Fields and Galois Theory

math 370, yale university, spring 2019

These are lecture notes for math 370b, "Fields and Galois Theory," taught by Asher Auel at Yale University during the spring of 2019. These notes are not official, and have not been proofread by the instructor for the course. They live in my lecture notes respository at

https://github.com/jopetty/lecture-notes/tree/master/MATH-370.

If you find any errors, please open a bug report describing the error and label it with the course identifier, or open a pull request so I can correct it.

Contents

Syllabus

Instructor	Asher Auel, asher.auel@yale.edu
Lecture	TR 11:35 AM – 12:50 PM in LOM 215
Peer Tutor	Arthur Azvolinsky, arthur.azvolinsky@yale.edu
Section	Math Lounge
Exams	Midterm 1: Febuary 19; Midterm 2: April 9; Final: May 3.
Textbook	James S. Milne. *Fields and Galois Theory (v4.60)*. 2018

The main object of study in Galois theory are roots of single variable polynomials. Many ancient civilizations (Babylonian, Egyptian, Greek, Chinese, Indian, Persian) knew about the importance of solving quadratic equations. Today, most middle schoolers memorize the "quadratic formula" by heart. While various incomplete methods for solving cubic equations were developed in the ancient world, a general "cubic formula" (as well as a "quartic formula") was not known until the 16th century Italian school. It was conjectured by Gauss, and nearly proven by Ruffini, and then finally by Abel, that the roots of the general quintic polynomial could not be solvable in terms of nested roots. Galois theory provides a satisfactory explanation for this, as well as to the unsolvability (proved independently in the 19th century) of several classical problems concerning compass and straight-edge constructions (e.g., trisecting the angle, doubling the cube, squaring the circle). More generally, Galois theory is all about symmetries of the roots of polynomials. An essential concept is the field extension generated by the roots of a polynomial. The philosophy of Galois theory has also impacted other branches of higher mathematics (Lie groups, topology, number theory, algebraic geometry, differential equations).

This course will provide a rigorous proof-based modern treatment of the main results of field theory and Galois theory. The main topics covered will be irreducibility of polynomials, Gauss's lemma, field extensions, minimal polynomials, separability, field automorphisms, Galois groups and correspondence, constructions with ruler and straight-edge, theory of finite fields. The grading in Math 370 is very focused on precision and correct details. Problem sets will consist of a mix of computational and proof-based problems.

Your final grade for the course will be determined by

$$\max \left\{ \begin{array}{l} 20\%\text{ homework} + 25\%\text{ midterm 1} + 25\%\text{ midterm 2} + 30\%\text{ final} \\ 20\%\text{ homework} + 25\%\text{ midterm 1} + 15\%\text{ midterm 2} + 40\%\text{ final} \\ 20\%\text{ homework} + 15\%\text{ midterm 1} + 25\%\text{ midterm 2} + 40\%\text{ final} \end{array} \right\}.$$

References

[Mil18] James S. Milne. *Fields and Galois Theory (v4.60)*. 2018.

1 January 15, 2019

> "Daddy, the bears is wubbing his back!"
>
> Noah Auel

Asher's kids came up and they are soooooo cuuuuuuttteeeeee! That's so adorable. He also says that the course is really fun but honestly the kids are by far my favorite part of the course so far. Hi Noah! Sorry your great-grandfather died :(

1.1 What is Galois Theory?

Galois theory is an explanation of a trajectory we started in grade school. We start with the positive integers $\mathbb{Z}_{>0}$ and we learn to make bijections (bijections between apples on the table and positive integers). Then we discovered (or invented) the concept of zero which led us to $\mathbb{N}$. Then we started using negative numbers to arrive at $\mathbb{Z}$, and from there on to $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and so on. Each jump is necessitated by wanting or needing to solve some kind of equation. Galois theory mainly focuses on that last jump from $\mathbb{R}$ to $\mathbb{C}$.

