Lektioner 1 och 2 (3/11/00)

Målen med dagens lektioner är (i) att ge en översikt av hela kursen och ämnet som kallas för 'talteori', (ii) att bevisa aritmetikens fundamental sats.

Vi slösar inte bort någon tid med att diskutera Peano's axiom för aritmetik, men nöjer oss med en intuitiv beskrivning av heltalen $\mathbf{Z}$. Den algebraiska strukturen hos $\mathbf{Z}$ sammanfattas med

Proposition 1. $(\mathbf{Z}, +, \times)$ *är en kommutativ ring med enhet.*

De naturliga talen $\mathbf{N}$ har en viktig mängd-teoretisk egenskap som ofta utnytas i bevis inom talteori, nämligen

Faktum. $\mathbf{N}$ *är välordnad.*

Kom ihåg att en ordnad mängd kallas för välordnad om varje icke-tom delmängd har ett första element.

T.ex., *induktion* och Fermat's metod av *infinite descent* beror på väl-ordningen av $\mathbf{N}$.

Addition i $\mathbf{Z}$ är inte så 'algebraiskt' interessant, för $\mathbf{Z}$ genereras som en additiv grupp av ett enda element, nämligen 1 (eller -1). Multiplikation, däremot, är mycket mer fascinerande. Det mest fundamentala icke-triviala resultatet i talteori är

Aritmetikens fundamentalsats (Euclid). *Det finns en delmängd* $\mathcal{P} \subset \mathbf{N}$ *med följande egenskaper :*

(i) Låt $S \subseteq \mathbf{N}$. *Varje element av* $\mathbf{N}$ *kan skrivas som en produkt av element från* S *om och endast om* $\mathcal{P} \subseteq \mathcal{S}$.

(ii) Varje element av $\mathbf{N}$ *har en unik representation som en produkt av element från* $\mathcal{P}$.

Talen i mängden $\mathcal{P}$ kallas för *primtalen.*

BEVIS : Idéen bakom beviset är begreppet av *dividerbarhet.* Kom ihåg att talet a sägs *dela* talet b om det finns ett tal c så att $b = ca$. Man skriver $a \mid b$. Man säger lätt att $(\mathbf{N}, |)$ är en *partiellt ordnad* mängd. Euclid observerade att den faktiskt är ett *gitter*. Mer precist, bevisade han följande

Proposition 2. *Låt $a, b \in \mathbf{N}$. Då finns det (ett unikt) $d \in \mathbf{N}$ med följande två egenskaper :*

(i) $d \mid a$ och $d \mid b$.
(ii) om $c \mid a$ och $c \mid b$ då måste $c \mid d$.

Dessutom är d det minsta positiva tal som kan uttryckas i formen

$$\alpha a + \beta b$$

för något $\alpha, \beta \in \mathbf{Z}$.

Talet d kallas för den *största gemensamma delaren* (eng.: = greatest common divisor) av a och b och betecknas $\gcd(a, b)$, eller helt enkelt (a, b) när kontexten är klar. Det är en glb för a och b i po-mängden $(\mathbf{N}, |)$.

Man definierar på ett liknande sätt den *minsta gemensamma multiplen* (eng.: = least common multiple) av a och b som är en lub för a, b i gittret. Man bevisar lätt att

$$\mathrm{lcm}(a, b) = \frac{ab}{\gcd(a, b)}. \tag{1}$$

Det är naturligt att fråga hur många primtal det finns. I sin enklaste form, löstes detta problem redan av Euclid.

Sats (Euclid). *Det finns oändligt många primtal.*

Bevis : Som i boken, s. 4.

I detta läge är det naturligt att studera funktionen

$$\pi(x) = \text{antal primtal} \leq x, \tag{2}$$

och försöka ge en precis beskrivning av funktionens beteende. Det tog 2000 år från Euclid's tid för att ge en tillfredställande lösning av detta problem. Den är den 'crowning achievement' av 1800-talets talteori, när analytiska metoder först infördes för att attackera aritmetiska problem (se också Dirichlet's sats nedan).

Primtalssatsen (Hadamard o. de la Vallée Poussin 1896).

$$\pi(x) = li(x) + O(xe^{-c\sqrt{\log x}}), \tag{3}$$

där

$$li(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}. \tag{4}$$

The proof uses extraordinary complex-analytical properties of the so-called *Riemann zeta function*, which is defined in a half-plane by the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \mathrm{Re}(s) > 1. \tag{5}$$

In a groundbreaking and notorious paper from 1860 [1], Riemann showed how this function can be continued to a meromorphic function in the whole complex plane (with only a simple pole at $s = 1$) and that it satisfies a so-called *functional equation*, namely

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s). \tag{6}$$

The notoriety of the paper is due to the fact that in it Riemann made a conjecture about the zeroes of $\zeta(s)$ which remains unproven to this day, namely

Riemann hypothesis. *If $\zeta(s) = 0$, then either $s = -2n$ for a non-negative integer n or $Re(s) = 1/2$.*

The central importance of RH in number theory has only become clear over time. If we could prove it, or rather in many cases a generalistion of it called the *generalised Riemann hypothesis* (GRH), then many other impressive results would follow. The oldest of these is an improvement in the error term in the Prime Number Theorem, namely RH would imply that

$$\pi(x) = \mathrm{li}(x) + O(x^{1/2}\log x). \tag{7}$$

We may come back to these things later. We finish this section by mentioning two very famous unsolved problems, which also have something to do with the distribution of the prime numbers.

Twin primes conjecture. *There exist infinitely many primes p such that*

$p+2$ is also prime. More strongly, if $\pi_2(x)$ denotes the number of such primes $\leq x$, then

$$\pi_2(x) \sim \frac{x}{\log^2 x}. \tag{8}$$

Goldbach conjecture. *Every even number is the sum of two primes.*

Most of the methods used to tackle these two problems can be brought under the heading of *sieve methods.* At their most basic, these are purely combinatorial methods, but at the more advanced level there is a lot of analysis. I hope we will have some time later to discuss at least some simple combinatorial sieves.

