Development of modern algebra and number theory since Galois and Kummer

Yi Ouyang

School of Mathematical Sciences, University of Science and Technology of China

Contents

The main objective of this short course is to give a brief introduction of the development of algebraic ideas/notions/methods in number theory from the perspective of history of mathematics. We shall base our lectures mainly on two great problems— Solubility of equations by explicit formulae and Fermat's Last Theorem, and two great mathematicians— Évariste Galois and Ernst Edward Kummer in the 19th century. The final resolution of the insolubility of general equations of degree ≥ 5 by Galois led to the birth of group theory and Galois Theory. The attack of Kummer on Fermat's Last Theorem led to the birth of algebraic number theory and commutative ring theory. Armed with these tools and many more advancements by great mathematicians in the past two centuries, Andrew Wiles was finally able to prove Fermat's Last Theorem in 1995.

This note consists of five lectures (chapters). In Lecture 1, we shall talk about the resolutions of quadratic, cubic and quartic equations. We shall start with the work of Old Babylonians about quadratic equations in 1900BC-1600BC, then the legendary stories about the Italians and the resolutions of cubic/quartic equations in 15th Century. The second lecture is about the life and work of Abel and Galois, and also a brief sketch of Galois Theory and the insolubility theorem of Abel and Galois. In Lecture 3, we shall talk about the life and work of Kummer, in particular, Kummer's theory of ideal numbers. Lecture 4 is about the development of algebraic number theory in the next one hundred years (from roughly 1850 to 1950) after Kummer's discovery and before Tate's thesis. The last lecture is about the development since 1950 (after Tate's thesis).

CHAPTER 1

Resolutions of quadratic, cubic and quartic equations

1. Quadratic equations

It is well-known from secondary school mathematics that the two roots of the quadratic equation

$$ax^2 + bx + c = 0$$

are

$$x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This formula was actually known to the Old Babylonians (1900BC-1600BC), a remarkable achievement since Chinese was just entering their first Dynasty — Xia Dynasty during that period.

The Old Babylonians used cuneiform for writing, which was first developed by the ancient Sumerians of Mesopotamia c. 3500-3000 BC. Cuneiform BM 13901 (British Museum No. 13901) probably is the most well-known cuneiform for mathematics. It contained 24 problems and their solutions dealing with quadratic equations. It was eventually deciphered by French archaeologist François Thureau-Dangin (1872-1944) in 1936 and by Austrian mathematician Otto Neugebauer (1899-1990) in 1937, revealing the secret of resolution of quadratic equations by Old Babylonians. We shall give two examples.

Before we start, note that the Old Babylonians used Sexagesimal numerical systems, i.e. base 60 or sexagenary numeral system which was originated by the ancient Sumerians in 3000 BC and passed down to the Babylonians. However, there is some ambiguity for their recording: the number 1 could also stand for $\frac{1}{60}$ or $\frac{1}{3600}$, the number 30 could stand for $\frac{1}{2}$, $\frac{1}{120}$, 90 or 3630 etc. Hence the number $1, 30$ could represent either $1\frac{1}{2}$ or 90, depending on the context. We shall use $1, 30$ to stand for 90 and $1; 30$ to stand for $1\frac{1}{2}$.

Example 1 (Problem No.2 of BM 13901). I have subtracted the side of my square from the area, (and I got) $14, 30$.

In modern language, let x be the side of the square, note that $14, 30 = 870$, then this question is to find the (positive) root of

$$x^2 - x = 870.$$

The Babylonians actually solved equation of the type $x^2 - bx = c$ in the cuneiform. In this case $b = 1$ and $c = 14, 30 = 870$. The following table gives the solution by the Babylonians:

step	method	outcome	outcome
1	You write down 1 the coefficient	b	1
2	You break half of 1	$\frac{b}{2}$	$\frac{1}{2} = 0;30$
3	You multiply $0;30$ and $0;30$	$(\frac{b}{2})^2$	$0;30 \cdot 0;30 = 0;15$
4	You add $0;15$ to $14,30$, result $14,30;15$	$(\frac{b}{2})^2 + c$	$870\frac{1}{4} = 14,30;15$
5	This is the square of $29;30$	$\sqrt{(\frac{b}{2})^2 + c}$	$29\frac{1}{2} = 29;30$
6	You add $0;30$, result 30	$\frac{b}{2} + \sqrt{(\frac{b}{2})^2 + c}$	$29;30 + 0;30 = 30$

Answer: 30.

Example 2 (Problem No.7 of BM 13901). I added 7 times the side of my square and 11 times the area: $6;15$.

This is to solve

$$11x^2 + 7x = 6.$$

The Babylonians actually solved equations of the type $ax^2 + bx = c$ in the cuneiform. In this case $a = 11$, $b = 7$ and $c = \frac{25}{4}$.

step	method	outcome	outcome
1	You multiply 11 by $6;15$	ac	$11 \cdot \frac{25}{4} = 68\frac{3}{4} = 1,8;45$
2	You multiply $3;30$ by $3;30$	$(\frac{b}{2})^2$	$(\frac{7}{2})^2 = \frac{49}{4} = 12;15$
3	You add it to $1,8;45$	$\frac{b^2}{4} + ac$	$81 = 1,21$
4	This is the square of 9	$\sqrt{\frac{b^2}{4} + ac}$	$\sqrt{81} = 9$
5	You substract $3,30$	$-\frac{b}{2} + \sqrt{\frac{b^2}{4} + ac}$	$\frac{11}{2} = 5;30$
6	The inverse of 11 can not be computed		
7	What multiplied by 11, gives $5;30$	$\frac{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + ac}}{a}$	$\frac{11}{2}/11 = 0;30$

Answer: $0;30 = \frac{1}{2}$.

Other problems appeared in BM 13901 are all of this type. It looks like a textbook or a training book for the Babylonians.

Remark 1. Otto Neugebauer was an Austrian mathematician who made important contributions to the history of ancient mathematics and astronomy. He insisted that mathematics developed by Babylonians should be more important than previous acknowledged.

Neugebauer had and still has a huge impact for the well-beings of general mathematical community. He is the founder and first editor of both "Zentralblatt für Matematik" (1931-1938), and "Mathematical Reviews" (1939-1945), and so gave mathematics the essential tool of a working abstracting service. Neugebauer's policy regarding reviews was an interesting one. He always insisted that the length of the review was not intended to be directly proportional to the importance of the paper; indeed, a bad paper needed to have a review sufficiently detailed so that nobody needed to look at the paper itself, whereas a really important paper needed only to be called to the world's attention.

2. Cubic and quartic equations

2.1. The Greeks. The Greeks laid the foundation of modern mathematics, especially through the Elements, the great work of Euclid. Although the bulk of Greek geometry was constructed using plane methods, three problems, squaring the circle (or quadrature of a circle), trisecting an angle, and doubling a cube (or duplicating a cube), defied solution by these methods for centuries. Of the three problems, doubling a cube and trisecting an angle are both about cubic equations, the first $x^3 - 2$ and the second $4x^3 - 3x = c$.

The Greek mathematician Diophantus (c.200AD-c.284AD) was sometimes known as "the father of algebra". He is best known for his great work Arithmetica, an enormous influence work on the development of number theory. Diophantus solved hundreds of algebraic equations in the Arithmetica, and was the first person to use algebraic notation and symbolism. The method for solving indeterminate equations is now known as Diophantine analysis.

2.2. The Arabs: al-Khwārizmī, algebra and algorithm. Most of the Greek works in mathematics, including the Elements and the Arithmetica, were translated into Arabic and preserved by the Arabs. The Arabic mathematicians, most notably Al-Khwārizmī and Al-Karaji, studied the Greeks and made their own contribution to Algebra.

Al-Khwārizmī(c.780- c.850), in full Muḥammad ibn Mūsā al-Khwārizmī, was a Persian mathematician, astronomer, astrologer geographer and a scholar in the House of Wisdom in Baghdad, another candidate of "the father of algebra". He introduced Hindu-Arabic numerals and the concepts of algebra into European mathematics. His greatest mathematical work, Hisab al-Jabr wa-al-Muqabala, in short al-Jabr, is regarded as the foundation and cornerstone of the sciences. The book was translated into Latin in the mid 12th century under the title Liber Algebrae et Almucabola. Today's term "algebra" is derived from the term al-jabr, or al-ğabr, in the title of this book. In the book, Al-Khwārizmī shows how to solve linear and quadratic equations, how to calculate the area and volume of certain geometric shapes, and he introduces the concept of "balancing" when solving equations. In the 12th century a second work by al-Khwārizmī introduced Hindu-Arabic numerals and their arithmetic to the West. It is preserved only in a Latin translation, Algoritmi de numero Indorum ("Al-Khwārizmī Concerning the Hindu Art of Reckoning"). From the name of the author, rendered in Latin as Algoritmi, originated the term algorithm.

Al-Karaji (c.953 AD - c.1029 AD), in full Abū Bakr ibn Muḥammad ibn al-Ḥusayn al-Karajī, was a Persian mathematician who can be regarded as the first person to free algebra from geometrical operations and replace them with the type of operations which are at the core of algebra today. He perhaps is the first person to explicitly pose the congruent number problem, although Diophantus posed a similar one. A congruent number is a positive

whole number that can be the area of a right triangle with rational side lengths. Al-Karaji asked the equivalent problem: for which whole numbers n does there exist a square a^2 so that $a^2 - n$ and $a^2 + n$ are also squares? We now know that n is a congruent number if and only if the cubic equation $y^3 = x^3 - n^2x$ has nontrivial rational solutions.

2.3. Italians in the 16th century(The Renaissance). The discoveries of the algebraic solutions of cubic and quartic equations by the Italians in the 16 century were full of drama. At that time the renaissance was near the end and Italy was city states.

We start with the solution of cubic equations. Note that negative number was not in use at 16th century in Europe, so the general cubic equation was reduced to two types by mathematicians at that time: (I) "the cube and things equal to a number", i.e. $x^3 + px = q$ and (II) "the cube equal to things and number", i.e. $x^3 = px + q$, where p and q are positive numbers.

2.3.1. *del Ferro.* Scipione del Ferro (1465-1526) was a professor at University of Bologna which founded in the 11th century is the oldest university in Europe and was the top university during del Ferro's time. Around 1515, he found how to solve cubic equations. However, he did not publish his discovery and only revealed the secret before his death in 1525 to Antonio Fior, a student who apparently was not so good in mathematics and to Annibale della Nave, his son-in-law and successor as professor at Bologna. He also left a notebook containing the solutions to della Nave. Fior only knew how to solve cubic equations of type (I).

2.3.2. *Tartaglia.* Niccolò Tartaglia (1500-1557) was born in Brescia, Republic of Venice. During the sack of Brescia by the French Army in 1512, he was seriously wounded and could only speak with difficulty thereafter, hence his nickname Tartaglia, or the stammerer.

Tartaglia taught himself mathematics and earned his living teaching science and mathematics at Verona, then moved to Venice at 1534, and settled there until his death. Though very poor during his lifetime, he invested what little money he had on military science, in particular, developing his invention in the field of artillery.

After his mentor's death, Fior wanted to achieve fame for solving cubics. He also heard rumors that Tartaglia can solve cubic equations. Believing that Tartaglia was an impostor, Fior challenged Tartaglia to a public contest. Each was to submit 30 problems for the other by February 22, 1535, and two months were allowed to solve the problems. The loser was to pay 30 dinners to the winner and his friends.

Tartaglia realized the problems from Fior would be of the type (I), which he didn't know how to solve. After some hard work, he found the solution for all types of cubic equations during the night of February 12-13, 1535, eight days before the contest deadline. He gave cubic equations as well as other problems to Fior and Fior indeed offered Tartaglia thirty problems of the form $x^3 + px = q$. Tartaglia was able to solve all thirty of Fior's

problems in less than two hours and easily won the contest. Tartaglia did not take the 30 dinners, feeling that the honor of winning was enough.

We list here several of Fior's problems:

(1) $x^3 + x = 6$,
(2) $4x^3 + 3x = 40$,
(3) $x^3 + x = 5$,
(15) $x^3 + x = 500$,
(30) $x^3 + x = 700$.

Now let us explain Tartaglia's solution of cubic equations. Suppose the cubic equation is

$$x^3 + px + q = 0.$$

Let $x = u + v$, then

$$(u+v)^3 + p(u+v) + q = (u^3 + v^3) + (u+v)(3uv + p) + q = 0.$$

Let $3uv = -p$, $U = u^3$, $V = v^3$, then

$$\begin{cases} U + V = -q, \\ UV = -\frac{p^3}{27}. \end{cases}$$

Hence

$$U, V = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and one real root is

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{1}$$

let j be a primitive 3rd root of unity (i.e., $j^3 = 1$ but $j \neq 1$), then the other two roots are $x = ju + j^2 v$ and $x = j^2 u + jv$, i.e.,

$$x = j\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + j^2\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{2}$$

$$x = j^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + j\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{3}$$

2.3.3. *Cardano.* Girolano Cardano (1501-1576), also called Cardan, is a very colorful and fascinating Renaissance scholar. He was a physician with fame all over Europe, even being summoned to Scotland to treat the Archbishop of St. Andrews. He was also a very famous astrologist. He was also a prolific writer, with works in medicine, mathematics, physics, astronomy and games of chances (including advice on cheating). He even predicted his own death and starved himself to death to fulfill his prediction.

Cardano heard the challenge of Fior and Tartaglia and wanted to know how Tartaglia solved the cubic equations. After several unsuccessful attempt, Cardano promised to introduce Tartaglia to the Spanish Governor of Miilan to help him to secure the fund from the Governor to finance his

research in military science. Tartaglia revealed the secret to Cardano but Cardano should swear under oath that he would never publish it. Ferrari, a student of Cardano which we will talk more was the only other person presented.

Soon after, Ferrari found the method to solve quartic equations in 1540. Cardano began to work on the book Ars Magna (The Great Arts). The solutions of cubic and quartic equations were included in the book. He certainly knew it would be a great book. However, he could not publish this work because of his oath. In 1543, della Nave told Cardano and Ferrari about del Ferro's work, proving that Tartaglia was not the first to discover the solution of the cubics. Cardano published Ars Magna in 1545, convinced that he could break his oath since Tartaglia was not the first to solve the cubics. Ars Magna is the first Latin treatise devoted solely to algebra, perhaps the most important mathematical book published in the Renaissance.

Tartaglia was furious when he discovered that Cardan had disregarded his oath. Next year Tartaglia published a book, New Problems and Inventions which clearly stated his side of the story and his belief that Cardano had acted in extreme bad faith. In the following years, Tartaglia and Ferrari exchanged personal insults, until Tartaglia's death in 1557.

2.3.4. *Ferrari.* Lodovico Ferrari(1522-1565), is a student of Cardano since 1536 when he was 14 years old. After the publish of his solution of quartic equations in Ars Magna, and after he gained upper hand in the dispute with Tartaglia, he himself became famous. Later on he was a professor at Bologna, died quite young and suspicious, probably killed by his sister. In Cardano's obituary to Ferrari, he said: "Life is exceedingly short and old age rare, whoever you love, do not desire them to please too much."

Let us explain Ferrari's solution of the quartic equation

$$x^4 + px^2 + sx + r = 0.$$

Let $z = x^2 + y$, then

$$z^2 = x^4 + 2x^2y + y^2 = (2y - p)x^2 + qx + (y^2 - r).$$

Consider

$$\Delta = q^2 - 4(y^2 - r)(2y - p) = 0.$$

This is a cubic equation of y, which is solvable.

- If there exists $y \neq \frac{p}{2}$ such that $\Delta(y) = 0$, then $z^2 = (Ax + B)^2$ for some A and B, and
$$x = \pm\sqrt{-y \pm (Ax + B)}.$$
- If $y = \frac{p}{2}$ is a solution of $\Delta = 0$, then $q = 0$ and $z^2 = \frac{p^2}{4} - r$. Hence
$$x = \pm\sqrt{-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - r}}.$$

2.3.5. *More advances from the effort to solve cubics and quartics.* The first advance is the introduction of complex numbers. Use the root formulas for cubics, one would experience square roots of negative numbers, even though the root itself is real. Cardano presented the first calculation with complex numbers in Ars Magna. Solving a particular cubic equation, he writes:

> Dismissing mental tortures, and multiplying $5+\sqrt{-15}$ by $5-\sqrt{-15}$, we obtain $25-(-15)$. Therefore the product is 40. .... and thus far does arithmetical subtlety go, of which this, the extreme, is, as I have said, so subtle that it is useless.

Rafael Bombelli (1526-1572) published his influential textbook Algebra in 1572, where he gave extensive discussion of complex numbers and their computation rules.

Another advance is Viète's Theorem about the relationship between roots and coefficients. François Viète (1540-1603), unlike other mathematicians mentioned in this section who are Italians, is actually a French. He introduced the first systematic algebraic notation and presented methods for solving equations of second, third and fourth degree. Viète has been called "the father of modern algebraic notation," and his In artem analyticem isagoge (1591; "Introduction to the Analytical Arts") closely resembles a modern elementary algebra text. He knew the connection between the positive roots of equations and the coefficients of the different powers of the unknown quantity, which nowadays in a more general form is called Viète's Theorem:

THEOREM 1. *Let* $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0=(x-x_1)\cdots(x-x_n)$, *then*

$$a_{n-k}=(-1)^k\sum_{1\le i_1<\cdots<i_k\le n}x_{i_1}\cdots x_{i_k}=(-1)^kS_k(x_1,\cdots,x_n)$$

where $S_k(x_1,\cdots,x_n)$ *is the* k*-th elementary symmetric polynomial of* $x_1,\cdots,x_n$.

CHAPTER 2

Galois Theory

1. Life of Abel and Galois

The impossibility of solving algebraically the general equation of degree ≥ 5 was achieved by two brilliant young mathematicians Abel and Galois. We first give a brief sketch of the life of them.

1.1. Abel. Niels Abel (1802-1829) is a Norwegian Mathematician. When he was born, Norway was part of Denmark. The war between France (led by Napoleon) against other European powers caused huge political and economical trouble for the Norwegians. In 1814, Norway was handed over to Sweden after the end of the Napoleon war. In this difficult time Abel was growing up in Gjerstad in south-east Norway.

Abel went to the Cathedral School in Christiania (current Oslo) in 1815. At first, Abel was not good at school. A new mathematics teacher Bernt Holmboë in 1817 caused remarkable change for Abel. He began to study university level mathematics texts and, within a year of Holmboë's arrival, Abel was reading the works of Euler, Newton, Lalande and d'Alembert. Holmboë was convinced that Abel had great talent and encouraged him greatly, taking him on to study the works of Lagrange and Laplace. In 1820, Holmboë wrote about Abel

> "With the most incredible genius he unites ardour for and interest in mathematics such that he quite probably, if he lives, shall become one of the great mathematicians".

After the death of his father in 1820, there was no money to allow Abel to complete his school education, nor money to allow him to study at university. Holmboë was able to help Abel gain a scholarship to remain at school and Abel was able to enter the University of Christiania in 1821. He grduated in 1822 and published his first paper in 1823.