1.2 Moving from $\mathbb{R}$ to $\mathbb{C}$

We usually think of $\mathbb{C}$ in the presentation of $\mathbb{C} = \mathbb{R}[i] = \{x + iy \mid x, y \in \mathbb{R}\}$. This value i is a root of the equation $x^2 + 1$, one we can't solve with just real numbers. One could ask "what is so special about this polynomial?" Why is i the thing that builds complex numbers? What about $x^2 + x + 1$? That is also rather fundamental, with roots $\omega = (-1 \pm \sqrt{-3})/2$. If you draw the unit circle in the complex plane, these roots divide the circle into three pieces along with $(1, 0)$. We could form an object $\mathbb{R}[\omega]$ and call that the complex numbers. We don't use this construction because $\mathbb{R}[\omega] = \mathbb{C}$, since

$$x + y\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \left(x - \frac{1}{2}y\right) + \frac{\sqrt{3}}{2}yi,$$

by associativity via the substitution $x' = x - \frac{1}{2}y$ and $y' = \frac{\sqrt{3}}{2}y$. These transformations are always solvable, so the two systems are in fact equivalent.

Exercise 1.1. Let $f\colon x \mapsto ax^2 + bx + c$ where $a, b, c \in \mathbb{R}$ where $b^2 - 4ac < 0$. Prove that $\mathbb{C} = \mathbb{R}[\alpha]$ where α is a root of f.

But even if you do choose to ordain $x^2 + 1$ as special, there's still nothing special about i since it factors into $(x + i)(x - i)$. Then there are really two roots, $+i$ and $-i$. We have arbitrarily chosen i over $-i$, probably because it was invented by nineteenth century

German mathematicians living in the Northern Hemisphere. Algebraically, there is no way to distinguish between i and $-i$. However moving *between* the roots is special: it's a map $\sigma\colon \mathbb{C} \to \mathbb{C} : x+iy \mapsto x-iy$ called an $\mathbb{R}$-automorphism of $\mathbb{C}$, meaning that restricting σ to $\mathbb{R}$ is the identity. It's also a (unital) ring homomorphism, so $\sigma(z_1+z_2) = \sigma(z_1)+\sigma(z_2)$ and $\sigma(z_1 \cdot z_2) = \sigma(z_1) \cdot \sigma(z_2)$ and $\sigma(1) = 1$.

There are more such automorphisms! We already saw that we can write complex numbers as $\mathbb{C} = \mathbb{R}[\omega]$. We could create the map $\sigma\colon x + y\omega \mapsto x + y\bar{\omega}$. Notice that all these automorphisms are doing is exchanging the roots of the generating polynomials. We can check that this is in fact a valid automorphism by look at what it does to i.

$$\sigma\colon i = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\omega \mapsto \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\bar{\omega} = -i,$$

so it's actually just complex conjugation! In fact, $\operatorname{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$.

Example 1.1. Notice that $|\operatorname{Aut}_{\mathbb{R}}(\mathbb{C})| = 2 = \dim_{\mathbb{R}} \mathbb{C} = [\mathbb{C} : \mathbb{R}]$. We'll be seeing a lot of this later.

This shows that the special part of the complex numbers is not i or ω, but rather complex conjugation. This is actually the defining property of the complex numbers irrespective of how you define them.

Proposition 1.1. *More generally, given a field F and a polynomial $f(x) = ax^2 + bx + c$ for some $a, b, c \in F$ satisfying $f(x)$ has no root in F then there exists a field k with the following properties:*

1. *F is a subfield of k;*
2. $\dim_F k = [k : F] = 2$;
3. $|\operatorname{Aut}_F k| = 2$*; and*
4. *the polynomial f is separable which for us means that $b^2 - 4ac \neq 0$. This is called the quadratic extension of F.*

This will lead us to a new σ which will exchange the roots analogously to conjugation. We'll also need that the characteristic of F is not 2, since otherwise the quadratic formula doesn't work since we divide by $2a$. Implicit in the quadratic formula is the statement that $k = F[\sqrt{b^2 - 4ac}]$.

