The Real Holomorphy Ring and Sums of Powers in Rational and Elliptic Function Fields over The Field of Real Numbers

By
Natea Hunde

Advisor: Prof. Dr. Eberhard Becker
Co-advisor: Dr. Berhanu Bekele

A Thesis Submitted to
The Department of Mathematics
Presented in Fulfilment of The Requirements for Degree of
Doctor of Philosophy (Mathematics)

Addis Ababa University
Addis Ababa, Ethiopia
March 2017

Abstract

This thesis is devoted to a study of real holomorphy rings in $\mathbb{R}(x)$ and elliptic function fields $\mathbb{R}(x)(\sqrt{f(x)}), f$ is a monic polynomial of degree 3 with no multiple roots in $\mathbb{C}$ over $\mathbb{R}$ and sums of powers in $\mathbb{R}(x)$. The objects of study are real valuation rings, real holomorphy rings and real places in the rational function fields $\mathbb{R}(x)$ and then investigate their extension to elliptic function fields which are quadratic extension of $\mathbb{R}(x)$. We write down the full list of real valuation rings to give the description of holomorphy ring in both fields and finally we study applications to sums of powers.

Acknowledgements

Praise be to the LORD!

I believe that we are the sum total of all the individuals who have in some way, small or great, contributed to our lives. I learned almost everything I know from some one and my life depend on the labours of other men, living and dead. The likes of Serge Lang, T.Y.Lam, Bruce Reznick, Irving Kaplansky, David Eisenbud, William Fulton, Robin Hartshorne and many others who wrote on commutative algebra and algebraic geometry I am highly grateful for all of them having learned from their papers and books.

My sincere thanks to my Principal Advisor, Prof.Dr. Eberhard Becker, for introducing me to the fascinating topics of algebraic curves, real holomorphy rings, higher level orderings and sums of powers. I am highly favoured or privileged in that he was very patient with me in introducing me to new concepts and mathematical research. I appreciate and thank him for what I learnt from him during our conversation be it formal or informal that what research in mathematics and the unity of mathematics is. His meticulous edition gave life to my scratch works and to my surprise helped much in understanding sometimes even what I wrote. His edition also helped me to learn writing skills in mathematics. In fact it is advantageous to learn from the masters. Professor Becker invited me to his home university TU of Dortmund, Germany for eight months in three separate times by covering my expenses. He also showed me ancient churches or cathedrals in Cologne and Dortmund cities, St. Goarshausen with the famous rock " The LORELEY", VATER RHEIN, the nice city of "Limburg an der Lahn" and Museum at GOETHE university in FRANKFURT AM MAIN. He also took me to the game in the famous stadium of Borussia Dortmund.

I would like also to thank my co-advisor Dr. Berhanu Bekele for he helped me in changing my principal advisor to Prof. Becker and he invited him to give a lecture on algebraic curves at Addis Ababa University. His contribution to the department's graduate committee decision to invite Prof. Becker on my defense date of this thesis from ISP fund of the department is great. In my first trip to Germany he helped me much for which I am grateful. I also acknowledge the discussions made during seminar times.

I enjoyed the time I spent with my friends and also instructors in algebra stream and want to say thank you all.

No less important is Professor H.V.Kumbhojkar who taught me algebra courses, challenged and introduced me to fuzzy sets and logic. He encourages me by giving advice not only on algebra but also things helpful in the walk of life something for which I am grateful.

The prayer of my parents is always with me and God bless you all!

Last, but definitely not least, I would like to thank AMA for your writings kept me strong and inspired. JL I could never forget the way you told me everything by saying nothing.

I dedicated this thesis to Hayilamariyam Gammadaa Masqalee who paved the way and every generation after him who followed his way.

Contents

Introduction

This thesis is devoted to a study of real holomorphy rings, in $\mathbb{R}(x)$ and elliptic function fields $\mathbb{R}(x)(\sqrt{f(x)})$, f any monic polynomial of degree 3 with no multiple roots in $\mathbb{C}$ and sums of powers in these fields, mainly in $\mathbb{R}(x)$. It is the central objective to interpret the general theory of real holomorphy rings and sums of powers in arbitrary formally real fields by providing a more concrete approach and add additional results based on special properties of the fields in questions.

As in the general theory, the central objects are the so called real valuation rings, i.e. valuation rings with a formally real valuation residue field which in the cases of study will be just $\mathbb{R}$. Also they turn out to be discrete valuation rings. We list them completely as concretely as possible.

The next object to study is the real holomorphy ring, by definition the intersection of all real valuation rings. In the context of this thesis these rings are Dedekind domains. These real holomorphy rings show one astonishing feature known from the general theory: their totally positive units are sums of $2n-th$ powers for every n.

Connected to the real holomorphy ring is another central object of the theory: the so called real places of a formally real field which form a compact Hausdorff spaces M. The real holomorphy ring $H(K)$ of a formally real field K is isomorphic, in a natural way, to a dense subring of $C(M, \mathbb{R})$, by virtue of the Stone-Weierstraß approximation theorem. In the present situation, the space of real places can be realized as compact smooth real algebraic curves assigned to our fields of study. Regarding the rational function field we are dealing with the affine line, in the elliptic function fields we are concerned with the famous elliptic curves. In either case, the space of real places is homeomorphic to the space of real points on the projective closure of these curves. This fact allows to draw information about the real holomorphy rings and real valuation rings.

Methodologically, we first study these objects(real valuation rings, real holomorphy rings and real places) in the rational function field $\mathbb{R}(x)$ and then investigate the extension to elliptic function fields which are quadratic extension of $\mathbb{R}(x)$. Finally, we are using these results to draw conclusions on sums of powers.

The first chapter describes the mathematical scenario to which the topic of this thesis belongs. It is justified to state that the topic had started to evolve into a substantial theory with Hilbert's 17th Problem and its solution by Artin roughly 25 years later. In addition to this historical sketch we outline the concepts and general theorems we are going to use throughout this thesis.

Chapter 2 is devoted to the study of the rational function field $\mathbb{R}(x)$. It is possible to list all real valuation rings which turn out to be discrete valuation rings with residue field $\mathbb{R}$. As a consequence, a concrete description of the real holomorphy ring $H := H(\mathbb{R}(x))$ can be derived and it will be proven that this ring is a Dedekind ring with field of fraction equal to $\mathbb{R}(x)$. No maximal ideal is a principal ideal, but their squares are principal. In both cases explicit generators can be presented.
Finally, the space of real places is shown to be homeomorphic to the real projective line $\mathbb{P}^1$. We end up with a topological representation $H \to C(\mathbb{P}^1, \mathbb{R})$ and show, by virtue of the Stone-Weierstraß approximation theorem, that it admits a dense image.

Chapter 3 treats the case of an elliptic function field L in an analogue manner: finding a complete list of its real valuation rings, a description of $H(L)$, generators for its maximal ideals and their squares, proving that $H(L)$ is a Dedekind ring, presenting a geometric interpretation of its space of real places and the topological representation of $H(L)$. In this case, the space of real places turns out to be homeomorphic to the 1-point compactification of the set of real points on the affine elliptic curve given by the equation $Y^2 = f(X)$. In order to achieve all this, methods and results from commutative ring theory will be applied in combination with the detailed information on valuation rings we can provide.

In the final chapter 4 we apply the structural results of the previous chapters to the study of sums of powers. Originally, in the early work of E. Becker, sums of powers were studied by the so called orderings of higher level. Later on, it was observed that the real holomorphy ring is suitable to assume a central role. In fact, results on its groups of units and its ideal structure immediately lead to results on sums of powers. It is the objective to display this approach in the case of our fields by representing a few striking results. Whenever it comes to really concrete statements we confine ourselves to the rational function field case where the arguments can be given in a very clear manner.

Chapter 1

A Sketch of The General Scenario

1.1 Hilbert's 17th Problem

The material used as background theory is mainly drawn from **[12], [18], [19], [21], [25]** and lectures given to me in **Dortmund** and texts sent through **e-mail** to me by Professor Becker.
The following result from linear algebra is used in what follows.

Proposition 1 *For a real symmetric $n \times n$ matrix A, the following are equivalent:*
(1) $x^T Ax \geq 0$ for all $x \in \mathbb{R}^n$.
(2) All eigenvaues of A are ≥ 0.
(3) $A = U^T U$ for some $n \times n$ matrix U.
(4) A is a non-negative linear combination of matrices of the form $xx^T, x \in \mathbb{R}^n$.

(Here we view x as column vector in doing matrix computations. For example

$$x^T x = (x_1, ..., x_n) \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix} = x_1^2 + ... + x_n^2 = ||x||^2,$$

whereas $xx^T = \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix} (x_1, ..., x_n) = \begin{pmatrix} x_1 x_1 & \cdots & x_1 x_n \\ \vdots & \vdots & \vdots \\ x_n x_1 & \cdots & x_n x_n \end{pmatrix}$

the $n \times n$ matrix with ij entry $x_i x_j$.)
Proof. (1) $\Rightarrow$ (2). Since A is symmetric, we know the eigenvalues of A are real. Let d be an eigenvalue of A with associated eigenvector x. Then $Ax = dx$ so $x^T Ax = x^T dx = dx^T x = d||x||^2$. Since $x^T Ax \geq 0$ and $x \neq 0$, this forces $d \geq 0$.
(2) $\Rightarrow$ (3). Since A is symmetric, the Spectral theorem applies. (We recall that Spectral Theorem says that if A is a real symmetric $n \times n$ matrix, then there exists an orthogonal $n \times n$ matrix Q and a real diagonal matrix $\wedge$

such that $Q^TAQ = \wedge$, and the n eigenvalues of A are the diagonal entries of $\wedge$.) This yields $A = C^{-1}DC$, with C orthogonal, entries of D are the eigenvalues of A (counted with multiplicities), say $D = \text{diag}(d_1, ..., d_n)$. By (2), $d_i \geq 0$ for each i, so $D = \sqrt{D}^T\sqrt{D}$ where $\sqrt{D} := \text{diag}(\sqrt{d_1}, ..., \sqrt{d_n})$. Thus $A = C^{-1}DC = C^TDC = C^T\sqrt{D}^T\sqrt{D}C = U^TU$, where $U := \sqrt{D}C$.
(3) $\Rightarrow$ (4). $A = v_1v_1^T + ... + v_nv_n^T$ where $v_1, ..., v_n$ are the columns of U^T.
(4) $\Rightarrow$ (1). Suppose $A = r_1v_1v_1^T + ... + r_mv_mv_m^T$ with $r_i \geq 0$.
Then $x^TAx = \sum_{i=1}^m r_ix^Tv_iv_i^Tx = \sum_{i=1}^m r_i(v_i^Tx)^2 \geq 0$.

We say a square matrix A is positive semidefinite (PSD) if A is real symmetric and the equivalent conditions of proposition above hold. We say A is positive definite (PD) if A is real symmetric and $x^TAx > 0$ holds for all non-zero $x \in \mathbb{R}^n$. We note that if A is positive definite, then the eigenvalues of A are strictly positive and the matrix U in (3) is invertible.

Proposition 2 *Let $\mathbb{R}[X_1, ..., X_n]$ be a polynomial ring. If $f \in \mathbb{R}[X_1, ..., X_n]$, $f \neq 0$, then there exists a point $x \in \mathbb{R}^n$ such that $f(x) \neq 0$.*

In fact, one can do much better.

Proposition 3 *If $f \in \mathbb{R}[X_1, ..., X_n], f \neq 0$, then the set $\mathbb{R}^n \setminus Z(f) = \{x \in \mathbb{R}^n : f(x) \neq 0\}$ is dense in $\mathbb{R}^n$.*

The degree of the monomial $cx_1^{d_1}...x_n^{d_n} (c \in \mathbb{R}, d_1, ..., d_n \geq 0)$ is defined to be $\sum_{i=1}^n d_i$. Each $f \in \mathbb{R}[X_1, ..., X_n]$ decomposes (uniquely) as a finite sum of monomials. The degree of f is defined to be the maximum of the degrees of the various monomials appearing in this decomposition. By convention, the degree of the zero polynomial is $-\infty$.
If $\deg(f) \leq d$ then, collecting together monomials of the same degree, f decompose (uniquely) as

$$f = f_0 + f_1 + ... + f_d$$

where each $f_i \in \mathbb{R}[X_1, ..., X_n]$ is homogeneous of degree i (i.e., a sum of monomials of degree i or the zero polynomial).

Corollary 1 *Suppose $f = f_1^2 + ... + f_k^2, f_1, ..., f_k \in \mathbb{R}[X_1, ..., X_n], f_1 \neq 0$. Then*
(1) $f \neq 0$.
(2) $deg(f) = 2max\{deg(f_i) : i = 1, ..., k\}$.

Proof. (1) Since $f_1 \neq 0$ there exists $x \in \mathbb{R}^n$ such that $f_1(x) \neq 0$. Then

$$f(x) = f_1(x)^2 + ... + f_k(x)^2 > 0$$

so $f \neq 0$.

(2) Decompose f_i as $f_i = f_{i0} + ... + f_{id}$, where f_{ij} homogeneous of degree j, $d := \max\{\deg(f_i) | i = 1, ..., k\}$. Clearly $\deg(f) \leq 2d$ and the homogeneous part of degree $2d$ of f is $f_{1d}^2 + ... + f_{kd}^2$. Since $f_{id} \neq 0$ for some i, this is not zero, by(1).

Let $f \in \mathbb{R}[x_1, x_2, ..., x_n]$, the x_i different indeterminates.

If f is a sum of squares, say $f = f_1^2 + f_2^2 + ... + f_r^2$, then $f(x) = f_1(x)^2 + f_2(x)^2 + ... + f_r(x)^2 \geq 0$, for all $x \in \mathbb{R}^n$. It is natural to ask the following:

QUESTION: Is the converse true,i.e., is it true that $f \geq 0$ on $\mathbb{R}^n$ implies that f is a sum of squares in $\mathbb{R}[x_1, x_2, ..., x_n]$?

Hilbert showed that every non-negative polynomial is a sum of squares of polynomials only in the following three cases:

- univariate polynomials,
- quadratic polynomials, and
- bivariate polynomial of degree four.

Proposition 4 *Suppose f is a non-zero polynomial in the single variable x, and let*

$$f = d\prod_i (x - a_i)^{k_i} \prod ((x - b_j)^2 + c_j^2)^{l_j}$$

be the factorization of f into irreducibles in $\mathbb{R}[x]$. Then the following are equivalent:

(1) $f \geq 0$ on $\mathbb{R}$.

(2) $d > 0$ and each k_i is even.

(3) $f = g^2 + h^2$ for some $g, h \in \mathbb{R}[x]$.

Proof. For (2) $\Rightarrow$ (3), we use the "two squares identity" $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. The other cases are obvious.

The answer is 'no' if $n \geq 2$. A concrete example was given by Motzkin in 1967. The Motzkin example is

$$M(x, y) = 1 - 3x^2y^2 + x^2y^4 + x^4y^2$$

Proposition 5 *For M as above:*

(1) $M \geq 0$ on $\mathbb{R}^2$.

(2) M is not a sum of squares in $\mathbb{R}[x, y]$.

Proof. (1) follows from the standard inequality $\frac{a+b+c}{3} \geq \sqrt[3]{abc}$ (if $a, b, c \geq 0$) relating the arithmetic mean and the geometric mean, taking $a = 1, b = x^2y^4$, and $c = x^4y^2$.

For (2) suppose, to the contrary, that $M = \sum f_i^2$ for some polynomials $f_i \in \mathbb{R}[x, y]$. Then each f_i can have degree at most 3 (Corollary 1), so is some real combination of

$$1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3.$$

If x^3 appears in some f_i, then x^6 would appear in M with positive coefficient. Thus x^3 does not appear. Similarly, y^3 does not appear. Arguing in the same way, we see that x^2 and y^2 do not appear, and finally that x and y do not appear. Thus f_i has the form

$$f_i = a_i + b_ixy + c_ix^2y + d_ixy^2.$$

But then $\sum b_i^2 = -3$, a contradiction.

Remarks.

(1) The minimum value of M on $\mathbb{R}^2$ is zero. This occurs at each of the four points $(\pm 1, \pm 1)$.

(2) In fact, one can show that $N + M$ is not a sum of squares in $\mathbb{R}[x, y]$, for any real constant $N \geq 0$. The argument is exactly the same.
(3) In addition to the Motzkin example, many other examples have been considered. These include examples of Robinson in 1969:

$$f(x, y, z) = x^2(x-1)^2 + y^2(y-1)^2 + z^2(z-1)^2 + 2xyz(x+y+z-2).$$

The Choi-Lam example $q(x, y, z) = 1 + x^2y^2 + y^2z^2 + z^2x^2 - 4xyz$ in 1977; the Schmüdgen example in 1979, $r(x, y) = 200[(x^3 - 4x)^2 + (y^3 - 4y)^2] + (y^2 - x^2)x(x+2)[x(x-2) + 2(y^2 - 4)]$ (produced without prior knowledge of earlier explicit examples); and the modified Motzkin example $p(x, y) = 1 - x^2y^2 + x^4y^2 + x^2y^4$ given by Berg, Christensen and Jensen in 1979. Note that

$$p(x, y) = \frac{1}{27}(26 + M(\sqrt{3}x, \sqrt{3}y)).$$

(4) Although M is not a sum of squares of polynomials it is a sum of 4 squares of rational functions, for example:

$$M = \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2}$$

$$= \left(\frac{x^2y(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy^2(x^2+y^2-2)}{x^2+y^2}\right)^2$$

$$+ \left(\frac{xy(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{x^2-y^2}{x^2+y^2}\right)^2.$$

(The first term in the numerator gives rise to the first three squares. The last term gives the final square.)

Hilbert worked with homogeneous polynomials. Homogeneous polynomials are also called forms. Why did Hilbert restrict to this case? If f is any polynomial in $\mathbb{R}[x_1, x_2, ..., x_n]$ of degree $\leq d$, then $\bar{f}(x_0, ..., x_n) = x_o^d f(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})$ (called the homogenization of f) is homogeneous of degree d in $n+1$ variables $x_0, ..., x_n$.

If $f(x_1, x_2, ..., x_n) = \sum c x_1^{d_1} ... x_n^{d_n}$, then

$$\bar{f}(x_0, ..., x_n) = x_0^d \sum c \left(\frac{x_1}{x_0}\right)^{d_1} ... \left(\frac{x_n}{x_0}\right)^{d_n}$$

$$= \sum c x_0^{d - \sum d_i} x_1^{d_1} ... x_n^{d_n}$$

$$= \sum c x_0^{d_0} x_1^{d_1} ... x_n^{d_n}$$

where $d_0 := d - \sum d_i$.

Proposition 6 *Let $V_{d,n}$ = the vector space of all polynomials of degree $\leq d$ in n variables with coefficients in $\mathbb{R}$, $F_{d,n}$ = the vector space of forms of degree d in n variables with coefficients in $\mathbb{R}$. $f \mapsto \bar{f}$ defines a vector space isomorphism from $V_{d,n}$ onto $F_{d,n+1}$. If d is even, then $f \geq 0$ on $\mathbb{R}^n$ if and only if $\bar{f} \geq 0$ on $\mathbb{R}^{n+1}$, and f is a sum of squares of polynomials if and only if $\bar{f}$ is a sum of squares of forms of degree $\frac{d}{2}$ (if and only if $\bar{f}$ is a sum of squares of polynomials).*

Proof. One checks easily that the map $f \to \bar{f}$ is linear. Since it sends the basis $x_1^{d_1}...x_n^{d_n}$, $\sum d_i \leq d$ of $V_{d,n}$ to the basis $x_0^{d_0}x_1^{d_1}...x_n^{d_n}$, $\sum d_i = d$ of $F_{d,n+1}$, it is a vector space isomorphism. Suppose d is even, $deg(f) \leq d$. To prove $\bar{f} \geq 0$ on $\mathbb{R}^{n+1} \implies f \geq 0$ on $\mathbb{R}^n$, use $f(x_1, ..., x_n) = \bar{f}(1, x_1, ..., x_n)$. To prove $f \geq 0$ on $\mathbb{R}^n \implies \bar{f} \geq 0$ on $\mathbb{R}^{n+1}$, use $\bar{f}(x_0, ..., x_n) = x_0^d f(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})$, if $x_0 \neq 0$, and $\bar{f}(0, x_1, ..., x_n) = \lim_{\epsilon \to 0} \bar{f}(\epsilon, x_1, ..., x_n)$, if $x_0 = 0$. If $f = \sum_{i=1}^k f_i^2$, then $deg(f_i) \leq \frac{d}{2}$, and $\bar{f} = \sum_{i=1}^k [x_0^{\frac{d}{2}} f_i(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})]^2$, which is a sum of squares of forms of degree $\frac{d}{2}$. If $\bar{f} = \sum_{i=1}^k g_i^2$, then $f = \bar{f}(1, x_1, ..., x_n)$ $= \sum_{i=1}^k g_i(1, x_1, ..., x_n)^2$.

Remark. Counting the number of monomials $x_1^{d_1}...x_n^{d_n}$, $\sum d_i \leq d$, one sees that

$$\dim(V_{d,n}) = \dim(F_{d,n+1}) = \binom{d+n}{n} = \binom{d+n}{d}$$

We say $f \in \mathbb{R}[x_1, ..., x_n]$ is positive semidefinite (on $\mathbb{R}^n$) if $f \geq 0$ on $\mathbb{R}^n$. For $d, n \geq 1$, denote by $P_{d,n}$ the subset of the vector space $F_{d,n}$ consisting of forms of degree d in n variables which are positive semidefinite, and by $\sum_{d,n}$ the subset of $P_{d,n}$ consisting of sums of squares. The case where d is odd is not interesting.(Or we assume d is even, so that positive polynomials exist.) In his 1888 paper, Hilbert proved the following:

Theorem 1 *For d even, $P_{d,n} = \sum_{d,n}$ if and only if $n \leq 2$ or $d = 2$ or ($n = 3$ and $d = 4$).*

Proof. Applying proposition above, we see that the homogenized Motzkin polynomial

$$x^6 M(\frac{y}{x}, \frac{z}{x}) = x^6 + y^4z^2 + y^2z^4 - 3x^2y^2z^2$$

is in $P_{6,3} \setminus \sum_{6,3}$. Similarly, the homogenized Choi-Lam Polynomial

$$w^4 q(\frac{x}{w}, \frac{y}{w}, \frac{z}{w}) = w^4 + x^2y^2 + y^2z^2 + z^2x^2 - 4wxyz$$

is in $P_{4,4} \setminus \sum_{4,4}$. More generally, if $d \geq 6$ and $n \geq 3$, then $x_1^d M(\frac{x_2}{x_1}, \frac{x_3}{x_1})$ is in $P_{d,n} \setminus \sum_{d,n}$ and if $d \geq 4$ and $n \geq 4$, then $x_1^d q(\frac{x_2}{x_1}, \frac{x_3}{x_1}, \frac{x_4}{x_1})$ is in $P_{d,n} \setminus \sum_{d,n}$. $P_{d,1} = \sum_{d,1}$ is trivial. $P_{d,2} = \sum_{d,2}$ is immediate from proposition 4 (using proposition 6). $P_{2,n} = \sum_{2,n}$ follows from the fact that any quadratic form is expressible as

$$f(x_1, ..., x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j$$

where $A = (a_{ij})$ is a symmetric matrix.
If $f \geq 0$ on $\mathbb{R}^n$, then the matrix A is PSD, so A factors as $A = U^T U$ and

$$f(x_1, ..., x_n) = (x_1, ..., x_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = || \ U \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \ ||^2,$$

which is a sum of squares of linear forms. The case $P_{4,3} = \sum_{4,3}$ is highly non-trivial and first proved by Hilbert.