In 1824, Abel proved the impossibility of solving the general equation of the fifth degree in radicals. He published this work in French by his own expense, and sent this pamphlet to several mathematicians including Gauss, whom he intended to visit in Göttingen.

In 1825, he was given a grant by the Norwegian government to travel abroad. In Winter 1825/26, Abel met August Leopold Crelle in Berlin and they two became close friends. Crelle founded Journal für die reine und angewandte Mathematik (now called Crelle's journal) in 1826, with strong encouragement from Abel. Abel was encouraged by Crelle to write a clearer

version of his work on the insolubility of the quintic and this resulted in Recherches sur les fonctions elliptiques which was published in 1827 in the first volume of Crelle's Journal, along with six other papers by Abel. Abel began to work to establish mathematical analysis on a rigorous basis. While in Berlin, Abel learnt that the position of professor of mathematics at the University of Christiania, the only university in Norway, had been given to Holmboë.

Abel planned to continue his travel to Paris with Crelle and to visit Gauss in Göttingen on the way. However, Crelle couldn't go and news got back to Abel that Gauss was not pleased to receive his work on the insolubility of the quintic (Gauss actually never opened Abel's letter). Abel visited Paris in 1826, but failed to get the recognition he wanted. He returned to Berlin in the winter, disappointed and poor, and then back to Christiania in May 1827.

Now poor and sick, Abel taught first as a tutor then hold temporary position in university of Christiania. He began to compete with Jacobi on the theory of elliptic functions, continued to pour out high quality mathematics as his health continued to deteriorate. He rose to fame in the mathematical world and got a professorship at Berlin by the help of Crelle and French Academy of Science. Then he was seriously ill in winter 1828 and died in April 6, 1829. After Abel's death, unpublished work on the algebraic solution of equations was found:

> "If every three roots of an irreducible equation of prime degree are related to one another in such a way that one of them may be expressed rationally in terms of the other two, then the equation is soluble in radicals."

In 1830 the Paris Academy awarded Abel and Jacobi the Grand Prix for their outstanding work.

Nowadays in analysis and algebra textbooks, we can see many contribution of Abel: abelian group, abelian category, Abel's Lemma etc. He is undoubtedly "one of the great mathematicians" as claimed by his teacher in 1820. The Abel Prize by the Norwegian government was established on January 1, 2002, awarded annually for outstanding scientific work in the field of mathematics. It is one of the most prestigious awards given for outstanding contribution in mathematics, often considered as the Nobel Prize of Mathematics.

1.2. Galois. Évariste Galois (1811-1832) was born in October 25, 1811 at Bourg-la-Reine (a town near Paris), France. He was home schooled by his mother Adelaide Marie Demante until he was 12 years old. Galois' father Nicholas Gabriel Galois was an important man in the community and in 1815 he was elected mayor of Bourg-la-Reine.

First let us explain the political situation in France during Galois' lifetime. In 1811 when Galois was born, Napoleon was at the height of his power. The failed Russian campaign of 1812 was followed by defeats, the

Allies entering Paris on March 31, 1814. Napoleon abdicated on April 6 for the first time and Louis XVIII was installed as King by the Allies. The year 1815 saw the famous one hundred days. Napoleon returned from Elba and entered Paris on March 20, was defeated at Waterloo on June 18 and abdicated for the second time on June 22. Louis XVIII was reinstated as King but died in September 1824, his brother Charles X becoming the new King. In 1830, during July Revolution, Charles X fled and Louis Philippe became the new king of France. During 1815-1830, which was called the Second Restoration in France, the French politics was dominated by the fight between republicans/Bonapartists (supporter of Napoleon) and ultraroyalists (ultras). Galois's parents and himself were ardent republicans.

Galois enrolled at the Lycée of Louis-le-Grand, a prestigious secondary school located in Paris, in the 4th class on October 6, 1823. In February 1827, he enrolled in his first mathematics class and quickly became absorbed in mathematics. Galois' school reports described him as "singular, bizarre, original and closed", and his teacher reported him "intelligence, marked progress but not enough method". In 1828 Galois failed in his first try to enter the École Polytechnique, the most prestigious institute of France at that time.

Galois returned to Louis-le-Grand and took the class of Louis Richard, but mainly studied mathematics himself. In April 1829 Galois had his first mathematics paper published on continued fractions in the Annales de mathématiques. On May 25 and June 1, 1829, he submitted articles on the algebraic solution of equations to the Acaémie des Sciences. Cauchy was appointed as referee of Galois' paper. Cauchy rejected his paper (some parts of it overlapped with Abel's work) and suggested him to revise the manuscript and submit again.

In July 1829, Galois' father committed suicide after a royalist priest forged his signature on many letters to attack his relatives. His father's death great affected Galois' actions. Soon after Galois took the examination of École Polytechnique again and failed for the second time. Galois passed his Baccalaureate examinations and received his degree on December 29, 1829. His mathematics examiner reported:

> This pupil is sometimes obscure in expressing his ideas, but he is intelligent and shows a remarkable spirit of research.

His literature examiner reported:

> This is the only student who has answered me poorly, he knows absolutely nothing. I was told that this student has an extraordinary capacity for mathematics. This astonishes me greatly, for, after his examination, I believed him to have but little intelligence.

As a result of this examination, Galois was admitted to École e Préparatoire (now Écloe Normale Supérieure), at that time an annex to Louis-le-Grand.

After taking Cauchy's advice, Galois rewrote his paper and resubmitted it to compete for the Grand Prize in Mathematics of the Paris Academy. The paper was sent to Fourier, the secretary of Academy of science, however Fourier died in April 1830 and Galois's paper was never found again. Abel and Jacobi won the Grand Prize in June 1830.

On Jan 17, 1831, Galois submitted a third version of his proof to the Academy as invited by Poisson. Poisson and Lacroix rejected his paper on July 4, 1831, say that "his argument is neither sufficiently clear nor sufficiently developed to allow us to judge his rigour, and we are not in a position that enables us to give an opinion in this report".

After Fourier lost his paper, Galois became more and more involved in politics. In July 1830, the director Guigniault locked École e Préparatoire and prevented the students from joining the July Revolution outside. In December 1830, Galois scathingly responded to a letter that Guigniault had written in a student newspaper and was expelled from École e Préparatoire on January 4, 1931. After that Galois tried to give mathematical lessons and tutor low-level mathematics to support himself. He was arrested on May 9, 1831 and acquitted on June 15, 1831, then arrested again in Bastille Day (July 14, 1831). He was released from prison in April 29, 1832. Galois engaged the fateful duel in May 30, 1832 and died the next day in the hospital, with only his younger brother Alfred presented. "... Adieu! I had a lot of left for public good." His last word, to his brother Alfred: "Don't cry! I need all my courage to die at twenty."

On the night (May 29, 1832) before the duel, Galois was so convinced of his impending death that he stayed up all night writing letters to his friend Auguste Chevalier and composing what would become his mathematical testament. In the letter Galois said:

> "I have done several new things in analysis, some of these things concern the theory of equations others concern integral functions.
>
> In the theory of equations, I looked for conditions for the equations to be solvable by radicals,....
>
> My main meditations for sometime now has been directed towards the application of the theory of ambiguity to transcendental analysis. But I do not have time now and my ideas on this immense terrain are not yet well developed.
>
> You will publicly request Jacobi or Gauss to give their opinions, not on the truth but on the importance of these theorems.
>
> After that, I hope there will be people who find profit in attempting to decipher this mess."

Hermann Weyl (1885–1955) said

> "This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind."

After his death, Chevalier and Alfred Galois made copies of his papers and sent them to Gauss, Jacobi and others. They received no answer from Gauss and Jacobi. However the papers reached Liouville who, in September 4 1843, announced to the Academy that he had found in Galois' papers a concise solution.

> ...as correct as it is deep of this lovely problem: Given an irreducible equation of prime degree, decide whether or not it is soluble by radicals.

In 1846, Liouville published Galois' paper (without editing or comments as previously planned) in Journal de Mathématiques Pures et Aplliquées (Liouville's Journal, founded by Liouville in 1836, second oldest continually published Math Journal after the oldest one, Crelle's Journal).

2. Basic theory of groups and field extensions

Galois theory is a theory between groups and field extensions, the fundamental objects in modern abstract algebra. We first recall basic properties about these notions.

2.1. Basic Group Theory.

2.1.1. *Group.* In mathematics, a group is a set equipped with a binary operation (called the group operation or simply the product) that combines any two elements to form a third element in such a way that three conditions called group axioms are satisfied, namely associativity, the identity property and the inverse property. We denote the identity element of a group G by 1. Here are some examples of groups:

- $\mathbb{Z}$, the set of integers with the addition operation, is one of most familiar examples of groups.
- cyclic groups, which are groups generated by one element. An cyclic group of order n (resp. of infinite order) is isomorphic to the additive group $\mathbb{Z}/n\mathbb{Z}$ (resp. $\mathbb{Z}$).
- abelian groups, which are groups whose group law is commutative. The name is in honor of Niels Abel. The group operation of an abelian group is usually denoted as addition with the identity element 0. A finitely generated abelian group is always a direct product of finite copies of cyclic groups.
- S_n: Symmetric group of permutations of n objects, which is of order $n!$.
- $A_n \subseteq S_n$: the alternating group of even permutations of n objects, which is a subgroup of S_n of order $\frac{n|}{2}$.

- Classical groups: groups from linear algebra and matrix theory, such as general linear groups, special linear groups, orthogonal group, unitary groups and symplectic groups.

2.1.2. *Subgroup.* A subgroup H of G, denoted as $H \leq G$ is a subset of G closed under multiplication and inverse. $\{1\}$ and G are trivial subgroups of G. A Finite group of order n is a subgroup of the symmetric group S_n (Cayley's Theorem). For $H \leq G$, a left (right) coset is the set $gH = \{gh \mid h \in H\}$ (Hg). The group G is a disjoint union of left cosets (right cosets) of H. In particular, if G is a finite group, then the order of H is a factor of the order of G (Lagrange's Theorem).

2.1.3. *Normal subgroup.* A subgroup N is called a normal subgroup of G, denoted as $N \lhd G$, if it is closed under conjugacy, i.e., if $x \in N$ then $g^{-1}xg \in N$ for all $g \in G$. We have

$$\mathrm{SL}_n(\mathbb{F}) \lhd \mathrm{GL}_n(\mathbb{F}), \quad A_n \lhd S_n.$$

Furthermore,

- $\{1\}$ and G are trivial normal subgroups of G, and G is called a simple group if G has no nontrivial normal subgroup.
- If $N \lhd G$, then G/N is also a group, called a quotient group of G.

2.1.4. *Group homomorphism.* A group homomorphism $\varphi : G \to G'$ is a map that preserves multiplications, i.e. $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$, its image $\mathrm{im}(\varphi)$ is a subgroup of G', its kernel $\ker(\varphi)$ is a normal subgroup of G, and the induced map $G/\ker(\varphi) \to \mathrm{im}(\varphi)$ is a canonical isomorphism (Fundamental theorem of homomorphism).

2.1.5. *Solvable group.* A finite group G is called solvable if there exists a finite sequence

$$G_0 = \{1\} \lhd G_1 \lhd \cdots \lhd G_r = G,$$

such that G_{i+1}/G_i is abelian (or cyclic) for $0 \leq i \leq r-1$.

- Finite abelian groups are solvable.
- S_3, S_4 and A_4 are solvable. For instance,

$$\{1\} \lhd K_2 = \{(12)(34), (14)(23), (13)(24)\} \lhd A_4 \lhd S_4.$$

- Burnside's Theorem: If $|G| = p^a q^b$ where p, q are primes, then G is solvable.

THEOREM 2 (Galois). *If $n \geq 5$, then A_n is simple and hence not solvable, and S_n is not solvable.*

2.2. Basic Theory of Field Extensions.

2.2.1. *Field.* A field F is a set equipped with two binary operations, the addition $+$ and the multiplication $\times$, such that $(F, +)$ is an abelian group with identity element 0, $(F - \{0\}, \times)$ is an abelian group with identity 1, and the distribution law holds. The examples of fields are well-known:

- The fields of rational numbers $\mathbb{Q}$, of real numbers $\mathbb{R}$ and of complex numbers $\mathbb{C}$.
- For p a prime, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the finite field of p elements.

2.2.2. *Field extension.* If F is a subfield of E, then we call E/F a field extension. In this case, E is a canonical F-vector space. The degree of the extension E/F is defined as $[E : F] = \dim_F E$, the dimension of E as the canonical F-vector space.

- $\mathbb{C}/\mathbb{R}$ is an extension of degree 2, $\mathbb{R}/\mathbb{Q}$ is an infinite extension.
- Let $q = p^f$, then $\mathbb{F}_q/\mathbb{F}_p$ is an extension of degree f.

THEOREM 3. *If $K/E/F$ are field extensions, then $[K : F] = [K : E]\cdot[E : F]$.*

2.2.3. *Construction of fields.* One general way to construct new fields and field extensions is as follows: let R be a commutative ring and $\mathfrak{m}$ be a maximal ideal of R, then the quotient ring $R/\mathfrak{m}$ is a field.

- Take $R = \mathbb{Z}$ and $\mathfrak{m} - p\mathbb{Z}$, one get $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- Let F be a field, $p(x)$ be an irreducible polynomial of degree n over F. Then $F[x]/(p(x))$ is a finite extension of F of degree n.

2.2.4. *Algebraic and transcendental extensions.* Suppose E/F is a field extension and $\alpha \in E$. The field

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \,\middle|\, f(x), g(x) \in F[x], g(\alpha) \neq 0 \right\}$$

is an extension of F. α is called an algebraic element or algebraic over F if $[F(\alpha) : F]$ is finite and a transcendental element or transcendental over F if $[F(\alpha) : F]$ is infinite. E/F is called an algebraic extension if every element in E is algebraic and a transcendental extension if there exists some element in E transcendental over F.

- Any finite extension is algebraic.
- $\mathbb{R}/\mathbb{Q}$ is a transcendental extension.
- $F(x)$, the field of rational functions of one variable over F is transcendental over F. Ditto for $F(x_1, \cdots, x_n)$.

Let $\alpha_1, \cdots, \alpha_n$ be in some extension fields of F. Then

$$F(\alpha_1, \cdots, \alpha_n) = \left\{ \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)} \,\middle|\, f, g \in F[x_1, \cdots, x_n], g(\alpha_1, \cdots, \alpha_n) \neq 0 \right\}$$

is the field extension over F generated by $\alpha_1, \cdots, \alpha_n$. E/F is called finitely generated if $E = F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n$. If $E = F(\alpha)$ for some α, then E is called a simple extension over F.

PROPOSITION 1. (1) *Finite extensions and finitely generated algebraic extensions are the same.*

(2) *Extensions of prime degree are simple extensions.*

THEOREM 4. *Suppose E/F is a field extension and $\alpha \in E$. Let the evaluation homomorphism be* ev $: F[x] \to F[\alpha]$, $x \mapsto \alpha$.

(1) *If α is transcendental over F, then* ev *extends to an isomorphism $F(x) \cong F(\alpha)$.*

(2) *If α is algebraic over F, then there exists a unique monic irreducible polynomial $p(x)$, such that the evaluation map induces an isomorphism $F[x]/(p(x)) \cong F(\alpha) = F[\alpha]$. In this case, $F(\alpha) : F] = \deg p(x)$ and $\{\alpha^i \mid 0 \leq i < \deg p(x)\}$ is a basis of $F(\alpha)$ as an F-vector space, i.e., any element in $F(\alpha)$ can be uniquely written as $\sum_{i=0}^{\deg p-1} a_i\alpha^i$ with $a_i \in F$.*

The polynomial $p(x)$ above is called the minimal polynomial of α.

2.2.5. *Algebraically closed field and algebraic closure.* A field F is called algebraically closed if every polynomial $f(x) \in F[x]$ has a root (and hence all roots) in F. The Fundamental Theorem of Algebra tells us that $\mathbb{C}$ is algebraically closed.

Let F be a field. A field extension E is called an algebraic closure of F if E is an algebraic extension of F such that every polynomial $f(x) \in F[x]$ has a root in E. For any field, there exists a unique algebraic closure (up to isomorphism) which is also an algebraically closed field.

Remark 2. From now on, algebraic extensions of a field F described below are inside a fixed algebraic closure $\overline{F}$ of F.

Example 3. The algebraic closure of $\mathbb{F}_p$ is $\overline{\mathbb{F}}_p = \bigcup_m \mathbb{F}_{p^m}$.

For α an element in the algebraic closure of the field F, let $p(x)$ be its minimal polynomial over F, roots of $p(x)$ are called conjugates or F-conjugates of α. Note that for any polynomial $f(x) \in F[x]$, there are at most $\deg(f)$ roots in any field extension of F (Lagrange's Theorem).

2.2.6. *Homomorphism of fields.* Suppose E and F are fields, $\sigma : F \to E$ is homomorphism (hence $\sigma(0) = 0$, and $\sigma(1) = 1$), then $\ker\sigma = 0$ and σ must be an embedding of fields.

Suppose E and E' are extensions of F, a homomorphism $\sigma : E \to E'$ is called an F-homomorphism if $\sigma|_F$=id, i.e. $\sigma(x) = x$ for all $x \in F$. There is one key fact for F-homomorphism: if $\alpha \in E$ and $p(x) \in F[x]$ such that $p(\sigma) = 0$, then $\sigma(p(\alpha)) = p(\sigma(\alpha)) = 0$, hence the image $\sigma(\alpha) \in E'$ of α must be a root of $p(x)$.

Proposition 2. *Suppose E is a simple extension of degree n over F. Then for any field extension E'/F, there are at most n F-homomorphisms from E to E'.*

Proof. The minimal polynomial $p(x)$ of α is of degree n and has at most n roots in E', so there are at most n possibilities for the image of α, but an F-homomorphism is completely determined by the image of α. □

If $E = E'$ is a finite extension of F, then an F-homomorphism $\sigma : E \to E$ is an injective F-linear map of the finite dimensional F-vector space E to itself, hence σ must also be surjective, i.e., an F-homomorphism $E \to E$ must be an F-automorphism. Then Proposition 2 implies that there are at most n F-automorphisms for any simple extension of degree n, which can be generalized to

PROPOSITION 3. *For any finite extension E/F, there are at most $[E:F]$ F-automorphisms of E.*

3. Galois Theory

3.1. Galois Groups and Galois Extensions.

3.1.1. *Galois group.* Let E/F be a finite field extension, the Galois group of E/F is the group

$$\mathrm{Gal}(E/F) := \mathrm{Aut}_F(E) = \{\sigma : E \to E, \sigma \text{ is an } F\text{-automorphism}\}$$

with its group operation given by composition. Then Proposition 3 means that $\mathrm{Gal}(E/F)$ is a finite group of order $\leq [E:F]$.

DEFINITION 1. E/F is called a Galois extension if $|\mathrm{Gal}(E/F)| = [E:F]$.