1.3 Going Cubic

We have a similar story for cubic equations where $f(x) = x^3+px-q$ (the negative is there for historical reasons). This also leads us to the cubic formula. The Babylonians discovered the quadratic formula, and Italian mathematicians in the 16th century developed the cubic formula,

seriously, just look it up.

because they had these betting games where two mathematicians had to compete to find the roots of a cubic equation. Eventually, a guy named Cardano and his students started winning everything and then one of his students defected to a competitor. The important part is that this formula is a nested formula of certain finitely many operations depending just on the coefficients. There is a similar story for quartic equations.

Theorem 1.1 (Abel-Ruffini)**.** *Given a general polynomial $f \in \mathbb{Q}[x]$ with $\deg(f) \geq 5$, there is no explicit closed form formula for the roots of f only depending on taking nested roots.*

Galois theory is about understanding polynomials by looking at the symmetry of their roots.

2 January 17, 2019

> "This is true by the Freshma—First Year's Dream"
>
> Asher

2.1 *Reminders from MATH 350*

1. F is a field, or a commutative unital ring where every $F^{\times} = F \quad \{0\}$.
2. $F[x]$ is the ring of polynomials with coefficients in F.
3. $\partial : F[x] \to \mathbb{N}$ is the degree function. We know that $\partial(fg) = \partial(f) + \partial(g)$ and $\partial(f+g) \leq \max\{\partial(f), \partial(g)\}$. Because of multiplicativity, we know that $F[x]^{\times}$ are nonzero constant polynomials.

Theorem 2.1. *Given a field F, we know that $F[x]$ is a Euclidean Doman with respect to ∂. That us, given $f, g \in F[x]$ where $g \neq 0$, there exist $q, r \in F[x]$ such taht $f = q \cdot g + r$ where either $r = 0$ or $\partial(r) < \partial(g)$.*

Theorem 2.2. *Every Euclidean Doman is a Principal Ideal Domain.*

Ideal

Definition (Ideal)**.** A subset $I \subset R$ of a ring is an ideal if I is a subring and it is closed under multiplication, so that $rI \subset I$ for every $r \in R$ (we implicitly assume that R is commutative here). Any ideal which contains a unit is the whole ring.

Principal Ideal

Definition (Principal Ideal)**.** An ideal $I \subset R$ is principal if it is generated by one thing, so $I = (r) = rR$ for some $r \in R$,

Corollary 2.1. *$F[x]$ is a PID. If $I = (f)$ then $I = (cf)$ for some $c \in F^{\times}$, so we choose our polynomials to be* monic.

Corollary 2.2. *The set of all ideals $\{I \subseteq F[x]\}$ is in bijection with the set of monic polynomials $\{f \in F[x]\}$.*

Prime Idea

Definition (Prime Idea)**.** An ideal $I \subseteq R$ is prime if $ab \in I$ implies that either a or b is an element of I. Equivalently, this says that R/I is an integral domain.

Maximal Ideal

Definition (Maximal Ideal)**.** An ideal $I \subseteq R$ is maximal if $I \subseteq J \subseteq R$ then either $I = J$ or $J = R$. Equivalently, R/I is a field, so there are no nonzero nonunit elements of R/I.

Example 2.1 (Ideals in $\mathbb{Z}$)**.** A prime ideal I in $\mathbb{Z}$ is either (0) or (p) for some prime p. In any integral domain, (0) is prime. The only maximal ideals in $\mathbb{Z}$ are (p) by Bezout's Theorem.

Prime and Irreducible Elements

Definition (Prime and Irreducible Elements)**.** An element r in R is prime if (r) is prime, or if r divides ab then r divides either a or b. An element r is irreducible if $r = ab$ then $a \in R^{\times}$ or $b \in R^{\times}$. Primality always implies irreducibility, but the converse only holds in PIDs.