The crowning achievement so far of sieve methods is

Chen's theorem (1974). *(i) There are infinitely primes p such that $p+2$ is either prime or a product of two primes.*
(ii) Every sufficiently large integer can be written as a sum of two numbers, one of which is prime and the other of which is either prime or a product of two primes.

Construction of prime numbers

One of the oldest problems in the study of primes has been the attempt to find some kind of formula for generating prime numbers. More precisely, we may seek a function $f : \mathbf{N} \to \mathbf{N}$, which can be described as simply as possible, and such that $f(n)$ is prime for all n. Two classic candidate functions were proposed by Fermat and Mersenne respectively. We denote them by f_F and f_M and they are given by the formulas

$$f_F(n) = 2^{2^n} + 1, \tag{9}$$

$$f_M(n) = 2^{p_n} - 1 \quad \text{(where } p_n \text{ is the } n^{\text{th}} \text{ prime).} \tag{10}$$

Motivation for these suggestions is provided by the following easy result

Proposition 3. *(i) If x^n+1 is prime then $2 \mid x$ and n is a power of 2.*
(ii) If x^n-1 is prime then $x=2$ and n is prime.

Fermat conjectured that f_F was always prime and it was one of his biggest mistakes because one can show by hand that 641 divides $f_F(5)$.

Open Problem. *Are there infinitely many n for which $f_F(n)$ (resp. $f_M(n)$) is (not) prime ?.*

Perhaps the simplest type of formula one can write down (at least if one is an algebraist !) is that given by a polynomial in one variable. However, the following is not hard to prove

Proposition 4. *There is no polynomial $f(x)$ with integer coefficients such that $f(n)$ is prime for all $n \in \mathbf{N}$*[1].

PROOF : A proof similar to the one I gave is on p.5 of the book.

On the other hand, Euclid's theorem says that the polynomial $f(x) = x$ generates infinitely many primes. That the same is true for any linear function (with certain restrictions) was first proven by Dirichlet :

Dirichlet's theorem on AP's (1837). *Let $f(x) = ax + b$ where $a, b \in \mathbf{Z}$ and $(a, b) = 1$. Then $f(n)$ is prime for infinitely many n.*

This is a huge result in number theory, not only because of its' intrinsic interest, but because it was the first time that analytic methods were used in number theory and thereby it gave birth to a whole new field in mathematics. The objects studied by Dirichlet, namely the zeta function (later named after Riemann) and its' generalisations, the so-called L-functions, are still of basic importance in the subject today. I hope to prove Dirichlet's theorem in this course.

Wide open problem. *Does there exist a polynomial $f(x)$ of degree higher than 1, with integer coefficients whose gcd is 1, such that $f(n)$ is prime for infinitely many n ?*

APPLIED / ALGORITHMIC PROBLEMS CONCERNING PRIMES

Primality testing : The problem is to find an efficient algorithm for deciding whether a randomly chosen positive integer n is prime. Most of the

[1]The situation is quite different for polynomials of many (at least 12) variables - see p.5 of book.

suggested algorithms basically rely on Fermat's little theorem (which we'll prove soon) and the concept of a *pseudoprime*. An algorithm is known which can be proven to run in polynomial time in $\log n$ provided that GRH is true ! We'll come back to this.

Factorisation : None other than Bill Gates is on record as having said that he thought the search for a fast algorithm for factoring large numbers was one of the most important problems in mathematics. The reason he said this is presumably because many public-key cryptosystems rely for their security on the assumption that no such fast algorithm is likely to be found in the near future. The most famous of these is the so-called RSA (= Rivest, Shamir and Adleman) system which dates from 1976 and is still in use today. We will talk more about cryptography during the course.

WHAT'S THERE TO STUDY OTHER THAN THE PRIMES ?

Well, there's a lot, but much of the remaining research in number theory throughout history has been concerned with the problem of solving algebraic equations, specifically polynomial equations, in $\mathbf{Z}$. It should come as no surprise that it is in tackling this problem that the subject nowadays known as *algebraic number theory* was developed.

To be precise, we are interested in solving equations

$$p(x_1, ..., x_n) = 0, \tag{11}$$

where p is a polynomial with integer coefficients. The case $n = 1$ is not very interesting but the case $n = 2$ already opens up a whole can of worms. To break the problem down into more manageable pieces, we first consider polynomials of low degree. For degree 1, things are still not interesting as equation (1) above can easily be used to prove

Proposition 5. *The equation $ax + by = c$ has a solution if and only if $gcd(a, b)$ divides c.*

For degree 2 though, there is an extensive theory usually referred to as Gauβ' theory of *binary quadratic forms*. This theory takes up a substantial portion of Baker's book[2].

[2] There is also an extensive theory for polynomials of degree 2 in more than 2 variables,

For degree higher than 2, there is the following famous theorem of the Norwegian mathematician Thue :

Thue's theorem (1909). *Let $f(x,y)$ be a homogeneous polynomial with integer coefficients, of degree at least 3, and $n \in \mathbf{Z}$. Then the equation $f(x,y) = n$ has finitely many solutions.*

PROOF : Baker, section 8.2.

Thue's result was extended by Siegel (1929) to cover all functions $f(x,y)$ such that the associated projective curve $f(x,y) = 0$ over $\mathbf{C}$ has genus greater than 0. In particular it covers all functions $f(x,y) = y^2 - f(x)$, where $f(x)$ is a polynomial with integer coefficients, of degree at least 3[3]. Much later, Baker (1968) gave an 'effective' version of Thue's theorem ; that is, he gave explicit upper bounds on $|x|, |y|$ such that $f(x,y) = n$, which depended only on f. In practice, these bounds are generally too large to allow for the computation of all solutions, for a given f and n, but can be improved in specific cases.

The methods employed by all these authors use techniques of so-called *Diophantine approximation* which, informally, is the study of how well one can approximate a given irrational number by rationals ; that is, you want to get as close as possible to the irrational number while the denominators of your rationals grow as slowly as possible. Embedded in this subject is the very old conept of *continued fractions.* A very extensive introduction to this area is given in Chapter 6 of Baker's book.