EXAMPLE 4. Let $E = \mathbb{Q}(\sqrt[3]{2})$. The only $\mathbb{Q}$-conjugate of $\sqrt[3]{2}$ in E is itself, hence $\mathrm{Gal}(E/Q) = 1$.

EXAMPLE 5. Let $F = \mathbb{F}_p(x)$ and $E = F(\alpha)$ with α satisfying $\alpha^p = x$. The minimal polynomial of α is $X^p - x = (X-\alpha)^p$, hence $\mathrm{Gal}(E/F) = 1$.

EXAMPLE 6. Let $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$, then:

(1). $[E:F] = m$.

(2). $E^\times = \mathbb{F}_{q^m}^\times$ is a cyclic group of order $q^m - 1$, let α be a generator of $E^\times$ and $p(x)$ be the minimal polynomial of α in $F = \mathbb{F}_q$, then $\deg p(x) = m$.

(3). For any $c \in \mathbb{F}_q, c^q = c^{q-1} \cdot c = c$, hence $p(\alpha^q) = p(\alpha)^q = 0$, then $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$ are distinct roots of $p(x)$, and

$$p(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}).$$

(4). One checks that $\sigma_q : E \to E, t \mapsto t^q$ is an F-homomorphism of E (q-Frobenius). Hence $\sigma_q \in \mathrm{Gal}(E/F)$, moreover $\sigma_q^m = 1$ and $\sigma_q^i \neq 1$ for $i < m$, then $\langle \sigma_q \rangle$ is of order $m = [E:F] \geq |\mathrm{Gal}(E/F)|$. Hence E/F is a Galois extension and

$$\mathrm{Gal}(E/F) = \langle \sigma_q \rangle \cong \mathbb{Z}/m\mathbb{Z}$$

is cyclic of order m.

3.1.2. *Splitting Field and Normal extension.*

DEFINITION 2. Let F be a field and $f(x) \in F[x]$.

(1) $f(x)$ splits in a field extension E/F if $f(x)$ can be factorized into linear factors in E, i.e.

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n), \quad \alpha_i \in E.$$

(2) The splitting field of $f(x)$ is the minimal field extension E_f in an algebraic closure of F where $f(x)$ splits. In other words, $E_f = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_i (1 \leq i \leq n)$ are the roots of $f(x)$ in the algebraic closure.

EXAMPLE 7. (1) The splitting field of $f(x) = (x^2-2)(x^2-3)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(2) The splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

(3) The splitting field of $f(x) = x^{q^n} - x$ or any monic irreducible polynomial of degree n over $\mathbb{F}_q$ is $\mathbb{F}_{q^n}$.

(4) The algebraic closure $\overline{F}$ of F is the field that every polynomial over F splits.

DEFINITION 3. (1) An algebraic extension E/F is called a normal extension if for any $\alpha \in E$, the minimal polynomial $p(x)$ of α splits in E, i.e. all conjugates of α are also in E.

(2) For an algebraic extension L/F, the normal closure is the minimal normal extension of F containing L in the algebraic closure.

If L/F is a finite extension, write $L = F(\alpha_1, \cdots, \alpha_t)$, let E is the field generated by all conjugates of $\alpha_1, \cdots, \alpha_t$. Then E is the normal closure of L/F.

EXAMPLE 8. The normal closure of $L = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

3.1.3. *Separable extension.*

DEFINITION 4. (1) An irreducible polynomial $f(x) \in F[x]$ is called separable if it has no multiple roots in the algebraic closure of F, equivalently, if $\gcd(f(x), f'(x)) = 1$.

(2) A general polynomial $f(x)$ is separable if its irreducible factors are all separable, otherwise, $f(x)$ is called inseparable.

DEFINITION 5. Let E/F be an algebraic extension.

(1) An element $\alpha \in E$ is called separable over F if its minimal polynomial $p(x) \in F[x]$ is separable.

(2) E/F is called a separable extension if all elements in E are separable over F. Otherwise, it is called inseparable, and purely inseparable if there exists no separable elements in $E \backslash F$.

Let E/F be an algebraic extension. Then the set of separable elements over F form a subfield of E. The separable closure of F is the separable extension of F such that every separable polynomial in $F[x]$ splits, which is also the subfield of $\overline{F}$ of separable elements.

EXAMPLE 9. (1) Any algebraic extension of a finite field is separable.

(2) If F is a field of characteristic 0 (for example a subfield of $\mathbb{C}$), then any algebraic extension of F is separable over F. Hence the algebraic closure and the separable closure of F are the same thing.

(3) Let $F = \mathbb{F}_p(x)$ and $E = \mathbb{F}_p(x, \sqrt[p]{x}) = \mathbb{F}_p(\sqrt[p]{x})$, then $\sqrt[p]{x}$ is not separable over F and E/F is an inseparable extension.

The following statement is a key theorem in Galois theory.

THEOREM 5 (Primitive Element Theorem). *Finite separable extensions are simple extensions.*

3.1.4. *Equivalent definition of Galois Extension.* The following theorem gives equivalent definition of a Galois extension:

THEOREM 6. *Let E/F be a finite field extension. Then the following are equivalent:*

(1) *E/F is a Galois extension.*

(2) *E/F is a normal separable extension.*

(3) *E is the splitting field of a separable polynomial $f(x) \in F[x]$.*

Consequently, if L/F is a finite separable extension, then the normal closure E of L is Galois over F and called the Galois closure of L/F; if f is separable and irreducible, then E_f/F is Galois and $\mathrm{Gal}(E_f/F)$ is of order $\deg(f)$.

EXAMPLE 10. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbb{Q}$, then E is the splitting field of $(x^2-2)(x^2-3)$, so $E/\mathbb{Q}$ is Galois. Note that

(1). $[E : \mathbb{Q}] = 4 \Longrightarrow |\mathrm{Gal}(E/\mathbb{Q})| = 4$.

(2). For $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, σ is determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$, but $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Therefore $\mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong K_2$, where

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3};$$
$$\tau(\sqrt{2}) = \sqrt{2},\ \tau(\sqrt{3}) = -\sqrt{3}.$$

EXAMPLE 11. Suppose $p > 2$ is a prime, the p-th cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p-1}{x-1}$ is an irreducible polynomial and is the minimal polynomial of ζ_p, hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma(\zeta_p) = \zeta_p^a$, this gives an injective homomorphism: $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times, \sigma \mapsto a$. Since both sides are of order $p-1$ we have $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$.

3.2. Fundamental Theorem of Galois Theory. Let E/F be a finite Galois extension and $G = \mathrm{Gal}(E/F)$. Then clearly G acts on the field E and F is stable by the G-action. Moreover, for any subgroup $H \leq G$, set $E^H := \{x \in E \mid h(x) = x, \text{ for all } h \in H\}$, this is a subfield of E and called the invariant subfield of H.

THEOREM 7. *Let E/F be a finite Galois extension and $G = \mathrm{Gal}(E/F)$. Then there is a one-to-one correspondence between the set of intermediate fields in E/F and subgroups of G given by*

$$L \longrightarrow \mathrm{Gal}(E/L)$$
$$E^H \longleftarrow H$$

such that

(1) *For every intermediate field L of E, E/L is a Galois extension, i.e. $[E : L] = \mathrm{Gal}(E/L)$.*

(2) *For every subgroup H of G, $|H| = [E : E^H]$.*

(3) *L/F is Galois if and only if $H = \mathrm{Gal}(E/L)$ is a normal subgroup of G, and in this case $G/H \cong \mathrm{Gal}(L/F)$ induced by $g \mapsto g|_L$.*

EXAMPLE 12. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ The $G = \mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where $\sigma : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3}$ and $\tau : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}$.

G has 5 subgroups: $\{1\}, \{1, \sigma\}, \{1, \tau\}, \{1, \sigma\tau\}$ and G, corresponding to 5 subfields of E: $E, \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}$ respectively.

By the fundamental theorem, one sees immediately $E^G = F$. In fact, we have

THEOREM 8. *Suppose G is a finite group acting on the field E. Then E/E^G is a Galois extension with the Galois group G.*

EXAMPLE 13. Let K be a field and $E = K(x_1, \cdots, x_n)$ be the field of rational functions of n variables over K. Let s_i be the i-th symmetric polynomial of $x_1, \cdots, x_n$:

$$s_i = \sum_{1 \le k_1 < \cdots < k_i \le n} x_{k_1} \cdots x_{k_n}.$$

The symmetric group S_n acts on E by $\sigma(x_i) = x_{\sigma(i)}$, and $E^{S_n} = K(s_1, \cdots, s_n)$. Thus E/E^{S_n} is a Galois extension with Galois group S_n.

4. Applications of Galois Theory

4.1. Radical Extensions.

DEFINITION 6. A finite extension E/F is called a radical extension if there exists a sequence of field extensions

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = E$$

such that $F_{i+1} = F_i(\sqrt[k_i]{a_i})$ for some $a_i \in F_i$ and $k_i \in \mathbb{Z}_+$. In other words, E/F is a radical extension if every element of E is obtained by finite steps of addition, subtraction, multiplication, division and root extraction of elements of F.

The following Theorems answer the insolubility of general polynomial of degree ≥ 5:

THEOREM 9 (Galois). *Let F be a subfield of $\mathbb{C}$, Let a_i $(0 \le i \le n-1)$ be indeterminates over F and $K = F(a_0, a_1, \cdots, a_{n-1})$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - r_1) \cdots (x - r_n)$. Then $N = F(r_1, \cdots, r_n)$ is a Galois extension over K and $\mathrm{Gal}(N/K) \cong S_n$.*

REMARK 3. If $\sigma \in \mathrm{Gal}(N/K)$, then $\sigma : r_i \mapsto r_j$ and hence σ induces a permutation of $\{r_1, \cdots, r_n\}$, this defines an injective group homomorphism $\mathrm{Gal}(N/K) \hookrightarrow S_n$. Galois's result tells us that this is actually an isomorphism.

THEOREM 10 (Abel-Galois). *Let F be a subfield of $\mathbb{C}$, $f(x) \in F[x]$ and E_f be the splitting field of $f(x)$ over F. Then*

(1) *E_f is a radical extension of F if and only if $G_f = \mathrm{Gal}(E_f/F)$ is a solvable group.*

(2) *If f is irreducible, $\deg f = n \geq 5$ and f is in general position, then $G_f \cong S_n$ and E_f is not a radical extension of F.*

4.2. Revisit to cubic and quartic equations.

4.2.1. *Cubic equations.* It suffices to consider the cubic equation $x^3 + px + q = 0$ with p, q indeterminates. Let $K = \mathbb{Q}(p, q, j)$ with j being the third primitive root of unity. Let N be the splitting field of $x^3 + px + q$ over K, then $\mathrm{Gal}(N/K) \cong S_3$ by Galois. Suppose the three roots are a, b and c. Then S_3 can be identify with permutations of a, b, c. Let $\sigma = (abc)$, then $\sigma^2 = (acb)$ and the alternating group $A_3 = \{1, \sigma, \sigma^2\}$. Note that

$$\Delta := (a-b)^2(b-c)^2(c-a)^2 \in K,$$
$$\delta = \sqrt{\Delta} := (a-b)(b-c)(c-a) \notin K,$$

as Δ is fixed by all permutations and δ is not fixed by (ab). By Galois Theory, the only quadratic sub-extension L inside N/K is $K(\delta)$. Now $[N : L] = 3$ is a prime, then for any $\alpha \notin L$, one must have $N = L(\alpha)$.

$$\begin{array}{ccc} 1 & & N = L(\alpha) \\ {\scriptstyle 3}\big| & & {\scriptstyle 3}\big| \\ A_3 & & L = K(\delta) \\ {\scriptstyle 3}\big| & & {\scriptstyle 3}\big| \\ S_3 & & K \end{array}$$

Lagrange defined the so called Lagrange resolvent:

$$(j, a) = a + jb + j^2 c.$$

Similarly one defines (j^2, a). We see that $(j, a) \neq 0$. Indeed, if $(j, a) = 0$, then $\sigma(j, a) = \sigma^2(j, a) = 0$, and

$$\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix} \begin{pmatrix} 1 \\ j \\ j^2 \end{pmatrix} = 0,$$

which is impossible as the determinant of the matrix on the left hand side is $\delta \neq 0$. Now $\sigma(j, a) = j^2(j, a)$, we have $(j, a) \notin L$ and $N = L((j, a))$.

By Viète's Theorem, we know

$$a + b + c = 0,\ ab + bc + ca = p,\ abc = -q.$$

Then d and δ can be expressed in terms of p and q:

$$d = -27q^2 - 4p^3, \quad \delta = \pm\sqrt{-27q^2 - 4p^3}.$$

By calculation

$$(j,a)^3 = (a+jb+j^2c)^3 = -\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\delta.$$

Hence we obtain three values of (j,a). Similarly $(j^2,a)^3 = -\frac{27}{2}q + \frac{3i\sqrt{3}}{2}8\delta$. Moreover (j,a) and (j^2,a) are related by the relation:

$$(j,a)(j^2,a) = -3p.$$

Thus we obtain the three pairs of values of (j,a) and (j^2,a). Now the relations

$$\begin{cases} 3a = (j,a) + (j^2,a) \\ 3b = j^2(j,a) + j(j^2,a) \\ 3c = j(j,a) + j^2(j^2,a) \end{cases}$$

gives the values of a, b, c.

4.2.2. *Quartic equations.* Let p, q, r be indeterminates, $K = \mathbb{Q}(p,q,r,j)$ with $j^3 = 1$. The quartic polynomial we consider is

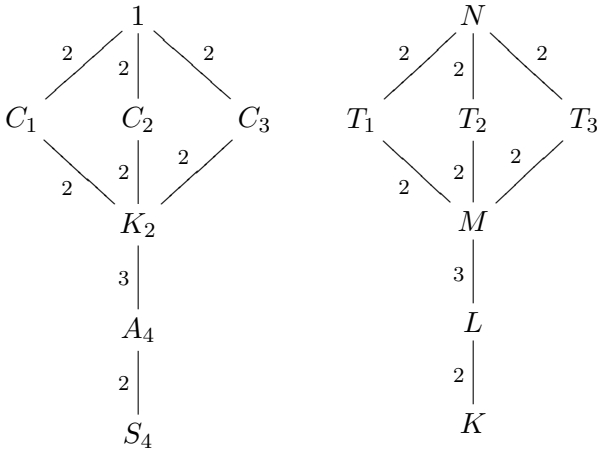
$$f(x) = x^4 + px^2 + qx + r = (x-a)(x-b)(x-c)(x-d).$$

Let $N = K(a,b,c,d)$ be the splitting field of $f(x)$. Then N/K is a Galois extension with $\mathrm{Gal}(N/K) = S_4$, identifying with permutations of a, b, c, d. We have the sequence

$$1 \subseteq K_2 = \{1, (ab)(cd), (ad)(bc), (ac)(bd)\} \subseteq A_4 \subseteq S_4$$

and K_2 has three subgroups of order 2:

$$C_1 = \{1, (ab)(cd)\},\ C_2 = \{1, (ac)(bd)\},\ C_3 = \{1, (ad)(bc)\}.$$



Again we have

$$\Delta = (a-b)^2(a-c)^2(a-d)^2(b-c)^2(b-d)^2(c-d)^2 \in K,$$
$$\delta = (a-b)(a-c)(a-d)(b-c)(b-d)(c-d) \in L \backslash K.$$

Then $L = K(\delta)$. Let

$$u = (a+b)(c+d),\ v = (a+c)(b+d),\ w = (a+d)(b+c).$$

We have

(1) For $\sigma = (abc) \in A_4$, $\sigma(u) \neq u$, then $u \notin L$. For all $\tau \in K_2$, $\tau(u) = u$, then $u \in M$, hence $M = L(u)$ (and $= L(v) = L(w)$).

(2) One knows $a+b \notin M$ but $a+b \in T_1$, then $T_1 = M(a+b)$. Similarly $T_2 = M(a+c)$ and $T_3 = M(a+d)$.

(3) By computation

$$\begin{cases} u+v+w = 2p \\ uv+vw+wu = p^2-4r \\ uvw = -q^2 \end{cases}$$

Then u, v, w, are roots of

$$y^3 - 2py^2 + (p^2-4r)y + q^2 = 0,$$

called the resolvent equation of the quartic equation. Then

$$\begin{cases} (a+b)+(c+d) = 0 \\ (a+b)(c+d) = u \end{cases} \implies \begin{cases} a+b = \sqrt{-u}, \\ c+d = -\sqrt{-u}. \end{cases}$$

similarly,

$$a+c = \sqrt{-v},\ b+d = -\sqrt{-v},\ a+d = \sqrt{-w},\ b+c = -\sqrt{-w},$$

one can get a, b, c, d.

4.3. Other Applications.

THEOREM 11. *If $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of prime degree $p \geq 5$ with only two imaginary roots, then $G_f \cong S_p$.*

PROOF. Let E be the splitting field of $f(x)$. We have

(1) The map $G_f \to S_p$, $\sigma \mapsto$ induced permutation of roots of $f(x)$ is injective and one may regard G_f as a subgroup of S_p.

(2) By $\deg f = p$, $p \mid [E:\mathbb{Q}]$, then G_f contains a p-cycle.

(3) Let τ be the complex conjugation, then $\tau|_E \in G_f$ fixes all real roots and interchanges the imaginary roots, hence $\tau|_E$ is a 2-cycle.

(4) A 2-cycle (ij) and a p-cycle $(a_1 a_2 \cdots a_p)$ generate S_p. □

THEOREM 12 (Galois). *If $f(x)$ is irreducible of prime degree over $K \subseteq \mathbb{C}$, $x_1, \cdots, x_p$ are roots of $f(x)$ and $N = K(x_1, \cdots, x_p)$, then N/K is a radical extension if and only if $N = K(x_i, x_j)$ for any pair $i \neq y$, i.e. any other root is a rational function of some two roots.*

The following theorem is about the construction with ruler and compass in field theory:

THEOREM 13. *For $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$, let $F = \mathbb{Q}(\alpha_1, \cdots, \alpha_k)$. Then the constructibility of some $\alpha \in \mathbb{R}$ with points $0, 1, \alpha_1, \cdots, \alpha_k$ given by ruler and compass if and only if there exists a tower of quadratic extensions: $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k$ such that $\alpha \in F_k$.*

EXAMPLE 14. (1) Duplication of cube, which is equivalent to construct $\sqrt[3]{2}$ from $\mathbb{Q}$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, then there exists no tower of quadratic extensions such that $\sqrt[3]{2}$ is in the tower.

(2) Trisection of the angle, $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Given $t = \cos 3\theta$, find x such that $4x^3 - 3x - t = 0$. But in general $[\mathbb{Q}(x, t) : \mathbb{Q}(t)] = 3$, for example $\theta = \frac{\pi}{9}, t = \frac{1}{2}$, again not possible.