Lemma 2.1. *If R is a PID then every irreducible element is prime.*

UFD

Definition (UFD)**.** A Unique Factorization Domain is a commutative unital ring R with the following two properties for every nonzero $r \in R$:

1. $r = r_1 \cdot r_n$ where r_1 through r_n are irreducible;
2. this finite product is unique, so if $r = r_1 \cdots r_n$ and $r = s_1 \cdots s_m$ then $n = m$ and $r_i = u_i s_i$ for some unit $u_i \in R^{\times}$.

Theorem 2.3. *Every PID is a UFD.*

Corollary 2.3. *$F[x]$ is a UFD. Equivalently, if $f \in F[x]$ is nonzero then $f = c \cdot f_1 \cdot f_2 \cdots f_n$ where $c \in F^{\times}$ and f_i are monic irreducible polynomials, and this decomposition is unique.*

Problem 2.1. Given a polynomial $f \in F[x]$, how do we check if f is irreducible?

2.2 Roots and Irreducibility

Definition. If f is a nonzero element of $F[x]$ then $a \in F$ is a root of f if $f(a) = 0$. We can use the division algorithm to write f as $g \cdot (x - a) + r$ where $r = 0$ or $\partial(r) \leq \partial(x - a) = 1$, so r is a constant.

Corollary 2.4. *An element $a \in F$ is a root of f if and only if we can write it as $f = g \cdot (x - a)$.*

Corollary 2.5. *If $f \in F[x]$ and $\partial(f) = n > 0$ then f has at most n roots.*

Proof. Either by induction using $f = g \cdot (x - a) = h \cdot (x - b) \cdot (x - a) = \cdots$ or we use the fact that $F[x]$ is a UFD, so we write f as $f_1 \cdots f_m$ and we know that $m \leq n$ and if any f_i is nonlinear then it has no roots. ■

Example 2.2 (Polynomials with no roots).
Consider $f\colon x \mapsto x^2 + 1$ in $\mathbb{R}[x]$.
Consdier $f\colon x \mapsto x^2 - 2$ in $\mathbb{Q}[x]$.
Consider $f\colon x \mapsto x^2 + x + 1$ in $\mathbb{F}_2[x]$.

Proposition 2.1. *If $f \in F[x]$ is irreducible of degree greater than or equal to 2 then f has no roots in F.*

Proof. $F[x]$ is a unique factorization domain, so we can't write it as a product of anything of a smaller degree, which we showed is the same as writing it as a $(x - r) \cdot g$ in some way. ■

Proposition 2.2. *If $f \in F[x]$ is a polynomial degree at most 3 and f has no roots then f is irreducible.*

Proof. Unique Factorization! Assume that f is reducible and $\partial(f) \leq 3$. Then $f = c \cdot f_1 f_2$ where f_1 and f_2 are nonconstant. If $\partial(f) \leq 3$ then $\partial(cf_1f_2) = \partial(f_1) + \partial(f_2) \leq 3$. Since $\partial(f_i) > 0$ then $\partial(f_1) = \partial(f_2) = 1$, which means that we found linear polynomials and therefore roots. ■

Example 2.3 (Warning). Be careful with the above! Consider $(x^2 + 1)^2 \in \mathbb{R}[x]$. This has no roots but is irreducible.

Example 2.4 (Warning). The fact that the number of roots is at most the degree fails if we don't work in a field. Consider $f(x) = x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[x]$. This has degree 2 but all odd numbers less than eight are roots.

Theorem 2.4 (Fundamental Theorem of Arithmetic). *Any nonconstant $f \in \mathbb{C}[x]$ has a root. Then any irreducible polynomial $f \in \mathbb{C}[x]$ is linear.*

Problem 2.2 (Proving Irreducibility).

(a) If $\partial f \leq 3$ then it is irreducbile if it has no roots.