One such type of equation which has received an enormous amount of attention is the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The associated projective curve over $\mathbf{C}$ is called an *elliptic curve*, and has genus 1. In fact, every curve of genus 1 is given by such an equation, called a *Weierstraß equation.* There is a voluminous literature about elliptic curves. Much of this deals, not only with the study of solutions over $\mathbf{Z}$, but over

but the results are not complete. If you'd like to hear more about this you should come to my graduate course.

[3]In separate work during the 1940s, Siegel used complicated analytical methods to study solutions of quadratic equations (genus 0 curves), and his methods actually apply to any number of variables. We'll come back to this later.

Q or more general fields. While there are usually no longer finitely many solutions in these cases, there turns out to be a tremendous amount of interesting mathematical structure. For example, the points (x, y) on an elliptic curve, where x, y belong to any given field, can be 'added' in such a way that they form an abelian group. There is the famous theorem of Mordell and Weil (1920s) which says that, in the case of **Q**, this group is finitely-generated. We will not have time in this course to study elliptic curves - a proper study would require a full course in itself, and would draw on methods from several fields : number theory, algebraic geometry, complex analysis and topology.

By the way, the study of polynomial equations over **Q** instead of just **Z** turns out to be fruitful in other instances also. Most notable is the case of quadratic forms (in any number of variables). There is the classic theorem of Hasse and Minkowski (1930s) which, in essence, says that solving a quadratic equation over **Q** is equivalent to solving a finite list of congruences. Once again, the interesting thing here is the algebraic structure, since there's no issue of actually 'counting' solutions. We'll say more about this when we come to study binary quadratic forms, though the H-M theorem applies to forms in arbitrarily many variables.

For more than 2 variables, a certain amount is known in degree 2 (quadratic forms), as has already been indicated above. For degree higher than 2, very little is known in general, but there are many famous results (and problems) of a seemingly isolated nature. We mention only two of the most famous here :

Waring's Problem. *For each n there exists $k_n >> 0$ such that every positive integer can be written as the sum of no more than k_n n^{th} powers.*

The case $n = 2$ of this theorem was already solved by Lagrange in 1770 (the same year that the problem was stated), who proved that $k_2 = 4$. It is perhaps his most famous result. The first general solution was given by Hilbert in 1909 and a later solution by Hardy and Littlewood (1920s) used the so-called *circle method* of analytic number theory, which has proved a very useful tool for the unravelling of many other problems.

Fermat's Last Theorem. *If $n > 2$ and $x^n + y^n = z^n$ then $xyz = 0$.*

Fermat himself actually wrote down a proof for the case $n = 4$ and it is a famous example of the use of his method of infinite descent. The case $n = 3$ was settled by Euler, and the ideas in his proof initiated the use of algebraic methods to tackle the problem, namely the development of the theory of finite field extensions of $\mathbf{Q}$ (what is now called algebraic number theory). The pinnacle of success for these methods was reached by Kummer in 1850 who used the theory of so-called *cyclotomic fields* (fields of the form $\mathbf{Q}(\zeta)$ where ζ is a root of unity) to prove FLT for so-called *regular primes*[4].

As everyone knows, the eventual proof of Fermat's theorem, accomplished by Wiles in 1994, employs rather different methods. It exploits some deep connections between two apparently quite different types of mathematical objects, namely *modular forms* and the aforementioned elliptic curves. The relevant connections were formally summarised in a conjecture of Shimura, Taniyama and Weil from the late 1960s. In the mid 1980s, work of Frey, Serre and Ribet established that FLT would follow from the STW conjecture. It then took Wiles eight years to prove the latter (for *semistable* elliptic curves).

WHAT ELSE ?

We mention two things :

Transcendental numbers : A complex number is called transcendental if it does not lie in any finite field extension of $\mathbf{Q}$. Otherwise it is called *algebraic*, because in that case it is a root of some polynomial with rational coefficients. There are many classic problems (both solved and unsolved) surrounding the issue of whether certain numbers are transcendental or algebraic. Two of the most famous transcendental numbers are e and π. Two of the most famous numbers which are not known to be either transcendental or algebraic are Euler's constant γ and the value $\zeta(3)$ of the Riemann ζ-function. A famous result of Lindemann (1844) gave a general method for constructing transcendental numbers (though it doesn't work for e or π !). Lindemann's theorem is about Diophantine approximation of algebraic numbers, and is also the basic ingredient in the proof of Thue's theorem mentioned above. The improvements on Thue's theorem by Siegel et al also rely on corresponding improvements on Lindemann's theorem.

[4]This material is discussed well in, for example, the book of Stewart and Tall. I don't know yet how much of it we will have time to do.

Combinatorial number theory : There are many interesting problems about whole numbers of a purely combinatorial flavour (see [2]). At this point, we mention just one such open problem, due to Paul Erdös, and worth 500 to the solver :

Open problem. *There exists an absolute constant* $C > 0$ *such that if* $S \subseteq \{1, ..., N\}$ *is such that all subset-sums from* S *are distinct, then* $|S| \leq \log_2 N + C$.

The trivial lower bound for C is $C = 1$, as is seen by considering $N = 2^k$ and $S = \{2^j : 0 \leq j \leq k\}$. In 1969, Conway and Guy found an example where $C = 2$. Nothing better is known !

References

[1] G. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, Gesammelte werke 145-155.

[2] Handbook of Combinatorics, North-Holland, 1995.

Lektion 3 (6/11/00)

En mycket effektiv algoritm för att beräkna gcd av två naturliga tal gavs redan av Euclid och kallas efter honom.

Euclid's algoritm. *Låt* $a, b \in \mathbf{N}$. *Antag att* $b > a$. *Sätt* $r_{-1} = b$, $r_0 = a$. *Definiera successivt en avtagande följd* (r_j) *av icke-negativa tal genom*

$$r_{j-1} = q_j r_j + r_{j+1}, \quad \text{där } 0 \leq q_j,\ 0 \leq r_{j+1} < r_j. \tag{12}$$

Låt k *vara det första indexet så att* $r_k = 0$. *Då är* $gcd(a, b) = r_{k-1}$.