Galois theory then implies the following famous theorem of Gauss:

THEOREM 14 (Gauss). *There exists a construction of regular p-polygon by straight ruler and compass if and only if $p = 2^{2^n} + 1$ is a Fermat prime.*

PROOF. On one side, the constructibility implies $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ is a power of 2, then p must be a Fermat prime. On the other side, if p is a Fermat prime, then $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a cyclic group of 2-power, then has a sequence of subgroups of index 2. □

CHAPTER 3

Kummer and the Birth of Algebraic Number Theory

1. Number Theory before Kummer

In short, number theory before Kummer can be described as: two great books: The Elements by Euclid (about 300 BC) and Disquisitiones Arithmeticae by Carl Friedrich Gauss (1777–1855); four great theorems: the fundamental theorem of arithmetic, Fermat's little theorem (and its generalization Euler's Theorem), Chinese Remainder Theorem and Quadratic Reciprocity Law; and one great problem: Fermat's Last Theorem.

Let us recall the definition of congruences. For $m > 1$ an integer (called the modulus), the congruence relation $x \equiv y \mod m$ means that $m \mid (x-y)$, i.e. x and y have the same remainder when divided by m. Congruence relation is an equivalence relation. The number of congruent classes modulo m is m.

1.1. Two great books.

1.1.1. *The Elements.* The Elements, perhaps the most important and successful mathematical textbook of all time, is the classic treatise in geometry and number theory written by Euclid in 300BC. The Elements are divided into 13 "books" (an archaic word for "chapters"). Three of them, Books VII-X, were dealing with numbers and integers. It is the real beginning of number theory, including a series of theorems on the properties of numbers and integers,

Among the great theorems about number theory in the Elements are Euclid's first theorem which we shall describe later, and Euclid's second theorem which states that the number of primes is infinite. This beautiful theorem was proved by Euclid in Proposition IX.20 of the Elements (Tietze 1965, pp. 7-9), the first theorem in the history of mathematics concerning the infinitude. Let's recall the elegant proof of Euclid.

THEOREM 15. *There are infinite number of primes.*

PROOF. Suppose there are only finite number of primes, say $p_1, \cdots p_n$. Let $N = p_1 \cdots p_n + 1$. Then any prime factor of N must be a new prime, a contradiction. □

The Euclidean algorithm, also called Euclid's algorithm, is an algorithm for finding the greatest common divisor of two numbers, was given in Book

VII for rational numbers and Book X for reals. It is the earliest example of an integer relation algorithm and still in use.

1.1.2. *Disquisitiones Arithmeticae.* This classic is the most important mathematical work by Gauss, published in 1801 when he was 24 years old. This book is the end of elementary number theory and the beginning of algebraic number theory. In it Gauss organized and summarized much of the work of his predecessors before moving boldly to new and deeper directions in the frontier of research.

Gauss provided the first modern proof of the Fundamental Theorem of Arithmetic. To expedite his work, Gauss introduced the idea of congruence among numbers—i.e., he defined a and b to be congruent modulo m (written $a \equiv b \mod m$) if m divides evenly into the difference ab. Through this innovation, he was able to present the theory of numbers before him in a very elegant way.

Gauss also gave the first rigorous proof of the quadratic reciprocity law. His work suggested that there were profound connections between the original question and other branches of number theory, a fact that he perceived to be of signal importance for the subject. He extended Lagrange's theory of quadratic forms by showing how two quadratic forms can be "multiplied" to obtain a third. Later mathematicians were to rework this into an important example of the theory of finite commutative groups. And in the long final section of his book, Gauss gave the theory (Theorem **??**) that lay behind his first discovery as a mathematician: that a regular 17-sided figure can be constructed by circle and straightedge alone.

> "Whatever set of values is adopted, Gauss's Disquisitiones Arithmeticae surely belongs among the greatest mathematical treatises of all fields and periods."—Asger Aaboe.

1.2. Four great theorems.

1.2.1. *Fundamental Theorem of Arithmetic.* Known also as the unique factorization theorem, this theorem states that

THEOREM 16. *Every positive integer (except* 1*) is uniquely factorized as a finite product of one or more prime numbers.*

The first strict proof of this theorem was given by Gauss in Disquisitiones Arithmeticae, which is a consequence of Euclid's Lemma (Euclid's first theorem) in the Elements:

THEOREM 17. *If prime* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

1.2.2. *Fermat's Little Theorem and Euler's Theorem.* Pierre de Fermat (1601-1665) is a French mathematician who is often called the founder of the modern theory of numbers. Independently of René Descartes (1596-1650), Fermat discovered the fundamental principle of analytic geometry. Through his correspondence with Blaise Pascal (1623-1662) he was a co-founder of the theory of probability. Fermat's favorite field of study is the

theory of numbers, but unfortunately he found no correspondent to share his enthusiasm.

THEOREM 18 (Fermat). *If p is a prime number, then for any integer a not divisible by p, $a^{p-1} \equiv 1 \bmod p$, i.e. $p \mid a^{p-1} - 1$.*

Note that Euler's totient function $\varphi n \mapsto \varphi(n)$ where $\varphi(n)$ is the order of the multiplicative group

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \mid 0 < a < n,\ \gcd(a, n) = 1\}.$$

Then $\varphi(p) = p - 1$ and Fermat's Little Theorem has the following generalization by Swiss great mathematician Leonhard Euler(1707-1783):

THEOREM 19 (Euler). *Let n be a position integer. Then for any integer a prime to n, $a^{\varphi(n)} \equiv 1 \bmod n$, i.e. $n \mid a^{\varphi(n)} - 1$.*

Certainly Euler's Theorem can be regarded as a special case of Lagrange's Theorem that the order of a group element divides the order of the group.

1.2.3. *Chinese Remainder Theorem.* Originating from a problem in Sunzi Suanjin (Master Sun's Mathematical Classic) in the third century and therefor known as Sun Zi's Theorem in China, this is probably the greatest theorem discovered by Chinese mathematicians. Today this theorem has evolved into a systematic theorem about rings and modules that can easily be found in any standard textbook about elementary number theory and abstract algebra.

For $m > 1$ an integer, the congruent relation $x \equiv y \mod m$ means that $m \mid (x - y)$, i.e. x and y have the same remainder when divided by m. Then Chinese Remainder Theorem is about the solution of simultaneous systems of linear congruences.

THEOREM 20. *Suppose m and n are coprime integers. Then the system of congruent equations*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

is solvable and the set of all solutions forms a congruent class modulo mn.

1.2.4. *Quadratic reciprocity law.* Let p be a prime. For $a \in \mathbb{Z}$, the Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{if } p \nmid a \text{ and } a \mod p \text{ is a square;} \\ -1, & \text{if } a \mod p \text{ is not a square;} \\ 0, & \text{if } p \mid a. \end{cases}$$

We may assume p is an odd prime. By definition $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$, so the Legendre symbol $\left(\frac{a}{p}\right)$ is determined by the values of $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$

($q \neq p$ is an odd prime) by the Fundamental Theorem of Arithmetic. One can first find

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \tag{4}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{5}$$

The quadratic reciprocity law is the following theorem of Gauss:

THEOREM 21 (Gauss). *Let p and q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{6}$$

This deep result was previously conjectured by Euler and falsely proved by Legendre. It is the starting point of modern number theory. From then on, seeking higher reciprocity laws became the main theme of number theory study.

1.3. One great problem: Fermat's Last Theorem. This assertion is one of the most famous statements from the history of mathematics. While reading Diophantus's Arithmetica, Fermat wrote in 1637 in the book's margin: "To divide a cube into two cubes, a fourth power, or in general any power whatever into two powers of the same denomination above the second is impossible." He added that "I have assuredly found an admirable proof of this, but the margin is too narrow to contain it." In symbols, this statement came to be known as Fermat's Last Theorem:

PROBLEM 1. For $n \leq 3$, $x^n+y^n = z^n$ has no non-trivial integer solutions, i.e. has no solutions $(x, y, z) \in \mathbb{Z}$ such that $xyz \neq 0$.

For three and a half centuries, Fermat's Last Theorem defeated all who attacked it, earning a reputation as the most famous unsolved problem in mathematics.

1.4. Birth of analytic number theory. It was Euler who started to use analytic tools to study number theory. In 1737, Euler introduce the Euler-Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \ (s \in \mathbb{R},\ s > 1).$$

He also obtained the Euler product that for $s > 1$,

$$\zeta(s) = \prod_{p\ prime} \frac{1}{1-p^{-s}}.$$

Through the product and the fact that the harmonic series is divergent, he was able to prove Euclid's second Theorem (Theorem 15) that there are infinite many prime numbers.

Lejeune Dirichlet (1805-1859) proved in 1837 that in any arithmetic progression with first term coprime to the difference there are infinitely many primes. This had been conjectured by Gauss. Dirichlet introduced the now-called Dirichlet series (as complex functions) and employed the techniques of calculus to establish his theorem. This surprising but ingenious strategy marked the beginning of a new branch of the subject: analytic number theory.

1.5. Effort to develop higher reciprocity laws. Inspired by Gauss's works on the theory of numbers, especially his proof of quadratic reciprocity law, young German mathematicians, notably Jacobi, Eisenstein and Kummer, were drawn to the subject to develop higher reciprocity laws.

2. Status of Fermat's Last Theorem before Kummer

The study of sum of squares had a long history. It was initiated by the Babylonians. They found, for example, $119^2 + 120^2 = 169^2$. By elementary technique, we know that

THEOREM 22. *Any triple of positive integers* (a, b, c) *satisfying*
(1) $a^2 + b^2 = c^2$,
(2) a, b, c *are pairwise coprime,*
(3) b *is even*
must be of the form

$$a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2,\ (\gcd(m, n) = 1\ \ 2 \mid mn).$$

Fermat claimed that an odd prime is a sum of two squares if and only if it is of the form $4k + 1$. This fact (and many other claims of Fermat) was proved by Euler. Joseph-Louis Lagrange (1736-1813) proved in 1770 that

THEOREM 23 (Lagrange's four square theorem). *Every positive integer is a sum of at most four squares (of integers).*

In Disquisitiones Arithmeticae Gauss proved

THEOREM 24. *A positive integer* n *is a sum of three squares if and only if* n *is not of the form* $4^k(8m + 7)$.

Fermat's Last Theorem is about sum of powers. The case $n = 4$ was proved by Fermat himself. He invented the infinite descent technique to show that $x^4 + y^4 = z^2$ is not solvable over $\mathbb{Z}$. This method would play an important role in the eventual proof of FLT by Andrew Wiles in 1995. Euler deduced the $n = 3$ case, though there were some gap in his proof. He introduced a proof involving numbers of the form $a + b\sqrt{3}$ for integers a and b. His approach would eventually lead to Kummer's major work which we shall explain soon.

If $n = 5$, assuming (x, y, z) is a primitive solution, then $10 \mid xyz$. There are two cases to consider: (i) one of x, y, z is divisible by 10, (ii) One of x, y, z is even and a different one is divisible by 5. In 1825, Dirichlet proved

(i) and then Legendre proved (ii). Dirichlet's proof (which is his first paper) brought him instant fame. He also proved the case $n = 14$ and nearly proved $n = 7$ which was solved by Gabriel Lamé (1795-1870).

Now to prove Fermat's Last Theorem, one may assume that

> $n = l$ is an odd prime, x, y, z are pairwise coprime, and either (I) $l \nmid xyz$ or (II) $l \mid z$ (hence $l \nmid x$).

French female mathematician Sophie Germain(1776-1831) proved the following theorem, the most important result related to Fermat's Last Theorem until the contributions of Kummer in 1840s.

THEOREM 25 (Sophie Germain). *If there exists an auxiliary prime p, such that*

(1) If $A^l + B^l + C^l \equiv 0 \mod p$, then one of A, B, C must be divisible by p,
(2) $X^l \equiv l \mod p$ has no solution,

then Case I of FLT is true for l.

PROOF. Suppose x, y, z are pairwise relatively prime, prime to l and $x^l + y^l + z^l = 0$. Then

$$-x^l = y^l + z^l = (y + z)\sum_{i=0}^{l-1}(-1)^i y^i z^{l-1-i}.$$

Note that

$$\begin{aligned}\gcd(y + z, \sum_{i=0}^{l-1}(-1)^i y^i z^{l-1-i}) &= \gcd(y + z, \sum_{i=0}^{l-1}(-1)^i y^i (y + z - y)^{l-1-i}) \\ &= \gcd(y + z, l y^{l-1}) = 1,\end{aligned}$$

since $l \nmid y + z$ (otherwise $l \mid x$) and $\gcd(y, z) = 1$. Hence,

$$y + z = a^l, \quad \sum_{i=0}^{l-1}(-1)^i y^i z^{l-1-i} = \alpha^l, \quad x = -a\alpha.$$

By the same argument,

$$z + x = b^l, \quad \sum_{i=0}^{l-1}(-1)^i z^i x^{l-1-i} = \beta^l, \quad y = -b\beta,$$

$$x + y = c^l, \quad \sum_{i=0}^{l-1}(-1)^i x^i y^{l-1-i} = \gamma^l, \quad z = -c\gamma.$$

Now $x^l + y^l + z^l \equiv 0 \mod p$ implies that one of $x, y, z \equiv 0 \mod p$.

Assume $x \equiv 0 \mod p$. Then $2x = b^l + c^l + (-a)^l = 0 \mod p$, hence one of $a, b, c \equiv 0 \mod p$.

If b or $c \equiv 0 \mod p$, then $y \equiv 0 \mod p$ and $z \equiv 0 \mod p$, which is impossible. Hence $a \equiv\equiv 0 \mod p$ and $y \equiv -z \mod p$. Hence

$$\left.\begin{array}{ll} \alpha^l \equiv l y^{l-1} & \mod p \\ \gamma^l \equiv y^{l-1} & \mod p \end{array}\right\} \Rightarrow \alpha^l \equiv l\gamma^l \mod p.$$

and since

$$\left.\begin{array}{ll} y \neq 0 & \mod p \\ \alpha, \gamma \neq 0 & \mod p \end{array}\right\} \Rightarrow \frac{\alpha^l}{\gamma^l} \equiv l \mod p.$$

This is a contradiction to (2): $x^l \equiv l \mod p$ has no solution. □

Example 15. Suppose both l and $2l+1$ are odd primes. Then, $l = \frac{p-1}{2}$ and

$$x^{\frac{l-1}{2}} \equiv \begin{cases} \pm 1 \mod p & , \text{ if} p \nmid x; \\ 0 \mod p & , \text{ if} p \mid x. \end{cases}$$

This implies that

(1) If $x^l + y^l + z^l = 0 \mod p$, then one of x, y, z must be divisible by p;
(2) $x^l \neq l \mod p$.

Hence we can apply Germain's Theorem to get:

Corollary 1. *If l and $2l+1$ are both primes, then $x^l + y^l = z^l$ implies that one of x, y, z must be divisible by l.*

3. A Brief Biography of Kummer

Ernest Eduard Kummer was born in January 29 1810 in Brandenburg, Prussia (now Germany) and died in May 14, 1893 in Berlin. His father died when he was three years old and he and his elder brother were brought up by his mother. Kummer entered the University of Halle in 1828 with the intention of studying Protestant theology, but was drawn to mathematics by his teacher H. F. Scherk. He graduated with a doctorate degree in 1831.

From 1832 to 1842, he was a high school teacher at the Gymnasium in Liegnitz, now Legnica in Poland. He was a very good teacher and his best student there was Leopold Kronecker (1823-1891). He published a paper on hypergeometric series in Crelle's Journal in 1836 and he sent a copy of the paper to Jacobi. This led to Jacobi, and later Dirichlet, corresponding with Kummer on mathematical topics and they soon realised the great potential for the highest level of mathematics that Kummer possessed. In 1839, although still a school teacher, Kummer was elected to the Berlin Academy on Dirichlet's recommendation.

In 1840 Kummer married a cousin of Dirichlet's wife, both from the Mendelssohn family. In 1842, with strong support from Jacobi and Dirichlet, he was appointed a full professor at the University of Breslau, now Wrocław in Poland. In 1855, Dirichlet left Berlin to succeed Gauss at Göttingen and Kummer became his successor at Berlin. One year later, Weierstrass (1815-1897) Joined Berlin. Kummer's former Kronecker also came to Berlin

in 1855. From 1855, Berlin became the leading mathematical center in the world, in charge by two former high school teachers Kummer and Weierstrass and a wealthy Kronecker who studied mathematics for his own enjoyment.

In Berlin Kummer became an extremely popular teacher, famous for the clarity and vividness of his presentations. Kummer supervised a large number of doctoral students there, including Cantor, Gordan (advisor of Emmy Noether) and Schwarz (also Kummer's son-in-law, Cauchy-Schwarz inequality). He also held high office in the University of Berlin, being Dean in 1857-58 and again in 1865-66. He was rector of the university in 1868-69.

4. Kummer's work on Fermat's Last Theorem

4.1. Cyclotomic integers, a setup. Let $l > 3$ be an odd prime, $\alpha = \zeta_l$ is a primitive l-th root of unity. Suppose $x, y.z \in \mathbb{Z} - \{0\}\}$, $\gcd(x, y) = 1$, and

$$x^l + y^l = z^l.$$

Then

$$(x + y)(x + \alpha y) \cdots (x + \alpha^{l-1} y) = z^l. \tag{7}$$

Kummer was trying to factorize $x + \alpha^j y$, just like the approach by Euler for the proof of the case $l = 3$. This led to the study of the cyclotomic integers $f(\alpha)$ for all polynomials $f(x) \in \mathbb{Z}[x]$. Let

$$\mathbb{Z}[\alpha] = \{f(\alpha) \mid f(X) \in \mathbb{Z}[X]\}.$$

We know that the minimal polynomial of α is $\Phi_l(X) = X^{l-1} + \cdots + X + 1$. Then $1 + \alpha + \cdots + \alpha^{l-1} = 0$ and any cyclotomic integer in $\mathbb{Z}[\alpha]$ can be uniquely written as

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{l-2}\alpha^{l-2} \text{ with } a_i \in \mathbb{Z}.$$

Actually Kummer wrote the elements as

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{l-1}\alpha^{l-1},$$

which is equal to $(a_0 + c) + (a_1 + c)\alpha + \cdots + (a_{l-1} + c)\alpha^{l-1}$ for any $c \in \mathbb{Z}$.

Just like the case for $\mathbb{Z}$,

$$f(\alpha) \mid g(\alpha) \text{ if } g(\alpha) = f(\alpha)h(\alpha) \text{ for some } h(\alpha) \in \mathbb{Z}[\alpha],$$

$$f(\alpha) \equiv g(\alpha) \mod h(\alpha) \text{ if } h(\alpha) \mid (f(\alpha) - g(\alpha)).$$

To study the factorization of cyclotomic integers, Kummer introduced

Definition 7. (1) A cyclotomic integer $f(\alpha)$ is called a unit if there exists another (unique) cyclotomic integer $g(\alpha)$ such that $f(\alpha)g(\alpha) = 1$, and $g(\alpha)$ is called the inverse of $f(\alpha)$.

(2) A cyclotomic integer $h(\alpha)$ is called a prime element if $h(\alpha)$ is not a unit and the condition holds: $h(\alpha) \mid f(\alpha)g(\alpha)$ implies that either $h(\alpha) \mid f(\alpha)$ or $h(\alpha) \mid g(\alpha)$.