The sets $P_{d,n}$ and $\sum_{d,n}$are closed under addition and multiplication by positive reals, i.e., they are cones in the vector space $F_{d,n}$.(see [**28**].)
Hilbert then showed that every bivariate non-negative polynomial is a sum of squares of rational functions and Hilbert's 17th problem asked whether this is true in general. In **1900**, at the International Congress of Mathematicians in Paris, **Hilbert** gave a lecture in which he proposed **23 open problems**. Most of these have since been solved, and the solutions have led to fundamental discoveries in mathematics. As one of his famous set of problems, Hilbert posed the following as his 17th problem:
HILBERT'S 17th PROBLEM. For any $f \in \mathbb{R}[x]$, is it true that $f \geq 0$ on $\mathbb{R}^n$ $\Longrightarrow$ f is a sum of squares of rational functions?
- This is trivial when n = 1.
- Hilbert proved it, already in 1893, in the case n = 2 .
- Artin furnished an affirmative answer to Hilbert's 17th problem, joining the "honors class" of mathematicians who solved a Hilbert problem. He proved it in the general case (and with $\mathbb{R}$ replaced by an arbitrary real closed field) in 1927. Artin's work represented a major breakthough. His proof combined two new ingredients. The first ingredient - a description of elements of a field positive at every ordering - has since developed into the larger subject known as real algebra. The second ingredient - certain 'specialization lemmas' which exploit the theorem of Sturm for real closed fields - has evolved over time into what is referred to now as Tarski's Transfer Principle, which is an important result in the model theory of real closed fields.

The starting point of the history of the 17th problem of Hilbert was the oral defense of the doctoral dissertation of Hermann Minkowski at the University of Königsberg in 1885. The 21 year old Minkowski expressed his opinion that there exist real polynomials which are non-negative on the whole of $\mathbb{R}^n$ and cannot be written as a finite sum of squares of real polynomials. David Hilbert was an official opponent in this defense. Minkowski had convinced Hilbert about the truth of this statement. In 1888 Hilbert proved the existence of a real polynomial in two variables of degree six which is non-negative on $\mathbb{R}^2$ but not a sum of squares of real polynomials.(The proof of Hilbert used some basic results from the theory of algebraic curves.)

1.2 Ordered Fields, Real Closed Fields

Given any field the following are pertinent questions to ask:
- can the field be ordered, and if so, in how many ways?
- What sort of interplay is there between the notion of an ordering and other algebraic notions definable for fields?
- Can we regard the set of orderings of a field as some kind of space?
- What happens to orderings under field extensions, and how do the various orderings on a field reflect the properties of the field itself?
The study of these questions (and their applications) constitutes essentially the theory of ordered fields.

Definition 1 *An ordering on a field F is given by the assignment of a set $P \subseteq F$ which satisfies the following axioms:*

(1) $P + P \subseteq P$,
(2) $PP \subseteq P$,
(3) $P \cup (-P) = F$,
(4) $P \cap (-P) = \{0\}$.

The first three axioms above imply that all sums of squares in F belong to P. If P defines an ordering on F, we shall speak of the pair (F, P) as an ordered field.

As usual, we can define $x \leq_P y$ (resp., $x <_P y$) to mean that $y - x \in P$ (resp., $y - x \in P^* = P \setminus \{0\}$); this "inequality" relation results in a total ordering of the elements of F.
An ordered field (F, P) has necessarily characteristic equal to zero, hence we will always assume $F \supseteq \mathbb{Q}$ where $\mathbb{Q}$ denotes the field of rational numbers.

The following two ways of "operating" with orderings are useful. First, if F_0 is a subfield of a field F, then any ordering on F induces an ordering on F_0 (by (restriction) an ordering on F_0). Thus, one way of finding orderings on a field F_0 is to try to imbed F_0 into other ordered fields. Secondly, if (F, P) is an ordered field and σ is any automorphism of F, then F can also be ordered by σP. In this way, a given ordering can sometimes be used to generate many new orderings.
Remark: The notion of an ordered field can be alternatively defined as follows:
Given a relation $\leq$ on F, we say that the pair $(F, \leq)$ is an ordered field if
(i) $\leq$ is a total order.
(ii) $x \leq y$ implies $x + z \leq y + z$.
(iii) $x \leq y$ and $0 \leq z$ imply $xz \leq yz$.

Because of (ii) we have in an ordered field $x \leq y \Rightarrow y - x \geq 0$.
Thus the order $\leq$ of an ordered field F is entirely determined by the set

$$P = \{a \in F | a \geq 0\},$$

called the positive set (or set of positive elements) of $\leq$.
We have $P + P \subseteq P$ and $PP \subseteq P$; $P \cap -P = \{0\}; P \cup -P = F$.
Conversely, if P is a subset of a field F satisfying properties above, the relation $\leq$ defined by

$$x \leq y \Leftrightarrow y - x \in P$$

makes F in to an ordered field (with positive set P). For this reason we also call such a subset P of F an order of F. This allows us to switch freely from P to $\leq$ and to call a pair (F, P) or $(F, \leq)$ an ordered field.
Let F be an ordered field. Then $x^2 > 0$ for every $x \in F^*$. Thus all sums of squares of elements in F^* are also strictly positive : $x_1^2 + ... + x_n^2 > 0$ for every $x_1, ...x_n \in F^*$.

Definition 2 *The ordering $\leq$ on F is called Archimedean if for each $x \in F$ there is an $n \in \mathbb{N}$ such that $x \leq n$. If $\leq$ is Archimedean we call $(F, \leq)$ an Archimedean ordered field.*

Lemma 1 *If $(F, \leq)$ is Archimedean, then $\mathbb{Q}$ is (isomorphic to) a dense subfield of F.*

Proof. Suppose $\leq$ is Archimedean, $x, y \in F$ and $x < y$.
Choose $m \in \mathbb{N}$ such that $(y-x)^{-1} < m$. Multiplication by the positive element $y - x$ gives $1 < m(y-x)$, where $mx < my - 1$.
Choose $n \in \mathbb{Z}$ minimal such that $my \leq n + 1$.

Then $mx < my - 1 \leq n < my$ implies $x < \dfrac{n}{m} < y$.
Examples:
(1) The fields $\mathbb{Q}$ and $\mathbb{R}$ are the simplest examples of ordered fields and both are Archimedean with respect to their "usual" orderings. For either of these fields, the usual ordering is the only ordering possible.
(2) As another example, consider the field $F = \mathbb{Q}(\theta)$ where $\theta^2 = 2$. There are two orderings on F, constructed from the two imbeddings of F into $\mathbb{R}$, one sending θ to $\sqrt{2}$, the other sending θ to $-\sqrt{2}$. These orderings are "conjugate" under the action of $\sigma \in Aut(F)$ which sends θ to $-\theta$. In a similar fashion, we can construct four different orderings on $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, eight orderings on $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, ... and uncountably many orderings on $\mathbb{Q}(\sqrt{p} : p$ prime). (see **Corollary 3**)
(3) $\mathbb{R}(x)(x$ a single indeterminate)
First, for $a_i \in \mathbb{R}$ and $a_k \neq 0$ we define

$$0 < a_k x^k + a_{k+1} x^{k+1} + ... + a_n x^n :\Leftrightarrow 0 < a_k$$

Second, for $p, q \in \mathbb{R}[x] \setminus \{0\}, 0 < \dfrac{p}{q} :\Leftrightarrow 0 < pq$.
Finally, for $r, s \in \mathbb{R}(x), r < s :\Leftrightarrow 0 < s - r$.

We define $\frac{f(x)}{g(x)} \geq 0 \Leftrightarrow f(x)g(x) \geq 0$

This is a total order on $\mathbb{R}(x) = \{\dfrac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x], g(x) \neq 0\}$ which makes $(\mathbb{R}(x), \leq)$ an ordered field.

With this ordering the field $\mathbb{R}(x)$ is not Archimedean. It contains infinitely small elements (i.e. positive and smaller than $\frac{1}{n}$ for every $n \in \mathbb{N}$, such as x, or $f(x) = x - r < 0, \forall r \in \mathbb{R}, r > 0$) and also infinitely large elements (i.e. bigger than n, for any $n \in \mathbb{N}$ such as $\dfrac{1}{x}$) i.e $\frac{1}{x} > n$ for all $n \in \mathbb{N}$.
To get an algebraic criterion for fields which admit some ordering, we generalize the notion of positive cones or orderings to pre-positive cones or pre-orderings of fields.

Definition 3 *Suppose T is any subset of F. We call T a pre-positive cone of F or pre-ordering of F if $T + T \subseteq T, TT \subseteq T, F^2 \subseteq T$, and $-1 \notin T$.*

If in addition, $T \cup -T = F$ then T is an ordering of F. Any ordering of F is also a pre-ordering, since for any $x \in F$ we have $x \in P$ and hence $x^2 \in P$ or $-x \in P$ and hence $x^2 = (-x)(-x) \in P$. In particular we have $1^2 = 1 \in P$, which implies $-1 \notin P$.

Lemma 2 *Let T be a pre-ordering of F and let $x \in F \setminus T$. Then $T - xT =: T'$ is a pre-ordering of F with $T \cup \{-x\} \subseteq T'$.*

Proof. $(T - xT)(T - xT) \subseteq T - xT + x^2T \subseteq T - xT$. If -1 were equal to $t_1 - xt_2$ for some $t_1, t_2 \in T$, then $x = (1 + t_1)(\frac{t_2}{t_2^2}) \in T$ contradiction. ($t_2 \neq 0$ otherwise $t_1 = -1 \in T$ contradiction.)

Theorem 2 *Every pre-ordering T of F is contained in an ordering P. Furthermore,*

$$T = \bigcap_{T \subseteq P} P$$

Proof. Let P be a maximal pre-ordering of F containing T (such P exists by Zorn's lemma). To show that P is an ordering, suppose $x \in F \setminus P$; then $P - xP$ is a pre-ordering.
$-x \in P - xP$ and $P \subseteq P - xP$, then $P = P - xP$, since P is maximal; thus $-x \in P$ as required.

The inclusion $T \subseteq \bigcap_{T \subseteq P} P$ is trivial. For the reverse, suppose $x \in F \setminus T$. Then $T - xT$ is a pre-ordering. By the first half of this theorem, $T - xT$ is contained in an ordering P which, of course, cannot contain x.

For a field F let $\sum F^2$ denotes the set of finite sums of squares of elements of F. That is $\sum F^2 = \{x_1^2 + ... + x_r^2 | r \in \mathbb{N}, x_i \in F\}$

If F has characteristic 2, then $\sum F^2 = F^2$ (as $x_1^2 + x_2^2 = (x_1 + x_2)^2$) and if $charF \neq 2$ and $-1 \in \sum F^2$, it follows from the formula $x = (\frac{x+1}{2})^2 - (\frac{x-1}{2})^2$ that $\sum F^2 = F$ or if $-1 = \sum a_i^2$, then $x = (\frac{1+x}{2})^2 + \sum (a_i(\frac{1-x}{2}))^2$.

F is called **formally real** if $-1 \notin \sum F^2$. This condition is equivalent to whenever $x_1^2 + x_2^2 + ... + x_r^2 = 0$ in F, all x_i must be zero.

$\sum F^2$ is pre-ordering $\Leftrightarrow -1 \notin \sum F^2 \Leftrightarrow F$ has an ordering; note that if $-1 \notin \sum F^2$, then F has an ordering containing $\sum F^2$. Hence, we can quote Artin's basic discovery (see [**2**]) that a field

F is formally real if and only if it admits an ordering.

Remark. If P is an ordering of F, the elements $P^* = P \setminus \{0\}$ are called positive, the elements of $-P^*$ are called negative (with respect to P). The elements of $\bigcap P^*$ are totally positive, since they are positive for every ordering. Thus the totally positive elements are exactly the non-zero sums of squares.

Let K/F be a field extension. Any ordering $\leq$ on K induces (by restriction) an ordering on F. If $\leq$ is an ordering on F , we seek an extension of $\leq$ to K. Equivalently, given an ordering $P \subseteq F$, we seek an ordering $P' \subseteq K$ such that $P' \cap F = P$. In that case we shall call (K, P') or $(K, \leq)$ an order - extension of (F, P) or $(F, \leq)$; and we shall call (F, P) or $(F, \leq)$ an ordered subfield of (K, P') or $(K, \leq)$.

Lemma 3 *An ordering P of F can be extended to K if and only if*

$$T_K(P) := \{\sum_{i=1}^{n} p_i \beta_i^2 : n \in \mathbb{N}, p_i \in P, \beta_i \in K\}$$

is a pre-ordering of K.

Proof. ($\Rightarrow$) Let $P^{'}$ be an ordering of K with $P^{'} \cap F = P$. Then $T_K(P) \subseteq P^{'}$, whence $-1 \notin T_K(P)$.
($\Leftarrow$) Suppose $T_K(P)$ is a pre-ordering of K. Let $P^{'} \supseteq T_K(P)$ be an order of K (as every pre-order is contained in an ordering). Then $P^{'} \cap F := P_1$ is an order of F with $P \subseteq P_1$; then $P = P_1$.
Remark: If $P \subseteq P_1$ are orderings of F, then $P = P_1$.
(For $0 \neq x \in P_1 \Rightarrow -x \notin P_1 \Rightarrow -x \notin P \Rightarrow x \in P$.)

Theorem 3 *Suppose $K = F(\sqrt{a}), a \in F \setminus F^2$. Let P be an ordering of F. Then P extends to an ordering $P^{'}$ of K if and only if $a \in P$.*

Proof. ($\Rightarrow$)$P^{'} \cap F = P$ implies $a = (\sqrt{a})^2 \in P^{'} \cap F = P$.
($\Leftarrow$) Let $a \in P$. If -1 were of the form $\sum a_i(x_i + y_i\sqrt{a})^2$ with $a_i \in P$ and $x_i, y_i \in F$, then we would have $-1 = \sum a_i x_i^2 + a_i a y_i^2 \in P$, a contradiction. Now we apply lemma above.

Theorem 4 *Suppose $[K : F]$ is finite and odd. Then every ordering P of F extends to K.*

Proof : Suppose that $[K : F]$ is finite, > 1, odd, and minimal with respect to the property that P does not extend to K. We write $K = F(\alpha) = F[X]/(f), f = Irr(\alpha, F)$(the monic irreducible polynomial of α over F), and $degf = 2n + 1(n \geq 1)$, using the primitive element theorem. Since P does not extend to K, $-1 = \sum_{i=1}^{m} a_i\gamma_i^2$, with $a_i \in P, \gamma_i \in K$ (Lemma above). Then there exist $f_1, ..., f_m \in F[X]$ such that

$$0 = 1 + \sum_{i=1}^{m} a_i f_i(X)^2 (\mathrm{mod}\, f(X)).$$

Therefore we get $1 + \sum_{i=1}^{m} a_i f_i(X)^2 = f(X)h(X)$, for some $h \in F[X]$. We (may) choose these f_i to have degrees $\leq 2n$; then

$$deg(1 + \sum_{i=1}^{m} a_i f_i(X)^2) \leq 4n.$$

Moreover, this degree is even, since all $a_i \in P$. Therefore $degh$ is odd and $\leq 2n - 1$. Let h_1 be an odd-degree irreducible factor of h in $F[X]$. Let β be a zero of h_1, and let $K^{'} = F(\beta)$. Then
(i) $[K^{'} : F]$ is odd and $\leq 2n - 1$, and
(ii) $1 + \sum_{i=1}^{m} a_i f_i(\beta)^2 = 0$, i.e., $-1 = \sum_{i=1}^{m} a_i \delta_i^2$ with $\delta_i \in K^{'}$.
Thus P does not extend to $K^{'}$ and $[K^{'} : F] < [K : F]$, a contradiction.

Theorem 5 *Every ordering P of F extends to $F(x)$ (where x is a single indeterminate).*

Proof. Otherwise, $-1 = \sum_{i=1}^{m} a_i f_i(X)^2$ for some $a_i \in P \setminus \{0\}$ and $f_i \in F(X)-$say, $f_i = g_i/h$ with $g_i, h \in F[X]$ and no factor of h divides all g_i in $F[X]$. Then $-h(0)^2 = \sum_{i=1}^{m} a_i g_i(0)^2$. If $h(0) \neq 0$, then $-1 \in P$, contradiction. And if $h(0) = 0$, then $0 = \sum a_i g_i(0)^2, X|h$, what implies that all $g_i(0) = 0$, hence $X|g_i$ for all i, another contradiction.

Definition 4 *An ordered field $(F, \leq)$ is called maximal ordered if $\leq$ does not extend to any proper algebraic field extension K of F.*

Lemma 4 *Suppose $(F, \leq)$ is maximal ordered. Then every non-negative element of F is a square; thus $\leq$ is the only ordering on K.*

Proof. First, to prove $P_{\leq} \subseteq F^2$, suppose, on the contrary, that $0 \leq a \in F \setminus F^2$. Then $\leq$ would extend to $K := F(\sqrt{a}) \neq F$, contradicting the maximality of $(F, \leq)$.

Second, let P be any ordering of F. Then $P_{\leq} \subseteq F^2 \subseteq P$ implies $P_{\leq} = P$.

Definition 5 *An ordered field is called real closed if it has no proper, real, algebraic extension.*

Lemma 5 *A field F is real closed if and only if F has a unique ordering $\leq$, and $(F, \leq)$ is maximal ordered.*

Proof. ($\Rightarrow$) Suppose P is an ordering of F, and $a \in P$. Then $a \in F^2$ (Lemma above). Thus $P = F^2$, and (F, F^2) is maximal ordered, (using that F has unique ordering if F^2 is an order and the fact that F is real closed.)
($\Leftarrow$) If F had a formally real, proper, algebraic extension K, then K would have an ordering, which would restrict to the unique ordering $\leq$ of F, contradicting the maximality of $(F, \leq)$.

The facts above finally lead to following fundamental characterization of real closed fields.

Theorem 6 *The following are equivalent:*
(a) F is real closed;
(b) F^2 is an ordering of F, and every odd-degree $f \in F[x]$ has a root in F; and
(c) $F \neq F(\sqrt{-1})$, and $F(\sqrt{-1})$ is algebraically closed.

Examples.
(1) The field $\mathbb{R}$ is real closed.
(2) The real algebraic numbers (the numbers algebraic over $\mathbb{Q}$) form a real closed field denoted by $\mathbb{R}_{alg}$.
(3) Let $\mathbb{R}(x)^{\wedge}$ (resp. $\mathbb{C}(x)^{\wedge}$) be the field of puiseux series with real (resp. complex) coefficients, i.e., the set of expressions $\sum_{i=k}^{+\infty} a_i x^{i/q}$ with $k \in \mathbb{Z}, q \in \mathbb{N}, a_i \in \mathbb{R}$ (resp. $\mathbb{C}$). Then $\mathbb{C}(x)^{\wedge}$ is algebraically closed. Since $\mathbb{C}(x)^{\wedge} = \mathbb{R}(x)^{\wedge}[i], \mathbb{R}(x)^{\wedge}$ is real closed. A positive element of $\mathbb{R}(x)^{\wedge}$ is a puiseux series of the form $\sum_{i=k}^{+\infty} a_i x^{i/q}$ with $a_k > 0$.

Theorem 7 *Suppose F is real closed; let $\leq$ be the unique ordering on F. Then for any $f \in F[x]$,*
(a) f factors into F-irreducible polynomials of the form $x - a, (a \in F)$ and $(x - a)^2 + b^2, (a, b \in F, b \neq 0)$;
(b) if $a < b \in F$ and $f(a) < 0 < f(b)$, then there is some $c \in F$ with $a < c < b$ such that $f(c) = 0$.

Proof.(a) $F(\sqrt{-1})$ is algebraically closed. So any irreducible polynomial in $F[X]$ must have degree ≤ 2; so if it is monic, it must be of the form $X - a$ or $X^2 - 2aX + c$, for some $a, c \in F$. The latter equals $(X-a)^2 + (c-a^2)$; in order for it to be irreducible, we must have $c - a^2 \notin -F^2$, whence $c - a^2 = b^2$, for some $b \in F \setminus \{0\}$.
(b) Factor f as in (a), and note that a sign-change of $f(x)$ for x between a and b can come only from a linear factor.

Definition 6 *Let $(F, \leq)$ be an ordered field, and $(K, \leq)$ an order extension of $(F, \leq)$.*
$(K, \leq)$ (or simply K) is called a real closure of $(F, \leq)$ if K is real closed and K/F is algebraic.

Theorem 8 *Every ordered field has a real closure.*

Theorem 9 *Every two real closures of an ordered field $(F, \leq)$ are $F-$isomorphic.*

Corollary 2 *Let (R, R^2) be a real closure of (F, P). Let F_1, F_2 be intermediate fields of R/F, and let $\sigma : F_1 \to F_2$ be an isomorphism that fixes F and respects the orderings induced by R^2. Then $F_1 = F_2$ and $\sigma = id$. In particular, $Aut(R/F) = \{id\}$.*

Consequently, the $F-$isomorphism between two real closures R_1 and R_2 of (F, P) given by theorem above is unique. On the other hand, there can be other isomorphisms between R_1 and R_2 that do not fix F.
Remark. The hypothesis in (Corollary above) that σ fixes F can not be dropped. For example, let $F = F_1 = F_2 = \mathbb{R}(\{X_r | r \in \mathbb{Q} \text{ and } r > 0\})$, where the X_r are indeterminates. We define a lexicographic ordering $<$ on F by declaring that for each $r \in \mathbb{Q}$ with $r > 0$, $\mathbb{R}(\{X_s | s \in \mathbb{Q} \text{ and } 0 < s < r\}) < X_r$. Let R be the real closure of $(F, <)$. Then the order preserving permutation $X_r \mapsto X_{2r}$ induces an order-preserving $\mathbb{R}-$automorphism $\sigma : F_1 \to F_2$, but $\sigma \neq id$. Moreover, one can show that σ extends to a non-trivial automorphism of R.

Corollary 3 *Let (R, R^2) be a real closure of (F, P). Suppose $\alpha \in \mathbb{R}$. Then the number of extensions of P to an ordering of $F(\alpha)$ is equal to the number of F-embedding of $F(\alpha)$ in R, i.e., the number of zeros of $Irr(\alpha, F)$ in R.*

The following result is the key to Artin's solution of Hilbert's 17th problem.

Theorem 10 *(Artin-Lang Homomorphism Theorem). Let R be a real-closed field and A an R-algebra of finite type. If there exists an R-algebra homomorphism $\varphi : A \to R_1$ into a real closed extension R_1 of R, then there exists an R-algebra homomorphism $\psi : A \to R$.*

Theorem 11 *Let R be real closed field and $f \in R[x_1, ..., x_n]$. If f is non-negative on R^n, then f is a sum of squares in the field of rational functions $R(x_1, ..., x_n)$.*

Proof. If f is not a sum of squares in $R(x_1, ..., x_n)$, then, by corollary 1, there exists an ordering on $R(x_1, ..., x_n)$ for which f is negative. Let K be a real closure of $R(x_1, ..., x_n)$ equipped with this ordering. Then $-f$ has a non-zero square root in K, and hence there is an R-algebra homomorphism $R[x_1, ..., x_n][T]/(fT^2+1) \to K$. By the Artin-Lang homomorphism theorem, there is an R-algebra homomorphism $R[x_1, ..., x_n][T]/(fT^2+1) \to R$. This implies the existence of a point x in R^n such that $f(x) < 0$.

1.3 The Space of Orderings of a Field

(This section is from **[31]**). We saw that for the characterization of sums of squares we considered all orderings of a field. So it is important to investigate the set of all orderings of a field F:

$$X(F) := \{P : P \text{ ordering of F}\}.$$

Our aim is to define a canonical topology on $X(F)$. Every ordering P defines the sign-function

$$s_P : F^* \to \{\pm 1\}, s_P(x) = 1 \Leftrightarrow x \in P^*.$$

The set of all mappings $F^* \to \{\pm 1\}$ denoted by $\{\pm 1\}^{F^*}$ or $\Pi_{F^*}\{\pm 1\}$. Since P is completely determined by s_P we get an injection

$$X(F) \to \Pi_{F^*}\{\pm 1\}.$$

We give $\{\pm 1\}$ the discrete topology and $\Pi\{\pm 1\}$ the product topology. By the Tychnoff theorem $\Pi\{\pm 1\}$ is *quasi-compact*. We consider $X(F)$ as a subset of $\Pi\{\pm 1\}$ and endow it with the relative topology. $X(F)$ is called the space of ordering of F.