Bevis : Ungefär som i boken, s.3.

Man kan visa att algoritmen har komplexitet $O(\log^3 b)$. Komplexiteten av en algoritm är max. antalet så kallade *bit operationer* som behövs för att genomföra den. En algoritm som har polynom komplexitet i log av beloppet av dess inputs (? svenska) betraktas 'bra' eller 'effektiv'. För en mer komplett introduktion till dessa idéer, se t.ex. boken 'A course in number theory and cryptography', av Neal Koblitz.

Kongruenser

När man letar efter heltalslösningar till en polynomekvation av formen (11), är det ett vanlig trick att först reducera ekvationen modulo n, för olika n, och i stället studera kongruenserna

$$p(x_1, ..., x_n) \equiv 0 \pmod{n}. \tag{13}$$

Intuitivt är det klart att (13) är lättare att lösa än (11) för det finns bara ändliga många möjligheter för en lösning. Dessutom, om n är prim då har $\mathbf{Z}/n\mathbf{Z}$ mer algebraisk struktur än $\mathbf{Z}$, nämligen att den är en kropp (se nedan).

Visst finns det oändligt många ekvationer (13) svarande mot en enda ekvation av formen (11), men t.ex. om kongruensen inte har någon lösning för något n då har den urprungliga ekvationen ingen lösning heller. I den andra riktningen finns det också situationer där existensen av en lösning till kongruensen för varje n räcker till existensen av en lösning i $\mathbf{Q}$, men inte nödvändigtvis i $\mathbf{Z}$. Men även sådana satser brukar vara mycket svårare att bevisa. Den mest berömda är kanske *Hasse-Minkowski satsen* som säger att om $p(x_1, ..., x_n)$ är en kvadratisk form, då har (11) en lösning i $\mathbf{Q}$ omm den har en lösning i $\mathbf{R}$ och en lösning modulo p för varje primtal p. För ett bevis av denna sats, se t.ex. Kap. IV av Serre's bok 'A course in arithmetic'.

Nu börjar vi från början.

DEFINITION : Fixera $n \in \mathbf{N}$. Låt $a, b \in \mathbf{Z}$. Säg att a är *kongruent till* b modulo n, och skriv $a \equiv b \pmod{n}$, om $n \mid a - b$.

Proposition 6. $\equiv \pmod{n}$ är en ekvivalens relation på $\mathbf{Z}$.

Ekvivalensklassen av ett tal x betecknas $\bar{x}$. Mängden av ekvivalensklasser betecknas $\mathbf{Z}/n\mathbf{Z}$ och dess element kallas för *residue klasser* modulo n. Det är lätt att se att

$$\mathbf{Z}/n\mathbf{Z} = \{\bar{x} : 0 \leq x < n\}, \quad \#(\mathbf{Z}/n\mathbf{Z}) = n. \tag{14}$$

Proposition 7. *Fixera n. Avbildningen $x \to \bar{x}$ är en surjektiv ring homomorfism från $\mathbf{Z}$ till $\mathbf{Z}/n\mathbf{Z}$ med kärna $n\mathbf{Z} = \{x \in \mathbf{Z} : n \mid x\}$.*

Låt R vara en ring med enhet. Kom ihåg att $x \in R$ kallas för en *unit* om det finns $y \in R$ så att $xy = yx = 1$. Mängden av units betecknas $R^{\times}$. Den är en multiplikativ grupp. Låt nu $R_1, ..., R_n$ vara ringar med enheter. Deras *direkt produkt* är en ring som, som en mängd, är den Cartesiska produkten av R_i, och där addition och multiplikation definieras komponentvis. Den betecknas $\prod_i R_i$.

Proposition 8. *Låt $x \in \mathbf{Z}$. Då är $\bar{x}$ en unit i $\mathbf{Z}/n\mathbf{Z}$ omm $(x, n) = 1$.*

Korollarium 9. *$\mathbf{Z}/n\mathbf{Z}$ är en kropp omm n är prim.*

Vi definierar

$$\phi(n) := \#(\mathbf{Z}/n\mathbf{Z})^{\times} = \#\{x : 0 \leq x < n \text{ och } (x, n) = 1\}. \tag{15}$$

ϕ kallas för *Euler's ϕ-funktion.* Under kommande lektioner skall vi studera den vidare. Den stora satsen för idag är

Chinese Remainder Theorem (CRT). *Låt* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. *Då är*

$$\mathbf{Z}/n\mathbf{Z} \cong \prod_{i=1}^{k} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}, \tag{16}$$

där $\cong$ *betyder isomorfism av ringar.*

Bevis : Mer eller mindre som i boken, s.19.

Korollarium 10.

$$(\mathbf{Z}/n\mathbf{Z})^{\times} \cong \prod_{i=1}^{k} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^{\times}, \tag{17}$$

där $\cong$ *betyder isomorfism av grupper.*

Bevis : Ett element av en direkt produkt av ringar är en unit omm alla dess komponenter är units.

Lektion 4 (8/11/00)

I dagens lektion använder vi flera resultat från elementär gruppteori i bevisen av några satser. Eftersom det kan vara länge sedan några av er tog kursen Algebraiska Strukturer, först gör jag en lista här av de definitioner och resultat som vi behöver. Ni uppmuntras att kolla upp denna material innan kommande lektioner.

En kort återblick på lite gruppteori

(i) Låt G vara en ändlig grupp. Antalet element i G betecknas $|G|$ och kallas för *ordningen* av G. Enhetselementet i G kan betecknas med e, men 1 är mer vanligt.

(ii) Låt $x \in G$. Eftersom G är ändlig, potenserna x^n kan inte alla vara olika element i G. Det följer att det finns $n > 0$ så att $x^n = 1$. Det minsta sådana n kallas för *ordningen* av x och betecknas $\mathrm{ord}(x)$. Tydligen är $\mathrm{ord}(x) \leq |G|$.