(3) $h(\alpha)$ is called irreducible if $h(\alpha)$ is not a unit and the condition holds: $h(\alpha) = f(\alpha)g(\alpha)$ implies that one of $f(\alpha)$ and $g(\alpha)$ is a unit.

DEFINITION 8. Two cyclotomic integers $f(\alpha)$ and $g(\alpha)$ are called equivalent if $f(\alpha) = g(\alpha)u$ where u is a unit.

LEMMA 1. *If $f(\alpha)$ and $g(\alpha)$ are two prime elements and $f(\alpha) \mid g(\alpha)$, then $f(\alpha)$ and $g(\alpha)$ are equivalent.*

PROOF. Write $g(\alpha) = f(\alpha)h(\alpha)$. Then by the primality of $g(\alpha)$, $g(\alpha) \mid f(\alpha)$ or $g(\alpha) \mid h(\alpha)$. In the first case, write $f(\alpha) = g(\alpha)h'(\alpha)$, then

$$g(\alpha) = g(\alpha)h(\alpha)h'(\alpha),$$

hence $h'(\alpha)h(\alpha) = 1$ and $h'(\alpha)$ is a unit. In the second case write $h(\alpha) = g(\alpha)f'(\alpha)$, the same argument implies that $f(\alpha)f'(\alpha) = 1$ and $f(\alpha)$ is a unit, not possible. □

In Galois' language, we know

$$\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) = \{\sigma_a : \alpha \mapsto \alpha^a,\ 1 \le \alpha \le l-1\} \cong (\mathbb{Z}/l\mathbb{Z})^\times. \tag{8}$$

Kummer would use the substitution $\sigma_a : \alpha \mapsto \alpha^a$ often. The conjugates of α are α^i $(1 \le i \le l-1)$, thus the conjugates of $f(\alpha)$ are $f(\alpha^i)$ $(1 \le i \le l-1)$. Kummer defined

DEFINITION 9. The norm of a cyclotomic integer $f(\alpha)$ is

$$Nf(\alpha) = f(\alpha)f(\alpha^2)\cdots f(\alpha^{l-1}) \in \mathbb{Z}.$$

PROPOSITION 4. *The following facts hold:*
(1) *$f(\alpha) = 0$ if and only $Nf(\alpha) = 0$.*
(2) *If $f(\alpha) \neq 0$, then*

$$Nf(\alpha) = \prod_{i=1}^{\frac{l-1}{2}} f(\alpha^i)f(\alpha^{l-1-i}) = \prod_{i=1}^{\frac{l-1}{2}} |f(\alpha^i)|^2 \in \mathbb{Z}_+.$$

(3) *The norm map is multiplicative: $N(f(\alpha)g(\alpha)) = Nf(\alpha)Ng(\alpha)$.*
(4) *$f(\alpha)$ is a unit if and only if $Nf(\alpha) = 1$.*

4.2. Study of prime elements. The goal of Kummer was to determine prime elements which are factors of $x + \alpha^j y$ for $0 \le j \le l-1$, $x, y \in \mathbb{Z}$ and $\gcd(x, y) = 1$. Suppose $h(\alpha) \mid (x + \alpha^j)y$ is one such prime element. Then

$$h(\alpha) \mid (x + \alpha^j)y \mid N(x + \alpha^j) = p_1 p_2 \cdots p_n,$$

Then $h(\alpha) \mid p$ for $p = p_1, \cdots, p_n$, a prime factors of $N(x + \alpha^j)$. If $h(\alpha) \mid q$ for another prime $q \neq p$, then $h(\alpha) \mid ap + bq$ for all $a, b \in \mathbb{Z}$, and in particular $h(\alpha) \mid 1$ is a unit, not possible. Hence p is the only prime number such that $h(\alpha) \mid p$. This implies that

$$h(\alpha) \mid n \Leftrightarrow p \mid n \quad (n \in \mathbb{Z}),$$

equivalently

$$m \equiv n \mod h(\alpha) \Leftrightarrow m \equiv n \mod p \quad (m, n \in \mathbb{Z}).$$

Now from $x + \alpha^j y \equiv 0 \mod h(\alpha)$, certainly $p \nmid y$, otherwise $p \mid y$ and $h(\alpha) \mid y$, and hence $h(\alpha) \mid x$ and $p \mid x$, contradicts to $\gcd(x, y) = 1$. Suppose $a \in \mathbb{Z}$ such that $ay \equiv 1 \mod p$, then $ay \equiv 1 \mod h(\alpha)$ and hence

$$\alpha^j \equiv -ax \mod h(\alpha).$$

Suppose $i \in \mathbb{Z}$ and $ij \equiv 1 \mod l$, then

$$\alpha = \alpha^{ij} \equiv (-ax)^i \mod h(\alpha).$$

Let $k = (-ax)^i \mod p$, then we may assume there exists $0 < k < p$ depending only on x, y, j such that

$$\alpha \equiv k \mod h(\alpha).$$

Hence

$$g(\alpha) \equiv g(k) \mod h(\alpha) \text{ for any } g(\alpha) \in \mathbb{Z}[\alpha].$$

This means that

PROPOSITION 5. *If $h(\alpha)$ is a prime element dividing $x + \alpha^j y$ for $0 \le j \le l - 1$, $x, y \in \mathbb{Z}$ and $\gcd(x, y) = 1$. Then there exists a unique prime factor of $N(x + \alpha^j y)$ and a unique $0 < k < p$ depending only on x, y, j such that*

$$g(\alpha) \equiv f(\alpha) \mod h(\alpha) \Leftrightarrow g(k) \equiv f(k) \mod p. \tag{9}$$

The second step of Kummer was to find more information about k and the prime elements.

By the fact $\alpha^{l-1} + \cdots + \alpha + 1 = 0$ and (9), then $k^{l-1} + \cdots + k + 1 \equiv 0 \mod p$. Hence $k^l \equiv 1 \mod p$. Note that we also have $k^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem. There are two cases to treat:

Case 1: $k \equiv 1 \mod p$. Then $l \equiv k^{l-1} + \cdots + k + 1 \equiv 0 \mod p$ and hence $l = p$. In this case, for $1 \le i \le l - 1$, $N(\alpha - 1) = l = N(\alpha^i - 1) = l$. Then $\frac{\alpha^i - 1}{\alpha - 1} = 1 + \cdots + \alpha^{i-1}$ whose norm is 1, so $\frac{\alpha^i - 1}{\alpha - 1}$ is a unit and

$$l = (\alpha - 1)^{l-1} u, \ \ u \text{ is a unit.}$$

Since $(\alpha - 1) \mid f(\alpha) - f(1)$, we know that $(\alpha - 1) \mid f(\alpha)$ if and only if $(\alpha - 1) \mid f(1)$. If this is the case, then $l = N(\alpha - 1) \mid N(f(1)) = f(1)^{l-1}$ and $l \mid f(1)$. Hence $(\alpha - 1) \mid f(\alpha)$ if and only if $l \mid f(1)$. If $(\alpha - 1) \mid f(\alpha)g(\alpha)$, then $l \mid f(1)g(1)$ i.e. $l \mid f(1)$ or $g(1)$, hence $(\alpha - 1) \mid f(\alpha)$ or $(\alpha - 1) \mid g(\alpha)$. Thus $\alpha - 1$ is a prime element of $\mathbb{Z}[\alpha]$.

On the other hand, by (9), if $h(\alpha)$ is a prime element dividing l, then $\alpha \equiv 1 \mod h(\alpha)$ i.e., $h(\alpha) \mid (\alpha - 1)$. Thus up to equivalence, $\alpha - 1$ is the only prime element of $\mathbb{Z}[\alpha]$ dividing l.

Case 2: Order of $k \mod p$ is l. This implies $l \mid p - 1$ and hence $p \equiv 1 \mod l$.

Take the Galois action into consideration, we see that

$$\alpha \equiv k \mod h(\alpha) \iff \alpha^j \equiv k \mod h(\alpha^j) \text{ for any } 1 \le j \le l - 1,$$

and

A cyclotomic integer $f(\alpha)$ is a prime element if and only if $f(\alpha^j)$ is a prime element for any $1 \le j \le l-1$.

If $h(\alpha^i) \mid h(\alpha^j)$, then $h(\alpha^j) = h(\alpha^i)u$ by Lemma 1, and

$$\alpha^j \equiv k \mod h(\alpha^j), \quad \alpha^i \equiv k \mod h(\alpha^i)$$

implies that $\alpha^i \equiv \alpha^j \mod h(\alpha^i)$, i.e. $(\alpha-1) \mid h(\alpha^j)$, which is not possible. Hence $h(\alpha), \cdots, h(\alpha^{l-1})$ are all non-equivalent prime elements, and $h(\alpha^j) \mid p$ for all j. This implies $N(h(\alpha))) = h(\alpha)\cdots h(\alpha^{l-1}) \mid p$ and $Nh(\alpha) = p$.

THEOREM 26. *The followings hold:*

(1) *Suppose $h(\alpha)$ is a prime element and $h(\alpha) \mid x+\alpha^j y$ for some coprime $x, y \in \mathbb{Z}$ and $1 \le j \le l-1$. Then $Nh(\alpha) = p$ is a prime, and either $p = l$ or $p \equiv 1 \mod l$.*

(2) *If $p = l$ or $p \equiv 1 \mod l$ and $h(\alpha)$ is a cyclotomic integer such that $Nh(\alpha) = p$, then $h(\alpha)$ is a prime element and $h(\alpha) \mid x + \alpha^j y$ for some coprime $x, y \in \mathbb{Z}$ and $1 \le j \le l-1$.*

(3) *If $p = l$, then the only prime element up to equivalence is $\alpha - 1$.*

PROOF. Only need to show (2) in the case $p \equiv 1 \mod l$.

Since $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ and $l \mid p-1$, we let $\{m, \cdots, m^l = 1\}$ be the only subgroup of $\mathbb{F}_p^\times$ of order l. For $Nh(\alpha) = p$, we have

$$h(X)h(X^2)\cdots h(X^{l-1}) = p+(1+X+\cdots+X^{l-2})g(X) \text{ for some } g(X) \in \mathbb{Z}[X].$$

Hence $h(m)h(m^2)\cdots h(m^{l-1}) = 0 \in \mathbb{F}_p$ as $1 + m + \cdots + m^{l-2} = 0 \in \mathbb{F}_p$. Over the integers, then

$$h(m)h(m^2)\cdots h(m^{l-1}) \equiv 0 \bmod p.$$

Suppose $h(m^j) \equiv 0 \bmod p$. By division, then $h(X) = q(X)(X - m^j) + h(m^j) \in \mathbb{Z}[X]$, then $h(\alpha) \equiv q(\alpha)(\alpha - m^j) \bmod p$, and

$$h(\alpha^\nu) \equiv q(\alpha^\nu)(\alpha^\nu - m^j) \bmod p \text{ for all } 1 \le \nu \le l-1.$$

Therefore

$$(\alpha - m^j)h(\alpha^2)\cdots h(\alpha^{l-1}) \equiv N(\alpha - m^j)q(\alpha^2)\cdots q(\alpha^{l-1}) \bmod p.$$

However, $N(\alpha - m^j) = \frac{m^{jl}-1}{m^j-1} \equiv 0 \bmod p$, then $(\alpha - m^j)h(\alpha^2)\cdots h(\alpha^{l-1}) \equiv 0 \bmod p$. In other words, $p = h(\alpha)h(\alpha^2)\cdots h(\alpha^{l-1}) \mid (\alpha - m^j)h(\alpha^2)\cdots h(\alpha^{l-1})$ and hence $h(\alpha) \mid \alpha - m^j$. Thus $\alpha \equiv m^j \bmod h(\alpha)$.

To prove $h(\alpha)$ is a prime element, suppose $h(\alpha) \mid f(\alpha)g(\alpha)$ and $\alpha \equiv k \bmod h(\alpha)$. Then $f(k)g(k) \equiv 0 \bmod h(\alpha)$. This implies $f(k)g(k) \equiv 0 \bmod p$ over $\mathbb{Z}$, and $f(k)$ or $g(k) \equiv 0 \bmod p$. Hence $f(k)$ or $g(k) \equiv 0 \bmod h(\alpha)$ and $f(\alpha)$ or $g(\alpha) \equiv 0 \bmod h(\alpha)$, i.e., $h(\alpha)$ is a prime element. □

For $p \equiv 1 \bmod l$, Kummer tried to find $h(\alpha)$ whose norm $Nh(\alpha) = p$ (hence $h(\alpha)$ is a prime element). However, he found that for $l = 23$ and $p = 47$,

(1) there exists no cyclotomic integer $h(\alpha)$, $Nh(\alpha) = 47$;
(2) $N(-\alpha + \alpha^{21}) = 47 \times 139$.

This would mean there is no unique factorization in the ring $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_{23}]$.

4.3. General case ($p \neq l$).

4.3.1. *Prime divisor.* For a prime $p \neq l$, the exponent of p is its order in $\mathbb{Z}/l\mathbb{Z} = \mathbb{F}_l$, i.e. the smallest integer $f > 0$ such that $p^f \equiv 1 \bmod l$. Let $g = \frac{l-1}{f}$. Let $(\mathbb{Z}/l\mathbb{Z})^\times = \langle\gamma\rangle \cong \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$, $\gamma\alpha = \alpha_\gamma$.

Definition 10. For $i = 1, \cdots, g$, the Gauss period of p is

$$\eta_i := \gamma^i(1 + \gamma^g + \cdots + \gamma^{(f-1)g})\alpha = \alpha^{\gamma^i} + \alpha^{\gamma^{i+g}} + \cdots + \alpha^{\gamma^{i+g(f-1)}}.$$

Remark 4. Gauss period is still widely used, for example in coding theory.

By explicit computation, Kummer proved the following results:

Proposition 6. *There exist integers u_i for $i = 1, \cdots, g$, $0 \leq u_i < p$, such that for $F(X_1, \cdots, X_g) \in \mathbb{Z}[X_1, \cdots, X_g]$,*

$$F(\eta_1, \cdots, \eta_g) = 0 \Longleftrightarrow F(u_1, \cdots, u_g) \equiv 0 \bmod p.$$

Moreover, if $(u_1, \cdots, u_g)$ satisfies the above property, then $(u_1, \cdots, u_g)$, $(u_2, \cdots, u_g, u_1)$, $\cdots$, $(u_g, u_1, \cdots, u_{g-1})$ are the only groups of integers satisfying the property and they are all different.

Theorem 27. *Giving $(u_1, \cdots, u_g)$ above, one can define one and only one equivalence relation in the cyclotomic integers satisfying*

(1) $\eta_i \sim u_i$, $p \sim 0$, $1 \not\sim 0$;
(2) if $f(\alpha) \sim g(\alpha)$, then $h(\alpha)f(\alpha) \sim h(\alpha)g(\alpha)$ for all $h(\alpha) \in \mathbb{Z}[\alpha]$;
(3) if $f(\alpha) \sim g(\alpha)$ and $f'(\alpha) \sim g'(\alpha)$, then $f(\alpha) \pm f'(\alpha) \sim g(\alpha) \pm g'(\alpha)$ and $f(\alpha)f'(\alpha) \sim g(\alpha)g'(\alpha)$;
(4) if $f(\alpha)g(\alpha) \sim 0$ then either $f(\alpha) \sim 0$ or $g(\alpha) \sim 0$.

Moreover, the number of equivalent classes is p^f.

Definition 11. The equivalence relation in above theorem is called the prime divisor of p corresponding to $(u_1, \cdots, u_g)$. We write $f \sim g$ as $f \equiv g \bmod \mathfrak{P}$, and call $\mathfrak{P}$ the prime divisor of p corresponding to $(u_1, \cdots, u_g)$.

Hence there are $g = \frac{l-1}{f}$ prime divisors of p corresponding to $(u_1, \cdots, u_g)$, $\cdots$, $(u_g, u_1, \cdots, u_{g-1})$ respectively.

Definition 12. Let $\mathfrak{P}$ be the prime divisor of p corresponding to $(u_1, \cdots, u_g)$.
(1) We call $\mathfrak{P}^\mu \mid g(\alpha)$ if $p^\mu \mid g(\alpha)\psi(\eta)^\mu$, where

$$\psi(\eta) = \prod_{i=1}^{g} \prod_{\substack{j=0 \\ j \neq \mu_i}}^{p-1} (j - \eta_i)$$

(2) We call $\mathfrak{P}^\mu \mid\mid g(\alpha)$ if $\mathfrak{P}^\mu \mid g(\alpha)$ but $\mathfrak{P}^{\mu+1} \nmid g(\alpha)$. In this case, $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) := \mu$

It was shown by Kummer that $\mathrm{ord}_{\mathfrak{P}}(g(\alpha))$ is uniquely determined if $g(\alpha) \neq 0$. If set $\mathrm{ord}(0) = +\infty$, we get the usual additive valuation map:

$$\mathrm{ord}_{\mathfrak{P}} : \mathbb{Z}[\alpha] \to \mathbb{Z}_{\geq 0} \cup \{\pm\infty\}.$$

We note the fact

$$\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) \neq 0 \text{ if only if } p \not\sim Ng(\alpha).$$

EXAMPLE 16. If $p = l$, $\mathfrak{P} = (\alpha - 1)$, $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) = \mu$ if $(\alpha-1)^{\mu} \mid g(\alpha)$ but $(\alpha-1)^{\mu+1} \nmid g(\alpha)$.

Kummer proved

THEOREM 28. *If $g(\alpha), h(\alpha) \neq 0$, then $g(\alpha) \mid h(\alpha)$ if and only if for every prime number p and every prime divisor $\mathfrak{P}$ of p, $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) \leq \mathrm{ord}_{\mathfrak{P}}(h(\alpha))$.*

As a consequence, $g(\alpha) = uh(\alpha)$ for some unit u if and only if for every prime number p and every prime divisor $\mathfrak{P}$ of p, $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) = \mathrm{ord}_{\mathfrak{P}}(h(\alpha))$.

4.3.2. *Divisors.*

DEFINITION 13. For a cyclotomic integer $g(\alpha) \neq 0$, the principal divisor associated to $g(\alpha)$ is the formal product $\prod_{\mathfrak{P}} \mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}}(g(\alpha))}$.

A divisor (or an effective divisor in Modern language) is a formal product

$$A = \prod_{\mathfrak{P}} \mathfrak{P}^{n_{\mathfrak{P}}(A)},\ n_{\mathfrak{P}}(A) \geq 0, \text{ and } n_{\mathfrak{P}}(A) = 0, \text{all but finitely many } \mathfrak{P}.$$

In the beginning a divisor A was called an ideal complex number according to Kummer.

DEFINITION 14. Let A be a divisor. We call $f(\alpha) = g(\alpha) \mod A$ if $\mathrm{ord}_{\mathfrak{P}}(f(\alpha) - g(\alpha)) \geq n_{\mathfrak{P}}(A)$ for all prime divisors $\mathfrak{P}$.