The topology in $\Pi\{\pm 1\}$ is defined by taking the following sets as a sub-basis

$$\pi_a^{-1}(\varepsilon) = H(a, \varepsilon) = \{f : F^* \to \{\pm 1\} | f(a) = \varepsilon\}$$

where $a \in F^*, \varepsilon = \pm 1$, and $\pi_a : \Pi\{\pm 1\} \to \{\pm 1\}$ is the projection on the $a - th$ factor. Since the following union is *disjoint*

$$\Pi\{\pm 1\} = H(a, \varepsilon) \cup H(a, -\varepsilon)$$

the sets $H(a, \varepsilon)$ are open and closed. Such subsets of a topological space are called *clopen*. A topological space is called *totally disconnected* if any two points can be separated by clopen sets. In our case this is possible: For, if $f, g \in \Pi\{\pm 1\}$ and $f(a) \neq g(a)$, then f and g are separated by $H(a, \varepsilon)$ and $H(a, -\varepsilon)$. Thus $\Pi\{\pm 1\}$ is a *boolean space*, that is , it is hausdorff, quasi-compact, and totally disconnected.

Theorem 12 *$X(F)$ is a closed subset of $\Pi\{\pm 1\}$. Thus $X(F)$ is a boolean space with respect to the induced topology.*

Proof. We show that the complement of $X(F)$ is open. Let $s : F^* \to \{\pm 1\}$ be a function which is not defined by an ordering. One of the three defining conditions of an ordering must be violated. Therefore

$$s(a) = s(b) = 1 \quad but \quad s(a+b) = -1$$

or

$$s(a) = s(b) = 1 \quad but \quad s(ab) = -1$$

or

$$s(a) = s(-a)(= \varepsilon)$$

for suitable $a, b \in F^*$. In each of the three cases we can find an open neighborhood of s in the complement of $X(F)$, namely

$$H(a,1) \cap H(b,1) \cap H(a+b,-1)$$

or

$$H(a,1) \cap H(b,1) \cap H(ab,-1)$$

or

$$H(a,\varepsilon) \cap H(-a,\varepsilon)$$

respectively.
A subbasis for the topology of $X(F)$ is given by the following sets

$$H_F(a) = H(a) = H(a,1) \cap X(F) = \{P \in X(F) | a \in P\}.$$

(This follows from $H(a,-1) \cap X(F) = H(-a)$.) This is the so called *Harrison subbasis.*

1.4 Valuations

Definition 7 *Let F be a field.*
A surjective mapping $\upsilon : F \to \Gamma \cup \infty$ where Γ is an ordered abelian group, amended by an element ∞, being considered larger than every element in Γ, is called a valuation if it satisfies the following axioms:
(i) $\upsilon(x) = \infty \Leftrightarrow x = 0$
(ii) $\upsilon(xy) = \upsilon(x) + \upsilon(y)$
(iii) $\upsilon(x+y) \geq min\{\upsilon(x), \upsilon(y)\}$

Proposition 7 *Let F be a field and let υ be a valuation over F. Then*
(i) $\upsilon(1) = 0$,
(ii) $\upsilon(a^{-1}) = -\upsilon(a)$ *for all* $a \neq 0$,
(iii) $\upsilon(a) = \upsilon(-a)$,
(iv) if $\upsilon(a) \neq \upsilon(b)$, *then* $\upsilon(a+b) = min\{\upsilon(a), \upsilon(b)\}$,
(v) $\upsilon(\sum_{i=1}^n a_i) \geq min_{1 \leq i \leq n}\{\upsilon(a_i)\}$ *and equality holds if* $\upsilon(a_i) \neq \upsilon(a_j)$ *for all* $i \neq j$,
(vi) if $\sum_{i=1}^n a_i = 0, n \geq 2$, *then there exist* $i \neq j$ *such that* $\upsilon(a_i) = \upsilon(a_j)$.

Consider an arbitrary field F and a valuation of F with values in an ordered group Γ.

Let $\mathcal{O}_\upsilon = \{x \in F : \upsilon(x) \geq 0\}$.
Then since $\upsilon(x) = \upsilon(-x), \upsilon(xy) = \upsilon(x) + \upsilon(y)$ and since Γ is an ordered group it follows that $\mathcal{O}_\upsilon$ is a ring.
Furthermore, for $x \in F$, if $x \notin \mathcal{O}_\upsilon$, we have $\upsilon(x) < 0$.
Thus $\upsilon(x^{-1}) = -\upsilon(x) > 0$, that is $x^{-1} \in \mathcal{O}_\upsilon$.

Hence given $x \in F$, we have $x \in \mathcal{O}_\upsilon$ or $x^{-1} \in \mathcal{O}_\upsilon$.
Furthermore, for $x \in F$, if $x \in \mathcal{O}_\upsilon$, then $x = \dfrac{x}{1} \in \mathcal{O}_\upsilon$ and if $x \notin \mathcal{O}_\upsilon$, then $x^{-1} \in \mathcal{O}_\upsilon$ and therefore $x = \dfrac{1}{x^{-1}} \in quot\mathcal{O}_\upsilon$ where $quot\mathcal{O}_\upsilon$ denotes the field of quotients of $\mathcal{O}_\upsilon$, which proves that $F = quot\mathcal{O}_\upsilon$.

Now, $x \in \mathcal{O}_\upsilon$ is a unit if and only if $x^{-1} \in \mathcal{O}_\upsilon$, that is, $\upsilon(x) \geq 0$ and $\upsilon(x^{-1}) = -\upsilon(x) \geq 0$.
Therefore, $\mathcal{O}_\upsilon^* = \{x \in F : \upsilon(x) = 0\}$.

Let $\mathfrak{m}_\upsilon = \{x \in F : \upsilon(x) > 0\}$ consists of the non-units of $\mathcal{O}_\upsilon$. In fact $\mathfrak{m}_\upsilon$ is an ideal.

Therefore, $\mathcal{O}_\upsilon$ is a local ring with maximal ideal $\mathfrak{m}_\upsilon$.

Finally, $\upsilon : (F^*, \cdot) \to (\Gamma, +)$ is a group epimorphism with $ker\upsilon = \mathcal{O}_\upsilon^*$. Thus $(\Gamma, +) \cong (F^*/\mathcal{O}_\upsilon^*, \cdot)$.
The above discussion can be summed up as follows

Proposition 8 *If F is a field and υ a valuation over F, then $\mathcal{O}_\upsilon = \{x \in F : \upsilon(x) \geq 0\}$ is a subring of F such that for all $x \in F$, $x \in \mathcal{O}_\upsilon$ or $x^{-1} \in \mathcal{O}_\upsilon$. In particular, $\mathcal{O}_\upsilon$ is a local ring with maximal ideal $\mathfrak{m}_\upsilon = \{x \in F : \upsilon(x) > 0\} = \mathcal{O}_\upsilon \setminus \mathcal{O}_\upsilon^*$ and $\mathcal{O}_\upsilon^* = \{x \in F : \upsilon(x) = 0\}$.*
Furthermore, we have quot $\mathcal{O}_\upsilon = F$ and the value group of υ is isomorphic to $F^*/\mathcal{O}_\upsilon^*$.

In our study of rational and elliptic function fields we will be dealing with the nice class of **discrete valuations** defined as valuations the value group of which are (isomorphic to) the additive group $\mathbb{Z} = (\mathbb{Z}, +)$ of the integers.

Examples.
(1) **The discrete p-adic valuations**
(a) Let $F = \mathbb{Q}, \Gamma = \mathbb{Z}$ and $\upsilon = \upsilon_p$ the $p-$adic valuation, for $p \in \mathbb{Z}$ a rational prime. That is , for $x \in \mathbb{Q}^*$, we write $x = p^n \frac{a}{b}, n \in \mathbb{Z}, p \nmid ab$ and $\upsilon_p(x) = n$.
Similarly, we define the $p-$adic valuation for every irreducible polynomial $p \in K[x], K$ a field. For $h \in K(x) \setminus \{0\}$ there are $f, g \in K[x] \setminus \{0\}$ such that $h = p^r \frac{f}{g}, r \in \mathbb{Z}$ where f, g are not divisible by p and we define $\upsilon_p(p^r \frac{f}{g}) = r$.
We note that in the second case, υ_p restricted to K is trivial.

(2)There is one more interesting discrete valuation on $K(x)$ trivial on K. This is the socalled **degree valuation or infinite valuation** υ_∞ defined by
$\upsilon_\infty(0) = \infty$ and , for non-zero polynomials $f, g \in K[x]$, by
$\upsilon_\infty(f/g) = \deg g - \deg f$. We observe that f/g is a unit in the valuation ring V_∞ if and only if $\deg g = \deg f$.

(3) Let F be a field, and let $K = \{\sum_{n \in \mathbb{Z}} a_n x^n : a_n \in F$ for all n, the set $\{n \in \mathbb{Z} : a_n \neq 0\}$ is bounded below $\}$ be the set of all formal Laurent series

over F in one variable x. For a non-zero element $f \in K$ there is a minimum exponent of x occurring in f, which implies that we can write f uniquely as $f = x^n g$ for some $n \in \mathbb{Z}$ and $g \in F[[x]]$ with non-zero constant coefficient. Now,

$$v : K^* \to \mathbb{Z}, \quad \sum_{n \in \mathbb{Z}} a_n x^n \mapsto \min\{n \in \mathbb{Z} : a_n \neq 0\}$$

is a valuation on K.

(4) The idea of (3) can be generalized to construct a valuation with value group $\mathbb{Q}$: for a field F we now consider the set $K = \{\sum_{q \in \mathbb{Q}} a_q x^q : a_q \in F$ for all q, the set $\{q \in \mathbb{Q} : a_q \neq 0\}$ is bounded below and has bounded denominators $\}$ of all formal power series with rational exponents, and the same map

$$v : K^* \to \mathbb{Q}, \quad \sum_{q \in \mathbb{Q}} a_q x^q \mapsto \min\{q \in \mathbb{Q} : a_q \neq 0\}$$

as above. v is a valuation with value group $\mathbb{Q}$. The field K is called the field of (formal) puiseux series over F.

Chapter 2

Real Holomorphy Rings of Rational Function Fields

2.1 Algebraic Function Fields of One Variable

Definition 8 *An algebraic function field F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.*

In other words, there exists $x \in F$, transcendental over K, and there exist $y_1, ..., y_n \in F$, all algebraic over $K(x)$, such that $F = K(x, y_1, ..., y_n)$.
Examples.

1. Rational Function Fields

The simplest example of an algebraic function field is the rational function field; F/K is called rational if $F = K(x)$ for some $x \in F$ which is transcendental over K.
We have a similar definition in any number of variables: a finitely generated extension F/K is called rational if there exist $x_1, ..., x_r \in F$ algebraically independent over K such that $F = K(x_1, ..., x_r)$.

In several ways, the rational function fields in one variable are analogous to $\mathbb{Q}$ (and in the same way the function fields are analogous to number fields, i.e. finite extensions of $\mathbb{Q}$). For instance, once a generator x of F/K is given, we can see F as field of quotients of the ring $K[x]$ which is an euclidean ring, analogous to $\mathbb{Z}$.

2. Elliptic Function Fields over $\mathbb{R}$

Definition 9 *Let $f(x) \in \mathbb{R}[x]$, $degf = 3$, $f(x) \notin \mathbb{R}(x)^2$ and f without multiple roots in $\mathbb{C}$. Then $\mathbb{R}(x)(\sqrt{f})$ is called an elliptic function field over $\mathbb{R}$.*

2.2 Real Valuation Rings and Description of The Real Holomorphy Ring

In this section we want to write down the full list of real valuation rings and to give the description of real holomorphy ring , as well as of its group of

units and its group of totally positive units.

2.2.1 Real Valuation Rings of $\mathbb{R}(x)$

We start with the general definitions.

Definition 10 *Let V be a subring of a field K. We say that V is a valuation ring of K if $x \in V$ or $x^{-1} \in V$ for any $x \in K$.*

Examples of Valuation rings
(The field K is trivial valuation ring.)
1. Let $K = \mathbb{Q}$, with a fixed prime p.
Let V_p contain 0 and all rationals of the form $p^r \frac{m}{n}$, where $r \geq 0$ and p divides neither m nor n.
It follows from the definition that V_p is a valuation ring referred to as the **p-adic valuation ring** of $\mathbb{Q}$.
2. Let $K = F(x)$, where F is a field.
Let V_p contain 0 and all rational functions $p^r \frac{f}{g}$, where $r \geq 0$, p irreducible over $F[x]$ and f, g are arbitrary polynomials in $F[x]$ not divisible by p. V_p is called the **p-adic valuation ring** of K.
3. Let $K = F(x)$, and let V_∞ contain 0 and all rational function $\frac{f}{g} \in F(x)$ such that $\deg f \leq \deg g$. V_∞ is called the **degree valuation ring** or the **valuation ring at infinity** of K.
4. Let K be the field of formal Laurent series over F.
Thus a non-zero element of K looks like $f = \sum_{i=r}^{\infty} a_i x^i$ with $a_i \in F, r \in \mathbb{Z}$ and $a_r \neq 0$. We may write $f = a_r x^r g$ where g belongs to the ring $V = F[[x]]$ of formal power series over F.
Moreover, the constant term of g is 1, and therefore g, hence can be inverted in V (by long division).
The ring $\mathcal{O}v$ in proposition 8 (chap.1) is a valuation ring. We saw there that every valuation v on a field K determines a valuation ring V in K. ($V = \mathcal{O}_v = \{x \in K : v(x) \geq 0\}$.)
Now we show that conversely, every valuation ring V in K determines a valuation v on K. The basic sample for this relationship is provided by the p-adic valuations and the p-adic valuation rings.

Proposition 9 *If V is a valuation ring and K = quot V, then K^*/V^* is an ordered group and the natural projection is a valuation with valuation ring V and the value group K^*/V^*.*

Proof. The multiplicative quotient group K^*/V^* is an abelian group. We rewrite it additively by setting for the cosets xV^* and yV^*:

$$xV^* + yV^* := xyV^*.$$

Furthermore we define a binary relation $\leq$ on K^*/V^* by

$$xV^* \leq yV^* \Leftrightarrow \frac{y}{x} \in V$$

It is easily checked that this turns $K^*/V^* = \Gamma$ in to an ordered abelian group. The desired valuation is now defined by

$\upsilon(x) = xV^* \in \Gamma$ for $x \in K^*$, and $\upsilon(0) = \infty$.

Properties of Valuation Rings

Let V be a valuation ring of the field K.

1. The field of quotients of V is K.
2. The ideals of a valuation ring V are ordered by inclusion.
3. Every overring of a valuation ring is a valuation ring; if $\{P_\lambda\}$ is the set of proper prime ideals of V, then $\{V_{P_\lambda}\}$ is the set of overrings of V.
4. Every valuation ring is a local ring, i.e., a ring with a unique maximal ideal.
5. Every valuation ring is integrally closed.
6. The valuation rings between V and K form a chain.
7. If P is a prime ideal of a valuation ring V, then V_P and V/P are also a valuation ring.
8. If V is a Noetherian valuation ring, then V is a PID. Moreover, for some prime $p \in V$ every ideal is of the form $(p^m), m \geqslant 0$. For any such p, $\cap_{m=1}^{\infty}(p^m) = 0$.
9. Let R be a subring of the field K. The integral closure $\tilde{R}$ of R in K is the intersection of all valuation rings V of K such that $V \supseteq R$.
10. Let V be a valuation ring and let $\mathfrak{a}$ be an ideal of V.

(1) $rad(\mathfrak{a})$ is prime ideal of V.

(2) If $\mathfrak{b} = \cap_{n=1}^{\infty}\mathfrak{a}^n$, then $\mathfrak{b}$ is a prime ideal of V which contains every prime ideal of V which is properly contained in $\mathfrak{a}$.

Let $\mathfrak{m}_V$ be the maximal ideal of a local ring V. Since the ring is local, we conclude that $V - \mathfrak{m}_V$ is the multiplicative group of invertible elements(units) of the ring V.The quotient field $V/\mathfrak{m}_V$ is called the **residue field** of V.

Let $\mathfrak{m}_V$ be the maximal ideal of a valuation ring V of a field K. Then for any $a \in K - \{0\}$ we have $a \notin V \iff a^{-1} \in \mathfrak{m}_V$.

A valuation or a valuation ring is called **real** if its residue field is formally real, the valuation rings attached to discrete valuations are called **discrete valuations rings**.

Let K be a field and $\upsilon : K^* \to \mathbb{Z}$ a discrete valuation with valuation ring V and maximal ideal $\mathfrak{p}$. Let $\pi \in \mathfrak{p}$ such that $\upsilon(\pi) = 1$ (π is called a **prime element** or **uniformizing element** of the valuation.) Then given $x \in K^*$ such that $\upsilon(x) = n$, we have $\upsilon(\pi^{-n}x) = 0$, that is, $\pi^{-n}x \in V^*$, so that x can be written as $x = a\pi^n$ with $a \in V^*$ and $n \in \mathbb{Z}$. This representation is unique since if $x = b\pi^m$ with $b \in V^*$ and $m \in \mathbb{Z}$, we have $\upsilon(x) = \upsilon(b\pi^m) = m = n$. Thus $a = b$. In particular, if $x \in \mathfrak{p}$ then $x = a\pi^n$ with $n \geq 1$, and $a \in V^*$ so $\mathfrak{p} = (\pi)$. Therefore $\mathfrak{p}$ is principal.

Let $\mathfrak{b}$ be any ideal of V such that $\mathfrak{b} \neq 0$ and $\mathfrak{b} \subseteq \mathfrak{p}$. Let $n = min\{\upsilon(x) : x \in \mathfrak{b}\}$. Then $n \geq 1$. Then there exists $x \in \mathfrak{b}$ such that $\upsilon(x) = n$, that is, $x = a\pi^n \in \mathfrak{b}$ with $a \in V^*$. This implies that $\pi^n \in \mathfrak{b}$ and $(\pi^n) \subseteq \mathfrak{b}$. If y is an arbitrary non-zero element of $\mathfrak{b}$, we have $\upsilon(y) \geq n$. Therefore $y \in (\pi^n)$, that is, $\mathfrak{b} = (\pi^n) = \mathfrak{p}^n$.

Hence, every non-zero ideal of V is a power of $\mathfrak{p}$. We have the following theorem:

Theorem 13 *If υ is a discrete valuation over a field K with valuation ring V then the maximal ideal $\mathfrak{p}$ of V is principal and is generated by any prime element. Every non-zero ideal of V is a power of $\mathfrak{p}$ and the groups K^* and $V^* \times \mathbb{Z}$ are isomorphic.*

Proof. To prove the last part, let $x \in K^*$, we can write $x = a\pi^n$ in a unique way, and therefore the function $\varphi : K^* \to V^* \times \mathbb{Z}$, defined by $\varphi(x) = (a, n)$, is the isomorphism needed.

Corollary 4 *Let R be a discrete valuation ring with maximal ideal $\mathfrak{m}$. If $t \in \mathfrak{m} \setminus \mathfrak{m}^2$, then t is a uniformizer.*

Proof. $\mathfrak{m} \neq \mathfrak{m}^2$. We choose $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. We have $(t) = \mathfrak{m}^n$ for some $n \geq 0$. We can not have $n = 0$ because $(t) \subseteq \mathfrak{m} \subseteq R$, and we can not have $n \geq 2$ by choice of t. The only possibility is $n = 1$, hence $\mathfrak{m} = (t)$.

Corollary 5 *(Ideals in a discrete valuation ring). Let V be a discrete valuation ring with unique maximal ideal p. Then the non-zero ideals of V are exactly the powers p^n for some $n \in \mathbb{N}$. They form strictly decreasing chain*

$$V = p^0 \supsetneq p^1 \supsetneq p^2 \supsetneq ....$$

The following theorem is central for what follows.

Theorem 14 *Every non-trivial valuation on $K(x)$ which is trivial on K is either the degree valuation or a $p-$adic valuation for some irreducible polynomial $p \in K[x]$.*

Proof. We are going to verify that given any non-trivial valuation
$\upsilon : K(x) \to \Gamma$ such that Γ is an ordered group and $\upsilon(a) = 0$ for all $a \in K^*$, then υ is equivalent to υ_∞ or to some υ_p, where $p(x) \in K[x]$ is monic and irreducible.
Let V be the valuation ring of υ and let $\mathfrak{m}$ be its maximal ideal. Now, if $x \in V$, then $K[x] \subseteq V$. Let $\mathcal{P} = \mathfrak{m} \cap K[x]$. We have that $\mathcal{P}$ is a prime ideal of $K[x]$, $K \cap \mathcal{P} = \{0\}$ and $1 \notin \mathcal{P}$.
It follows that $\mathcal{P} = (p)$, where p is monic and irreducible polynomial or $p = 0$.
If $p = 0$, then $\upsilon(K[x])^* = \{0\}$, so $\upsilon(K(x)^*) = 0$, then we have $K(x) = V$, which contradicts the hypothesis that υ is non-trivial. Therefore $\mathcal{P} = (p)$ with $p \neq 0$.
Let $g, h \in K[x]$ with $p \nmid h$ and $h \notin \mathcal{P}$, that is h is a unit in V. We have $\upsilon(\frac{g}{h}) \geq 0$, which implies $V_p \subseteq V$.
Now assume that $u(x) \in K(x) \setminus V_p$. Then $u = \frac{g}{h}$ with $gcd(g, h) = 1$ and $p|h$.
If $u \in V$, since $g \in V_p^* \subseteq V$, it follows that $h^{-1} = g^{-1}u \in V$.
However, we have $h \in \mathcal{P} \subseteq V$, and this implies that h is a non-unit which is absurd.
Hence $u \notin V$ and we have $V \subseteq V_p$, so $V = V_p$. Therefore v and v_p have isomorphic value groups, and are essentially the same.

If $x \notin V$, then $y = \frac{1}{x} = x^{-1} \in V$. From the above discussion, we conclude that $\mathcal{P} \cap K[y] = (l(y))$, where $l(y)$ is a monic and irreducible polynomial.
Now $x = y^{-1} \notin V$, which is equivalent to saying that y is not a unit. Thus

$y \in \mathcal{P} \cap K[y] = (l(y))$ and $l(y)|y$, which proves that $l(y) = y$.
Therefore v_∞ and v have isomorphic value groups, and are essentially the same.

As a consequence we obtain the complete list of the valuation rings of $\mathbb{R}(x)$ which are trivial on $\mathbb{R}$. We note that a real valuation ring of any field K which contains $\mathbb{R}$ must be trivial on $\mathbb{R}$, otherwise we would get a non-archimedean ordering on the field of real numbers which does not exist.

Now, the monic irreducible polynomials p over $\mathbb{R}$ are known and we get

(a) $\deg p = 1$. Then $p = x - \alpha$, $V_\alpha := V_{x-\alpha}$, $V_\alpha/(x-\alpha) = \mathbb{R}$,
(b) $\deg p = 2$. In this case $\mathbb{R}[x]/(p) = \mathbb{C}$,
(c) Finally $V_\infty/m_\infty = \mathbb{R}$.

Therefore, the complete **list of real valuation rings for** $\mathbb{R}(x)$ reads as follows:

$$V_\alpha, \alpha \in \mathbb{P}^1 := \mathbb{R} \cup \infty.$$

2.2.2 Real Holomorphy Rings

At the beginning of the extension of Artin-Schreier theory which Becker started in the 1970s valuation rings and higher level orderings were the most crucial notions. Later on, it is found that real holomorphy rings have great influence in the study of sums of $2n-th$ powers. In fact the ideal structure of holomorphy rings and the structure of its group of units have great influence.