(iii) *Lagrange's sats* säger att om H är en delgrupp av G, då är $|H|$ en delare av $|G|$.

(iv) En grupp kallas för *cyklisk* om det finns $x \in G$ så att varje element av G är någon potens av x. En sådan x kallas för en *generator* av G. Alltså är G cyklisk omm det finns $x \in G$ med $\mathrm{ord}(x) = |G|$.

(v) För varje $n > 0$ är den additiva gruppen i ringen $\mathbf{Z}/n\mathbf{Z}$ en cyklisk grupp av ordning n som genereras av $\bar{1}$. Varje cyklisk grupp av ordning n är isomorfisk med $\mathbf{Z}/n\mathbf{Z}$ så att man får prata om DEN cykliska gruppen av ordning n. Den betecknas oftast med antingen $\mathbf{Z}/n\mathbf{Z}$ eller C_n.

(vi) För godtyckligt G och $x \in G$, potenserna av x utgör en delgrupp av G som betecknas $< x >$ och kallas för den *cykliska delgruppen genererad av* x. Om vi tillämpar Lagrange's sats till delgruppen $< x >$ då ser vi att $\mathrm{ord}(x)$ är en delare av $|G|$ för alla $x \in G$.

(vii) Den direkta produkten av grupper definieras som för ringar (se lektion 3). Alltså låt $G_1, ..., G_n$ vara grupper. Deras *direkt produkt* är en grupp som, som en mängd, är den Cartesiska produkten av G_i, och där multiplikation definieras komponentvis. Den betecknas $G_1 \times ... \times G_n$ eller, mer concis

$\prod_{i=1}^{n} G_i$.

(viii) Låt G vara en grupp. En delgrupp $A \subseteq G$ kallas för en *direkt faktor* av G om det finns en delgrupp B av G så att $G = A \times B$.

(ix) I en abelsk grupp betraktas oftast grupp operationen som en 'addition' i stället för en 'multiplikation'. Dvs, man skriver 0 i stället för 1 för enhetselementet, och nx i stället för x^n.

(x) För ändliga abelska grupper har vi följande två fundamentala fakter. Den första brukar användas i beviset av den andra, faktiskt. Notera att Faktum 2 är en generalisering av CRT (se lektion 3), eftersom den ger den senare när $G \cong \mathbf{Z}/n\mathbf{Z}$. Den kallas för den *fundamentala satsen om ändliga abelska grupper.*

Faktum 1 : Låt G vara en ändlig abelsk grupp och $g \in G$. Då är den cykliska gruppen $< g >$ en direkt faktor av G omm, för varje $n \in \mathbf{N}$ och $x \in G$,

$$nx = g \Rightarrow x \in < g > \text{ och } x = mg \text{ med } mn \equiv 1 \pmod{\operatorname{ord}(g)}.$$

I så fall säger man att elementet g är inte *dividerbar* i G.

Faktum 2 : Varje ändlig abelsk grupp G är den direkta produkten av cykliska delgrupper av primpotens ordningar (det kan vara fler än en faktor för ett givet primtal p som delar $|G|$). Antalet faktorer och deras ordningar i en sådan faktorisering av G är unika.

Nu förtsätter vi med lektionen.

En välkänd faktum till från algebra är

Proposition 11. *Den multiplikativa gruppen av en ändlig kropp är cyklisk.*

Särskilt då ser vi från Korollarium 9 att $(\mathbf{Z}/p\mathbf{Z})^{\times}$ är en cyklisk grupp av ordning $p-1$ för varje primtal p. Gruppteori antyder direkt att

Fermat's (lilla) sats. *Låt p vara ett primtal och a ett heltal så att*

$(a,p)=1$. *Då är*

$$a^{p-1} \equiv 1 \ (mod\, p). \tag{18}$$

Mer allmänt, om vi tillämpar samma gruppteoretiska idéerna till gruppen $(\mathbf{Z}/n\mathbf{Z})^\times$ då får vi

Euler's sats. *Låt* $a, n \in \mathbf{Z}$ *med* $(a,n)=1$. *Då är*

$$a^{\phi(n)} \equiv 1 \ (mod\, n). \tag{19}$$

ANMÄRKNING : Talet n kallas för ett *pseudoprimtal* om

$$(x,n)=1 \Rightarrow x^{n-1} \equiv 1 \ (\mathrm{mod}\ n). \tag{20}$$

Det finns pseudoprimtal som inte är primtal (se supplementära övningarna). Från Euler's sats, ser vi att n är ett pseudoprimtal om $\phi(n) \mid n-1$, men detta villkor är inte nödvändigt. Å andra sidan är sådana tal ganska sällsynta. Därför finns det många primalitets provningar som börjar med att testa om (20) stämmer. Ganska effektiva algoritmer för att bestämma om ett givet tal är prim är kända, trots att de bästa algoritmerna antar GRH för deras maximal effektivitet. Se Koblitz' bok för vidare diskussion.

Korollarium 10 reducerar problemet av att ange strukturen av $(\mathbf{Z}/n\mathbf{Z})^\times$ som en abstrakt abelsk grupp till fallet där n är en primpotens. Följande sats löser då sista delen av problemet.

Sats 12. *(i) Om* p *är ett udde primtal, då är* $(\mathbf{Z}/p^n\mathbf{Z})^\times$ *cyklisk av ordning* $\phi(p^n)=p^{n-1}(p-1)$ *för alla* n.

(ii) $(\mathbf{Z}/2\mathbf{Z})^\times = <\bar{1}> \cong C_1$.
$(\mathbf{Z}/2^n\mathbf{Z})^\times = <\bar{-1}> \times <\bar{5}> \cong C_2 \times C_{2^{n-2}}$, *för* $n>1$.

BEVIS : För del (i) och $n=1$ använder man Prop. 11. Annars samma idéer som i boken s.23-25, men notera att flera av de mer 'gory' detaljerna utelämnas där.

Följande klassiska faktum kan också bevisas mycket lätt med hjälp av gruppteori :

Proposition 13. *Låt* p *vara ett udde primtal. Då har kongruensen* $x^2 \equiv$

-1 $(mod\, p)$ en lösning omm $p \equiv 1 (mod\, 4)$.