Kummer proved many additional results:

THEOREM 29. *Suppose $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ are prime divisors of p. If $Ng(\alpha) = p^f$, then $g(\alpha)$ is a prime element and there exists $1 \leq i \leq g$ such that*

$$\mathrm{ord}_{\mathfrak{P}_i}(g(\alpha)) = 1 \quad \textit{and} \quad \mathrm{ord}_{\mathfrak{P}_j}(g(\alpha)) = 0 \textit{ for } j \neq i.$$

THEOREM 30. *For each i, there exists $\psi_i(\eta) = a_1\eta_1 + \cdots + a_g\eta_g$ $(a_i \in \mathbb{Z})$, such that*

$$\mathrm{ord}_{\mathfrak{P}_i}(\psi_i(\eta)) = 1 \quad \textit{and} \quad \mathrm{ord}_{\mathfrak{P}_j}(\psi_i(\eta)) = 0 \textit{ for } j \neq i.$$

REMARK 5. From now on, write a prime divisor $\mathfrak{P} = (p, \psi_{\mathfrak{P}}(\eta))$. Then
(1) A divisor $A = (p_1, \psi_1(\eta))^{\mu_1} \cdots (p_m, \psi_m(\eta))^{\mu_m}$.
(2) The principal divisor associated to p is

$$\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g = (p_1, \psi_1(\eta)) \cdots (p_g, \psi_g(\eta)).$$

4.3.3. *Norm of a divisor.* The Galois group acts on prime divisors via

$$\sigma(p, \psi(\eta)) := (p, \sigma\psi(\eta))$$

and extends by multiplicity to divisors.

DEFINITION 15. For a divisor A, set $N(A) = A\sigma(A)\cdots\sigma^{l-2}(A)$ where σ is a generator of the Galois group.

THEOREM 31. *$N(A)$ as a divisor is generated by a positive integer, by abuse of notation, we call it the norm of A, which is decided by the two relations:*

$$N(AB) = N(A)N(B),$$

and

$$N(p, \psi(\eta)) = p^f = \#\textit{of equivalent classes of } (p, \psi(\eta)).$$

THEOREM 32 (Chinese Remainder Theorem). *Suppose A and B are relatively prime divisors. Then for any cyclotomic integers a and b, there exists $x \in \mathbb{Z}[\alpha]$ satisfying*

$$\begin{cases} x \equiv a \mod A, \\ x \equiv b \mod B. \end{cases} \tag{10}$$

Moreover, all cyclotomic integers satisfying (10) *form an equivalent class modulo AB.*

4.3.4. *Class number.*

DEFINITION 16. Two divisors $A \sim A'$ if for all divisors B, AB is principal if and only if $A'B$ is principal.

LEMMA 2. *This relation is indeed an equivalence relation, i.e., it is reflexive, symmetric and transitive.*

Let $[A]$ be the equivalent class of A.

THEOREM 33. *The number of equivalent classes of divisors is finite, i.e. there exist divisors $A_1, \cdots, A_k$ such that every divisor is equivalent to one of the A_i's. Moreover, by multiplication $[A][B] = [AB]$, the equivalent classes of $\mathbb{Z}[\alpha]$ form a finite abelian group, with the identity the class of principal divisors.*

DEFINITION 17. The finite group of equivalent classes of $\mathbb{Z}[\alpha]$ is called the class group (of $\mathbb{Z}[\alpha]$ or $\mathbb{Q}[\alpha]$), its order is called the class number.

COROLLARY 2. *Let h be the class number of $\mathbb{Z}[\alpha]$. Then for any divisor C, C^h is a principal divisor.*

4.4. Kummer's work on Fermat's Last Theorem.

DEFINITION 18. A prime l is called a regular prime if $l \nmid h$, the corresponding class number of $\mathbb{Z}[\alpha]$.

LEMMA 3. *If ε is a unit, then $\varepsilon/\bar{\varepsilon} = \alpha^r$ for some r.*

PROOF. Suppose $E(X) = a_0 + a_1X + \cdots + a_{l-1}X^{l-1}$ that $E(\alpha) = \varepsilon/\bar{\varepsilon}$. Suppose

$$E(X^{l-1})E(X) = Q(X)(X^l - 1) + R(X) \text{ with } R(X) = A_0 + \cdots + A_{l-1}X^{l-1}.$$

Take $X = \alpha$, then $R(\alpha) = 1$ and $A_0 - 1 = A_1 = \cdots = A_{l-1}$. Assume this number is k. Take $X = 1$, then

$$(a_0 + a_1 + \cdots + a_{l-1})^2 = A_0 + \cdots + A_{l-1} = 1 + kl$$

and $a_0 + a_1 + \cdots + a_{l-1} \equiv \pm 1 \bmod l$. Replace a_i by $a_i + c$, we may assume $a_0 + a_1 + \cdots + a_{l-1} = \pm 1$ and for this new $E(X)$, $A_0 = 1$ and $A_i = 0$ for $0 < i < l - 1$. Note that

$$a_iX^{(l-1)i}a_jX_j \equiv a_ia_jX^r \mod X^l - 1$$

where $0 \le r < l$ and $j - i \equiv r \mod l$, then

$$A_r = \sum_{j-i\equiv r} a_ia_j$$

and in particular, $A_0 = a_0^2 + \cdots + a_{l-1}^2$. For $A_0 = 1$, one and only $a_r = \pm 1$ and all others 0, and $E(\alpha) = \pm\alpha^r$.

If $\varepsilon/\bar{\varepsilon} = -\alpha^r$, as r or $r + l$ is even, we assume $\varepsilon/\bar{\varepsilon} = -\alpha^{2s}$, then $\varepsilon\alpha^{-s} = -\bar{\varepsilon}\alpha^s$. Let $F(\alpha) = \varepsilon\alpha^{-s}$ such that $F(0) = 0$, then $F(\alpha) = -F(\alpha^{-1})$. This would lead to that a non-unit $(\alpha - \alpha^{-1}) \mid F(\alpha)$ which is a unit, certainly this is impossible. □

One also needs the following Lemma (called Kummer's Lemma):

LEMMA 4. *If l is regular, then for a unit ϵ in $\mathbb{Z}[\alpha]$, if $\epsilon \equiv$ an integer $\bmod l$, then $\epsilon = (\epsilon')^l$ for some unit ϵ'.*

REMARK 6. The statement was originally Condition (B) according to Kummer, and that l is a regular prime is Condition (A). Kummer was able to deduce (B) from (A). Kummer proved the class number formula for $\mathbb{Q}(\alpha)$ by the analytic method introduced by Dirichlet, and showed that the regular condition is equivalent to that l does not divide the numerators of the Bernoulli numbers $B_2, B_4, \cdots, B_{l-3}$ where the Bernoulli number is defined by

$$\frac{x}{e^x - 1} = \sum_n B_n \frac{x^n}{n!}.$$

The structure of the units of $\mathbb{Q}(\alpha)$ was then analyzed, again this was the idea of Dirichlet (Dirichlet's unit Theorem).

THEOREM 34. *If l is a regular prime, then $x^l + y^l = z^l$ has no nontrivial integer solution.*

PROOF. We may assume x, y, z are pairwise relatively prime and one of the following two cases holds:

I : all x, y, z are prime to l;
II : $l \nmid xy$ and $l \mid z$.

Write

$$x^l + y^l = (x+y)(x+\alpha y)\cdots(x+\alpha^{l-1}y) = z^l.$$

If $x + \alpha^j y$ and $x + \alpha^{j+k} y$ have a common divisor, this divisor must be a common divisor of

(1) $(x + \alpha^{j+k}y) - (x + \alpha^j y) = \alpha^j(\alpha^k - 1)y = unit \cdot (\alpha - 1)y$;
(2) $(x + \alpha^{j+k}y) - \alpha^k(x + \alpha^j y) = unit \cdot (\alpha - 1)x$.

Since $\gcd(x, y) = 1$, it must be $\alpha - 1$. Hence,

- either $(x + \alpha^{j+k}y)$ are coprime and $(\alpha - 1) \nmid z^l$; (Case I)
- or all $(x+\alpha^{j+k}y)$ have a factor $\alpha-1$ and their quotients are pairwise relatively prime, and $l \mid z$. (Case II)

Case I. Now $x + y, x + \alpha y, \cdots x + \alpha^{l-1}y$ are pairwise coprime and their product is an l-th power, hence the divisor of each $x + \alpha^j y$ is C_j^l for some C_j. However, $[C_j]^h = 1 = [C_j]^l$ and $l \nmid h$, then C_j is a principal divisor. Hence $x + \alpha^j y = \epsilon_j t_j^l$ for every j, where ϵ_j is a unit and t_j is a cyclotomic integer.

Take $j = 1$. Let $^-$ be the complex conjugation. Then

$$x + \alpha y = \epsilon t^l, \quad x + \alpha^{-1} y = \overline{x + \alpha y} = \bar{\epsilon}\bar{t}^l.$$

By Lemma 3, $\frac{\epsilon}{\bar{\epsilon}} = \alpha^r$ for some $0 \le r \le l$. We also have $t^l \equiv \bar{t}^l \mod l$. Hence

$$x + \alpha^{-1} y = \alpha^{-r}\epsilon\bar{t}^l \equiv \alpha^{-r}\epsilon t^l \equiv \alpha^{-r}(x + \alpha y) \mod l.$$

If $r = 0$, then $(\alpha - \alpha^{-1})y \equiv 0 \mod l$, then $\alpha - 1 \mid y$ and hence $l \mid y$, impossible. Hence $0 < r < l$. We have

$$\alpha^{r-1}(\alpha x + y) \equiv x + \alpha y \mod l,$$

$$[(\alpha - 1) + 1]^{r-1}[(\alpha - 1)x + x + y] \equiv (x + y) + (\alpha - 1)y \mod (\alpha - 1)^{l-1}$$

Comparing the $(\alpha - 1)^2-$terms in both sides, we obtain $x \equiv y \mod l$. By the same argument $x \equiv -z \mod l$. From $x^l + y^l \equiv x + y \equiv z^l \equiv z \mod l$, then $3x \equiv 0 \mod l$ and $l = 3$. This was already proved by Euler.

Case II. In this case $(\alpha - 1) \mid x + \alpha^j y$ for all j,

$$\prod_{i=0}^{l-1} \left(\frac{x + \alpha^j y}{\alpha - 1} \right) = z^l (\alpha - 1)^{-l}$$

is an l-th power and $\frac{x+\alpha^j y}{\alpha-1}$ are relatively prime. Then we can write

$x+\alpha^j y=(\alpha-1)\epsilon_j t_j^l$ for every j, where ϵ_j is a unit, t_j are coprime to each other.

As $l \mid z$, $l \mid x+y$ and $(\alpha-1) \mid t_0$, and hence $(\alpha-1) \nmid t_j$ for all other j.

Let $t_0=(\alpha-1)^k\omega$, $(\alpha-1)\nmid\omega$, then $k\geq 1$. Write

$$\begin{cases} x+\alpha^{-1}y=(\alpha-1)\epsilon_{-1}t_{-1}^l; \\ x+y=(\alpha-1)\epsilon_0(\alpha-1)^{kl}\omega^l; \\ x+\alpha y=(\alpha-1)\epsilon_1 t_1^l. \end{cases}$$

By $\alpha\times[(x+y)-(x+\alpha^{-1}y)]=(x+\alpha y)-(x+y)$, we have

$$0=\epsilon_1 t_1^l+\alpha\epsilon_{-1}t_{-1}^l-(1+\alpha)\epsilon_0(\alpha-1)^{kl}\omega^l.$$

It has the form

$$E_0(\alpha-1)^{kl}\omega^l=t_1^l+E_{-1}t_{-1}^l, \text{ where } E_1,\ E_{-1} \text{ are units.}$$

Modulo l on both sides, note that $t_1^l\equiv$ an integer $\mod l$ and $t_{-1}^l\equiv$ an integer $\mod l$ and that they are both not zero as $(\alpha-1)\nmid t_1$ and $(\alpha-1)\nmid t_{-1}$, then the unit $E_{-1}\equiv$ an integer $\mod l$. By Kummer's Lemma (Lemma 4), $E_{-1}=\epsilon^l$ for some unit ϵ. We have

$$E_0(\alpha-1)^{kl}\omega^l=t_1^l+(\epsilon t_{-1})^l.$$

Consider an equations of the form

$$x^l+y^l=\epsilon(\alpha-1)^{kl}\omega^l \tag{11}$$

where ϵ is a unit, $k>0$ and $x,y,\alpha-1,\omega$ are pairwise relatively prime. Note that at least one $x+\alpha^j y$ is divisible by $\alpha-1$, then all are divisible by $\alpha-1$ and the quotients are relatively prime. Write

$$x\equiv a_0+a_1(\alpha-1) \mod (\alpha-1)^2,\quad y\equiv b_0+b_1(\alpha-1) \mod (\alpha-1)^2,$$

where $a_0,a_1,b_0,b_1\in\mathbb{Z}$, then

$$x+\alpha^j y\equiv(a_0+b_0)+[a_1+b_1+jb_0](\alpha-1) \mod (\alpha-1)^2.$$

As $\alpha-1\nmid y$, then $b_0\neq 0 \mod l$. Hence there exists exactly one j such that $l\mid a_1+b_1+jb_0$, i.e. there exists exactly one j such that $(\alpha-1)^2\mid x+\alpha^j y$. Hence $(\alpha-1)^{l+1}\mid\prod_{j=0}^{l-1}(x+\alpha_j y)$, which means that $k>1$. In other words, if $k=1$, (11) has no solution.

Write $k=K+1$. Replace y by $\alpha_j y$ for the j satisfying $(\alpha-1)^2\mid x+\alpha^j y$. Then

$$\begin{cases} x+\alpha^{-1}y=(\alpha-1)\epsilon_{-1}t_{-1}^l \\ x+y=(\alpha-1)\epsilon_0(\alpha-1)^{Kl}\omega^l \\ x+\alpha y=(\alpha-1)\epsilon_1 t_1^l \end{cases}$$

Repeat our previous argument, then we get

$$X^l+Y^l=E(\alpha-1)^{Kl}\omega^l$$

where $X, Y, \omega, \alpha - 1$ are pairwise relatively prime, E a unit and $K = k - 1$. This then by decent would lead a solution for the $K = 1$ case, which is not possible. □

5. Kummer's further work in number theory

5.1. Kummer extension and Kummer pairing. Let $n > 1$ be an integer. Suppose F is a field, char F is either 0 or prime to n, containing a primitive n-th root of unity ζ_n, then $E = F(\sqrt[n]{a})$ is called a Kummer extension. As E is the splitting field of $x^n - a$ which is a separable polynomial, then E is Galois over F. Moreover, any $\sigma \in \mathrm{Gal}(E/F)$ is determined by the image $\zeta_n^t \sqrt[n]{a}$ of $\sqrt[n]{a}$, then

$$\mathrm{Gal}(E/F) \to \mathbb{Z}/n\mathbb{Z},\ \sigma \mapsto t \mod n$$

is an injective homomorphism. We have

Lemma 5. *If E/F is a Kummer extension, then* $\mathrm{Gal}(E/F)$ *is a cyclic group of order dividing n.*

Definition 19. A field extension L/K is called abelian if L/K is a Galois extension and $\mathrm{Gal}(L/K)$ is abelian. If furthermore, every element in $\mathrm{Gal}(L/K)$ is of order $\mid n$, then L/K is called abelian of exponent n.

Kummer had the following theorem:

Theorem 35. *Assume $\mu_n \subseteq F$,* char F *is either* 0 *or prime to n, containing a primitive n-th root of unity ζ_n. Then L/F is abelian of exponent n if and only if $L = F(\sqrt[n]{\Delta})$ where Δ is a finite subgroup of $F^\times/(F^\times)^n$.*

5.2. Kummer congruence.

Theorem 36. *If $p \nmid a$, then*

$$n_1 \equiv n_2 \mod p^{k-1}(p-1) \Longrightarrow (1-a^{1+n_1})\zeta(-n_1) \equiv (1-a^{1+n_2})\zeta(-n_2) \mod p^k.$$

Kummer's congruence is the starting point to construct p-adic L-functions.

CHAPTER 4

Further Work in Number Theory (Before 1950)

1. Commutative ring theory

1.1. Dedekind's notion of ideal. Richard Dedekind(1831-1916) was the last student of Gauss, receiving his doctorate from Göttingen in 1852. However he was not well trained in advanced mathematics yet. After Dirichlet succeeded Gauss in 1955 in Göttingen, Dedekind along with Riemann attended many courses by Dirichlet, which improved him a lot as a mathematician. His major contribution in analysis was a redefinition of irrational numbers in terms of Dedekind cuts, but his introduction the notion of an ideal gives him lasting fame in algebra and number theory.

After Dirichlet's death in 1859, Dedekind started to edit Dirichlet's lectures on number theory. It was published these as Vorlesungen über Zahlentheorie in 1863. It was noted that

> Although the book is assuredly based on Dirichlet's lectures, and although Dedekind himself referred to the book throughout his life as Dirichlet's, the book itself was entirely written by Dedekind, for the most part after Dirichlet's death.

In the 3rd and 4th editions of Vorlesungen über Zahlentheorie published in 1879 and 1894, Dedekind wrote supplements in which he introduced the notion of ideal. Dedekind formulated his theory in the ring of integers of an algebraic number field, as the general term 'ring' was not available yet.

For the ideal complex number (divisor) A defined by Kummer, let

$$I(A) = \{f(\alpha) \in \mathbb{Z}[\alpha] \mid f(\alpha) \equiv 0 \mod A\}.$$

Dedekind observed that A is completely determined by $I(A)$ and for $f(\alpha)$ and $g(\alpha) \in I(A)$, $h(\alpha) \in \mathbb{Z}[\alpha]$,

$$f(\alpha) \pm g(\alpha) \in I(A), \quad h(\alpha)f(\alpha) \in I(A) \tag{12}$$

He called subsets of $Z[\alpha]$ satisfying (12) an ideal, and proved that if I is an ideal of $Z[\alpha]$, then there exists a divisor A such that $I = I(A)$.

Dedekind developed the theory of ideal to the ring of algebraic integers for any number field, which is now an example of Dedekind domain, and then introduced the Zeta function for a number field, now called Dedekind Zata functions. Dedekind also introduced the term field (Körper in German)

By the work of Kummer, Dirichlet and Dedekind, we now have the basic algebraic number theory. Namely, let K be a number field and O_K be the ring of integers of K. Then

THEOREM 37 (Dedekind). *Every nonzero prime ideal of O_K is a maximal ideal and every ideal of O_K is uniquely a product of prime ideals.*

THEOREM 38 (Dirichlet unit Theorem, 1846). *The group of units $O_K^{\{}times\}$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$, where r_1 is the number of real embeddings of K, r_2 is the number of pair of complex embedding of K*

THEOREM 39 (Kummer). *The ideal class group* Cl_K *of K is a finite abelian group.*

Dedekind Zata function for the number field K is

$$\zeta_K(s) = \sum_{\mathfrak{a}} (N\mathfrak{a})^{-s} \ (\mathrm{Re}(s) > 1)$$

where $\mathfrak{A}$ passes through integral ideals of O_K. It was shown by Hecke that $\zeta_K(s)$ has a functional equation and its leading coefficient at $s = 0$ is related to the class number of K (called the analytic class number formula).