Definition 11 *The real holomorphy ring H(K) of a formally real field K is the intersection of all real valuation rings of K, i.e. valuation rings of K with a formally real residue class field. By* $\mathbb{E}(K)$ *we denote the group of units of H(K), by* $\mathbb{E}_+(K) := H(K)^* \cap \sum K^2$ *the subgroup of totally positive units.*

In the case of $\mathbb{R}(x)$ we know all real valuation rings. Consequently, the real holomorphy ring of $\mathbb{R}(x)$ denoted by $H(\mathbb{R}(x))$ and its group of units can be described as follows.

$$H(\mathbb{R}(x)) = \bigcap_{\alpha\in\mathbb{R}} V_\alpha \bigcap V_\infty = \bigcap_{\alpha\in\mathbb{R}\cup\infty} V_\alpha = \bigcap V_{\alpha\in\mathbb{P}^1}$$

$$= \{\frac{f}{g} : g(\alpha) \neq 0, \forall\alpha \in \mathbb{R}\} \bigcap \{\frac{f}{g} : \deg f \leq \deg g\}$$

$$= \{\frac{f}{g} : \deg f \leq \deg g, g(\alpha) \neq 0, \forall\alpha \in \mathbb{R}\}$$

As to the units we start with the observation that $H(\mathbb{R}(x))^* = \bigcap_{\alpha\in\mathbb{P}^1} V_\alpha^*$. It follows that the units of can be described in the following way:

$$(\mathbb{E}(\mathbb{R}(x))) = \{\frac{f}{g} : f, g \neq 0, \gcd(f,g) = 1, f \text{ and } g \text{ without roots in } \mathbb{R}, \deg f = \deg g\}.$$

$$(\mathbb{E}_+(\mathbb{R}(x))) = \{\frac{f}{g} : f, g \neq 0, \gcd(f,g) = 1, f \text{ and } g \text{ positive definite on } \mathbb{R}, \deg f = \deg g\}.$$

2.3 Real Places

In this section we are summarizing general facts about real places which are needed to sketch the general theory of the real holomorphy rings of arbitrary formally real fields.

Definition 12 *A place of a field K is a mapping φ of K in to $F \cup \{\infty\}$ (where F may be any field) such that*
(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$
(ii) $\varphi(xy) = \varphi(x)\varphi(y)$
(iii) $\varphi(1) = 1$.

Here for all $a \in F$ the following operations are defined:

$$a + \infty = \infty + a = \infty, \quad a.\infty = \infty.a = \infty.\infty = \infty$$

The operations $\infty + \infty$, $0.\infty$ and $\infty.0$ are not defined.

Consider the set V_φ of elements $a \in K$ such that $\varphi(a) \neq \infty$. Then V_φ is a subring of K, and φ is a homomorphism of this ring into F. Since F is a field, the kernel of this homomorphism is a prime ideal $\mathfrak{p}$ of V_φ.

Let b be an element in K which is not in V_φ. We contend that $\varphi(1/b) = 0$. For if this were not true, we would get $1 = \varphi(1) = \varphi(b)\varphi(1/b) = \infty$, by (ii). Thus, $1/b \in \mathfrak{p}$, and thus $\mathfrak{p}$ is precisely the set of non-units of V_φ.

Since any ideal strictly containing $\mathfrak{p}$ would contain a unit, we see that $\mathfrak{p}$ is a maximal ideal and hence the image of V_φ in K is again a field. We shall therefore assume that F is precisely the image of V_φ by φ is a mapping onto $F \cup \{\infty\}$.
OR, Given a place φ we define $V_\varphi = \{a \in K : \varphi(a) \neq \infty\} = \varphi^{-1}(F)$. Then V_φ is an integral subdomain of K.

We observe that $\varphi : V_\varphi \to F$ is a homomorphism such that

$$ker\varphi = \{a \in V_\varphi : \varphi(a) = 0\} = \mathfrak{m}_\varphi = \varphi^{-1}(0).$$

Then $V_\varphi/\mathfrak{m}_\varphi \cong \varphi(V_\varphi) \subseteq F$ and $ker\varphi = \mathfrak{m}_\varphi$ is a prime ideal of V_φ. (We know that if $b \in K \setminus V_\varphi, \varphi(b) = \infty$ and $\varphi(1/b) = 0$. Thus for any $x \in K$ we have $x \in V_\varphi$ or $x^{-1} \in V_\varphi$ i.e. V_φ is a valuation ring.

We saw above how to obtain a valuation ring from a place. Conversely, consider a valuation ring $V, \mathfrak{m}$ its maximal ideal and $K = quotV$.

Let F be the field $V/\mathfrak{m}$ and $F_1 = F \cup \{\infty\}$.
Let $\varphi : K \to F_1$ be given by

$$\varphi(x) = \begin{cases} x \text{ mod m} & \text{if } x \in V \\ \infty & \text{if } x \notin V \end{cases}$$

Then φ is a place.

Thus we summarize it by re-writing the definition of a place again.

Definition 13 *A place $\lambda : K \to F \cup \infty$, where K and F are fields, is a ring homomorphism $\lambda : V \to F$ of a valuation ring V of K into F with $ker\lambda = \mathfrak{m}$ whereby we set $\lambda(x) = \infty$ if $x \notin V$. Places $\lambda : K \to \mathbb{R} \cup \infty$ are called real places.*

Examples of Places

(1) **The real places of** $\mathbb{R}(x), \lambda_\alpha, \alpha \in \mathbb{P}^1$
The complete list of real valuation rings of $K := \mathbb{R}(x)$ is known: $V_\alpha, \alpha \in \mathbb{P}^1$. They all have residue field $\mathbb{R}$. Consider any real place $\lambda : K \to \mathbb{R} \cup \infty$ and its associated valuation ring V_λ. This latter ring is a real valuation ring, say, $V_\lambda = V_\alpha$, some $\alpha \in \mathbb{P}^1$. Hence, $\mathbb{R} \subseteq V_\lambda, \mathfrak{m}_\lambda = \mathfrak{m}_\alpha$ and we deduce that the place λ induces, by restriction, a field homomorphism $\lambda_0 : \mathbb{R} \to \mathbb{R} = V_\alpha/\mathfrak{m}_\alpha$. There is just one field homomorphism, namely the identity.
We summarize: $V_\lambda = V_\alpha, \lambda|\mathfrak{m}_\alpha = 0$ and $\lambda|\mathbb{R} = id$. These three informations alone allow to determine the place uniquely.
First consider $V_\alpha, \alpha \neq \infty$ and any $r \in V_\alpha$, i.e. $r = f/g, f, g \in \mathbb{R}[x], g(\alpha) \neq 0$. Then $r(\alpha) := f(\alpha)/g(\alpha) \in \mathbb{R}$ is well-defined and we find that $r - r(\alpha) = (f \cdot g(\alpha) - f(\alpha) \cdot g)/g \cdot g(\alpha) \in \mathfrak{m}_\alpha = (x - \alpha)V_\alpha$. Finally, $\lambda(r) = r(\alpha)$.
This place is denoted by

$$\lambda_\alpha, \text{ defined by } \lambda_\alpha(r) = r(\alpha) \quad \forall r \in V_\alpha.$$

We next turn to $r \in V_\lambda = V_\infty$. Following the reasoning just given we have to find $r(\infty)$ with $r - r(\infty) \in \mathfrak{m}_\infty$. Then we would get $\lambda(r) = r(\infty)$. In view of the presentation $r = f/g, f, g \in \mathbb{R}[x], g \neq 0, degf \leq degg$ we can assume $f = \sum_0^k a_i x^i, g = \sum_0^k b_i x^i, b_k \neq 0$. Then $r - (a_k/b_k) \in \mathfrak{m}_\infty = 1/xV_\infty$ and we obtain $\lambda(r) = a_k/b_k$. In particular, as claimed, λ is uniquely determined denoted by λ_∞.
There is a more conceptual way of describing this **"place at infinity"**. In fact one verifies for any $r \in V_\infty$ the equation

$$\lambda_\infty(r) = \lim_{|\gamma| \to \infty} r(\gamma).$$

Therefore, the complete **list of real places of** $\mathbb{R}(x)$ reads as follows:

$$\lambda_\alpha, \alpha \in \mathbb{P}^1.$$

(2) Let K be a field.

For all $u \in K((t))^*$, let us write $f(u) = \infty$ if $u \notin K[[t]]$ and define $f(u)$ to be the constant term of u if $u \in K[[t]]$.

Then f is a place of $K((t))$, with residue field K and ring $K[[t]]$.

For $K[[t]]$ is a valuation ring of $K((t))$ and the restriction of f to $K[[t]]$ is identified with the cannonical homomorphism of $K[[t]]$ onto its residue field.
(3) Let S be a connected complex analytic variety of dimension 1 and K the field of meromorphic functions on S.

For all $z_0 \in S$, the mapping $f \mapsto f(z_0)$ from K to $\mathbb{C} \cup \{\infty\}$ is a place of K whose ring is the set of $f \in K$ which are holomorphic at z_0 and whose ideal is the set of $f \in K$ which are zero at z_0.

Space of real Places

Details can be found in **[2],[19]**.Let K be a formally real field and let P be an ordering of K. Then set

$$A(P) = \{a \in K : r \pm a \in P \text{ for some r } \in \mathbb{Q}, r > 0\}.$$

$A(P)$ is shown to be a valuation ring of K. That is P determines a valuation v_P whose ring $A(P)$ is the convex hull of the rationals $\mathbb{Q}$ with respect to P.

$A(P)$ is called the **ring of finite elements relative to P**.
In $A(P)$ we have the ideal

$$I(P) := \{a \in K : r \pm a \in P \text{ for all } r \in \mathbb{Q}, r > 0\}$$

of the **infinitely small elements**, that are elements which, with respect to P, are smaller in absolute value than all positive rationals.

Theorem 15 *(i) $A(P)$ is a real valuation ring with maximal ideal $I(P)$,*
(ii) $\bar{P} := \{a + I(P) : a \in P \cap A(P)\}$ is an Archimedean order of the residue field $A(P)/I(P)$. Thus $A(P)/I(P)$ is naturally embedded in $\mathbb{R}$, and we can think about it as a subfield of $\mathbb{R}$,
(iii) given any real valuation ring V of K there exists an ordering P such that $A(P) \subseteq V$.

Above, we had seen how places arise from valuation rings. This can be applied to the valuation ring A(P) and yields the first statement of the following theorem. The second one uses a method of pulling back orderings from a residue field to the the field in question.

Theorem 16 *(i) An order P of K gives rise to a real place $\lambda_P : K \to \mathbb{R} \cup \infty$ with valuation ring $A(P)$,*
(ii) every real place on K is of the type λ_P for some ordering P of K,
(iii) for $P \in X(K), \lambda_P$ is the only real-valued place $\xi : K \to \mathbb{R} \cup \infty$ with the property $\xi(P) \geq 0$.

Corollary 6 *A field K is formally real if and only if it admits a real place $\lambda : K \to \mathbb{R} \cup \infty$.*

From theorem 15 we draw the conclusion that H(K) can already be described by the rings A(P) or the real places. To this end we set:

$$M(K) = \{\lambda_P : P \in X(K)\}, \text{ where } X(K) \text{ is the space of orderings of } K.$$

M(K) is called the space of real places of the field K. We now get:

$$H(K) = \bigcap_{P \in X(K)} A(P)$$

$$H(K) = \{a \in K : \forall_{\zeta \in M(K)} : \zeta(a) \neq \infty\}.$$

The following lemma provides a large supply of elements in $H(K)$.

Lemma 6 *Let K be a formally real field, and $b_1, ..., b_n \in K$. Then*
(i) $\frac{1}{1+b_1^2+...+b_n^2} \in H(K)$;
(ii) $\frac{b_i}{1+b_1^2+...+b_n^2} \in H(K)$ for all i;
(iii) K is the field of quotients of $H(K)$.

As before, for a formally real field K, $X(K)$ denotes the set of all orderings on K, topologized by taking as subbasis the Harrison sets
$H(a) = \{P \in X(K) : a \in P\}$ where $a \in K^*$.

From above, we have a map $\Lambda : X(K) \to M(K)$ which sends an ordering $P \in X(K)$ to λ_P, its associated real place. We know that λ_P has been characterized as the only place $\xi \in X(K)$ with the property that $\xi(P) \geq 0$.

Proposition 10 *The map $\Lambda : X(K) \to M(K)$ is onto.*

Using the surjection Λ in proposition above, we can view $M(K)$ as a quotient set of $X(K)$.
Therefore, we can make $M(K)$ into a topological space by giving it the quotient topology $\mathfrak{T}$ induced by the topology on $X(K)$. Since $X(K)$ is quasi-compact, $(M(K), \mathfrak{T})$ is also quasi-compact. To prove that it is in fact even a Hausdorff space one has to discusss functions on this space.
For any element $a \in K$, we have the following "evaluation map" at a:

$$\hat{a} : M(K) \to \mathbb{R} \cup \infty,$$

defined by $\hat{a}(\xi) = \xi(a)$ for any $\xi \in M(K)$.
We view $\mathbb{P}^1 := \mathbb{R} \cup \infty$ as the one-point compactification of $\mathbb{R}$. In other words, we identify $\mathbb{R} \cup \infty$ with the unit circle S^1 with its usual topology, details in the subsequent section.

Theorem 17 *For any $a \in K$, the evaluation map $\hat{a} : M(K) \to \mathbb{R} \cup \infty$ is continuous on $(M(K), \mathfrak{T})$.*

Lemma 7 *The ring of evaluation maps $\{\hat{a} : a \in H(K)\}$ from $M(K)$ to $\mathbb{R}$ separates points on $M(K)$.*

That we are dealing with a ring of functions $M(K) \to \mathbb{R}$ follows from the properties:

$$\hat{a} + \hat{b} = \widehat{a+b}, \hat{a} \cdot \hat{b} = \widehat{a \cdot b} \ \forall a, b \in H(K).$$

Theorem 18 *$(M(K), \mathfrak{T})$ is a Hausdorff space.*

Corollary 7 *The continuous map $\Lambda : X(K) \to M(K)$ is a closed mapping.*

Using the results obtained above, we can now describe the topology on $M(K)$ in a somewhat concrete way.

Theorem 19 *The topology $\mathfrak{T}$ on $M(K)$ coincides with the coarest topology $\mathfrak{T}'$ for which all the functions $\{\hat{a} : a \in H(K)\}$ into $\mathbb{R}$ are continuous. A subbasis for this topology is given by the sets
$H'(a) := \{\xi \in M(K) : \xi(a) > 0\} = \hat{a}^{-1}(0, \infty)$, where $a \in H(K)$.*

The description of the topology on $M(K)$ given above points to the fundamental difference between the space $M(K)$ and the space $X(K)$. In $X(K)$, the Harrison sets $H(a), (a \in K^*)$ are closed with respect to complements (since $X(K) \setminus H(a) = H(-a)$), so each $H(a)$ is a clopen (closed and open set), and so $X(K)$ is a totally disconnected (hence Boolean) space. In $M(K)$,

however, the complement of a subbasic set $H'(a) = \{\xi \in M(K) : \xi(a) > 0\}$ is $\{\xi \in M(K) : \xi(a) \leq 0\}$, which is no longer of the form $H'(b)$, and may not be even open. Therefore, we have no reason to expect $M(K)$ to be a Boolean space. In the special case when all the orderings on K are archimedean, the map Λ is a bijection, so $M(K)$ homeomorphic to $X(K)$, hence a Boolean space. In general, however, $M(K)$ need not be totally disconnected. In fact, there exist many examples of fields K for which $M(K)$ even turn out to be connected.

Let $C(M(K), \mathbb{R})$ be the ring of real-valued continuous functions on $M(K)$. Since $M(K)$ is compact, we can define the sup-norm on $C(M(K), \mathbb{R})$, by

$$||f|| = sup\{f(\xi) : \xi \in M(K)\} \qquad (f \in C(M(K), \mathbb{R})).$$

In this context, the classical Stone-Weierstraß Theorem can be brought into play. In fact, consider the family of functions

$$E := \{\hat{a} : a \in H(K)\} \subseteq C(M(K), \mathbb{R}).$$

Since E separates points on $M(K)$, and E contains the constant function $1(= \hat{1})$, the Stone-Weierstraß Theorem implies that this set lies dense in $C(M(K), \mathbb{R})$. This is an important fact. In order to formulate it in a most meaningful way we introduce the ring homomorphism

$$\Phi : H(K) \to C(M(K), \mathbb{R}), a \mapsto \hat{a}.$$

That Φ is a ring homomorphism was already noted above. With all this we get:

Theorem 20 *The representation $\Phi : H(K) \to C(M(K), \mathbb{R})$ has a dense image.*

For the application of theorem above we consider the problem "separating" two sets of orderings in $X(K)$. Let A, B be two disjoint closed sets in $X(K)$. We say that we can *separate A from B* if there exists an element $c \in K^*$ which is positive with respect to any ordering in A, and negative with respect to any ordering in B. If this is the case, we shall say that A is separated from B by c.

Proposition 11 *(SEPARATION CRITERION). Let A, B be disjoint closed sets in $X(K)$. The following three statements are equivalent:*
(1) $\Lambda(A)$ is disjoint from $\Lambda(B)$ in $M(K)$;
(2) we can separate A from B by an element $c \in H(K)$ which is a valuation unit at any place in $\Lambda(A \cup B)$;
(3) we can separate A from B by an element $c \in K^*$ which is a valuation unit at any place in $\Lambda(A)$.

2.4 Topological Representation of $H(\mathbb{R}(x))$

We show that $\mathbb{P}^1$ is a compact (= quasi compact + Hausdorff) space, and that is homeomorphic to S^1 via the stereographic projection.

The one-point compactification of $\mathbb{R}$
$S^1 = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}$.

We stereographically project the one-dimensional unit circle S^1 from its "north-pole" N = (0, 1) onto $\mathbb{R}$.

Every point $x \in S^1 \setminus \{N\}$ is thus associated to the point $\varphi(x)$ at which the line containing N and x intersects $\mathbb{R}$. This gives us a continuous bijection

$\varphi : S^1 \setminus \{N\} \to \mathbb{R}, \varphi(x_1, x_2) = \frac{x_1}{1-x_2}$

and the inverse map $\varphi^{-1} : \mathbb{R} \to S^1 \setminus \{N\}, \varphi^{-1}(x) = \frac{2x}{x^2+1} + i\frac{x^2-1}{x^2+1}$

is also continuous.

If we extend φ to a bijection $\varphi' : S^1 \to P^1 = \mathbb{R} \cup \infty$

where $\varphi'(x) = \varphi(x)$ for $x \neq N, \varphi(N) = \infty$

Then both φ' and its inverse are continuous.
We may thus identify $\mathbb{P}^1$ and the circle S^1 as topological spaces. We therefore can state the
Fact: $\mathbb{P}^1$ is compact, connected topological space and carries a metric(inherited from S^1).

We next show that the elements of $\mathbb{R}(x)$ operates on $\mathbb{P}^1$ as a continuous functions with values in $\mathbb{P}^1$.

Let $f = \frac{g}{h} : g, h \in \mathbb{R}[x], gcd(g, h) = 1$ or $g = 0, h \neq 0$

For $\alpha \in \mathbb{R}$,

$$f(\alpha) = \begin{cases} \infty & \text{if } h(\alpha) = 0 \\ \frac{g(\alpha)}{h(\alpha)} & \text{if } h(\alpha) \neq 0 \end{cases}$$

For $\alpha = \infty$,

$$f(\infty) = \begin{cases} \infty, & \text{if } k > l; \\ \frac{a_k}{b_l}, & \text{if } k = l; \\ 0, & \text{if } k < l \end{cases}$$

where $f(x) = \frac{a_k x^k + \ldots + a_0}{b_l x^l + \ldots + b_0}$

Each $f \in \mathbb{R}(x)$ gives rise to a continuous function $\tilde{f} : \mathbb{P}^1 \to \mathbb{P}^1$,
where $\tilde{f}(\alpha) = f(\alpha)$, $\tilde{f}(\infty) = f(\infty)$ as defined above. For later use, we note that for all $\alpha \in \mathbb{P}^1$ we have $\tilde{f}(\alpha) = \lambda_\alpha(f)$.

So we get a representation $\Psi : \mathbb{R}(x) \to C(\mathbb{P}^1, \mathbb{P}^1), f \mapsto \tilde{f}$, the latter being the set of all continuous functions between these spaces.
Clearly Ψ is injective and one can observe that

$$f \in H := H(\mathbb{R}(x)) \Leftrightarrow \tilde{f} \in C(\mathbb{P}^1, \mathbb{R}).$$

Now applying Stone-Weierstraß Theorem we get that the image $\Psi(H)$ is dense in $C(\mathbb{P}^1, \mathbb{R})$ relative to the supremum norm.
From the description of H we deduce the following facts (where we drop the reference to the field $\mathbb{R}(x)$ as in the case of H):

$$f \in \mathbb{E} \Leftrightarrow \tilde{f} \text{ has no zero on } \mathbb{P}^1, f \in \mathbb{E}_+ \Leftrightarrow \tilde{f} > 0 \text{ on all points of } \mathbb{P}^1.$$

At present we are facing two representations. i.e. ring homomorphisms $\Phi : H \to C(M, \mathbb{R}), f \mapsto \hat{f}, \Psi : H \to C(\mathbb{P}^1, \mathbb{R}), f \mapsto \tilde{f}$ where we set
$M = M(\mathbb{R}(x))$. That they essentially the same will follow below.

Identification of M with $\mathbb{P}^1$

We have to show that M is homeomorphic with $\mathbb{P}^1$ and that the representation Ψ is nothing but the concrete geometric version of the representation $\Phi : H \to C(M, \mathbb{R})$ of the general theory .

We begin the proof by recalling the bijection $\sigma : \mathbb{P}^1 \to M, \alpha \mapsto \lambda_\alpha$ and want to prove that it is a homeomorphism. Since both spaces in question are compact it is enough to deduce that the bijection σ is continuous, by general topology of compact spaces.
Further note the equation $\hat{f} \circ \sigma = \tilde{f}$ what follows from

$$\hat{f}(\sigma(\alpha)) = \hat{f}(\lambda_\alpha) = \lambda_\alpha(f) = f(\alpha) = \tilde{f}(\alpha).$$

We have seen above that the topology on M is characterized as the smallest(= coarsest) topology such that all maps $\hat{f} : M \to \mathbb{R}, \lambda \mapsto \lambda(f)$, $f \in H$ are continuous. A subbasis is given by the sets $U_f := \hat{f}^{-1}(0, \infty)$. In view of $\hat{f} \circ \sigma = \tilde{f}$ we obtain $\sigma^{-1}(U_f) = \tilde{f}^{-1}(0, \infty)$. As $\tilde{f}$ is continuous this latter set is open, and σ is shown to be continuous, finally a homeomorphism between $\mathbb{P}^1$ and the space of real places $M(\mathbb{R}(x))$.

The relation above between yields $\phi(f) \circ \sigma = \Psi(f) \quad \forall f \in H$, meaning that both representations Φ and Ψ are equivalent. In other words, Ψ is nothing but the geometric version of the general type representation Φ.

2.5 $H(\mathbb{R}(x))$ a Dedekind Ring

There are various ways to prove that in this case the real holomorphy ring is a Dedekind ring. We have chosen an approach where we start by achieving explicit information how the prime ideals can be generated by finitely many elements. After sketching the proof of the known result that H is a Prüfer ring anyway we then conclude that H is a Dedekind ring where, as said, we explicitly know generators of the maximal ideals and their squares. This information allows to derive a somewhat explicit presentation in proposition 16 and chapter 4.

Fractional Ideals

Here we introduce the notion and results needed to prove that the real holomorphy rings of formally real fields are Prüfer rings.

Let R be an integral domain with quotient field K.

A fractional ideal is any $R-$submodule $\mathfrak{a} \subseteq K$ such that there is $f \in R, f \neq 0$ with $f\mathfrak{a} \subseteq R$.

