains*.

In this post I would like to give the proof of Theorem 1.2.1 based on finite fields as mentioned by Serre, as well as another elegant proof of Rudin [**Ru1995**] that combines algebra with some elementary complex variable

methods. (There are several other proofs of this theorem and its generalisations, for instance a topological proof by Borel [**Bo1969**], which I will not discuss here.)

1.2.1. Proof via finite fields. The first observation is that the theorem is utterly trivial in the finite field case:

Theorem 1.2.2 (Ax-Grothendieck theorem in F). *Let F be a finite field, and let $P : F^n \to F^n$ be a polynomial. If P is injective, then P is bijective.*

Proof. Any injection from a finite set to itself is necessarily bijective. (The hypothesis that P is a polynomial is not needed at this stage, but becomes crucial later on.) □

Next, we pass from a finite field F to its algebraic closure $\overline{F}$.

Theorem 1.2.3 (Ax-Grothendieck theorem in $\overline{F}$). *Let F be a finite field, let $\overline{F}$ be its algebraic closure, and let $P : \overline{F}^n \to \overline{F}^n$ be a polynomial. If P is injective, then P is bijective.*

Proof. Our main tool here is *Hilbert's nullstellensatz*, which we interpret here as an assertion that if an algebraic problem is insoluble, then there exists a finitary algebraic obstruction that witnesses this lack of solution (see also Section 1.15 of *Structure and Randomness*). Specifically, suppose for contradiction that we can find a polynomial $P : \overline{F}^n \to \overline{F}^n$ which is injective but not surjective. Injectivity of P means that the algebraic system

$$P(x) = P(y), \quad x \neq y,$$

has no solution over the algebraically closed field $\overline{F}$; by the nullstellensatz, this implies that there must exist an algebraic identity of the form

$$(P(x) - P(y)) \cdot Q(x, y) = (x - y)^r \tag{1.21}$$

for some $r \geq 1$ and some polynomial $Q : \overline{F}^n \times \overline{F}^n \to \overline{F}^n$ that specifically witnesses this lack of solvability. Similarly, lack of surjectivity means the existence of an $z_0 \in \overline{F}^n$ such that the algebraic system

$$P(x) = z_0$$

has no solution over the algebraically closed field $\overline{F}$. By another application of the nullstellensatz, there must exist an algebraic identity of the form

$$(P(x) - z_0) \cdot R(x) = 1 \tag{1.22}$$

for some polynomial $R : \overline{F}^n \to \overline{F}^n$ that specifically witnesses this lack of solvability.

Fix Q, z_0, R as above, and let k be the subfield of $\overline{F}$ generated by F and the coefficients of P, Q, z_0, R. Then we observe (thanks to our explicit