Bevis : En lösning finns omm $\overline{-1}$ är en kvadrat i den multiplikativa gruppen $(\mathbf{Z}/p\mathbf{Z})^\times$. Men denna grupp är cyklisk av ordning $p-1$ och $\overline{-1}$ är ett element av ordning 2, så det är en kvadrat i gruppen omm $(p-1)/2$ är ett jämt tal, dvs omm $p \equiv 1 \pmod 4$.

Vi ger två klassiska tillämpningar av denna proposition (vars bevis inte finns i boken !).

Proposition 14. *Det finns oändligt många primtal av formen $4n+3$.*

Bevis : Idé : Låt $N > 1$ och $m = (N!)^2 + 1$. Varje prim delare p av m satisfierar $p > N$ och $p \equiv 1 (\text{mod } 4)$.

Notera att det är en övning på inlämningsuppgiften att bevisa samma sak för tal av formen $4n+1$. Alltså, kan vissa enkla fall av Dirichlet's sats (se lektion 1) bevisas utan analytiska metoder. För fler exempel se boken 'Theory of Numbers' av W. Sierpiński.

Sats 15 (Fermat 1654). *Låt p vara ett udde primtal. Ekvationen*

$$x^2 + y^2 = p \tag{21}$$

har en lösning $(x, y) \in \mathbf{Z}^2$ omm $p \equiv 1 (mod\, 4)$.

Bevis : Om $p \equiv 3 \pmod 4$, finns det ingen lösning, eftersom kvadraten av varje heltal är kongruent till 0 eller 1 modulo 4, så att en summa av två kvadrater är kongruent till 0,1 eller 2 modulo 4.

Antag nu att $p \equiv 1 \pmod 4$. Enligt Prop. 13, finns det ett heltal x så att $x^2 \equiv -1 \pmod p$. Fixera ett sådant x och betrakta funktionen $f : \mathbf{Z} \to \mathbf{Z}$ som ges av

$$f(u, v) = u + xv.$$

Låt $K = [\sqrt{p}]$ så att $K < \sqrt{p} < K+1$. Det finns $(K+1)^2 > p$ par (u, v) av heltal så att $0 \leq u, v \leq K$. Alltså, måste det finnas två olika par $(u_1, v_1), (u_2, v_2)$ så att

$$f(u_1, v_1) \equiv f(u_2, v_2) \pmod p \Rightarrow (u_1 - u_2) \equiv -x(v_1 - v_2) \pmod p.$$

Låt $a := u_1 - u_2, b := v_1 - v_2$. Eftersom $x^2 \equiv -1 \pmod p$, har vi då att $a^2 + b^2 \equiv 0 \pmod p$. Minst ett av $a, b \neq 0$ - annars skulle $(u_1, v_1) = (u_2, v_2)$ - så att $a^2 + b^2 \neq 0$. Men eftersom alla u_i, v_i ligger i intervallen $[0, K]$, måste då både a, b ligga i intervallen $[-K, K]$, så att $a^2 + b^2 \leq 2K^2 < 2p$.

Därför, har vi bevisat att $a^2 + b^2$ är en multipel av p, och ligger strängt mellan 0 och $2p$. Det följer att $a^2 + b^2 = p$.

Lektion 5 (10/11/00)

DEFINITION : En funktion $f : \mathbf{N} \to \mathbf{Z}$ kallas för en *aritmetisk* funktion.

DEFINITION : En funktion $f : \mathbf{N} \to \mathbf{C}$ kallas för *multiplikativ* om

$$(m, n) = 1 \Rightarrow f(mn) = f(m)f(n). \tag{22}$$

Vi är interesserad av att studera multiplikativa aritmetiska (MA) funktioner.

Korollarium 10 ger följande formel för Euler's ϕ-funktion :

$$\phi(n) = \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{23}$$

Då ser man direkt att ϕ är MA.

ASIDE : Det finns ett annat sätt att bevisa (23) som är ett mycket lätt exempel av en så -kallad *sieve metod.* Kom ihåg

Inklusion-exklusion principen. *Låt $A_1, ..., A_k$ vara ändliga mängder. Då är*

$$|A_1 \cup ... \cup A_k| = \sum_{r=1}^{k} (-1)^{r-1} \sum_{1 \le i_1 < \, ... \, < i_r \le k} |A_{i_1} \cap ... \cap A_{i_r}|. \tag{24}$$

Om vi skriver $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ då får man (23) genom att tillämpa I-E principen till mängderna

$$A_i = \{x : 0 \le x < n, \; p_i \mid x\},$$

eftersom

$$\phi(n) = n - |A_1 \cup ... \cup A_k|.$$

Vad man gör har kan beskrivas som att 'sifting out' de tal i intervallen $[0, n)$ som inte är relativt prima med n.

Nu förtsätter vi med att ge fler exempel av MA funktioner.

EXEMPEL 1 (DUMMA EXEMPEL) : $f(n) = 0$, $f(n) = 1$, $f(n) = n^k$ för något fixerad k.

Exempel 2 : Den *Möbius funktionen* definieras genom

$$\mu(n) = \begin{cases} 1, & \text{om } n = 1. \\ 0, & \text{om } p^2 \mid n \text{ för något primtal } p. \\ (-1)^k, & \text{om } n = p_1 ... p_k \text{ för olika primtal } p_i. \end{cases} \quad (25)$$

Notera att (23) kan skrivas i formen

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{26}$$

Exempel 3 : Vi definierar

$$\tau(n) := \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d. \tag{27}$$

Det är lätt att bevisa att dessa funktioner är multiplikativa. Det är också lätt att se att

$$\tau(p^\alpha) = 1 + \alpha, \qquad \sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}. \tag{28}$$