Example. Set of fractional ideals in $\mathbb{Q} = \{r\mathbb{Z} \mid r \in \mathbb{Q}\}$.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of R.
Their sum $\mathfrak{a}+\mathfrak{b} = \{a+b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$ and their product $\mathfrak{ab} = \{\sum_{finite} a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ as well as their intersection $\mathfrak{a} \cap \mathfrak{b}$ are fractional ideals of R.

If both fractional ideals are finitely generated (as $R-$modules), say $\mathfrak{a} = (a_1, ..., a_r), \mathfrak{b} = (b_1, ..., b_s)$, then $\mathfrak{ab} = (a_1 b_1, ..., a_r b_s)$. Multiplication of fractional ideals is compatible with the order relation between fractional ideals:

$$\text{if } \mathfrak{a} \subseteq \mathfrak{b}, \text{ then } \mathfrak{ac} \subseteq \mathfrak{bc}$$

The non-zero fractional ideals form a multiplicative semi-group with R as its unit element.

Definition 14 *A fractional ideal $\mathfrak{a}$ of a ring R is invertible if there exists a fractional ideal $\mathfrak{b}$ of R such that $\mathfrak{ab} = R$.*

Proposition 12 *Let $\mathfrak{a} \neq (0)$ be an invertible fractional ideal such that $\mathfrak{ab} = R$ for a fractional ideal $\mathfrak{b}$. Then $\mathfrak{b} = [R : \mathfrak{a}]$, i.e if $\mathfrak{a}$ is invertible then $\mathfrak{a}^{-1} = [R : \mathfrak{a}] := \{r \in K : r\mathfrak{a} \subseteq R\}$.*

We note that the invertible ideals form an abelian group.

Lemma 8 *Let $\mathfrak{a}$ be a fractional R-ideal. If $\mathfrak{a}$ is invertible, then $\mathfrak{a}$ is finitely generated as R-module.*

Definition 15 *A ring R is called a Prüfer domain if and only if all non-zero finitely generated fractional ideals are invertible.*

Theorem 21 *H(K) = H is a Prüfer ring.*

Proof. Let $\mathfrak{a} = (a_1, ..., a_r)$ be a non-zero finitely generated $H-$module.

$$\mathfrak{a} = \{\sum_{i=1}^{r} f_i a_i : f_i \in H\}$$

$\mathfrak{a}^2 = \mathfrak{a} \cdot \mathfrak{a}$ is generated by $(\sum_{i=1}^r f_i a_i)(\sum_{j=1}^r g_j a_j), f_i, g_j \in H$.

$$= \sum_{i,j} (f_i g_j)(a_i a_j)$$

$$= (..., a_i a_j, ...) \supseteq (\sum_{i=1}^{r} a_i^2)$$

$$\Longrightarrow \mathfrak{a}^2 = (..., a_i a_j, ...)$$

Now as $\frac{a_i a_j}{\sum_{i=1}^r a_k^2} \in H$ we have that $a_i a_j = \frac{a_i a_j}{\sum_{i=1}^r a_k^2} \sum_{i=1}^r a_i^2 \in H \cdot \sum_{i=1}^r a_i^2$

$$\Longrightarrow \mathfrak{a}^2 \subseteq H \cdot (\sum_{i=1}^{r} a_i^2) \subseteq \mathfrak{a}^2$$

i.e. $(a_1, ..., a_r)^2 = (\sum_{i=1}^r a_i^2)$. If $f = \sum_{i=1}^r a_i^2$, then it follows that $(a_1, ..., a_r)[(a_1, ..., a_r).f^{-1}] = H$ as principal ideal is invertible.

i.e. $\mathfrak{a}$ is invertible and hence H is Prüfer. We now turn to the proof that

$$H(\mathbb{R}(x)) \textbf{ is a Dedekind Ring.}$$

Given $\alpha \in \mathbb{P}^1$ let $\nu_\alpha, V_\alpha, I_\alpha, \lambda_\alpha$ be the corresponding (real) valuation, valuation ring, maximal ideal and real place. We know that

$$I_\alpha = (x-\alpha)V_\alpha \text{ if } \alpha \in \mathbb{R}, I_\infty = (1/x)V_\infty, \nu_\alpha(x-\alpha) = 1, \nu_\infty(1/x) = 1$$

From $H \subseteq V_\alpha$ we get that $\mathfrak{m}_\alpha := H \cap I_\alpha$ is a maximal ideal of H with residue field $\mathbb{R}$. We are going to prove the following three facts:

1. $\mathfrak{m}_\alpha$ is generated by elements $\frac{x-\alpha}{1+x^2}, \frac{(x-\alpha)^2}{1+x^2}$ if $\alpha \in \mathbb{R}$,
2. $\mathfrak{m}_\infty$ is generated by $\frac{1}{1+x^2}, \frac{x}{1+x^2}$,
3. the prime ideals of H are the $\mathfrak{m}_\alpha, \alpha \in \mathbb{P}^1$ and the zero ideal (0). Thus, the Krull dimension of H is equal to 1.

The proofs start with the observation that each non-zero element of H can be written in the form

$$a = \epsilon \cdot \Pi_1^r \frac{x-\alpha_i}{(1+x^2)^k}, \epsilon \in H^*, r \leq 2k.$$

So, in dealing with ideals we can ignore the units and focus on elements $f = \Pi_1^r \frac{x-\alpha_i}{(1+x^2)^k}$

Now let $\mathfrak{p}$ be a non-zero prime ideal in H. We look at the elements $f \neq 0$ in this prime ideal with a smallest $r \geq 0$.
Case 1: $r = 0$. Then $\frac{1}{1+x^2} \in \mathfrak{p}$ since the ideal is prime ideal. From $[\frac{x}{1+x^2}]^2 = [\frac{x^2}{1+x^2}].[\frac{1}{1+x^2}] \in \mathfrak{p}$ we get that $\frac{x}{1+x^2} \in \mathfrak{p}$ since this ideal is a prime ideal. Define the H-ideal $\mathfrak{a} := (\frac{1}{1+x^2}, \frac{x}{1+x^2})$. These two generators also lie in I_∞, hence $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{a} \subseteq \mathfrak{m}_\infty$. To show equality in both cases it will be proven that $H/\mathfrak{a} = \mathbb{R}$, in particular, that $\mathfrak{a}$ is a maximal ideal, whence the claim. Firstly, from $\mathbb{R} \subseteq H$ we get $\mathbb{R} \subseteq H/\mathfrak{a}$. Secondly, we have to prove that for each $f \in H$ there exists $\alpha \in \mathbb{R}$ such that $f \equiv \alpha \bmod \mathfrak{a}$, i.e. $f + \mathfrak{a} = \alpha$. To obtain this it is enough to consider the elements $g := \frac{x^i}{(1+x^2)^k}$ where $i \leq 2k$ since an arbitrary $f \in H$ is a $\mathbb{R}$-linear combination of those elements. If

$$i \leq 2k-2 \text{ we have } g = \frac{x^i}{(1+x^2)^{k-1}} \cdot \frac{1}{1+x^2} \in \mathfrak{a}.$$

If

$$i = 2k-1 \text{ then } g = \frac{x^{2k-1}}{(1+x^2)^k} = \frac{x^{2k-2}}{(1+x^2)^{k-1}} \cdot \frac{x}{1+x^2} \in \mathfrak{a}.$$

Finally, look at

$$g = \frac{x^{2k}}{(1+x^2)^k}.$$

This special element g does not belong to the ideal $\mathfrak{a}$. Instead we get $g-1 \in \mathfrak{a}$ as can be shown as follows. From $\frac{x^2}{1+x^2} \equiv 1 \bmod \mathfrak{a}$ we get by taking the k-th power $g \equiv 1 \bmod \mathfrak{a}$ as well. This settles this special subcase and $\mathfrak{m}_\infty = \mathfrak{a} = \mathfrak{p}$ is proven.

Case 2: $r \geq 1$. Here $\frac{1}{1+x^2} \notin \mathfrak{p}$. Consider an element f with smallest number r. If $r = 2k$, minimality of r and the fact that $\mathfrak{p}$ is a prime leads to $r = 2$. So, $f \cdot [\frac{1}{1+x^2}] = [\frac{x-\alpha}{1+x^2}].[\frac{x-\beta}{1+x^2}] \in \mathfrak{p}$. Primality of $\mathfrak{p}$ shows that for some

α the element $g := \frac{x-\alpha}{1+x^2} \in \mathfrak{p}$. Then $[\frac{(x-\alpha)^2}{1+x^2}].[\frac{1}{1+x^2}] = g^2 \in \mathfrak{p}$. Since $\frac{1}{1+x^2} \notin \mathfrak{p}$ we get $\frac{(x-\alpha)^2}{1+x^2} \in \mathfrak{p}$. This time we get that the H-ideal $\mathfrak{b} := (\frac{(x-\alpha)^2}{1+x^2}, \frac{x-\alpha}{1+x^2})$ is contained in $\mathfrak{m}_\alpha$ and $\mathfrak{p}$. Similarly if $r < 2k$. To prove equality of the three ideals we proceed in an analogue manner. We first note that any polynomial can be presented as linear combination of the powers $(x-a)^i, i = 0, 1, \ldots$. So we have to look at the elements $\frac{(x-\alpha)^i}{(1+x^2)^k}$ for $0 \leq i \leq 2k$. If $1 \leq i \leq 2k$ then $\frac{(x-\alpha)^i}{(1+x^2)^k} \in \mathfrak{b}$ readily follows. It remains to look at the elements $g_k := \frac{1}{(1+x^2)^k}$. If $k = 1$ then

$$\frac{1}{1+x^2} - \frac{1}{1+a^2} = -[(x-a)^2 + 2a(x-a)]/[(1+x^2)(1+a^2)] \in \mathfrak{b}$$

implying $g_k \equiv \frac{1}{(1+a^2)^k} \bmod \mathfrak{b}$. This again proves $\mathfrak{m}_\alpha = \mathfrak{b} = \mathfrak{p}$

So far it has been proven that each prime ideal is finitely generated, in fact the zero ideal by 0, otherwise it is maximal and generated by two elements. Since a ring in which each of its prime ideal is finitely generated is Noetherian Ring (See Kaplansky: Commutative rings, Theorem 8.). So we could apply this fact and get that H is Noetherian. Since H is Prüfer ring, using the Noetherian property we see that each ideal of H is invertible. So H turns out to be a Dedekind domain.(See Kaplansky: Commutative rings, Theorem 96.)
Then each non-zero ideal $\mathfrak{a}$ of H is a product of finitely many maximal ideals. This representation as a product of maximal ideals is unique up to the order of the maximal ideals.(Kaplansky: Commutative rings, Theorem 97.)
Therefore, we have proven

Theorem 22 *H is a **Dedekind domain**.*

A bit more has been proven in fact. The ideals $\mathfrak{m}_\alpha, \alpha \in \mathbb{P}^1$ form a complete list of the maximal ideals of H. From $\mathfrak{m}_\alpha = H \cap I_\alpha \subseteq V_\alpha$ we get $H_{\mathfrak{m}_\alpha} \subseteq V_\alpha$. Localizations of Dedekind rings are discrete valuations rings, hence maximal subrings of their field of quotients. So, $H_{\mathfrak{m}_\alpha} = V_\alpha$.

Invoking the general theory of Dedeking rings we therefore get the formula,

$$\text{if } f \in K^*, \text{ then } fH = \Pi_{\alpha \in \mathbb{P}^1} \mathfrak{m}_\alpha^{\upsilon_\alpha(f)}.$$

As said above, this formula describes the unique factorization of a principal fractional ideal as a product of maximal ideals.

We note that the formula implicitly takes into account that the values $\upsilon_\alpha(f)$ are equal to 0 apart from finitely many α's.

Lemma 9 *1. For each $f \in \mathbb{R}(x)^*$ the sum $\sum_\alpha \upsilon_\alpha(f)$ is an even integer,*

2. for any two, not necessarily distinct maximal ideals $\mathfrak{m}_1$ and $\mathfrak{m}_2$ the product $\mathfrak{m}_1\mathfrak{m}_2$ is a principal ideal.

Proof. (1) Any non-zero element f can be written as
$f = const \cdot \prod_1^r (x-\alpha_i)^{e_i} \cdot q$ where the α_i are pairwise distinct and q is a non-zero sum of squares in $\mathbb{R}(x)$. Note first that $\upsilon(q) \in 2\mathbb{Z}$ for any real

valuation of $\mathbb{R}(x)$. If v is a real valuation different from the $v_{\alpha_i}, i = 1, \ldots, r$ and v_∞ then $v(f) = v(q) \equiv 0 \bmod 2$. Next, we get $v_{\alpha_i}(f) \equiv e_i \bmod 2$ and $v_\infty(f) \equiv -\sum_i e_i \bmod 2$. Hence claim (1) is settled.
(2) We will provide explicit generators for the product.
First consider distinct elements $\alpha, \beta \in \mathbb{R}$ and set $f := \frac{(x-\alpha)(x-\beta)}{1+x^2}$. We see that $v(f) = 0$ for any real valuation $\neq v_\alpha, v_\beta$ and $v(f) = 1$ if $v = v_\alpha$ or $= v_\beta$. This implies $fH = \mathfrak{m}_\alpha \mathfrak{m}_\beta$. In a similar fashion one proves $\frac{x-\alpha}{1+x^2} H = \mathfrak{m}_\infty \mathfrak{m}_\alpha$. Again, by calculating the values $v(f)$ one verifies $\frac{1}{1+x^2} H = \mathfrak{m}_\infty^2$ and $\frac{(x-\alpha)^2}{1+x^2} H = \mathfrak{m}_\alpha^2$.

Proposition 13 *(1) No maximal ideal in $H(\mathbb{R}(x))$ is a principal ideal,*
(2) given finitely many distinct ideals $\mathfrak{m}_1, ..., \mathfrak{m}_k$ and exponents $e_1, ..., e_k \in \mathbb{Z}$, then $\Pi_1^k \mathfrak{m}_i^{e_i}$ is a principal fractional ideal if and only if $\sum_1^k e_i$ is even.

Proof. (1) The assumption $fH = \mathfrak{m}$ would contradict the first statement of the previous lemma. (2) If the given product is a principal fractional ideal then, by the previous lemma, the sum $\sum_1^k e_i$ is even. Conversely, assume this to hold. If e_i is even then, by the lemma above, the fractional ideal $\mathfrak{m}_i^{e_i}$ is a principal fractional ideal. Otherwise, $e_i = 2f_i + 1$ and we get that $\mathfrak{m}_i^{e_i} = (a_i H)\mathfrak{m}_i$. Altogether, our product in question is a product of a principal fractional ideal with a product $\prod_1$ of an even number of maximal ideals. By the second statement of the last lemma $\prod_1$ is a principal fractional ideal as well. Hence, the proof is complete.

To prepare the next statement let H denote an arbitrary real holomorphy ring of a formally real field K.

Proposition 14 *Let $\mathfrak{a}$ be an H-fractional ideal, finitely generated by $a_1, ..., a_k$. Then for each $n \in \mathbb{N}$ we get*

$$\mathfrak{a}^{2n} = (\sum_{i=1}^{k} a_i^{2n}).$$

Proof. $\mathfrak{b} := \mathfrak{a}^{2n}$ is generated as an H-module by the finitely many products $a_{i_1}.a_{i_2}...a_{i_{2n}}$ where for all indices $1 \leq i_j \leq k$. Denoting such a product by b and considering $c := \frac{b}{\sum_{i=1}^k a_i^{2n}}$ gives that $v(c) \geq 0$ for any real valuation v of K. Thus c is contained in H. Finally one gets that $\mathfrak{b}$ is a principal fractional ideal generated by the element as announced.

We apply this proposition to the case $K = \mathbb{R}(x)$ and its maximal ideal $\mathfrak{m}_\alpha$.

Proposition 15 *Let $\mathfrak{m}$ be a maximal ideal of $H(\mathbb{R}(x))$ and $l \geq 1$. Then*
(1) if l is odd then m^l is not a principal ideal,
(2) if l is even then $m^l = (a^l + b^l)$ for some $a, b \in H$.

Proof. The first statement is just a special case of a previous result. The second one results from the previous proposition and the fact that a maximal ideal is generated by two elements.

The representation of a principal fractional ideal allows a nice description of arbitrary non-zero sums of squares in $\mathbb{R}(x)$. To spell it out we use generators of the squares of the maximal ideals of the real holomorphy rings as given above.

Proposition 16 *Any non-zero sum of squares in* $\mathbb{R}(x)$ *admits a unique presentation of the type*

$$f = \epsilon \cdot [\frac{1}{1+x^2}]^{e_\infty} \prod_{\alpha \in \mathbb{R}} [\frac{(x-\alpha)^2}{1+x^2}]^{e_\alpha} \text{ where } \epsilon \in \mathbb{E}_+.$$

Proof. We know that $v(f)$ is even for any real valuation. Taking this into account the formula for the fractional ideal fH directly translates into the product formula for the element f where the unit factor must be sum of squares necessarily.

Chapter 3

Real Holomorphy Rings of Elliptic Function Fields

3.1 Quadratic Extension of Fields

Definition 16 *Let L be a field extension of a field K. We can always regard L as a vector space over K where addition is field addition multiplication by K is simply multiplication.*
We say that the degree of L as an extension of K is the dimension of the vector space (denoted $[L : K]$).

Extension of degree 2 (i.e $[L : K] = 2$)are called quadratic extensions.

Theorem 23 *Suppose $char(K) \neq 2$. Then any extension $K \subset L$ of degree 2 can be obtained by adjoining a square root: $L = K(\beta)$, where $\beta^2 = b \in K$. Conversely if β is an element of L and if $\beta^2 \in K$, but $\beta \notin K$ then $K(\beta)$ is a quadratic extension.*

Proof. Let $K-$basis be $1, \alpha$. Then $L = K1 + K\alpha$. $(\alpha \in L \setminus K)$.
$L \ni \alpha^2 = a\alpha + b, \quad (a, b \in K)$
α satisfies quadratic equation $x^2 - ax - b = 0$, i.e.$\alpha^2 - a\alpha - b = 0 \quad (a, b \in K)$.
Then $(\alpha - \frac{a}{2})^2 = b + (\frac{a}{2})^2$. Let $\beta = \alpha - \frac{a}{2}$
$1, \beta$ $K-$basis, $\beta^2 = \gamma \in K, \gamma \neq 0, \gamma \notin K^2$ and L generated by $1, \sqrt{\gamma}$.
$Irr(\alpha, K) = x^2 - ax - b$ irreducible over K. If not $x^2 - ax - b = (x - r)(x - s), (r, s \in K)$.
Inserting $x = \alpha$, we get $0 = (\alpha - r)(\alpha - s) \Rightarrow \alpha = r \in K$ or $\alpha = s \in K$
$\Rightarrow L = K \Rightarrow [L : K] = 1$.
i.e. L/K quadratic $\rightsquigarrow x^2 - ax - b \in K[x], (a, b \in K)$ irreducible.
Conversely, every quadratic irreducible polynomial is associated with a quadratic field extension of K. To show this, let $f \in K[x], f = x^2 + ax + b, a, b \in K$ be irreducible.
1^{st}: $(f) = fK[x]$ is maximal (true for all $PIDs$).
Assume not!
Then $(f) \subsetneqq \mathfrak{m} \subsetneqq K[x]$. Let $g \in \mathfrak{m} \setminus (f)$
$\Longrightarrow gcd(g, f) = h$. Then $h|f \Rightarrow f = h.h_1$.
f irreducible $\Rightarrow h = const.$ or $h_1 = const.$
$h = const \neq 0 \Rightarrow gcd(g, f) = 1$. Then $1 = Ag + Bf \in \mathfrak{m}$. Contradiction.

$h_1 = const. \Rightarrow p = gcd(g, f) \Rightarrow f|g$, thus $g = f.f_1 \in (f)$. Contradiction.
2^{nd}: $K[x]/(f) = L$ is a field. $K \hookrightarrow L, \alpha \mapsto \alpha + (f)$ field embedding.
Claim: $L = K + K\bar{x}, \quad \bar{x} = x + (f)$.
$g + (f) \equiv h + (f), g \equiv hmodf, f|(g - h)$.
$1, x, x_2 \equiv -ax - bmodf \Rightarrow ... \Rightarrow x^k \equiv (\alpha_k + \beta_k)modf$
$\Longrightarrow 1, \bar{x} \quad K-$basis for L, $[L : K] = 2$.
That is to say if L/K is a quadratic extension there is associated irreducible quadratic polynomial $x^2 - \beta x - \alpha \in K[x], \beta, \alpha \in K$. Conversely quadratic irreducible polynomial is associated with a quadratic field extension of K.
Remark: f irreducible of $degf = n \Rightarrow [K[x]/(f) : K] = n$.

Proposition 17 *Let K be a formally real field, $L = K(\sqrt{a})$ a quadratic extension. Then the following are equivalent:*
(i) L is formally real,
(ii) $a \notin -\sum K^2$,
(iii) there exists an ordering P of K with $a \in P$.

Proof. Assume(i). If (ii) were not true, then $-1 \in \sum L^2$, a contradiction.
Assume (ii). If no ordering as in(iii) exists, then $-a \in \cap P = \sum K^2$, a contradiction.
Assume (iii). We consider the set $T = \{\sum_1^n x_i^2 p_i | n \in \mathbb{N}, x_i \in K, p_i \in P\}$. Then T is a preordering of L, so it is contained in an ordering P' of L. This means that L is formally real.

Corollary 8 *Let L/K be a field extension of finite degree n and let $\alpha \in L$. Then α is algebraic over K and its degree divides n.*

Corollary 9 *Every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2.*

From above theorems we get that given any $\gamma \notin K^2$, then $x^2 - \gamma \in K[x]$ is irreducible.
$L = K[x]/(x^2 - \gamma) = K1 + K\bar{x}$, $\bar{x}^2 = \gamma$. That is to say quadratic extension $(char(K) \neq 2)$ they come from $\gamma \notin K^2$.
Let now $f \in \mathbb{R}[T]$ and $degf$ odd. Then $f \notin \mathbb{R}(T)^2$ and it follows that $x^2 - f \in \mathbb{R}(T)[x]$ is irreducible.

Special case: If $degf = 3$, then $f \notin \mathbb{R}(T)^2$. If in addition f is without multiple roots in $\mathbb{C}$ over $\mathbb{R}$ we call $\mathbb{R}(T)(\sqrt{f})$ an **Elliptic Function Field over $\mathbb{R}$.**

Let $\gamma \notin K^2$ and assume $L = K(\sqrt{\gamma})$.
Then $\sigma : L \to L$ be given by $\sigma(\alpha + \beta\sqrt{\gamma}) := \alpha - \beta\sqrt{\gamma}$ is a K-automorphism of L.
As usual we define the trace and norm:

trace $= tr(\alpha + \beta\sqrt{\gamma}) = (\alpha + \beta\sqrt{\gamma}) + \sigma(\alpha + \beta\sqrt{\gamma}) = 2\alpha$
norm $= N(\alpha + \beta\sqrt{\gamma}) = (\alpha + \beta\sqrt{\gamma})\sigma(\alpha + \beta\sqrt{\gamma}) = \alpha^2 - \beta^2\gamma$
Each $z \in L$ satisfies $z^2 - tr(z)z + N(z) = 0$.

3.2 Extension of Valuation Rings from $\mathbb{R}(x)$ to Elliptic Function Fields

Our aim here is to understand valuation rings of elliptic function fields on the basis of valuation rings of $\mathbb{R}(x)$.
By a valued field we mean a pair (K, V) where V is a valuation ring of K. If (K, V) and (L, W) are valued fields, then we say that (L, W) is an extension of (K, V) (we write $(K, V) \subseteq (L, W)$) if K is a subfield of L and $W \cap K = V$.
For field extensions $K \subseteq L$ and a valuation ring W of L, $V = W \cap K$ is a valuation ring of K.
Then if (L, W) is an extension of (K, V), we have that $W \cap K = V$ and $\mathfrak{m}_W \cap K = \mathfrak{m}_W \cap V = \mathfrak{m}_V$.
Consequently,the field $V/\mathfrak{m}_V$ is naturally isomorphic to a subfield the field $W/\mathfrak{m}_W$.
$(V \to W/\mathfrak{m}_W, a \mapsto \bar{a} = a + \mathfrak{m}_W)$
Then $Ker = \mathfrak{m}_W \cap K = \mathfrak{m}_V$ and thus $V/\mathfrak{m}_V \hookrightarrow W/\mathfrak{m}_W$.