1.2. Birth of commutative ring theory. The general notion of a ring was introduced by David Hilbert (1862-1943). Hilbert's first work was on invariant theory and, in 1888, he proved his famous Basis Theorem which was published in 1890. Twenty years earlier Paul Gordan, a student of Kummer, had proved the finite basis theorem for binary forms using a highly computational approach. Hilbert discovered a completely new approach which proved the finite basis theorem for any number of variables but in an entirely abstract way. He published his Nullstellensatz in 1893. It was during time Hilbert introduced the notion of ring. Nowadays, these two theorems are extensively used in commutative ring theory and algebraic geometry.

1.3. Noether. As a student of Gordan, Emmy Noether(1882-1935) also studied invariant theory at first. Noether's doctoral thesis followed the constructive approach of Gordan and listed systems of 331 covariant forms. But she gradually shifted to the abstract approach of Hilbert. In 1915 Hilbert and Klein invited Noether to work in Göttingen. She proved a fundamental theorem in theoretical physics then. After 1919, Noether moved away from invariant theory to work on ideal theory, developed the theory of abstract algebra with Emil Artin and her students. Idealtheorie in Ringbereichen (1921) was of fundamental importance in the development of modern algebra. In this paper she gave the decomposition of ideals into intersections of primary ideals in any commutative ring with ascending chain condition, extending the result of Emanuel Lasker (1868-1941, world chess champion 1894-1921, student of Emmy's father Max Noether) for a polynomial ring over a field. Many of results by Noether's school were included in the two

volume Modern Algebra (Vol. I 1930, Vol. II 1931) by van der Waerden (1903-1996). This textbook popularized abstract algebra to general public.

2. Kronecker's Jugendtraum and Class field theory

2.1. Kronecker and his Jugendtraum. Leopold Kronecker (1823-1891), as we mentioned before, was a high school student of Kummer. He was also a doctoral student of Dirichlet. His famous slogan is

"God created integers, all else in the work of man".

In 1853, he claimed the following Theorem:

THEOREM 40. *If $K/\mathbb{Q}$ is finite abelian, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.*

This theorem is called Kronecker-Weber's Theorem, Weber gave a proof in 1886, but a gap was found about 90 years later. The first correct proof was given by Hilbert in 1896.

Kronecker's Jugendtraum (dream of youth) was his attempt to construct finite abelian extension of an imaginary quadratic field, stated by him in a letter to Dedekind in 1880.

CONJECTURE 1 (Kronecker's Jugendtraum). *Every finite abelian extension of an imaginary quadratic field k is contained in an extension of k generated by special values of elliptic functions with complex multiplication.*

Here we remark that

(1) Abel(1829) constructed abelian extensions of $\mathbb{Q}(i)$ by using special values of elliptic functions
(2) Kronecker himself extended Abel's work.
(3) Theory of elliptic functions was the main topic in mathematics in 19th century, there were so many great mathematicians working in this field: Abel, Jacobi, Galois, Weierstrass, Kronecker, $\cdots$.

Kronecker was the leader of mathematical world in 1870's until his death, so his problem got a lot of attention. Weber, in his attempt to prove Kronecker-Weber Theorem, introduced the notions of congruence ideal class group and congruence class field. Then Hilbert introduced the concept now called Hilbert class field, i.e. maximal unramified abelian extension H of a number field K, $\mathrm{Gal}(H/K) = \mathrm{Cl}_K$. In 1914 Fueter proved

THEOREM 41. *Kronecker's Jugendtraum is true for abelian extensions of k of odd degrees.*

2.2. Takaji. Teij Takagi(1875-1960) is the first great Japanese mathematician in modern times. In Takagi's thesis which was based on work he had undertaken in Göttingen, he proved Kronecker's Jugendtraum for $k = \mathbb{Q}(i)$, generalizing the results of Abel and Kronecker. His thesis was published in 1903. From then on to 1914, he concentrated himself on writing textbooks in Japan and did not work on any research project. Then World War I broke out and Japan was isolated from the academic world in

Europe. The last paper he received from Europe before WWI was Fueter's paper. To stay in the front line of mathematics, from 1914, he started to work on class field theory, which he succeeded in proving the main theorem.

Let us describe Takagi's work.

DEFINITION 20. Let $\mathfrak{m} = \mathfrak{m}_f \cdot \mathfrak{m}_\infty$, where $\mathfrak{m}_f$ is a nonzero ideal in O_K and $\mathfrak{m}_\infty$ is a formal product of real embeddings of K.

(1) Then $I_\mathfrak{m}$ is the group of fractional ideals relatively prime to $\mathfrak{m}$ (to $\mathfrak{m}_f$), $P_\mathfrak{m}$ is the subgroup of $I_\mathfrak{m}$ generated by principal fractional ideals (α/β) satisfying

(i) (α) and (β) are relative prime to $\mathfrak{m}_f$.
(ii) $\alpha \equiv \beta \mod \mathfrak{m}_f$.
(iii) $v(\alpha/\beta) > 0$ for any $v \mid \mathfrak{m}_\infty$, $v : K \longrightarrow \mathbb{R}$.

(2) $I_\mathfrak{m}/P_\mathfrak{m}$ is called the generated ideal class group of K modulus $\mathfrak{m}$.

(3) A subgroup H of I_K is called an ideal group if there exists $\mathfrak{m}$ such that $P_\mathfrak{m} \subseteq H \subseteq I_\mathfrak{m}$.

EXAMPLE 17. Let $N_\mathfrak{m}(L/K) = \{\mathfrak{A} \subseteq K \mid \mathfrak{a} = N_{L/K}(\mathfrak{A}) \text{ is prime to } \mathfrak{m}\}$, then $H_\mathfrak{m}(L/K) = P_\mathfrak{m} N_\mathfrak{m}(L/K)$ is an ideal group.

DEFINITION 21. L/K is called a class field if $[I_\mathfrak{m} : H_\mathfrak{m}(L/K)] = [L : K]$ for some K-modulus $\mathfrak{m}$, such $\mathfrak{m}$ is called admissible. The smallest admissible modulus is called the conductor of L/K and denoted as $\mathfrak{f}_{L/K}$.

THEOREM 42 (Takagi 1920). *Let K be a number field.*

(1) *Existence: To every ideal group H, there exists a class field over K.*

(2) *Isomorphism: If H is an ideal group of modulus $\mathfrak{m}$ and has the class field L/K, then* $\mathrm{Gal}(L/K) \cong I_\mathfrak{m}/H$.

(3) *Completeness: Every finite abelian extension of K is a class field.*

(4) *Comparison: If $H_1 \& H_2$ are with common modulus $\mathfrak{m}$ and they have class fields L_1 and H_2, then $L_1 \subseteq L_2$ if and only if $H_2 \subseteq H_1$.*

(5) *Conductor: For any finite abelian L/K, the places of K appearing in the conductor $\mathfrak{f}_{L/K}$ are the ramified places for L/K.*

(6) *Decomposition: If H is an ideal group with modulus $\mathfrak{m}$ and class field L/K, then every prime $\mathfrak{p} \nmid \mathfrak{m}$ is not ramified in L and its residue degree $f_\mathfrak{p}(L/K)$ is equal to the order of $\mathfrak{p}$ in $I_\mathfrak{m}/H$.*

THEOREM 43 (Takagi). *Kronecker's Jugendtraum is true.*

THEOREM 44. *Let K be a quadratic imaginary field, $E : y^2 = 4x^3 - g_2 x - g_3$ bee an elliptic curve over $\mathbb{C}$, such that* $\mathrm{End}(E) \cong O_K$, *then*

(1) *The maximal unramified abelian extension of K (Hilbert class field of K) is $K(j(E))$, where $j(E) = \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}$ is the j-invariant of E.*

(2) *The composite of all finite abelian extensions of K is $K^{ab} = K(j(E), \phi_E(T) : T \in E_{\text{tors}})$, where $\phi_E : E \longrightarrow \mathbb{P}'$ is the Weber function:*

$$P \longmapsto \begin{cases} \frac{g_2 g_3}{g_2^3 - 27 g_3^2} \cdot x(P), & \text{if } j(E) \neq 0, 1728, \\ \frac{g_2^2}{\Delta} x(P)^2, & \text{if } j(E) = 1728, \\ \frac{g_3}{\Delta} x(P)^3, & \text{if } j(E) = 0 \end{cases}$$

where $\Delta = g_2^3 - 27 g_3^2$.

2.3. Artin's reciprocity law. Before he made major contribution in abstract algebra, Emil Artin (1898-1962) completed the class field theory. Takagi's Isomorphism Theorem claimed that there ia an isomorphism $I_{\mathfrak{m}}/H_{\mathfrak{m}} \cong \text{Gal}(L/K)$. Artin clarified this isomorphism:

THEOREM 45 (Artin, 1927). *If $\mathfrak{m}$ is a K-modulus divisible by places of K ramified in L, then the Artin map*

$$\Phi_{L/K,\mathfrak{m}} : I_{\mathfrak{m}} \longrightarrow \text{Gal}(L/K) \quad \mathfrak{p} \longmapsto \text{Frob}_{\mathfrak{p}}(L/K) \text{ for } \mathfrak{p} \nmid \mathfrak{m}$$

is surjective. If $\mathfrak{m}$ is admissible, then $\Phi_{L/K,\mathfrak{m}}$ induces an isomorphism

$$I_{\mathfrak{m}}/H_{\mathfrak{m}}(L/K) = I_{\mathfrak{m}}/P_{\mathfrak{m}} N_{\mathfrak{m}}(L/K) \cong \text{Gal}(L/K).$$

Artin obtained his proof by following the idea in the proof of Chebotarev density theorem, which is also part of class field theory and a generalization of Dirichlet's density theorem.

THEOREM 46 (Chebotarev). *For a Galois extension L/K, the density of those primes ideals in L whose Frobenius automorphisms belong to a given conjugacy class C of $G = \text{Gal}(L/K)$ is $|C|/|G|$.*

3. From Local to Global

3.1. Hensel. Kurt Hensel (1861-1941), his grandmother is the famous composer Fanny Mendelssohn, was a student od Kronecker. He invented p-adic numbers in 1897. Over the ring of integers $\mathbb{Z}$, if $p^a || n$, set $|n|_p = p^{-a}$, by this way the p-adic metric on $\mathbb{Z}$ for each p is defined, which then is extended to $\mathbb{Q}$ by setting $|\frac{a}{b}|_p = |a|_p \cdot |b|_p^{-1}$. Then $\mathbb{Q}$ becomes a metric space under the p-adic metric.

THEOREM 47 (Ostrowski). *$|\cdot|$ and $|\cdot|_p$ are the only metrics up to equivalence in $\mathbb{Q}$.*

Hensel completed $\mathbb{Q}$ by the p-adic metric and obtained the field of p-adic numbers $\mathbb{Q}_p$. The ring of p-adic integers, denoted as $\mathbb{Z}_p$, is the p-adic completion of $\mathbb{Z}$.

Nowadays, finite extensions of $\mathbb{Q}$ and of the function fields $\mathbb{F}_p(t)$ are called global fields, and their completions by various valuations are called local fields. Finite extensions of $\mathbb{Q}$ are also called number fields and of $\mathbb{F}_p(t)$ global function fields. Generalization of Ostrowski's Theorem tells us the metrics up to equivalence of a number field K are given by prime ideals of

the ring of integers O_K, and the real and complex embeddings (which is equivalent by complex conjugate, so is grouped in pairs). These metrics are called places of K. For global function field one has analogous result.

This built the following correspondence:

$$\text{Valuation theory} \Longleftrightarrow \begin{cases} \text{prime ideals of } K \\ \text{real embeddings} \\ \text{complex embeddings} \end{cases}$$

3.2. Hasse principal (Hasse -Minkowski principal). Helmut Hasse(1898-1979) is a German mathematician who did fundamental work in algebra and number theory. He was so interested in the p-adic numbers of Hensel that he went to study under Hensel at Marburg in 1920. He obtained his thesis in 1921. In 1920, he proved

THEOREM 48. *Let $f(x_1, \cdots, x_n)$ be a quadratic polynomial over $\mathbb{Q}$, then that $f(x_1, \cdots, x_n) = 0$ is solvable in $\mathbb{Q}$ is equivalent to that $f(x_1, \cdots, x_n) = 0$ is solvable in $\mathbb{Q}_p$ for every p and in $R = \mathbb{Q}_\infty$.*

This theorem leads to the Hasse principal which is now widely used: to study a global field one should first study its local fields and then look for the gap between local and global properties, which is evaluated by certain cohomology.

3.3. Adèles and Idèles. Claud Chevally (1909-1984) introduced adèles and idèles respectively in 1936 and 1941.

Let K be a number field. The ring of adèles of K is the restricted product of K_v by O_{K_v}:

$$\mathbb{A}_K = \prod\nolimits' K_v = \{(a_v) \in \prod_v K_v \mid a_v \in O_{K_v} \text{ for almost all } v\}.$$

The group of idèles of K is the restricted product of $K_v^\times$ by $O_{K_v}^\times$:

$$J_K = \mathbb{A}_K^\times = \prod\nolimits' K_v^\times v = \{(a_v) \in \prod_v K_v^\times \mid a_v \in O_{K_v}^\times \text{ for almost all } v\}.$$

Now Class field theory can be stated in the language of idèles. Note that

$$K^\times \hookrightarrow J_K, \quad a \longmapsto (a, a, \cdots).$$

Let $U = \prod O_{K_v}^\times$ and the idèle class group $C_K = J_k/K^\times$.

THEOREM 49. *Let K be a number field.*

(1) *If L/K is abelian, then $J_K/K^\times N_{L/K} J_L \cong \mathrm{Gal}(L/K)$.*

(2) *If H is an open subgroup of finite index in J_K and $K^\times \subseteq H$, then there exists a unique abelian extension L/K such that $K^\times N_{L/K} J_L = H$.*

(3) *$L_1 \subseteq L_2$ if and only if $K^\times N_{L_1/K} J_{L_1} \supseteq K^\times N_{L_2/K} J_{L_2}$.*

4. Mendelssohn family and mathematics in 19th century

Moses Mendelssohn (September 6, 1729 – January 4, 1786) was a German Jewish Enlightenment philosopher whose advocacy of religious tolerance resounded with forward-thinking Christians and Jews alike. Mendelssohn's most important contribution to philosophy was to refine and strengthen the philosophical proofs for the existence of God, providence and immortality. In 1763, Mendelssohn won the prize offered by the Berlin Academy for an essay on the application of mathematical proofs to metaphysics; Immanuel Kant received an honorable mention.

Mendelssohn had six children. His son Abraham Mendelssohn (1776-1835) has two sons Felix and Paul and two daughters, Fanny and Rebecka. Felix Mendelssohn (1809-1847) is a German composer, pianist, musical conductor, and teacher, a child prodigy and one of the most-celebrated figures of the early Romantic period. Among his most famous works are Overture to A Midsummer Night's Dream (1826), Italian Symphony (1833), a violin concerto (1844), two piano concerti (1831, 1837), the oratorio Elijah (1846), and several pieces of chamber music.

Fanny Mendelssohn (1805-1847), married name Fanny Hensel, pianist and composer, is the eldest sister and confidante of Felix. Fanny is said to have been as talented musically as her brother. They two were very close to her brother, and Funny's death in May 1847 greatly contributed to Felix's own demise six months later. Fanny married the Prussian court painter Wilhelm Hensel in 1829. Their son Sebastian Hensel wrote a biography of the Mendelssohn family based partly on Fanny's diaries and letters, which provide a great deal of information about her brother Felix. Sebastian has two sons, philosopher Paul Hensel and mathematician Kurt Hensel whose contribution in number theory we just mentioned. As we also know, Kronecker is a student of Kummer and Dirichlet and the advisor of Kurt Hensel.

Rebecka Mendelssohn (1811-1858), the younger sister of Fanny and Felix, then married Dirichlet. She died one year before her husband's death.

Nathan Mendelssohn (1781-1852), the younger brother of Abraham, was a maker of mathematical instruments. Nathan's daughter, Ottilie Ernestine married Kummer. One of their daughters, Marie Elisabeth Kummer, married Kummer's own student Hermann Schwarz.

CHAPTER 5

Galois cohomology and Galois representations

1. Galois theory revisited

We now return to Galois theory. One of the key problems in this area is

1.1. Inverse problem of Galois theory/Inverse Galois problem.

PROBLEM 2. Given a finite group G, is there a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) = G$?

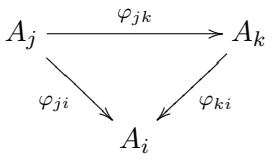
REMARK 7. (1) If replace $\mathbb{Q}$ by some other fields F, then the answer is yes:

(1) $F = \mathbb{C}(t)$.
(2) $F = K(t)$ where K is a p-adic field.

(2) Kronecker-Weber Theorem means the answer is true for G abelian.
(3) For G non-abelian, the problem is still open:

(1) Hilbert in 1892 proved the case for $G = S_n$ or A_n.
(2) A famous theorem of Noether claims that: let $M = \mathbb{Q}(t_1, ..., t_n)$ and G be a transitive subgroup of S_n and $K = M^G$, if K is isomorphic to a field of rational functions over $\mathbb{Q}$, then the inversoe Galois problem is true for the group G.
(3) Scholz-Reichardt (1937) proved the case that G is a p-group for prime $p > 2$.
(4) Shafarevich in 1954 proved the case that G is a solvable group.
(5) For simple groups, the cases for $\mathrm{PSL}(2, p)$ if $p \mid 42$ and all sporadic simple group except M_{23} (the Mathieu group) are known.

1.2. Infinite Galois extensions. Let I be a directed set, which means that there exists a partial order in I satisfying the condition: for i and $j \in I$, there exists k such that $i < k$ and $j < k$. A projective system $(A_i)_{i \in I}$ can be described as follows: A_i $(i \in I)$ is an object in certain abelian category with infinite product like sets, groups, rings or modules, and for any triple $i < k < j$, there is a commutative diagram in this category:



The projective limit is then

$$\varprojlim_{i\in I} A_i := \{(a_i)_{i\in I} \mid \varphi_{ji}(a_j) = a_i \quad \text{for all } j > i\} \subseteq \prod_{i\in I} A_i.$$

If the objects A_i are topological spaces, then $\prod_i A_i$ is assigned with the product topology and $\varprojlim_i A_i$ is regarded as a closed subset of $\prod_i A_i$. For example, if the A_i's are finite sets, usually we assign them with discrete topology, then by Tychnoff's Theorem, $\prod_i A_i$ is a compact Hausdorff topological space and so is the projective limit $\varprojlim_i A_i$, which is called a profinite limit.