Exempel 4 : Om f är multiplikativ, så också är funktionen g som definieras av

$$g(n) := \sum_{d|n} f(d).$$

T.ex., om $f(n) = n$ då är $g(n) = \sigma(n)$. Om $f(n) = \mu(n)$ och $\nu(n) := \sum_{d|n} \mu(n)$, då är ν multiplikativ och man bevisar lätt (se nästa anmärkning) att

$$\nu(n) = \begin{cases} 1, & n = 1. \\ 0, & n > 1. \end{cases} \quad (29)$$

Anmärkning : För att kunna beräkna en multiplikativ funktion f, räcker det att kunna beräkna den vid primpotenser, eftersom om $n = \prod_i p_i^{\alpha_i}$ då är

$$f(n) = \prod_i f(p_i^{\alpha_i}). \tag{30}$$

T.ex., från (28) får vi då att

$$\tau(n) = \prod_{p^\alpha \| n} (1+\alpha), \qquad \sigma(n) = \prod_{p^\alpha \| n} \frac{p^{\alpha+1}-1}{p-1}. \tag{31}$$

Näst bevisar vi en sats som motiveras av exempel 4 ovan, men som gäller godtyckliga funktioner.

Sats (Möbius inversion formel). *Låt $f, g : \mathbf{N} \to \mathbf{C}$. Då är följande ekvivalenta*

(i) $g(n) = \sum_{d|n} f(d)$,

(ii) $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.

BEVIS : Ungefär som i boken. Notera att funktionen ν från exempel 4 ovan spelar en central roll.

Om vi tillämpar inversion formeln till (26) då får vi att

$$\sum_{d|n} \phi(d) = n. \tag{32}$$

En mer imponerande tillämpning av formeln ges av problem 4 i de supplementära övningarna.

Ekvation (30) säger att en MA funktion $f(n)$ kan skrivas som en produkt av ändligt många faktorer, en för varje primtal från någon mängd som beror på n. I (multiplikativ) analytisk talteori träffer man många ANALYTISKA funktioner $f(s)$ som kan skrivas som en Oändlig produkt av faktorer, en för varje primtal från någon mängd (oftast mängden av ALLA primtal). Den mest berömda formeln av denna typ är

Sats 16 (Euler). *Om $Re(s) > 1$, då är*

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}. \tag{33}$$

BEVIS : Kommer nästa gång. För att förstå vad den oändliga produkten i (33) betyder, gå till s.23 av detta dokument.

Sats 16 är kanske det mest grundläggande resultatet i hela analytiska talteorin. Bland annat är det början av beviset av Dirichlet's sats, så att vi kommer tillbaka till den senare. Just nu (dvs under nästa lektion) vill vi använda den för att bevisa den imponerande Sats 17 nedan. Först en definition :

DEFINITION : Låt P vara en egenskap av oordnade par (p, q) av olika icke-negativa heltal. Vi definierar *sannolikheten* att ett sådant par har egenskapen P genom

$$\text{Prob}(P) := \lim_{n\to\infty} \frac{\text{antal par } (p,q) \text{ som har egenskap } P \text{ och så att } p,q \leq n}{\frac{1}{2}n(n+1)},$$

om gränsvärdet existerar. Intuitivt är $\text{Prob}(P)$ lika med sannolikheten att ett slumpligt valt par p, q av olika icke-negativa heltal har egenskapen P.

Sats 17. *Låt P vara egenskapen 'är relativt prima'. Då är Prob$(P) = \frac{6}{\pi^2}$.*

Infinite products in complex analysis

I will only give the basic ideas without any proofs because we will only encounter essentially one simple example of an analytic function defined by an infinite product in this course. If you want to study the subject properly, please check out a good complex analysis text, for example Chapter 5 of the book by Ahlfors. In fact, if you want to study analytic number theory beyond the level of this course, you really should know everything in the first three sections of that chapter.

First, recall Weierstraβ' theorem :

Theorem A. *Suppose the sequence of functions $f_n(z)$ is analytic in a domain Ω, that the sequence converges pointwise, and uniformly in each compact subset of Ω. Then $f(z) := \lim_{n\to\infty} f_n(z)$ defines an analytic function in Ω and $f_n'(z) \to f'(z)$, uniformly in compact subsets of Ω.*

Weierstraβ' theorem is usually applied to series whose terms are analytic functions. Uniform convergence of the series in compact sets is often easy to prove using, say, Weierstraβ' own M-test. Let us state Weierstraβ' theorem for series for completion[5] :

Theorem A1. *Suppose each of the functions $f_n(z)$ is analytic in a region Ω and that the series*

$$\sum_{n=1}^{\infty} f_n(z) := f(z)$$

converges pointwise in Ω and uniformly in compact subsets of Ω. Then the limit function $f(z)$ is analytic in Ω and

$$f'(z) = \sum_{n=1}^{\infty} f_n'(z),$$

where the right-hand side also converges uniformly on compact subsets of Ω.

For example, the Riemann ζ-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

[5]It is worth noting that the analogue of Weierstraβ' theorem in real analysis does NOT hold. See page 55 of my notes from flervariabelanalys (del 2) from last year.

is analytic in the half-plane $\mathrm{Re}(s) > 1$ because each term in the series is obviously analytic, the series converges pointwise in the half-plane and uniformly in compact subsets of it, in fact in any smaller half-plane $\mathrm{Re}(s) \geq 1+\delta$ where $\delta > 0$. (You learned all this in flervariabelanalys). Furthermore, the series can be differentiated termwise so that

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s} \qquad (\mathrm{Re}(s) > 1).$$

We now turn to infinite products. The following definition is not the most general one but is sufficient for our purposes.

DEFINITION : Let (p_n) be a sequence of complex numbers, all different from zero. We define

$$\prod_{n=1}^{\infty} \stackrel{def}{=} \lim_{N\to\infty} \prod_{n=1}^{N} p_n, \tag{34}$$

provided that the limit exists and is different from zero (the value zero is excluded for technical reasons).