The relation $W \cap K = V$ and $W^* \cap K = W^* \cap V = V^*$ (which follows from the equality $W \cap K = V$) imply that the linearly ordered group $\Gamma_V = K^*/V^*$ is naturally isomorphic to a subgroup of the linearly ordered group $\Gamma_W = L^*/W^*$. We often identify $V/\mathfrak{m}_V$ with the corresponding subfield of $W/\mathfrak{m}_W$ $(V/\mathfrak{m}_V \subseteq W/\mathfrak{m}_W)$ and Γ_V with the corresponding subgroup of Γ_W $(\Gamma_V \subseteq \Gamma_W)$.
We recall some basic facts which can be found in **[12]**.
The following theorem is crucial for what follows.

Theorem 24 *(Chevalley's Theorem) Let K be a field, $R \subseteq K$ be a subring and $P \subseteq R$ be a prime ideal of R. Then there exists a valuation ring V of K such that*

$R \subseteq V$ *and* $m \cap R = P$

Where m is the maximal ideal of V.

Remark 1 *We can add the condition that $P \neq \{0\}$ to the theorem if we want to avoid the choice that $R = K$.*

Theorem 25 *Let L/K be a field extension, and let V be a valuation ring of K. Then there is an extension W of V in L.*

Next we state an application of Chevalley's Theorem to characterize the integral closure of a domain D by means of valuation rings containing D.

Theorem 26 *Let D be a subring of a field K. Then the integral closure of D in K is the intersection of the valuation rings of K containing D.*

Integral Elements and Integral Extensions

Definition 17 *Given rings $R \subseteq S$ and $b \in S$, we say that b is integral over R if b is the root of a monic polynomial $f(x) \in R[x]$.*

S is integral over R if every $b \in S$ is integral over R. In this case we call S an integral extension of R.
E.g. $\sqrt{2}$ is integral over $\mathbb{Z}$.
Ring $\mathbb{Z}[\sqrt{2}]$ is an integral extension of $\mathbb{Z}$.
$\frac{1}{2}$ is not integral over $\mathbb{Z}$ (although it is algebraic.)

Lemma 10 *(Integral elements and finite modules). Let S be a ring, $R \subseteq S$ a subring, and $s \in S$. Then the following statements are equivalent:*
(a) The element s is integral over R.
(b) The subalgebra $R[s] \subseteq S$ generated by s is finitely generated as an R-module.
(c) There exists an $R[s]$- module M with $Ann(M) = \{0\}$ such that M is finitely generated as an R-module.

The following theorem is in perfect analogy to the result that a finitely generated field extension is finite if and only if it is algebraic. It also implies that sums and products of integral elements are again integral.

Theorem 27 *(Generated by integral elements implies integral). Let S be a ring and $R \subseteq S$ a subring such that S is finitely generated as an R-algebra, i.e. $S = R[a_1, ..., a_n]$. Then the following statements are equivalent:*
(a) All a_i are integral over R.
(b) S is integral over R.
(c) S is finitely generated as an R- module.

Corollary 10 *(Integral elements form a subalgebra). Let S be a ring and $R \subseteq S$ a subring. Then the set*

$$S' := \{s \in S : s \, is \, integral \, over \, R\} \subseteq S$$

is an R-subalgebra.

Corollary 11 *(Towers of integral extensions). Let T be a ring and $R \subseteq S \subseteq T$ subrings. If T is integral over S and S is integral over R, then T is integral over R.*

Theorem 28 *Let R be a commutative ring, u an invertible element of a ring containing R. Then u^{-1} is integral over R if and only if $u^{-1} \in R[u]$.*

Theorem 29 *Let R be an integral domain contained in a field L. If L is integral over R, then R is a field.*

Let $(K_1, V_1) \subset (K_2, V_2)$ be an arbitrary extension of valued fields . To each $V_i, i = 1, 2$, corresponds a valuation $\upsilon_i : K_i \twoheadrightarrow \Gamma_i \cup \{\infty\}$. We recall that $\upsilon_i|_{K_i^*} : K_i^* \twoheadrightarrow \Gamma_i$ is a group homomorphism with kernel V_i^* and $K_i^*/V_i^* \cong \Gamma_i$. Moreover, the composite mapping

$$K_1^* \overset{id}{\hookrightarrow} K_2^* \twoheadrightarrow K_2^*/V_2^* \cong \Gamma_2$$

has kernel $V_2^* \cap K_1^* = V_1^*$, whence $\Gamma_1 \cong K_1^*/V_1^* \hookrightarrow K_2^*/V_2^* \cong \Gamma_2$, by the homomorphism theorem. Therefore we could replace the valuation v_1 by the restriction of v_2 and may regard Γ_1 as an ordered subgroup of Γ_2. This procedure works well in the general situation where we follow this fashion. However,in the context of discrete valuation which are usually assumed to have the value group $\mathbb{Z}$, i.e. they are normalized, one prefers to keep this nice fact and accepts that the value groups are not contained in each other. Details will follow below.
Let us call $e := e(V_2|V_1) := [\Gamma_2 : \Gamma_1]$ the ramification index of this extension.

Similarly, denoting the maximal ideals by $\mathfrak{m}_1, \mathfrak{m}_2$ the composite mapping

$$V_1 \overset{id}{\hookrightarrow} V_2 \twoheadrightarrow V_2/\mathfrak{m}_2 = \mathfrak{K}_2$$

has kernel $\mathfrak{m}_2 \cap V_1 = \mathfrak{m}_1$. Thus , $\mathfrak{K}_1 = V_1/\mathfrak{m}_1 \hookrightarrow V_2/\mathfrak{m}_2 = \mathfrak{K}_2$. Therefore we may regard $\mathfrak{K}_1$ as a subfield of $\mathfrak{K}_2$.
Now, we define $f := f(V_2|V_1) := [\mathfrak{K}_2 : \mathfrak{K}_1]$ as the residue degree of this extension.
Remark: The ramification index and the residue degree are multiplicative. If $(K_1, V_1) \subset (K_2, V_2) \subset (K_3, V_3)$ are valued extension of fields, then

$$e(V_3|V_1) = e(V_3|V_2)e(V_2|V_1) \text{ and}$$
$$f(V_3|V_1) = f(V_3|V_2)f(V_2|V_1).$$

For the following lemmas, corollary and theorems upto fundamental equality one can see the proof in **[12]**.

Lemma 11 *Suppose $(K_1, V_1) \subseteq (K_2, V_2)$, and , for $i = 1, 2$,*

$$v_i : K_i \twoheadrightarrow \Gamma_i \cup \{\infty\}$$

is the valuation corresponding to V_i.
Choose $w_1, ..., w_f \in V_2$ and $\pi_1, ..., \pi_e \in K_2^*$ so that:
(1) the residues $\bar{w_1}, ..., \bar{w_f} \in \mathfrak{K}_2$ are linearly independent over $\mathfrak{K}_1$;
(2) the values $v_2(\pi_1), ..., v_2(\pi_e)$ are representatives of the distinct cosets of $\Gamma_2|\Gamma_1$.
Then for all $a_{ij} \in K_1$,

$$v_2(\sum_{i=1}^{f}\sum_{j=1}^{e} a_{ij}w_i\pi_j) = min\{v_2(a_{ij}w_i\pi_j) : 1 \leq i \leq f, 1 \leq j \leq e\}.$$

In particular, the product $\{w_i\pi_j : i = 1, ..., f, j = 1, ..., e\}$ are linearly independent over $\mathfrak{K}_1$.

The above lemma has the following immediate consequence:

Corollary 12 *Suppose $(K_1, V_1) \subseteq (K_2, V_2)$, and set $n = [K_2 : K_1], e = e(V_2|V_1)$, and $f = f(V_2|V_1)$. If $n < \infty$, then $e, f < \infty$ and $ef \leq n$.*

More generally, we can state:

Theorem 30 *For $(K_1, V_1) \subseteq (K_2, V_2)$ with K_2 algebraic over K_1 the following statements hold:*
(1) for every $\gamma \in \Gamma_2$ there is an $n \in \mathbb{N}$ such that $n\gamma \in \Gamma_1$; i.e., Γ_2/Γ_1 is a torsion group;
(2) $\mathfrak{K}_2$ is algebraic extension of $\mathfrak{K}_1$.

Theorem 31 *(Conjugation Theorem). Suppose L/K is an arbitrary normal extension of fields, V is a valuation ring of K, and V_1 and V_2 are valuation rings in L extending V. Then there exists $\sigma \in Aut(L/K)$ with $\sigma(V_1) = V_2$.*

Lemma 12 *Let N/K be a finite Galois extension of degree n. Assume that $V_1, ..., V_r$ are all extensions of the valuation ring V from K to N. Then $ref \leq n$, where $e = e(V_i/V)$ and $f = f(V_i/V)$ for all i with $1 \leq i \leq r$.*

Theorem 32 *(Fundamental Inequality). Let L/K be a finite extension of the valued field (K, V), and assume that $V_1, ..., V_r$ are all extensions of V to L. Then*

$$\sum_{i=1}^{r} e(V_i/V) f(V_i/V) \leq [L : K].$$

The next theorem shows that in case V has value group $\mathbb{Z}$ and L/K is separable, even equality holds in Fundamental Inequality.

Theorem 33 *(Fundamental Equality). Let (K, V) be a valued field with value group $\mathbb{Z}$, and let $V_1, ..., V_m$ be all extensions of V to a finite separable extension L of K. Then*

$$[L : K] = \sum_{i=1}^{m} e(V_i/V) f(V_i/V).$$

Now, let $L = \mathbb{R}(x)(\sqrt{f})$, f is a cubic polynomial over $\mathbb{R}$ with no multiple roots in $\mathbb{C}$.
$f = k(x-a)(x-b)(x-c), a, b, c$ are distinct or $f = k(x-a)(x^2+bx+c)$ where x^2+bx+c is quadratic irreducible.
If W is a real valuation ring of L, then $W \cap \mathbb{R}(x)$ is a real valuation ring of $\mathbb{R}(x)$.
So $W \cap \mathbb{R}(x) = V_\alpha, \alpha \in \mathbb{P}^1$ since $V_\alpha, \alpha \in \mathbb{P}^1$ is the collection of real valuation rings of $\mathbb{R}(x)$.

First we consider the case $\alpha \in \mathbb{R}$.

Let $y = \sqrt{f}$. Then $y^2 = f(x) \in \mathbb{R}[x] \subseteq V_\alpha \subseteq W$

Passing to the residue field $W/\mathfrak{m}_W = \mathfrak{L}$, $\overline{y}^2 = \overline{f(x)}$.

Now $f(x) - f(\alpha) = (x-\alpha)g(x) \in \mathfrak{m}_\alpha = \mathfrak{m}_V$ (as α is a root of the left hand side .)

$\Rightarrow (\overline{f(x)} - \overline{f(\alpha)} = 0$ i.e. $\overline{f(x)} = f(\alpha)$, $\overline{y}^2 = f(\alpha)$ in $\mathfrak{L}$.

$\Rightarrow f(\alpha) \geq 0$ because $\overline{y}^2 \geq 0$.

Thus if V_α has a real extension, then $f(\alpha) \geq 0$

Therefore, if L is an elliptic function field, which is a quadratic extension of $\mathbb{R}(x)$ and if W is a real valuation ring of L, then $W \cap \mathbb{R}(x) = V_\alpha, \alpha \in \mathbb{P}^1$ and $f(\alpha) \geq 0$ or $\alpha = \infty$. This latter condition is a necessary condition for the V_α, to be extendible to a real valuation ring of L. It remains to be shown that it is also a sufficient condition.

Again $V_\alpha, \alpha \in \mathbb{P}^1$ denotes the collection of real valuation rings of $\mathbb{R}(x)$ and ν_α the list of their associated discrete valuations where the value group is $\mathbb{Z}$. The valuation rings of L are denoted by W, their normalized valuation by ω, always with subscript added. $L = \mathbb{R}(x)(\sqrt{f})$, f is a cubic polynomial without multiple roots.
Since we are keeping the feature that both discrete valuations admit the value group $\mathbb{Z}$ ramification now gets expressed in the form

$$\omega|K^* = e(\omega|v).v.$$

Then V_α extends to a real valuation ring of L if and only if $f(\alpha) \geq 0$ or $\alpha = \infty$.
It remains to show that the right hand side yields a sufficient condition what will be done in three steps.
(1) $f(\alpha) = 0$

From the fundamental equality $\sum_{i=1}^{g} e_i f_i = [L : K]$, where $f_i = [\mathfrak{L} : \mathfrak{K}]$, $e_i = [\Gamma_i : \Gamma]$, g = number of extensions.
Since $[L : K] = 2$, it follows that $g \leq 2$.

Let $\omega|v_\alpha$, then $\omega|_{K^*} = e(\omega|v)v_\alpha$.
We know that extending pairs $W|V$ with associated discrete valuations ω, v exist and that in each case $\omega(K^*) = e(W|V)\mathbb{Z}$.
$y^2 = f(x) = (x - \alpha)g(x), g(\alpha) \neq 0$.
Then $2\omega(y) = \omega(x - \alpha) + \omega(g(x))$ where $\omega(g(x)) = 0$ necessarily.
Thus $2\omega(y) = \omega(x - \alpha) \Longrightarrow 2|\omega(x - \alpha)$ as $\omega(x - \alpha) = ev_\alpha(x - \alpha)$ it follows that $2|e$ since $v_\alpha(x - \alpha) = 1$. From the fundamental equality it follows that $e = 2$ and hence as $\sum_1^g e_i f_i = 2$, and $efg = 2$ we have $f = g = 1$
Then V_α has exactly one extension, it is also real and ramified.
Also $\omega(y) = 1$. Then y is a generator of maximal ideal in this case.

(2) $f(\alpha) > 0$

Let W be an extension of V_α. Then in the residue field $\mathfrak{L}$ of W we have $\overline{y}^2 = f(\alpha) > 0$, so $\overline{y} = a \in \mathbb{R}$, $a = \sqrt{f(\alpha)}$. This shows in L, $y - a \in \mathfrak{m}_W$. (since $\overline{y - a} = \overline{y} - \overline{a} = \overline{y} - a = 0$ in $\mathfrak{L} = W/\mathfrak{m}_W$). Passing to the conjugate valuation ring W' we obtain $\sigma(y - a) = -y - a \in \mathfrak{m}'$. This shows $W \neq W'$ (Otherwise $y - a, -y - a \in \mathfrak{m}_W$) that leads to $2a \in \mathfrak{m}_W$.
A contradiction as a is a real number different from zero, hence a unit.
Therefore, we have at least two extensions, and from the fundamental equality we conclude that V_α has exactly two extensions $W_\alpha^{\pm}$ each of which has residue degree equal to 1. Hence both extensions are real.

(3) $\omega|v_\infty$. Then $\omega|_K = ev_\infty$.
From $y^2 = f(x)$, $2\omega(y) = \omega(y^2) = ev_\infty(f(x)) = -3e$.

$\Longrightarrow 2|e$. Then $e = 2$ from the fundamental equality and $\omega(y) = -3$.
In particular, there is unique extension, it is ramified, has residue degree 1, therefore a real valuation.

Then $\omega(\frac{y}{1+x^2}) = -3 - ev_\infty(1+x^2) = -3 - 2(-2) = 1$.
Thus $\frac{y}{1+x^2}$ is a generator of maximal ideal in this case.

Regarding the extension of the real valuation rings $V_\alpha, \alpha \in \mathbb{P}^1$ of $\mathbb{R}(x)$ to elliptic function field L we can now summarize:

Theorem 34 *1. V_α, where $f(\alpha) = 0$, and V_∞ have just one extension W to L, it is ramified with index 2 and real, also $\sigma(W) = W$,*
2. if $f(\alpha) < 0$, then V_α has just one extension to L, it is not real, has the residue field $\mathbb{C}$, so residue degree $f = 2$,
3. if $f(\alpha) > 0$, then V_α has two extensions to L, both are real and conjugate under σ.

3.3 The Valuation Theoretic Approach to Elliptic Function Fields

Let L be an elliptic function field (or $L = \mathbb{R}(x)(\sqrt{f})$, f- monic, cubic polynomial without multiple roots in $\mathbb{C}$). We will be proceeding by quoting general theorems on Dedekind rings, e.g. cf. **[16, 38]**, and then applying those to our special situation.

Theorem 35 *The integral closure of a Dedekind ring in a finite-dimensional field extension is a Dedekind ring.*

Theorem 36 *If $A \subseteq B \subseteq K$, K the quotient field of A and A is a Dedekind ring, then B is a Dedekind ring.*

Both theorems are needed in the proof of the next proposition. Assume L/K be a finite field extension and hence it is an algebraic extension. Further, let both fields be formally real.

Proposition 18 *(1) $H(K) \subseteq H(L)$,*
(2) if H(K) is a Dedekind domain, then H(L) is as well.

Proof. To show the first statement we note that if W is a real valuation ring of L, then its restriction $V := W \cap K$ is a real valuation ring since the residue field of V is a subfield of the residue field of W and the property of being formally real goes down from larger field to any of its subfield.
For the second statement pass to the integral closure R of $H(K)$ in L. Then the ring R is a Dedekind domain by the theorem 35 above. Since $H(L)$ is integrally closed in L, being a prüfer domain, we get that $H(K) \subseteq R \subseteq H(L)$. So , by theorem 36 above, we get that $H(L)$ is a Dedekind ring provided it can be shown that L is the quotient field of R.

To prove this let $a \in L$. Since the field extension L/K is algebraic we get an equation $a^n + \sum_1^n \alpha_i a^{n-i} = 0$ where the coefficients α_i belong to K. This implies that we have a representation $\alpha_i = h_i/s$ where $h_i, s \in H(K)$. Inserting this in the equation for a and multiplying the whole equation by s^n we find that the element sa is integral over $H(K)$, so belongs to R. Hence $a = (as)/s \in quot(R)$, and the final claim is proven.

Theorem 37 *A, K as in preceding theorem. If $A = \cap V_\alpha$, each V_α discrete valuation ring of K, then the family (V_α) is the family of all localizations A_M, M running through all maximal ideals of A.*

Theorem 38 *If A is Dedekind, $f \in K^*$, then $fA = \Pi_{\mathfrak{m}} \mathfrak{m}^{v_{\mathfrak{m}}(f)}$ where $\mathfrak{m}$ runs over all maximal ideals of A and $v_{\mathfrak{m}}$ is the normalized discrete valuation attached to the valuation ring $A_{\mathfrak{m}}$.*

Let $K = \mathbb{R}(x)$ and $L = \mathbb{R}(x)(\sqrt{f})$, where f is a cubic polynomial with no multiple roots. Invoking proposition 18 we first state

Proposition 19 *H(L) is a Dedekind ring.*

By definition, H(L) $= \cap W$, where W runs through the real valuation rings of L.
Since $W \cap \mathbb{R}(x)$ is a real valuation ring of $\mathbb{R}(x)$, it follows that
$W \cap \mathbb{R}(x) = V_\alpha$, some $\alpha \in \mathbb{P}^1$. We know that the α' s that occur are characterized by $f(\alpha) \geq 0$ or $\alpha = \infty$.

Therefore,

$$H(L) = (\bigcap_{\alpha: f(\alpha)=0} W_\alpha) \cap W_\infty \cap \bigcap_{\alpha: f(\alpha)>0} (W_\alpha^+ \cap W_\alpha^-).$$

As $L = \mathbb{R}(x)(\sqrt{f})$ where f is monic, cubic polynomial without multiple roots in $\mathbb{C}$. i.e. $L = \{a + b\sqrt{f} : a, b \in \mathbb{R}(x)\}$, we can write out $H(L)$ even more explicitly.

Now, we calculate

$$H(L) \cap K = \bigcap_{f(\alpha)=0} (W_\alpha \cap K) \cap (W_\infty \cap K) \cap \bigcap_{f(\alpha)>0} [(W_\alpha^+ \cap K) \cap (W_\alpha^- \cap K)]$$

$$= \bigcap_{f(\alpha)=0} V_\alpha \cap V_\infty \cap \bigcap_{f(\alpha)>0} V_\alpha = \bigcap_{f(\alpha)\geq 0} V_\alpha \cap V_\infty$$

.

Clearly,

$$H(K) = \bigcap_{\beta \in \mathbb{R}} V_\beta \cap V_\infty \subseteq H(L) \cap K$$

Now, by theorem 26 the integral closure of $H(L) \cap K$ in L can be computed as follows. First of all:

$$\widetilde{H(L) \cap K} = \bigcap_{H(L) \cap K \subseteq W} W.$$

From the presentation of $H(L) \cap K$, theorem 37 and the fact that W is a real valuation ring we have that $W = W_\alpha, W_\alpha^\pm, f(\alpha) \geq 0$ or $\alpha = \infty$.
$\Longrightarrow \widetilde{H(L) \cap K} = \bigcap_{f(\alpha)\geq 0} W_\alpha \cap (W_\alpha^\pm) \cap W_\infty$
i.e. $\widetilde{H(L) \cap K} = H(L)$. Hence we have

Theorem 39 *H(L) is the integral closure of* $H(L) \cap K$.

Using trace and the norm we can characterize when an element is integral. Using the above informations, let $z \in L$ that is $z = a + b\sqrt{f}, a, b \in \mathbb{R}(x)$ and z be integral over $H(L) \cap K$.

Then we know that (i) z is integral implies that $\sigma(z)$ integral,
(ii) Sums and products of integral elements also integral.
We can conclude that z integral over $H(L) \cap K$ if and only if $tr(z), N(z)$ in $H(L) \cap K$. As $tr(z) = 2a$, $N(z) = a^2 - b^2 f$, thus z integral over $H(L) \cap K$ if and only if $a \in H(L) \cap K$, $a^2 - b^2 f \in H(L) \cap K$. From statements in (i) and (ii) above we get that $b^2 f \in H(L) \cap K = V_\alpha, f(\alpha) \geq 0$ or $\alpha = \infty$. Now $\upsilon_\alpha(b^2 f) \geq 0$ since $b^2 f \in H(L) \cap K$ where υ_α is a valuation correspond to the valuation ring V_α in K. Thus, $\upsilon_\alpha(b) \geq 0$ since $\upsilon_\alpha(f) = 1, f = (x - \alpha)g(x)$

For $\alpha = \infty, \upsilon_\alpha(b) \geq 2$.

Therefore if $z \in L$ is integral over $H(L) \cap K$ it is of the form $z = a + b\sqrt{f}, a, b \in H(L) \cap K, \upsilon_\infty(b) \geq 2$.

In contrast, $L = \mathbb{R}(x)\sqrt{f} = \{a + b\sqrt{f} : a, b \in \mathbb{R}(x)\}$ where f is a monic, cubic polynomial over $\mathbb{R}$ without multiple roots in $\mathbb{C}$.
A similar presentation can be obtained for $H(L)$. To this end we choose any $t \in K$ subject to $\upsilon_\alpha(t) = 0$ if $f(\alpha) \geq 0, \upsilon_\infty(t) = 2$, e.g. $t = \frac{1}{1+x^2}$. Then, it can be deduced from the result above:

Proposition 20 *i.* $H(L) = \{z = a + b\sqrt{f} : a, b \in H(L) \cap K, \upsilon_\infty(b) \geq 2\}$
ii. Choose any $t \in H(L) \cap K$ *with* $\upsilon_\infty(t) = 2, \upsilon_\alpha(t) = 0$ *if* $f(\alpha) \geq 0$ *then* $H(L) = \{z = a + b \cdot t\sqrt{f} : a, b \in H(L) \cap K\}$.