EXAMPLE 18. For p a prime number, the limit of the projective system $(\mathbb{Z}/p^n\mathbb{Z}))_n$ with the connecting map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}(n \geq m)$ by restriction

$$\varprojlim_{n} \mathbb{Z}/p^n\mathbb{Z}$$

is canonical isomorphic to the ring of p-adic integer $\mathbb{Z}_p$, with the topology given by the limit agreeing with the p-adic topology of $\mathbb{Z}_p$.

Now recall

DEFINITION 22. A Galois extension is an algebraic separable and normal extension.

Suppose L/K is an infinite Galois extension. Note that if M/K is a finite sub-extension of L, then the Galois closure N/K of M is a finite Galois sub-extension of L. Now let $I = \{E/K \mid K \subset E \subset L,\ E/K \text{ finite and Galois}\}$ ordered by inclusion. For $E \subset F \in I$, then one has the natural restriction map $\mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$. This gives a projective system $(\mathrm{Gal}(E/K))_{E\in I}$. Then

DEFINITION 23. The Galois group $\mathrm{Gal}(L/K)$ is defined as the projective limit of $\mathrm{Gal}(E/K)$, i..e.,

$$\mathrm{Gal}(L/K) = \varprojlim_{\substack{K\subset E\subset L \\ E/K \text{ finite Galois}}} \mathrm{Gal}(E/K).$$

By definition, we know that a Galois group is a profinite group, thus Hausdorff and compact. We remark that if L/K is finite, then the above definition agrees with the original one. For $x \in L$ and $\sigma = (\sigma_E)_{E\in I} \in \mathrm{Gal}(L/K)$, let M be a finite Galois sub-extension containing x (for example, the Galois closure of $K(x)$), set $\sigma(x) = \sigma_M(x)$. Note that $\sigma(x)$ is independent of the choice of M. In this way, we define the $\mathrm{Gal}(L/K)$-action on L.

THEOREM 50 (Fundamental Theorem of Galois Theory). *Let L/K be a Galois extension with Galois group $G = Gal(L/K)$, then there is a one-to-one correspondence:*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{closed subgroups} \\ \text{of } G \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{algebraic extensions} \\ \text{of } K \text{ inside } L \end{array} \right\} \\ H & \longmapsto & L^H \\ \mathrm{Gal}(L/M) & \longleftarrow & M \end{array}$$

Moreover, the correspondence implies that

(1) Normal subgroups correspond to Galois subextensions.

(2) Open subgroups correspond to finite subextensions. In this case, $[G : H] = [M : K]$.

(3) Open normal subgroups correspond to finite Galois subextensions. In this case, $G/H \cong \mathrm{Gal}(M/K)$.

EXAMPLE 19. (1) Let K^s be the separable closure of K, $G_K = \mathrm{Gal}(K^s/K)$ is called the absolute Galois group of K. Note that if $\mathrm{char}(K) = 0$, $K^s = \overline{K}$ = the algebraic closure of K.

(2) Suppose p is a prime. Suppose there is a field tower

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n \subseteq ... \subseteq \bigcup_{n \in N} K_n = K_\infty$$

such that

$$\begin{array}{ccc} \mathrm{Gal}(K_n/K_0) & \xrightarrow{\cong} & Z/p^n Z \\ {\scriptstyle res}\downarrow & & \downarrow{\scriptstyle res} \\ \mathrm{Gal}(K_{n-1}/K_0) & \xrightarrow[\cong]{} & Z/p^{n-1} Z \end{array}$$

Then

$$\mathrm{Gal}(K_\infty/K) = \varprojlim_n \mathrm{Gal}(K_n/K) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

K_∞/K is called a $\mathbb{Z}_p$-extension. As the only closed subgroups of $\mathbb{Z}_p$ are 0 (which is not open) and $p^n Z_p$ ($n \geq 0$, which is also open), then the only subextensions of K_∞/K are K_∞ and K_n.

The study of $\mathbb{Z}_p$-extensions of number fields is now called Iwasawa Theory, initiated by K. Iwasawa in lathe 1950's.

Let K be a number field and G_K be the absolute Galois group of K. For any place v of K (i.e. either prime ideals of O_K, real embeddings $K \to R$ or pairs of complex embeddings $K \to \mathbb{C}$), let $G_{K_v} = \mathrm{Gal}(\overline{K_v}/K_v)$. Then the diagram

$$\begin{array}{ccc} K & \xrightarrow{\subset} & K_v \\ \cap\downarrow & & \downarrow\cap \\ \bar{K} & \xrightarrow[\subset]{} & \bar{K}_v \end{array}$$

implies that G_{K_v} can be considered as subgroups of G_K.

The main problem in Number theory is to study G_K for K a number field, in particular for $K = \mathbb{Q}$.

(1) Let $G_K^{ab} = G_k/\overline{[G_K, G_K]}$ be the maximal abelian quotient of G_K. Then

$$\begin{array}{ccccc} \text{study of} & & \text{describing abelian} & & \text{class field} \\ G_K^{ab} & \longleftrightarrow & \text{extensions of } K & \longleftrightarrow & \text{theory.} \end{array}$$

This is known:

- Local Class Field Theory: for K a local field, study of G_K^{ab} is equivalent to study of the completion of $K_v^\times$.
- Global Class Field Theory: for K a global field, study of G_K^{ab} is equivalent to study of the idèle class group $C_K = J_K/K^\times$.

(2) Local-Global Principal (aka Hasse's Principal): first study all local pieces G_{K_v}, then find a way to patch them together.

(3) To study groups, one needs to study their representations. For number fields/local fields:

- Complex (i.e. $\mathbb{C}$-) representations;
- ℓ-adic and p-adic representations;
- $\mathbb{Z}_p$-representations;
- $\mathbb{F}_p$-representations.

2. Galois cohomology and Galois representations

2.1. Tate. In 1940's, algebraic topology and homological algebra enjoyed rapid growth in the hands of Levy, Henri Cartan-Eilenberg, Serre and other mathematicians. John Tate(1925-2019) was essential to integrating the cohomological tools to the study of number theory.

Tate is a student and son-in-law of Artin. Because of his fundamental contribution to number theory and arithmetic geometry, he won Abel Prize in 2010 and Wolf Prize in 2002/2003. Among his great achievements as one of the greatest mathematicians in our lifetime are

(1) Tate's 1950 Ph.D thesis at Princeton University developed Fourier analysis in number fields, paved the way for the study of automorphic representations and Langlands program. It is safe to say there are no theses with greater importance in mathematics than the two Johns' (John Tate and John Nash) in 1950 at Princeton.
(2) Artin and John Tate began to use cohomological language to rewrite class field theory in 1950s. Their work was contained in the classical book Class Field Theory (Harvard 1961, W.A.Benjamin 1967). Over there modern language of Galois cohomology was used to prove local and global class field theory.
(3) Tate is the founder of p-divisible group, also called Barsotti-Tate group (in the paper p-divisible group, Proc. of a Conference on Local fields, 158-183,1967). This is the starting point of p-adic Hodge theory, later developed by Jean-Marc Fontaine and others.

(4) Tate (Rigid analytic space. Invent.Math.12, 257-289 1971) also introduced the notion rigid analytic space as an analogue to complex analytic space, which perhaps is the hottest notion now in number theory.
(5) There are many terms named after Tate, perhaps more than any other modern mathematicians: Tate module, Tate curve, Tate cycle, Tate algebra, Hodge-Tate Decomposition, Tate cohomology, Lubin-Tate group, Shafarevich-Tate group, Néron-Tate height, $\cdots$

2.2. Galois cohomology. Let K be a number field and L/K be a Galois extension. Then there are numerous arithmetic objects with $\mathrm{Gal}(L/K)$-action:

$$L,\ L^\times,\ \mu(L),\ \text{etc.}$$

If $L = K^s$ is the separable closure of K, then we have G_K-modules (Galois modules)

$$K^{s\times},\ \mu_{p^\infty},\ \mu_n,\ A(K^s\ (A/K \text{ an abelian variety}),\ E(K^s)\ (E/K \text{ an elliptic curve}).$$

Thus it is nature to use group cohomology/homology to study these objects.

Suppose G is a finite group and A is a G-module.

(1) Set $H^0(G,A) = A^G$, the derived functors of the functor $A \mapsto A^G$ gives the higher cohomological groups $H^i(G,A)$;
(2) Set $H_0(G,A) = A_G == A/\langle ga - a :\ a \in A,\ g \in G\rangle$, the derived functors of the functor $A \mapsto A_G$ give higher homological groups $H_i(G,A)$.
(3) Tate introduced the Tate cohomology $\hat{H}^0(G,A)$ and $\hat{H}^{-1}(G,A)$, and united the cohomology and homology groups of A.

For G a profinite group and A a discrete G-module, again the cohomology groups $H^i(G,A)$ are derived from the functor $A \mapsto H^0(G,A) = A^G$.

For H^1, Hilbert's Theorem 90 states

THEOREM 51 (Hilbert Theorem 90). $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.

From tis theorem, one can deduce Kummer Theory (Kummer pairing and Kummer extension).

For H^2, the Brauer group $\mathrm{Br}(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$ and $\mathrm{Br}(K) = H^2(G_K, K^{s\times})$. Similarly, one can define $\mathrm{Br}(K_v)$ for local fields. Brauer group gives a classification of division algebras over K. Artin-Tate constructed Artin reciprocity map and proved local and global class field theory via the study of Brauer group.

Furthermore, Galois cohomology gives

- Tate local duality;
- Poitou-Tate exact sequence

which are essential in nmuber field study.

REMARK 8. For more about Galois Cohomology, see the following two classic books:

(1) Serre: Galois cohomology
(2) Neukirch, Schmidt and Wingberg: Cohomology of number fields.

2.3. ℓ-adic representations.

DEFINITION 24. Let K be a field and $G_K = \mathrm{Gal}(K^s/K)$ be the absolute Galois group of K.

(1) Suppose E is a (topological) field equipped with a (continuous) action of G_K. An E-representation V of G_K is a finite dimensional E-vector space equipped with a (continuous) semilinear action of G_K.

(2) Moreover, suppose R is a (topological) ring equipped with a (continuous) action of G_K. An R-representation M of G_K is an R-module of finite type equipped with a (continuous) semilinear action of G_K.

Note that if G_K acts trivially on E, then semilinear=linear in the above definition.

EXAMPLE 20. Let ℓ be a prime number, then a $\mathbb{Q}_\ell$-representation is called an ℓ-adic representation.

EXAMPLE 21. (1) For $\zeta \in \mu_{\ell^\infty}(K^s)$ and $g \in G_K$, the cyclotomic character $\chi(g)$ is the unique element in $\mathbb{Z}_\ell^\times$ such that $g(\zeta) = \zeta^{\chi(g)}$, which gives a homomorphism $G_K \to \mathbb{Z}_\ell^\times$.

The Tate twist of the multiplicative group is

$$T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n}(K^s) \cong \mathbb{Z}_\ell t = \mathbb{Z}_l(1),$$
$$V_\ell(\mathbb{G}_m) = \mathbb{Q}_\ell t = \mathbb{Q}_\ell(1) = \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

where $g(t) = \chi(g)t$ for $g \in G_K$. Then $T_\ell(\mathbb{G}_m)$ is a free $\mathbb{Z}_\ell$-representation of G_K of rank 1 and $V_\ell(\mathbb{G}_m)$ is a one-dimensional $\mathbb{Q}_\ell$-representation of G_K.

(2) For E an elliptic curve over K, or more general A an abelian variety over K, one can define the Tate modules $T_\ell(E)$ (and $V_\ell(E)$) and $T_\ell(A)$ (and $V_\ell(A)$).

(3) Let X be a proper smooth variety over K. The ℓ-adic cohomology groups $H^{\text{ét}}_m(X_{K^s}, \mathbb{Z}_\ell)$ and $H^{\text{ét}}_m(X_{K^s}, \mathbb{Q}_\ell)$ give more general examples of $\mathbb{Z}_\ell$ and ℓ-adic representations of G_K, with the Tate modules special cases.

2.4. p-adic Galois representations. If K is a local field, suppose its residue field k is of characteristic p, to study the ℓ-adic representation, then there are two cases to consider:

- $p \neq \ell$, this is easier to study;
- $p = \ell$, this is much more difficult. p-adic Hodge theory is the study of p-adic Galois representation of local fields whose residue characteristic is p.

Suppose V is a p-adic representation.

(1) The case $\dim_{\mathbb{Q}_p} V = 1$ is the work of Tate.

(2) Let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ be the p-adic completion of the algebraic closure of $\mathbb{Q}_p$. Let $W = V \bigotimes_{\mathbb{Q}_p} \mathbb{C}_p \mathbb{C}_p$. Then W is a $\mathbb{C}_p$-representation of G_K. Sen, a student of Tate, classified all $\mathbb{C}_p$-representations. This led to the notions of Hodge-Tate weight and Hodge-Tate decomposition.

Jean-Marc Fontaine (1944-2019) founded p-adic Hodge theory to study p-adic Galois representations. He constructed several big topological rings (rings of p-adic periods) with continuous G_K-action:

(1) B^+_{dR}, a discrete valuation ring with t a uniformizer and $\mathbb{C}_p$ the residue field (thus a huge ring), and its field of fractions B_{dR} which is called the field of p-adic periods;
(2) B_{cris} which is constructed from divided power envelope;
(3) B_{st} is the polynomial ring of B_{cris}.

Key for Fontaine's construction is as follows. Let k be the residue field of K. Fontaine observed that

$$R = \varprojlim_{x \mapsto x^p} O_{\overline{K}}/pO_{\overline{K}} = \varprojlim_{x \mapsto x^p} O_{\overline{K}}$$

is a perfect valuation ring mixed characteristic whose residue field is the algebraic closure of k, and

$$\mathrm{Fr}R = \varprojlim_{x \mapsto x^p} \overline{K}$$

is algebraically closed. Then $\pi = (1, \zeta_p, \cdots,) \in R$ and

- $k[[\pi]] \subseteq R$.
- $\mathrm{Fr}R$ is algebraically closed $= \widehat{k((\pi))^{sep}}$.
- Fontaine-Wittenberger showed that

$$\mathrm{Gal}(k((\pi))^{sep}/k((\pi))) \cong \mathrm{Gal}(\overline{K}/K(\zeta_{p^\infty}))$$

canonically.

Then from the Witt ring $W(R)$, Fontaine constructed B_{dR}, B_{cris} and B_{st}.

Definition 25. For $B = B_{\mathrm{dR}}, B_{\mathrm{st}}$ or B_{cris}, if $(B \otimes_{Q_p} V)^{G_K}$ generates $(B \otimes_{Q_p} V)$, then we call V a B-representation.

In general,

- crystalline representations are usually good ones;
- p-adic monodromy theorem claims that de Rham is potentially semistable (semi-stabe after finite base change), thus de Rham and semi-stable representations are almost the same.

Conjecture 2 (Fontaine-Mazur). *Suppose V is a continuous irreducible ℓ-adic representation of $G_{\mathbb{Q}}$. Then V "comes from geometry", i.e.*

$$V = \textit{sub-quotient of } H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}_\ell(j)}) \textit{ for some } i, j \textit{ and } X/\mathbb{Q}$$

if and only if the following conditions hold:

(1) V is unramified almost everywhere,

(2) Its restriction on $G_{\mathbb{Q}_\ell}$ is de Rham.

REMARK 9. Fontaine-Mazur Conjecture for dimension 2, proved by the work of Misin and Emerton, implies Fermat's Last Theorem.

2.5. Perfectoid fields and Perfectoid spaces. Finally we shall mention a little bit about the great work of Peter Scholze.

DEFINITION 26. A Perfectoid field K is a complete topological field whose topology is introduced by a non-discrete valuation of rank 1 and $\Phi : K^o/p \to K^o/p, x \mapsto x^p$ is surjective, where K^o is the set of power bounded elements of K.

EXAMPLE 22. $\mathbb{Q}_p(\zeta_{p^\infty})$, $\mathbb{Q}_p(\frac{1}{p^{p^\infty}})$, $\mathbb{C}_p$, and $\overline{\mathbb{Q}_p}$ are perfectoid fields.

Let K be a perfectoid field. Set

$$K^\flat = \varprojlim_{x \mapsto x^p} K.$$

Then Scholze found that $K^\flat$ is a perfectoid field of characteristic p. For $x \in K^\flat$, then $x = (x^{(0)}, x^{(1)}, ...)$, $(x^{(n+1)})^p = x^{(n)}$. Set

$$x^\sharp = x^{(0)} \in K.$$

Scholze generalized Fontaine-Wittenberger's Theorem to get

THEOREM 52. *$G_K \cong G_{K^\flat}$ are canonically isomorphic.*

DEFINITION 27. A Perfectoid K-algebra R is a Banach K-algebra, such that set R^o of power bounded elements of R is bounded and $\Phi : R^o/p \twoheadrightarrow R^o/p,\ x \mapsto x^p$ is surjective.

One similarly defines $R^\flat = \varprojlim_{x \mapsto x^p} R$ and $^\sharp$.

THEOREM 53. *There exists a natural equivalence of categories:*

$$\begin{array}{ccc} \left\{ \begin{array}{c} cat.\ of\ perfectoid \\ K-algebras \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} cat.\ of\ perfectoid \\ K^b-algebras \end{array} \right\} \\ R & \longmapsto & R^\flat \\ (R^\flat)^\sharp & \longleftarrow & R^\flat \end{array}$$

Then Scholze began to study rigid analytic spaces. He proved the equivalence of categories of affinoid perfectoid algebras over K and $K^\flat$ via the correspondence

$$(R, R^+) \longmapsto (R^\flat, R^{\flat +})$$

where R^+ passes through open and integrally closed subsets of R^o. Let $X = \mathrm{Spa}(R, R^+)$ be the Adic space of Huber whose points are equivalence of continuous valuations $x : \quad R \mapsto\to \Gamma \cup 0, f \mapsto |f(x)|$, which are ≤ 1 on R^+.

THEOREM 54. *Let $X = \mathrm{Spa}(R, R^+)$, $X^\flat = \mathrm{Spa}(R^\flat, R^{\flat +})$.*
(1) *The following map is a homeomorphism:*

$$\begin{aligned} X &\longrightarrow X^\flat \\ x &\longmapsto x^\flat \\ |f(x^\flat)| &= |f^\sharp(x)| \end{aligned}$$

(2) *It induces an isomorphism of sheaves $O_X \cong O_{X^\flat}$.*

Gluing all affinoid pieces, we get a perfectoid space.

THEOREM 55. *The category of perfectoid spaces over K and the category of perfectoid spaces over $K^\flat$ are equivalent.*

This gives a theorem of in the language of almost mathematics of Faltings:

THEOREM 56. *Let R be a perfectoid K-algebra, and S/R is finite étale. Then S is a perfectoid K-algebra, and S^o is almost finite étale over R_o.*

Finally let X be a perfectoid space, $X_{\text{ét}}$ be the étale site of X. Then

THEOREM 57. *$X_{\text{ét}} \cong X^\flat_{\text{ét}}$ is canonically equivalence of sites.*