(b)

2 January 17, 2019

Theorem 2.5. *Assume $f(x) \in \mathbb{Z}[x]$, and assume that p is a prime such that p doesn't divide a_n and $\bar{f}(x) = \bar{a}_n x^n$ is irreducible, then f is irreducible over $\mathbb{Z}[x]$. This is a reduction ring homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$.*

3 Tuesday, January 22

Recall that there is a ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{F}_p[x]$ which is reduction modulo p of the coefficients. There is subtlety when we talk about irreducibility in $\mathbb{Z}[x]$; consider that $2x-2 = 2\cdot(x-1)$ is not irreducible as an element of the ring $\mathbb{Z}[x]$, but it is irreducible as a polynomial in a polynomial ring over a field in the sense that we cannot factor it as $g \cdot h$ where $\partial g, \partial h > 0$. This is why we care about nonconstant factors. This discrepancy occurs when we have 2 appearing everywhere, which seems to present a problem. We need a way to distinguish between these two conflated notions.

> **Definition** (Primitive)**.** A polynomial $f \in \mathbb{Z}[x]$ if its coefficients are *all* relatively prime, so that the ideal $(a_0, \dots, a_n)$ is simply $\mathbb{Z}$, or equivalently that there exist $b_0, \dots, b_n \in \mathbb{Z}$ such that $\sum b_i a_i = 1$.

Primitive

Example 3.1. The polynomial $4x^3 + 6x^2 + 15x + 9$ is primitive while $4x^3 + 6x^2 + 16x + 18$ is not, since every term is divisible by 2.

Proposition 3.1. *A polynomial $f \in \mathbb{Z}[x]$ is primitive if and only if its reduction $\bar{f}$ modulo p is not the zero polynomial for all prime p.*

Lemma 3.1. *Let $f \in \mathbb{Q}[x]$. Then there exists a unique rational $c \in \mathbb{Q}$ and a unique primitive polynomial $f_0 \in \mathbb{Z}[x]$ such that $f = c \cdot f_0$.*

Proof. We first prove the existence, and then the uniqueness. Existence is given by clearing the denominators in a smart way, first be clearing the denominators and then by factoring out the GCD of the remaining integral coefficients. The uniqueness arises from the following. Suppose that $c \cdot f_0 = c' \cdot f_0'$ where $c, c' \in \mathbb{Z}$ and f_0, f_0' are primitive. Then if we write $f_0 = aa_n x^n + \dots + a_0$ and $f_0' = a_n' x^n + \dots + a_0'$ and the original polynomial as $f = A_n x^n + \dots + A_0$, then $\gcd(A_0, \dots, A_n) = \gcd(ca_0, \dots, ca_n) = \gcd(c'a_0', \dots, c'a_n')$. Since the GCD is multiplicative we know that these are $c \cdot \gcd(a_0, \dots, a_n)$ and $c' \cdot \gcd(a_0', \dots, a_n')$, and since these polynomials are primitive this GCD is 1, so $c = c'$. ■

Lemma 3.2. *If we start with a polynomial in $\mathbb{Z}[x]$, then the c which we pull out will also be an integer.*

Lemma 3.3. *Let $f, g \in \mathbb{Z}[x]$ be primitive. Then $f \cdot g \in \mathbb{Z}[x]$ is also primitive.*

Proof. If f, g are primitive then $\bar{f}, \bar{g} \in \mathbb{F}_p$ are nonzero for all p. Since $\mathbb{F}_p$ has no zero divisors (integral domain) then we know that $\bar{f} \cdot \bar{g}$ is also nonzero in $\mathbb{F}_p$ for all p. Then $fg \in \mathbb{Z}[x]$ is primitive. ■

Lemma 3.4. *If $f \in \mathbb{Z}[x]$ is primitive and $g \in \mathbb{Z}[x]$ is any polynomial, then if f divides g in $\mathbb{Q}[x]$ then f divides g in $\mathbb{Z}[x]$.*

Example 3.2 (Counter example when not primitive)**.** Consider that $4x$ divides $x(x-1)$ in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$ because $4x$ is not primitive.