The remaining part of this section is devoted to explicit computations in the elliptic function field L. The first task is to calculate the values of real valuations of L. This will then be applied to determing generators of the maximal ideals of $H(L)$.

Conjugate valuations and calculation of $\omega(z)$
As before $K = \mathbb{R}(x), L = \mathbb{R}(x)\sqrt{f}$ where f is monic, cubic polynomial with out multiple roots in $\mathbb{C}$ over $\mathbb{R}$.

The quadratic extension L/K admits the conjugation
$\sigma : L \to L, a + by \mapsto a - by$. This is a field automorphism, trivial on K.
L/K is a Galois extension with Galois group $\{id, \sigma\}$.

Lemma 13 *If W is any valuation ring of L with maximal ideal I, residue field k, then* $\sigma(W)$ *is also a valuation ring of L. Its maximal ideal* $\sigma(I)$*, its residue field is isomorphic to k.*

As a consequence we get that real valuation rings are transferred into real valuation rings.
Using our information on the real valuation rings of L, cf. theorem 34, we obtain:

Proposition 21 *(i) If* W_α *is ramified over* V_α*,i.e.* $f(\alpha) = 0$ *or* $\alpha = \infty$*, then* $\sigma(W_\alpha) = W_\alpha$*,*
(ii)if $f(\alpha) > 0$*, then* $\sigma(W_\alpha^+) = W_\alpha^-, \sigma(W_\alpha^-) = W_\alpha^+$.

This fact has nice consequences for the normalized discrete valuations attached to the valuation rings. Let W denote any discrete valuation ring and $W^{'} = \sigma(W), z = \epsilon\pi^k, \epsilon$ a unit, π a uniformizing element. Then $I = (\pi)$, so $I^{'} = (\sigma(\pi))$ is the maximal ideal of $W^{'}$, i.e. $\sigma(\pi) = \eta\pi^{'}, \eta$ a unit in $W^{'}$. We get $\sigma(z) = \sigma(\epsilon)\eta^k\pi^{'k}$. Now, units map to units under $\sigma|W : W \to W^{'}$. As a result we get:

Corollary 13 *(i) If $f(\alpha) = 0$, then $\omega_\alpha = \omega_\alpha \circ \sigma$,*
(ii) if $f(\alpha) > 0$, then $\omega_\alpha^- \circ \sigma = \omega_\alpha^+, \omega_\alpha^+ \circ \sigma = \omega_\alpha^-$.

These relationships allow an efficient way to calculate the values
$\omega(a + by), a, b \in K = \mathbb{R}(x), y^2 = f(x)$.
(1) If $f(\alpha) = 0$, then $\omega_\alpha(z) = \upsilon_\alpha(N(z))$,
(2) if $f(\alpha) > 0$, then $\omega_\alpha^+(z) + \omega_\alpha^-(z) = \upsilon_\alpha(N(z))$.
Where for $z = a + by, N(z) = a^2 - b^2 f = z.\sigma(z), tr(z) = 2a = z + \sigma(z)$.
To prove we use the fact $\omega(z) + (\omega \circ \sigma)(z) = \omega(N(z)) = e(w|v).\upsilon(N(z))$ and the corollary. Note that we know how to calculate the valuations υ_α, so $\upsilon_\alpha(N(z))$ is computable using the rules above.

We now turn to the determination of generators of the maximal ideals $\mathfrak{m} = I \cap H(L)$ where I runs through the maximal ideals of the real valuations rings W of L. $\upsilon_\mathfrak{m}$ denotes the normalized discrete valuation belonging to $H_\mathfrak{m} = W$ or to $\mathfrak{m}$, for short. The use of indices will indicate which real valuation ring we are considering. We recall that in our situation of $H = H(L)$: if $\mathfrak{a} = (a_1, ..., a_n)$ then $\mathfrak{a}^2 = (\sum_i a_i^2)$.

This fact allow us to find generators of maximal ideals of H in a systematic fashion . Let $\mathfrak{m}$ be a maximal ideal of H. Then clearly there is no ideal strictly between $\mathfrak{m}^2$ and $\mathfrak{m}$. Now, we know that $\mathfrak{m}^2 = (a)$. Choose any $b \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then we get $\mathfrak{m} = (a, b)$.

So, it remains to find such elements a, b. Applying theorem (38) we get
(1) $\mathfrak{m}^2 = (a)$ iff $\upsilon_\mathfrak{m}(a) = 2, \upsilon_{\mathfrak{m}^{'}}(a) = 0$ for all maximal ideals $\mathfrak{m}^{'} \neq \mathfrak{m}$,
(2) $b \in \mathfrak{m} \setminus \mathfrak{m}^2$ iff $b \in A, \upsilon_\mathfrak{m}(b) = 1$.

In the sequel $\alpha \in \mathbb{R}$, and we assume $f(0) = 0$ what can be reached by substituting x for $x - \alpha$ where $f(\alpha) = 0$. The ideals are ideals of H(L).
(1) $\mathfrak{m}_\infty$ must contain the elements $1/(1 + x^2), x/(1 + x^2), y/(1 + x^2)$ since they are in H(L) and their values with respect to ω_∞ are 4, 2, 1 respectively. In case of ω_0 we have the values 0, 2, 1, in case of $\omega_\alpha, \alpha \neq 0, f(\alpha) = 0$ (if this case occurs at all) the values are 0, 0, 1, in case of $\omega_\alpha^\pm, f(\alpha) > 0$ the values are 0, 0, 0. So we find that

$$a := (1/(1 + x^2)) + (y/(1 + x^2))^2 = (1 + x^2 + y^2)/(1 + x^2)^2$$

satisfies the condition (1). In doing the calculation we apply the fact that $\omega(\sum_i q_i) = min\{\omega(q_i)\}$ holds for any real valuation ω and sums of squares q_i. Finally we get that $\mathfrak{m}_\infty = (a, b := y/(1 + x^2))$,
(2) the ideal $\mathfrak{m}_0$ must contain the elements $x/(1+x^2), x^2/(1+x^2), y/(1+x^2)$. This time $a = \frac{x^2}{1+x^2} + (\frac{y}{1+x^2})^2, b = \frac{y}{1+x^2}$,
(3) in the case that α exists with $\alpha \neq 0, f(\alpha) = 0$ the ideal $\mathfrak{m}_\alpha$ must contain the elements $(x - \alpha)/(1 + x^2), (x - \alpha)^2/(1 + x^2), y/(1 + x^2)$. This time $a = \frac{(x-\alpha)^2(1+x^2+y^2)}{(1+x^2)^2}, b = \frac{y}{1+x^2}$,

(4) finally assume $f(\alpha) > 0$, and let $\beta^2 = f(\alpha)$. Then the ideal $\mathfrak{m}_\alpha^+$ must contain the elements $(x-\alpha)/(1+x^2), (x-\alpha)^2/(1+x^2), (y-\beta)/(1+x^2)$. This time $a = \frac{(x-\alpha)^2(1+x^2+(y-\beta)^2)}{(1+x^2)^2}, b = \frac{x-\alpha}{1+x^2}$.
To get $\mathfrak{m}_\alpha^-$ we change β into $-\beta$.

3.4 The Geometric Approach to Elliptic Function Fields

The following facts from ring theory are useful in understanding the geometric approach.
(1) Let A be a Dedekind domain with field of quotients K, $\mathfrak{m}$ a maximal ideal of A. Then the inclusion $\iota : A \to A_m, a \mapsto \frac{a}{1}$ induces an isomorphism $\tilde{\iota} : A/\mathfrak{m} \to A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$. Hence, $A_\mathfrak{m}$ is a real valuation ring iff the residue field $A/\mathfrak{m}$ is formally real.
(2) Let $\phi : A \to B$ be an epimorphism of rings. Then the assignment $\mathfrak{m} \mapsto \phi^{-1}(\mathfrak{m})$ is a bijection between the set of maximal ideals of B and the set of maximal ideals of A which contain the the kernel $ker(\phi)$. This bijection preserves the residue fields, i.e. ϕ induces an isomorphism
$\tilde{\phi} : A/\phi^{-1}(\mathfrak{m}) \to B/\mathfrak{m}$.

As before, let $K = \mathbb{R}(x), L = K(\sqrt{f}), y = \sqrt{f},$ and $W_\alpha, W_\alpha^\pm$ where $f(\alpha) \geq 0, W_\infty$ the collection of the real valuation rings of L. As usual, $\deg(f) = 3$, no multiple roots in $\mathbb{C}$
Set $A = \mathbb{R}[x]$,then $B = \mathbb{R}[x,y] = \mathbb{R}[x] + \mathbb{R}[x]y$ is the integral closure of A in L. This can be directly be seen by looking at the trace and norm of the elements in L.
Then the $W_\alpha, W_\alpha^\pm$ are overrings of B, and W_∞ is not, the latter in view of $w_\infty(x) = -2$. The ring B, being the integral closure of the Dedekind domain A (in fact a PID), is a Dedekind domain with field of quotients equal to L. By the first statement above, the $W_\alpha, W_\alpha^\pm$ are exactly the localizations $A_\mathfrak{m}$ where $\mathfrak{m}$ runs through the maximal ideals of A with a formally real residue field which in this case amounts to having $\mathbb{R}$ as residue field.

The kernel of the epimorphism

$$\phi : \mathbb{R}[X,Y] \to B, F(X,Y) \mapsto F(x,y).$$

equals the principal ideal $(Y^2 - f(X))$. The maximal ideals of $\mathbb{R}[X,Y]$ with residue field $\mathbb{R}$ are the ideals

$$\mathfrak{m}_{a,b} := (X-a, Y-b) = \{F(X,Y) \in \mathbb{R}[X,Y] : F(a,b) = 0\}, (a,b) \in \mathbb{R}^2$$

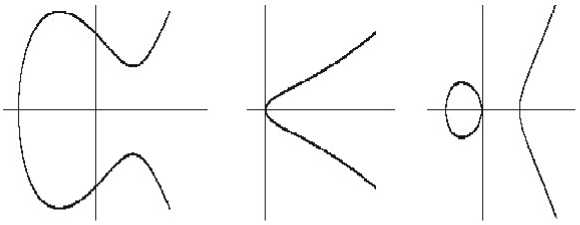
.
Finally we get that

$$(Y^2 - f(X)) \subseteq \mathfrak{m}_{a,b} \Leftrightarrow b^2 - f(a) = 0.$$

Hence, we are led to consider the elliptic curve defined by the equation $Y^2 - f(X) = 0$. More precisely, we have to study the set Γ of real points on this curve:

$$\Gamma = \{(\alpha, \beta) \in \mathbb{R}^2 : \beta^2 = f(\alpha)\}.$$

What was demonstrated above means, first of all, that the $W_\alpha, W_\alpha^\pm$ are in one-to-one correspondence with the points of the elliptic curve. But much more is true: we will use this fact to describe the real valuation rings and the real places of L in a different, i.e. geometric manner.



We first turn to

The valuation rings $W \neq W_\infty$ and their real places

With this curve at hand there is now no need to preserve the notation $W_\alpha^\pm$. Instead we are using uniformily the latter $\gamma = (\alpha, \beta)$ to denote the points on Γ. A point γ gives rise to a maximal ideal

$$\mathfrak{M}_\gamma = \{F(X,Y) : F(\gamma) = 0\} = (X - \alpha, Y - \beta) \subseteq \mathbb{R}[X,Y].$$

As said above, these are all the maximal ideals containing the kernel of Φ. Invoking the fact (2) from the beginning of this section we obtain that the images $\mathfrak{m}_\gamma := \Phi(\mathfrak{M}_\gamma)$ constitute the complete list of the maximal ideals of the $\mathbb{R}$-algebra admitting a real residue field. Using fact (1) from above we get all real valuation rings containing B as the localizations at these $\mathfrak{m}_\gamma$.

We can therefore summarize:

Theorem 40 *Let $\gamma = (\alpha, \beta) \in \Gamma$. Then*

$$\mathfrak{m}_\gamma = \{F(x,y) : F(\gamma) = 0\} = (x - \alpha, y - \beta)$$

is a maximal ideal of B with a real residue field inducing the real valuation ring

$$W_\gamma = B_{\mathfrak{m}_\gamma} = \{\frac{F(x,y)}{G(x,y)} : F, G \in \mathbb{R}[X,Y], G(\gamma) \neq 0\}.$$

In this way we obtain all real valuation rings of L, $\neq W_\infty$, in a one-to-one correspondence.

The result allows us to determine the real places attached to the real valuation ring W_γ. The real place attached to W_γ is denoted by λ_γ.

Corollary 14 *Given $z \in L$, then*
$\lambda(z) \neq \infty \Leftrightarrow z = F(x,y)/G(x,y)$ where $F, G \in \mathbb{R}[X,Y], G(\gamma) \neq 0$. In that case $\lambda(z) = F(\gamma)/G(\gamma)$.

Finally, we address

The case of W_∞

W_∞ is the only extension of V_∞, ramification index 2, $\omega_\infty(y) = -3$, $\omega_\infty(y/(1+x^2) = 1$. We set $\bar{y} := y/(1+x^2)$ and find that $\bar{y} \in J_\infty$, by definition the maximal ideal of W_∞. Also, $\bar{y} \in H(L)$ and

$$W_\infty = \{a(x) + b(x)\bar{y} : a(x), b(x) \in V_\infty\}.$$

Similar to the geometric interpretation of the infinite place λ_∞ of $\mathbb{R}(x)$ we consider the associated elliptic curve Γ and get completely analogous results.

If $\gamma \in \mathbb{R}^2$ we let $|\gamma|$ denote the Euclidean norm. First note that Γ admits points γ with $|\gamma| \to \infty$.

By F we denote the rational function $a(X) + b(X)Y \in \mathbb{R}(X, Y)$, set $z = F(x, y)$ and evaluate z at points of Γ. There are special instances, which follow directly:

$$\lim_{|\gamma|\to\infty} \bar{y}(\gamma) = 0, \lim_{|\gamma|\to\infty} a(\gamma) \text{ exists } \Leftrightarrow a \in V_\infty.$$

With the help of this remark and the arguments regarding the infinite place λ_∞ on $\mathbb{R}(x)$ one derives the following

Proposition 22 *(1) $lim_{\gamma\in\Gamma,|\gamma|\to\infty}F(\gamma)$ exists iff $z \in W_\infty$,*
(2) if $z \in W_\infty$, then $\lambda_\infty(z) = lim_{\gamma\in\Gamma,|\gamma|\to\infty}F(\gamma) = lim_{|u|\to\infty}a(u)$.

3.5 Topological Representation

In this section we briefly present the geometric interpretation of the general representation

$$H \to C(M, \mathbb{R})$$

along the line we had followed for the rational functional field in section 2.4. Since the arguments are completely parallel we omit the details.

Suggested by the previous section we are led to consider the one-point compactification $\widehat{\Gamma} := \Gamma \cup \infty$. In geometric terms, this means we are passing from the affine curve, given by $Y^2 - f(X) = 0$, to its projective closure described by $Y^2Z - f^*(X, Z) = 0$ where $f^*(Y, Z) = Z^3 f(X/Z)$. One realizes that only one point "at infinity" gets added, with homogeneous coordinates $[0 : 1 : 0]$.

Topologically, passing from Γ to $\widehat{\Gamma}$ means to add to the unbounded component (which always exists) of Γ a point at infinity. In this way, the unbounded component gets "compactified" to a homeomorphic image of S^1. The bounded component, if it exists, is also homeomorphic to S^1. Hence, up to homeomorphisms, $\widehat{\Gamma}$ is of the topological type of one or two copies of S^1.

In topological terms, the last two propositions of section 3.4 states that each $z \in H(L)$ induces by evaluation a continous function $\tilde{z} : \widehat{\Gamma} \to \mathbb{R}$. Appealing to the bijection between the space of real places and the $\widehat{\Gamma}$ and transfering the arguments from the situation in the rational function field case, cf. section 2.4, we get this time analogously:

Theorem 41 *1. The map $\widehat{\Gamma} \to M(L), \gamma \mapsto \lambda_\gamma$ is a homeomorphism,*

2. the representation $H(L) \to C(\widehat{\Gamma}, \mathbb{R})$ has a dense image.

Chapter 4

Totally Positive Units and Sums of Powers

4.1 The Units of H

In this section we confine ourselves to the rational function field case. This is done for getting greater clarity regarding results and proofs. It is clear that statements of this type can be obtained in greater generality but at the price of applying a more abstract approach. Instead, as explained in the introduction, we want to make use of all favourable features of the special fields we are considering. Not all what has been proven directly for $\mathbb{R}(x)$ has found a similar proof for the elliptic case so far.

As said we consider the field $\mathbb{R}(x)$ in this section. Here we will prove that each totally positive unit is a sum of $2n-th$ powers for every n, in particular this is true for the totally positive unit $\frac{1+x^2}{2+x^2}$.

The proof will make use of the density result and the famous Hilbert's identities. These results are the basis for the bounds on Pythagoras numbers.

We will make use of the characterization
$f \in \mathbb{E} \Leftrightarrow \hat{f}$ has no zero on $\mathbb{P}^1$,
$f \in \mathbb{E}_+ \Leftrightarrow \hat{f} > 0$ on $\mathbb{P}^1$.

We note also that $\sum_i a_i^{2n} \in H$ implies that all $a_i \in H$ and that every sum of squares is a sum of two squares.

Hilbert's Identities

(1.1) For $k, n \in \mathbb{N}$

$$\left(\sum_{i=0}^{k} x_i^2\right)^n = \sum_{i=1}^{l} \alpha_i L_i(x_0, ..., x_k)^{2n}$$

(1.2)

$$\left(\sum_{i=0}^{k} x_i^2\right)^n + 2nx_0^2\left(\sum_{i=0}^{k} x_i^2\right)^{n-1} = \sum_{i=1}^{l'} \alpha_i L_i(x_0, ..., x_k)^{2n}$$

with $\alpha_i \in \mathbb{Q}, \alpha_i > 0$, linear forms $L_i \in \mathbb{Q}[x_0, ..., x_k]$ and
$l \leq \binom{2n+k}{k}$, $l' \leq \binom{2n+k}{k}$

Let $a \in \mathbb{E}_+$.

We look at the associated continuous function $\hat{a} : \mathbb{P}^1 \to \mathbb{R}$. $\hat{a}$ is strictly positive on the compact space. Consider $\widehat{a^{-1}}$ and $2.\widehat{a^{-1}}$. Both are strictly positive continuous functions. One can find a strictly positive function $f : \mathbb{P}^1 \to \mathbb{R}$ whose $2n-th$ power strictly lies between these two functions. f can be approximated as closely as wanted (Stone-Weierstraß). In particular, this means we can find $b \in H$ such that

$$\hat{b}^{2n} \text{ also lies strictly between the two functions.}$$

We now pass to the element $c := ab^{2n}$. Then we get $\hat{c}$ lies strictly between 1 and 2. As $\hat{b}^{2n}$ is strictly between $\widehat{a^{-1}}$ and $2.\widehat{a^{-1}}$ i.e. to say $\widehat{a^{-1}} < \hat{b}^{2n} < 2.\widehat{a^{-1}}$ multiplying throughout by $\hat{a}$ we get $1 < \hat{a}\hat{b}^{2n} < 2$ where ($\hat{c} = \hat{a}\hat{b}^{2n}$). Thus $\widehat{c-1}$ is strictly positive on $\mathbb{P}^1$, and all its value are strictly smaller than 1. This implies that $c-1 = u^2+v^2, u, v \in H$. It follows that the absolute values of $\hat{u}, \hat{v}$ are strictly smaller than 1. As $1 \leq n$, both elements $n-u^2, n-v^2$ are sums of squares, i.e. $n-u^2 = u_1^2+u_2^2$, $n-v^2 = v_1^2+v_2^2$, where all elements are in H. We now apply the Hilbert identity (1.2) for $k=2, x_0 = u, x_i = u_i$ and $k=2, x_0 = v, x_i = v_i$ respectively.

In the first case we get

$$\left(\sum_{i=0}^{2} x_i^2\right)^n + 2nx_0^2\left(\sum_{i=0}^{2} x_i^2\right)^{n-1} = \sum_{i=1}^{l'} \alpha_i L_i(x_0, x_1, x_2)^{2n}$$

i.e. $(x_0^2+x_1^2+x_2^2)^n + 2nx_0^2(x_0^2+x_1^2+x_2^2)^{n-1}$

$$= (u^2+u_1^2+u_2^2)^n + 2nu^2(u^2+u_1^2+u_2^2)^{n-1}$$

$$= n^n + 2n.u^2.n^{n-1} \in \sum H^{2n}$$

Dividing by $2n^n$ we get

$$\frac{n^n + 2n.u^2.n^{n-1}}{2n^n} = \frac{1}{2} + u^2 \in \sum H^{2n}$$

The same conclusion holds for v i.e $\frac{1}{2} + v^2 \in \sum H^{2n}$

Then $\frac{1}{2}+u^2+\frac{1}{2}+v^2 \in \sum H^{2n}$. So we derive that $c = 1+u^2+v^2 \in \sum H^{2n}$ As $c := ab^{2n}$, finally that $a \in \sum H^{2n}$

That means we have proved (for $K = \mathbb{R}(x)$) the following.

Theorem 42 $\mathbb{E}_+ \subseteq \cap_n \sum K^{2n}$

In elliptic function field L also $H^* \cap \sum L^2 \subseteq \cap \sum L^{2n}$, i.e $\mathbb{E}_+ \subseteq \cap_n \sum L^{2n}$
Remark: J.Schmidt has proved that even more $\mathbb{E}_+ = \sum(\mathbb{E}_+)^{2n}$.
(See [4] for the details)
Note: This Schmidt's theorem has interesting application for the bound on Pythagoras numbers.

In 1981, at a conference on Real Algebraic Geometry and Ordered Fields in Rennes, France, Professor Becker gave a talk in which he proved that

$$B(t) := \frac{1+t^2}{2+t^2} \in \mathbb{Q}(t)$$

is a sum $2n-th$ powers of elements in $\mathbb{Q}(t)$ for all n.
That is for all $k \geq 1$, there exists $0 < \lambda_{j,k} \in \mathbb{Q}$ and polynomials $f_{j,k}$ and $g_{j,k}$ in $\mathbb{Q}[t]$ such that

$$B(t) = \frac{1+t^2}{2+t^2} = \sum \lambda_{j,k} \left(\frac{f_{j,k}(t)}{g_{j,k}(t)} \right)^{2k}$$

Explicit version for this are known for $k = 1, 2$ and there has been interest in finding them for all k. (For complete solution on $\mathbb{R}(t)$ see **([26], [27])**.

4.2 The Valuation Criterion for Sums of Powers

We begin with the following lemma.

Lemma 14 *Every fractional $H-$ideal is generated by two elements.*

Proof. Let $\mathfrak{a}$ be a fractional ideal. We know that it is finitely generated and we find $\mathfrak{a}^2 = (\sum_i^k a_i^2)$. Since every sum of squares is a sum of two squares we get that $\mathfrak{a}^2 = (b^2 + c^2) = \mathfrak{b}^2$ where $\mathfrak{b} = (b, c)$. Since all non-zero fractional ideals are invertible in this case we obtain that $\mathfrak{a}^2\mathfrak{b}^{-2} = (\mathfrak{a}\mathfrak{b}^{-1})^2 = H$. That is we get $\mathfrak{c}^2 = H$. This implies that $\mathfrak{c} = H$ and finally $\mathfrak{a} = \mathfrak{b}$.

Theorem 43 *(Becker's Valuation Criterion). Given $a \in \mathbb{R}(x)$ then the following statements are equivalent:*
(1) a is a sum of 2n-th powers in $\mathbb{R}(x)$,
(2) (a) a is a sum of squares, i.e. totally positive in $\mathbb{R}(x)$,
(b) $\upsilon(a) \in 2n\mathbb{Z}$ for every (surjective) real valuation $\upsilon : \mathbb{R}(x) \to \mathbb{Z} \cup \infty$.

Proof. Assume (2) and consider the element a with the given properties. We take $aH = \Pi_{\alpha \in \mathbb{P}^1} \mathfrak{m}_\alpha^{\upsilon_\alpha(a)}$. Since all values $\upsilon(a)$ are multiples of $2n$ we get that $aH = \mathfrak{a}^{2n}, \mathfrak{a}$ a fractional H-ideal. We know that every fractional ideal is generated by two elements. This leads to $aH = (b^{2n} + c^{2n})$. Two generators of a principal fractional ideal differ by a unit of H. Hence, $a = \epsilon[b^{2n} + c^{2n}], \epsilon$ a unit of H. Now as a is assumed to be a sum of squares, the unit ϵ is totally positive as well, i.e. $\epsilon \in \mathbb{E}_+$. Hence the claim.
The above theorem holds for elliptic case as well.

Theorem 44 *Let L be an ellptic function field. Then*
$f \in \sum L^{2n} \Leftrightarrow f \in \sum L^2, 2n | \upsilon_\gamma(f), \quad \forall \gamma \in \Gamma \cup \infty$

4.3 Sums of Mixed Powers

It was R. Berr who published in **[6]** an important generalization of the Valuation Criterion above to include sums of mixed even powers, i.e. elements of $\sum_i \sum K^{2n_i}$ where the n_i belong to some finite or infinite set of natural numbers. We quote it for arbitrary formally real fields.

Theorem 45 *Let K be any formally real field and I a non-empty set of natural numbers. Then the following statements are equivalent:*
(1) $a \in \sum_{n\in I} \sum K^{2n}$
(2) (i) $a \in \sum K^2$,
(ii) for each real valuation v we have $v(a) \in \cup_{n\in I} 2n\Gamma, \Gamma$ *the value group of* v.

From Berr's theorem we get that a polynomial $f \in \mathbb{R}[x]$ admits a representation

$$f \in \sum_{n\in I} \sum \mathbb{R}(x)^{2n}$$

if and only if f satisfies:
(1) f is positive semidefinite.
(2) $degf \in \cup_{n\in I} 2n\mathbb{Z}$.
(3) $ord(\alpha) \in \cup_{n\in I} 2n\mathbb{Z}$ for every real root α of f.

Before moving on we consider special cases.

(1) Let $q_1, ..., q_k \in \mathbb{R}[x]$ be irreducible, positive definite quadratic polynomials.
Then a polynomial f of the form

$$f = (x - r_1)^{2n_1} ... (x - r_t)^{2n_t} q_1 ... q_k$$

admits in $\mathbb{R}(x)$ a representation as a sum of mixed powers of degree I, i.e. $I = \{n_1, ..., n_t, \sum n_i + k\}$.

(2) Let $f = (x-1)^4(x-2)^6(x^2+1)$.
$degf = 12$. By the valuation criterion $f \notin \sum \mathbb{R}(x)^4$ and $f \notin \sum \mathbb{R}(x)^6$.

As f is positive semidefinite ($f \geq 0$), $degf \in \cup_{n\in I} 2n\mathbb{Z}$ where $I = \{2, 3, 6\}$ and $ord(\alpha) \in \cup_{n\in I} 2n\mathbb{Z}$ for $\alpha = 1, 2$ which are real roots of f.

Therefore, $f \in \sum \mathbb{R}(x)^4 + \sum \mathbb{R}(x)^6$.

How can we find such a presentation? The idea to find it in this special case is already strong enough to provide the basis for a quite general result which will be proven in a moment. In our given case we set

$$g = (x-1)(x-2)^2, h = (x-1)(x-2) \text{ then}$$

$$g^4 + h^6 = (x-1)^4(x-2)^6[(x-1)^2 + (x-2)^2] = f \cdot \epsilon \text{ where } \epsilon = \frac{2x^2 - 6x + 5}{x^2 + 1} \in \mathbb{E}_+$$

This implies

$$f = \epsilon^{-1}(g^4 + h^6).$$

ϵ^{-1}, as a totally positive unit, is contained in $\sum \mathbb{R}(x)^4 \cap \sum \mathbb{R}(x)^6$. Hence, the claim on f is proven.

To prepare the next result we recall some of the features of $H = H(\mathbb{R}(x))$: H is a Dedekind ring, the square of a maximal ideal is a principal ideal, the totally positive units are sums of $2n$th powers for every n. In fact,

$$\mathfrak{m}_\infty^2 = (\frac{1}{1+x^2}), \mathfrak{m}_\alpha^2 = (\frac{(x-\alpha)^2}{1+x^2}).$$

To facilitate notation we denote by p's the above generators of the square of the maximal ideals. Note that they are sums of squares.
Now consider any non-zero $f \in \sum \mathbb{R}(x)^2$. We know that all values $\upsilon_\alpha(f), \alpha \in \mathbb{P}^1$ are even, only finitely many of them are non-zero. Set $e_\alpha = (1/2)\upsilon_\alpha(f)$. Then

$$fH = \prod_{\alpha \in \mathbb{P}^1} \mathfrak{m}_\alpha^{2e_\alpha} \text{ implying } f = \eta \prod_{\alpha \in \mathbb{P}^1} p_\alpha^{e_\alpha}, \eta \in \mathbb{E}_+.$$

To simplify the notation even further we denote by $p_1, \ldots, p_k$ the generators occuring in the product formula, i.e. admitting a non-zero exponent e_i. In analogy to the example above we set

$$a_i = p_i \cdot \prod_{j \neq i} p_j^{l_i} \text{ where } l_i e_i \geq e_j \text{ if } j \neq i.$$

By summing up $a_i^{e_i}, i = 1, \ldots, k$ we calculate

$$\sum_1^k a_i^{e_i} = f \cdot \sum_i \prod_{j \neq i} p_j^{l_i e_i - e_j}.$$

The sum is denoted by S and belongs to the real holomorphy ring H since all exponents are non-negative. The individual terms in this sum are sums of squares, so we can easily compute the value $\upsilon_\alpha(S)$ by calculating the minimum of the values of the individual terms. Note that $(p_i) = \mathfrak{m}_i^2$. If $\mathfrak{m}_\alpha \neq \mathfrak{m}_i$ for all $i = 1, \ldots, k$ then all $\upsilon_\alpha(\prod_{j \neq i}) = 0$, whence $\upsilon_\alpha(S) = 0$. If $\mathfrak{m}_\alpha = \mathfrak{m}_i$ then $\upsilon_\alpha(\prod_{j \neq i}) = 0$ as $\upsilon_\alpha(p_j) = 0$ for $j \neq i$. Therefore, $\upsilon_\alpha(S) = 0$ as well.

Thus we have proven that $S \in \mathbb{E}_+$. Setting $\epsilon = S^{-1}$ we can formulate

Theorem 46 *Let $f \in \sum \mathbb{R}(x)^2, f \neq 0$, set $\upsilon_\alpha(f) = 2e_\alpha$ for $\alpha \in \mathbb{P}^1$. Denote by $e_1, \ldots, e_k$ the list of the non-zero e_α's. Then there are non-zero sums of non-squares $q_1, \ldots, q_k$ and a totally positive unit ϵ such that*

$$f = \epsilon \cdot \sum_1^k q_i^{e_i}.$$

This theorem implies Berr's characterization of sums of mixed powers. To see this note that a totally positive unit is a sum of $2n$-th powers for every n and that an e-th power of a sum of squares is a sum of $2e$-th powers due to the first Hilbert identity.

Analyzing the ingredients of the proof of this theorem we see that only facts are used which are known likewise for the real holomorphy rings of elliptic function fields: Dedekind property and sums-of-squares generation of the squares of the maximal ideals. As a consequence, the last theorem can be proven for such fields by appealing to the family of all discrete real valuations $\omega_\gamma, \gamma \in \Gamma \cup \infty$.

4.4 Topics of Complexity

Let $f \in \mathbb{R}[x]$ be a polynomial in one variable and let $n \geq 2$ be a natural number. In the context of the study of sums of powers the following questions arise quite natural.

(1) For which f does there exist a representation $f = \sum_1^N (\frac{g_i}{h})^{2n}$, some $N \in \mathbb{N}$ with $g_i, h \in \mathbb{R}[x]$?

(2) What can be said about the length N of such representation?

(3) What can be said about the degree of h?

The topic addressed in (1) is of a qualitative nature and finds a very satisfactory answer by the Valuation Criterion of section 4.2.

Recall that $f \in \mathbb{R}[x]$ has a representation (1) if and only if

(a) $f \geq 0$ (i.e. $f(a) \geq 0$ for all $a \in \mathbb{R}$,

(b) $2n|degf$, and

(c) $2n$ divides the multiplicity of $x - a$ in f for every $a \in \mathbb{R}$.

In contrast, the questions (2),(3) address topics of a quantitative nature and looks the complexity of a representation by sums of powers. Complexity topics are difficult to deal with, only a few results are known. A sample of them will be presented here, sometimes passing to more general formally real fields .

As usual, given any formally real field K, we call the least $N \in \mathbb{N}$ such that $\sum K^{2n} = \sum_1^N K^{2n}$ the $2n - th$ **Pythagoras number** $p_{2n}(K)$ of K. By a result of Becker **[3]**, this number is known to be finite for all $n \in \mathbb{N}$ provided $p_2(K) < \infty$. So, all Pythagoras numbers of $\mathbb{R}(x)$ are finite.

In the special case $n = 2$, in the paper **[10]** of Choi, Lam, Prestel and Reznick it was shown that $3 \leq p_4(R(x)) \leq 6$ for a real closed field R.

Concerning topic (3) very little is known. Gilbert Stengle in **[36]** showed that for the simple polynomial y^4+ty^2+1 , viewed as a one-parameter family of elements of $\mathbb{R}[y]$ if $y^4 + ty^2 + 1 = \sum (f_k/f_0)^4, t \geq 0$ the degree of f_0 tends to infinity with t in any such family and there exists a family and a constant C in which the degree of f_0 has the bound $C \log t$ for all large t.

The following result is a improved version of an older result by Becker. The main progress came from the observation that Caratheodory's theorem, cf. **[28]**, about the generation of cones in $\mathbb{R}$- or $\mathbb{Q}$-vectorpaces lead to shorter length in Hilbert's identities.

We recall the Hilbert's identity

$$\left(\sum_{i=0}^{k} {X_i}^2\right)^n + 2n{X_0}^2\left(\sum_{i=0}^{k} {X_i}^2\right)^{n-1} = \sum_{i=1}^{m} \beta_i L_i(X_0, \cdots, X_k)^{2n}$$

where $k, n \in \mathbb{N}, \beta_i \in \mathbb{Q}, \beta_i > 0$, linear forms $L_i \in \mathbb{Q}[X_0, \cdots, X_k]$ and $m \leq \binom{2n+k}{2n}$. Caratheodory's theorem yields this upper bound for the length of the sum on the right hand side since this bound is the $\mathbb{Q}$-dimension of the space $\mathbb{Q}[X_0, \ldots, X_k]_{2n}$

Proposition 23 *Let $\mathbb{R} \subseteq K$, K be formally real, $p := p_2(K) < \infty$ then $p_{2n}(K) \leq p^2\binom{2n+p}{2n}$.*

Corollary 15 *If $p_2 \leq 2$ then $p_{2n} \leq 2(2n+1)(2n+2)$.*

Proof. In Hilbert's identity the coefficients β_i can be merged with the linear forms since they are $2n$-powers.
1st step: $\sum_i a_i^{2n} = \epsilon \sum_1^p b_j^{2n}$ where ϵ is a totally positive unit ϵ, in particular $\epsilon = \sum_1^p x_i^2$. This can be obtained by considering fractional ideals: $(\sum_i a_i^{2n}) = (\dots, a_i^2, \dots)^n = (\sum_i a_i^2)^n = (\sum_1^p b_i^2)^n = (b_1^2, \dots, b_p^2)^n = (\sum_1^p b_i^{2n})$.
2nd step: we assume $\hat{\epsilon} < 1$. Since ϵ is totally positive we have $\epsilon = \sum_1^p x_i^2$. Then for all i we get $\widehat{x_i^2} < 1$, hence
$1 - x_i^2 = \sum_{j=1}^p y_{ij}^2$, i.e. $1 = x_i^2 + \sum_j y_{ij}^2$. Plugging in in Hilbert's identity we find for each index i

$$1 + 2nx_i^2 = \sum_1^N x_{ij}^{2n}, N = \tbinom{2n+p}{2n}.$$

Summing over all i and dividing by p this means

$$1 + (2n/p)\epsilon = \sum_1^{Np} y_j^{2n}.$$

3rd step: Given any totally positive unit ϵ find, by the density of the image of H in $C(M, \mathbb{R})$, a totally positive unit γ and define another totally positive unit η such that

$$1 < \hat{\epsilon} \cdot \widehat{\gamma^{2n}} < 1 + 2n/p, \text{ define } \eta \text{ by: } 1 + 2n/p \cdot \eta = \epsilon\gamma^{2n}.$$

η satisfies the condition in the second step, and ϵ turns out to be a sum of Np $2n$-th powers. Multiplying ϵ with the sum $\sum_1^p b_j^{2n}$ we get the claim on p_{2n}.

J.Schmid's approach
The bounds for p_{2n} from above might be correct assymptotically but are much too large for small exponents and small quadratic Pythagoras number p_2. In such cases the theorem of Schmid

Theorem 47 $\mathbb{E}_+ = \sum \mathbb{E}_+^n$ *for all n.*

can be applied to produce smaller bounds for p_{2n}.

To outline the idea we introduce the Pythagoras number

$$p_n^+ := p_n(\mathbb{E}_+) = \min\{k \mid \mathbb{E}_+ = \sum_1^k \mathbb{E}_+^n\} \text{ or } \infty.$$

The new idea runs as follows:

$$s = \sum_i a_i^{2n} = [\sum_i a_i^{2n}/q^n] \cdot q^n \text{ where } q = \sum_i a_i^2.$$

The element in [] is a totally positive unit ϵ as all real valuations assigns the value 0 to it, and it is a sum of squares. Hence, $\epsilon = \sum_1^{p_n^+} \epsilon_i^n$ where all $\epsilon_i \in \mathbb{E}_+$. Assuming $p_2 \leq 2$ we have $\epsilon_i = \eta_1^2 + \eta_2^2, q = a^2 + b^2$. This leads to

$$s = \sum_i [(\eta_1^2 + \eta_2^2)(a^2 + b^2)]^n = \sum_1^{p_n^+} (a_i^2 + b_i^2)^n$$

since the product of two sums of two squares is a sum of two squares. In the book of Reznick "Sums of even powers of real linear forms" [**28**] we find identities

$$(u^2+v^2)^n = \sum_1^{n+1} w_i^{2n}$$

[equation 1.50, page 23].
This gives

Proposition 24 *If* $p_2 \leq 2$ *then* $p_{2n} \leq (n+1)p_n^+$.

The following argument below shows that $p_2 \leq 2$ implies the statement $p_2^+ \leq 3$. For function fields in one variable over $\mathbb{R}$ it is known that even $p_2^+ \leq 2$, cf. [4,10]: so in the general case $p_4 \leq 9$ or in the special case $p_4 \leq 6$.

Now the general arguments for the case $n = 2$.

As a function on $M(K)$ $\hat{\epsilon}$ is strictly positive, hence strictly larger than some rational number $1/n$. Then $(\epsilon - 1/n)$ induces a function on M which is strictly positive. Hence, this element is a sum of squares. Therefore

$$\epsilon = 1/n + \textstyle\sum_1^p x_i^2$$

To keep the argument simple we restrict to the case $p \leq 2$ and $\mathbb{R} \subseteq K$. So, $\epsilon = 1/n(1+u^2+v^2)$. Necessarily, $u, v \in H$. The basic discovery of Schmid is this lemma:

Lemma 15 *If* $u \in H$ *then* $1+u^2 = \eta^2 + \omega^2, \eta, \omega \in \mathbb{E}_+$.

To prove this we consider the continuous function

$$f = (1/\sqrt{1+\widehat{u^2}})[\hat{u} - i] : M \to S^1.$$

The values of f lie in the lower half-circle. Therefore we can use the stereographic projection to find $a, b \in H$ where $a^2+b^2 = 1$ such that the function $g := \hat{a} + \hat{b}i$ is close to f, as close as we want and need in the sequel (using the density):
$f \approx (\hat{a} + \hat{b}i)$. Multiplying with the inverse function $g^{-1} = \hat{a} - \hat{b}i$ we find that fg^{-1} is close to the constant function 1, as close as needed for an argument below. Calculation shows:

1. $fg^{-1} = (1/\sqrt{1+\widehat{u^2}})[\hat{v} + \widehat{w}i], v = ua - b, w = -ub - a, v^2 + w^2 = 1 + u^2$,
2. $\hat{v} \approx \sqrt{1+\widehat{u^2}}, \hat{w} \approx 0$, so approximating sufficiently near:
3. $v \in \mathbb{E}_+$.

Hence, $1+u^2 = v^2+w^2$ where v is a totally positive unit. However, w need not be a unit, but $\hat{w}$ is small as wanted. This means that $v \pm w$ are totally positive units, and we have $1+u^2 = [(1/\sqrt{2})(v+w)]^2 + [(1/\sqrt{2})(v-w)]^2$, and the claim is proven.

As a consequence we get that $\epsilon = \sum_1^3 \epsilon_i^2, \epsilon_i \in \mathbb{E}_+$.

Proposition 25 *If* $\mathbb{R} \subseteq K, p_2 \leq 2$ *then* $p_4 \leq 9$

Proof. $\sum_i a_i^4 = (\sum_1^3 \epsilon_i^2)(a^2+b^2)^2$. Use the identity
$(X^2+Y^2)^2 = (X + 1/\sqrt{3}Y)^4 + (X - 1/\sqrt{3}Y)^4 + 8/9Y^4$.

Bibliography

[1] E. Becker, *Partial Orders on a field and valuation rings*, Comm. Alg., 7(18), 1933-1976 (1979)

[2] E. Becker, *Valuations and real places in the theory of formally real fields*,Geometrie algebrique reelle et formes quadratiques, Proceedings, Rennes, 1981, Lecture Notes in Math. No. 959, Springer-Verlag, Berlin,Heidelberg,New York, 1982,pp. 1-40.

[3] E. Becker, *The real holomorphy ring and sums of* $2n-th$ *powers*, Geometrie algebrique reelle et formes quadratiques, Proceedings, Rennes, 1981, Lecture Notes in Math. No. 959, Springer-Verlag, Berlin,Heidelberg,New York, 1982, pp.139-181.

[4] E. Becker, *Sums of powers in Fields and Orderings of Higher Level*, to appear.

[5] E. Becker, J. Harman, A. Rosenberg, *Signatures of fields and extension theory*, J. reine angew. Math. 330(1982), 53-75.

[6] R. Berr, *Sums of mixed powers in fields and orderings of prescribed level*, Math. Z. 210, 513 - 528 (1992).

[7] J. Bochnak, M. Coste, and M.-F. Roy, *Real algebraic geometry*, volume 36 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1998.

[8] N. BOURBAKI, *Commutative Algebra*, Paris: Hermann, 1972.

[9] M. D. Choi and T. Y. Lam, *An Old Question of Hilbert*, Queen's Papers in Pure and Appl. Math. (Proceedings of Quadratic Forms Conference, Queen's University (G. Orzech ed.)), 46(1976), 385-405.

[10] M. D. Choi, T. Y. Lam, A. Prestel, B. Reznick, *Sums of 2m-th powers of rational functions in one variable over real closed fields*, Math. Z. 221, 93 - 112 (1996).

[11] W. J. Ellison, *Waring's problem*, Amer. Math. Monthly 78 (1971), 10 - 36.

[12] A. J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag Berlin Heidelberg 2005.

[13] Y. L. Ershov, *Multi-Valued Fields*, Springer Science + Business Media New York 2001.

[14] M. Fontana, J. A. Huckaba, and I. J. Papick, *Prüfer domains*, volume 203 of Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker Inc., New York, 1997.

[15] R. Gilmer, *Multiplicative ideal theory*, volume 90 of Queen's Papers in Pure and Applied Mathematics. Queen's University, Kingston, ON, 1992.

[16] I. Kaplansky, *Commutative rings*, The University of Chicago Press, Chicago, Ill.-London, 1974.

[17] G. Kemper, *A Course in Commutative Algebra*, Springer-Verlag Berlin Heidelberg 2011.

[18] T. Y. Lam, *The theory of ordered fields*, Ring Theory and Algebra III, Proc. Third Oklahoma Conf., 1979, Lecture Notes in Pure and Appl. Math., Vol. 55, Marcel Dekker, New York, 1980, pp. 1-152.

[19] T. Y. Lam, *Orderings, Valuations, and Quadratic Forms*, CBMS Regional Conf. Series in Math., Vol. 52, Amer. Math. Soc., Providence, RI, 1983.

[20] T. Y. Lam, *An introduction to real algebra*, Rocky Mtn.J.Math.14(1984),767-814.

[21] M. Marshall, *Positive Polynomials and Sums of Squares*, Volume 146 Mathematical Surveys and Monographs. The American Mathematical Society 2008.

[22] A. Pfister, *Hilbert's 17th Problem and related problems on definite forms*, Proc. Symp. Pure Math., Vol. 28, Amer. Math. Soc., Providence, RI, 1976. 483-489.

[23] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series 217. Cambridge University Press 1995.

[24] V. Powers, *Hilbert's 17th Problem and the Champagne Problem*, The American Mathematical Monthly, Vol. 103, No. 10 (Dec., 1996), pp. 879 - 887.

[25] A. Prestel and C. N. Delzell, *Positive Polynomials: From Hilbert's 17th Problem to Real Algebra*, Mathematics - Monograph (English) Springer-Verlag Berlin Heidelberg 2004

[26] B. Reznick, *Uniform denominators in Hilbert's 17th Problem*, Math. Zeit. 220 (1995), 75-97

[27] B. Reznick, *Some concrete aspects of Hilbert's 17th Problem*, Seminarie de Structures Algebriques Ordonnees, Vol. 56, Equipe de Logique Mathematique, Universite Paris VII, 1996

[28] B. Reznick, *Sums of even powers of real linear forms*, Mem. Amer. Math. Soc. 96 (1992), no.463.

[29] W. Rudin, *Sums of Squares of Polynomials*, Amer. Math. Monthly 107(2000) 813 - 821.

[30] Gabriel Daniel Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhause, 2006.

[31] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag Berlin Heidelberg 1985.

[32] J. Schmid, *Sums of fourth powers of real algebraic functions*, Manuscripta Math. 83, 361-364(1994)

[33] J. Schmid, *On totally positive units of real holomorphy rings*, Israel J. of Math.85,339-350(1994)

[34] H. W. Schülting, *On real places of a field and their holomorphy ring*, Comm. Algebra, 10(12): 1239 - 1284, 1982.

[35] H. W. Schülting, *Real holomorphy rings in real algebraic geometry*, In Real algebraic geometry and quadratic forms (Rennes, 1981), volume 959 of Lecture Notes in Math., pages 433 - 442. Springer, Berlin, 1982.

[36] G. Stengle, *Estimates for parametric nonuniformity in representations of a definite polynomial as a sum of fourth powers*, Contemp. Math., 155: 243 - 246 (1994)

[37] R. J. Walker, *Algebraic Curves*, Dover, New York, 1962.

[38] O. Zariski and P. Samuel, *Commutative algebra*, Vol. II. Springer-Verlag, New York, 1975.

PSALM 124
A SONG OF ASCENTS. OF DAVID.

1 If the LORD had not been on our side − let Israel say −
2 if the LORD had not been on our side when men attacked us,
3 when their anger flared against us, they would have swallowed us alive;
4 the flood would have engulfed us, the torrent would have swept over us,
5 the raging waters would have swept us away.
6 Praise be to the LORD, who has not let us be torn by their teeth.
7 We have escaped like a bird out of the fowler's snare; the snare has been broken, and we have escaped.
8 Our help is in the name of the LORD, the Maker of heaven and earth.
(NIV)