Proof. There exists some unique way of writing g as $c \cdot g_0$. Since f divides g in $\mathbb{Q}[x]$ then $g = f \cdot h$ for some $h \in \mathbb{Q}[x]$. Thus $f \cdot h = c \cdot g_0$, and we can write $h = d \cdot h_0$. Then $g = d \cdot f \cdot h_0$, and since f and h_0 are primitive we know that fh_0 is primitive as well. Since this decomosition is unique, this implies that $c = d$ and $g_0 = fh_0$. Then f divides g_0 and g_0 divides g in $\mathbb{Z}[x]$, so f divides g in $\mathbb{Z}[x]$. ■

Lemma 3.5 (Gauss)**.** *Let $f \in \mathbb{Z}[x]$. If f is an irreducible polynomial in $\mathbb{Z}[x]$ then f is irreducible in $\mathbb{Q}[x]$.*

Proof. Assume $f = gh$ in $\mathbb{Q}[x]$ where $\partial g > 0$. Write $f = bf_0$, $g = cg_0$, and $h = dh_0$. Then $bf_0 = gh = cdg_0h_0$. Then g_0h_0 is primitive, so $f_0 = g_0h_0$ and $f = bg_0h_0$. ■

Lemma 3.6 (Eisenstein's Criterion)**.** *Let $f = \sum a_i x^i \in \mathbb{Z}[x]$. Fix a prime p and assume the following:*

1. *p does not divide a_n;*
2. *p divides all a_i where $0 \leq i \leq n-1$; and*
3. *p^2 does not divide a_0.*

Then f is irreducible in $\mathbb{Z}[x]$, and by Gauss' Lemma in $\mathbb{Q}[x]$ as well.

Proof. Proof by contradiction. Assume f has the requisite properties but f is reducible in $\mathbb{Z}[x]$, so $f = gh$. Let $g = \sum_{0 \leq i \leq m} g_i x^i$ and $h = \sum_{0 \leq i \leq \ell} h_i x^i$. Consdier $\bar{f} = \bar{a}_n x^n = \bar{g}\bar{h}$. Recall that $a_n = g_m h_\ell$ and $a_0 = g_0 h_0$. Then p divides g_0 and h_0; then p^2 divides $g_0 h_0 = a_0$ which is a contradiction. ■

Example 3.3. Consider that $x^2 - p$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein. Thus $\sqrt{p}$ is irrational. And just like that, most of ancient greek mathematics is solved.

Example 3.4. Notice that $x^p - 1 = (x-1) \cdot x^{p-1} + x^{p-2} + \cdots + 1 = (x-1)\Phi_p(x)$. This is irreducible by Eisenstein.

Proof. Consider $\Phi_p(x+1)$, so $(x+1)^p - 1 = x \cdot \Phi_p(x+1)$. We can use the binomial theorem to say that

$$(x+1)^p = \sum \binom{p}{i} x^i = x^p + px^{p-1} + \cdots + px + 1.$$

Then

$$\Phi_p(x+1) = x^{p-1} + px^{p-1} + \cdots + p.$$

Recall that p divides $\binom{p}{i}$ for all $1 \leq i \leq p-1$. Then $\Phi_p(x+1)$ is Eisenstein, and so $\Phi_p(x+1)$ is irreducible, and so $\Phi_p(x)$ is irreducible. ■

Problem 3.1 (Challenge, find a better proof than the current one which is terrible)**.** Prove that $x^n + x + 1 \in \mathbb{F}_2[x]$ is irreducible for $n \geq 2$.

4 Thursday, January 24

Extension

Definition (Extension)**.** Let k be a field. Then $F \subseteq k$ is a subfield if $F \subseteq k$ is a unital subring and F is a field. We say that k is an extension of F and write k/F.

Example 4.1. If k is an extension of F then k has the structure of an F-vector space. The cannonical example for this is thinking of $\mathbb{C}$ as a two-dimensional $\mathbb{R}$-vector space with basis $\{1, i\}$.

Definition. An extension k/F is finite if k is a finite dimensional F-vector space. The degree of k/F, written as $[k : F] = \dim_F k$ is the F dimension of k.

Example 4.2 (Examples of degrees)**.**

1. $\mathbb{C}/\mathbb{R}$ is finite and $[\mathbb{C} : \mathbb{R}] = 2$.
2. $\mathbb{R}/\mathbb{Q}$ is infinite since n-tuples of $\mathbb{Q}$ are countable and $\mathbb{R}$ is uncountable.
3. Let $\mathbb{Q}(i) = \{x + iy \in \mathbb{C} \mid x, y \in \mathbb{Q}\}$. Then $\mathbb{Q}(i)/\mathbb{Q}$ is finite with degree 2.

4.1 Field extensions generated by elements

Let F be a field contained in some field Ω. For $\alpha_1, \dots, \alpha_n \in \Omega$ we can consider two objects:

1. $F[\alpha_1, \dots, \alpha_n] \subseteq \Omega$ is a subring
2. $F(\alpha_1, \dots, \alpha_n) \subseteq \Omega$ is a subfield

We define these equantities in the following way.

$$F[\alpha_1, \dots, \alpha_n] = \bigcap_{\substack{R \subseteq \Omega \\ F \subseteq R, \alpha_i \in R}} R = \left\{ \sum a_{i_1} \cdots a_{i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \mid a_{i_1, \dots, i_n} \in F \right\}$$

and

$$F(\alpha_1, \dots, \alpha_n) = \bigcap_{\substack{k \subseteq \Omega \\ F \subseteq k, \alpha_i \in k}} k = \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in F[\alpha_1, \dots, \alpha_n], \beta \neq 0 \right\}.$$

We say that $F[\alpha_1, \dots, \alpha_n]$ is the subring of Ω generated by $\alpha_1, \dots, \alpha_n$ and $F(\alpha_1, \dots, \alpha_n)$ is the subfield of Ω generated by $\alpha_1, \dots, \alpha_n$.

Example 4.3. Consider $\mathbb{Q}[i]$ and $\mathbb{Q}(i)$. We say that $\mathbb{Q}[i]$ are rational polynomials in i and $\mathbb{Q}(i)$ are quotients of these polynomials, understanding that even powers of i and odd powers of i to collapse it into rational and imaginary components. These are equal to one another. However, $\mathbb{Q}[\pi] \subset \mathbb{Q}(\pi)$ but they are not equal (since the field extension is not finite as π is not algebraic).

The Laurent series $F((x))$ is important for Complex Analysis and is analogous to the formal power series $R[[x]]$.

Theorem 4.1 (Tower Law). *Let L/k and k/F be field extensions. Then $[L : F] = [L : k] \cdot [k : F]$.*

Proof. If L is a finite dimensional F-vector space then L is a finite dimensional k-vector space since if $z_1, \dots, z_p$ is an F-basis for L then in turn $\alpha = \sum a_i z_i \in F$ for all $\alpha \in L$ so $z_1, \dots, z_p$ is a generating set. On the other hand, $k \subseteq L$ is an F-vector space. Assume that $[L : k] = n$ with x_i a k-basis for L and $[k : F] = m$ with y_i and F-basis for k. Then we first show that $\{x_i y_j\}$ is an F-basis of L so $[L : F] = nm$. First, linear independence: assume that $\sum a_{i,j} x_i y_j = 0$ for $a_{i,j} \in F$. Rewrite this as $\sum \left(\sum a_{i,j} y_i\right) x_i = 0$, so $\sum a_{i,j} y_i = 0$ so $a_{i,j} = 0$ and the set is linearly independent. Next, we show this generates L over F. Let $\alpha \in L$ be written as $\alpha = \sum \beta_i x_i$ for $\beta_i \in k$. But for each i we have $\beta_i = \sum a_{i,j} y_i$ so $\alpha = \sum \left(\sum a_{i,j} y_i\right) x_i = \sum a_{i,j} x_i y_i$, so these generate. Then this is a basis, and the proposition holds. ■