An obvious necessary condition for the convergence of an infinite product is that $p_n \to 1$. It is therefore natural to write $p_n = 1 + a_n$ and the product as $\prod(1+a_n)$. Another very natural thing to do, since we know everything about infinite series, is to take logarithms and consider the series

$$\sum_{n=1}^{\infty} \log(1+a_n), \tag{35}$$

where, by convention, we choose the principal branch of the logarithm at all times. The following result should come as no surprise :

Theorem B. *The infinite product $\prod_{n=1}^{\infty}(1+a_n)$ with $1+a_n \neq 0$ converges iff the series (35) converges.*

DEFINITION : The infinite product $\prod(1+a_n)$ is said to converge *absolutely* if the series (35) converges absolutely.

From the formula

$$\lim_{z\to 0} \frac{\log(1+z)}{z} = 1, \tag{36}$$

one easily derives

Theorem C. *The infinite product* $\prod(1+a_n)$ *with* $1+a_n \neq 0$ *converges absolutely iff* $\sum_{n=1}^{\infty}|a_n|$ *converges.*

Now suppose we replace the complex numbers a_n by functions $f_n(z)$, all analytic in some region Ω. Pointwise convergence of the infinite product

$$\prod_{n=1}^{\infty}(1+f_n(z)) \tag{37}$$

is defined in the same way as above, whenever $1+f_n(z) \neq 0$ for all n and all $z \in \Omega$. What about uniform convergence ?

DEFINITION : The infinite product (37) is said to converge *uniformly* in a subset K of Ω if the series $\sum \log(1+f_n(z))$ converges uniformly in K.

We have the following counterpart to Theorem C which is most often used in practice to check uniform convergence of an infinite product :

Theorem D. *Suppose the functions* $f_n(z)$ *are all analytic in a region* Ω *and that* $1+f_n(z) \neq 0$ *for all* n *and all* $z \in \Omega$. *Let* K *be a subset of* Ω *and suppose there exists* $C > 0$, *such that*

$$\frac{1}{C} < |1+f_n(z)| < C$$

for all $z \in K$. *Then the infinite product (37) converges uniformly in* K *if and only if* $\sum f_n(z)$ *converges uniformly in* K.

We also have a counterpart to Weierstraβ' theorem.

Theorem E. *Suppose* $f_n(z)$ *is a sequence of functions each analytic a region* Ω, *that* $1+f_n(z) \neq 0$ *for all* n *and all* $z \in \Omega$, *and that the infinite product (37) converges pointwise in* Ω *and uniformly on compact subsets of* Ω. *Then* $f(z) := \prod(1+f_n(z))$ *defines an analytic function in* Ω.

Lektion 6 (13/11/00)

Bevis av sats 16 : Först bevisade vi att

$$\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) \cdot \zeta(s) = 1,$$

genom att skriva

$$\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \sum_{n=1}^{\infty} \frac{\nu(n)}{n^s} = 1,$$

där $\nu(n)$ ges av ekv. (29).

Näst bevisade vi att

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right),$$

genom att visa att, för varje $N > 0$,

$$\left[\prod_{p \leq N} \left(1 - \frac{1}{p^s}\right)\right] \cdot \zeta(s) = \sum_{p \nmid n \text{ för alla } p \leq N} \frac{1}{n^s}.$$

Ett alternativt (som föreslagits av Dennis Eriksson under pausen !) är att använda binomial satsen som ger att

$$\left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{m=0}^{\infty} \frac{1}{p^{ms}}.$$

Då kan vi skriva den oändliga produkten som

$$\prod_p \left(\sum_{m=0}^{\infty} \frac{1}{p^{ms}}\right),$$

och om man multiplicerar ut detta ser man att man får, för varje $n > 0$, termen $1/n^s$ precis en gång.

Bevis av sats 17 : Som i boken, s. 13-14.

En oändlig produkt över primtalen av formen (33) kallas för en *Euler produkt.* En serie av formen $\sum_1^\infty a_n/n^s$, där $a_n \in \mathbf{C}$, kallas för en *Dirichlet serie.* I (multiplikativ) analytisk talteori uppstår det överallt Dirichlet serier som kan uttryckas som en Euler produkt (vi skall se det viktigaste exemplet nedan). Först bevisar vi ett allmänt kriterium som garanterar att en Dirichlet serie har en Euler produkt utveckling :

Proposition 18. *Låt $(a_n)_1^\infty$ vara en följd av komplexa tal så att*

$$a_1 = 1 \quad och \quad a_{mn} = a_m a_n \ \ \text{för alla } m, n \geq 1. \tag{38}$$

Då är

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \left(1 - \frac{a_p}{p^s}\right)^{-1}, \tag{39}$$

när som helst båda sidorna konvergerar och definierar analytiska funktioner.

Bevis : Det är exakt samma idé som i beviset av Sats 16.

Definition : Låt $N \geq 1$. En grupp homomorfism

$$\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^*$$

kallas för en *karaktär modulo N*. χ kallas för *icke-trivial* om $\chi(x) \neq 1$ för något $x \in (\mathbf{Z}/N\mathbf{Z})^\times$. Notera att $\chi(x)$ måste a priori vara en $\phi(N)$:te enhetsrot.

Varje karaktär χ modulo N kan utvigas till en funktion $\hat{\chi} : \mathbf{Z} \to \mathbf{C}$ genom att sätta

$$\hat{\chi}(n) = \begin{cases} \chi(\bar{n}), & \text{om } (n, N) = 1, \\ 0, & \text{annars.} \end{cases} \tag{40}$$

Funktionen $\hat{\chi}$ satisfierar (jämför med (38))

$$\hat{\chi}(1) = 1, \qquad \hat{\chi}(mn) = \hat{\chi}(m)\hat{\chi}(n) \ \text{ för alla } m, n \geq 1. \tag{41}$$

Definition : En Dirichlet serie av formen

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\hat{\chi}(n)}{n^s}, \tag{42}$$

där χ är en karaktär (för något N), kallas för en *Dirichlet L-serie*[6]. Notera att om χ är den triviala karaktären modulo $N = 1$ (det finns bara den triviala karaktären modulo 1 !), då är $L(s, \chi) = \zeta(s)$.

Sats 19. *(i) Om χ är en trivial karaktär, då är $L(s, \chi)$ analytisk i $Re(s) > 1$.*

(ii) Om χ är icke-trivial, då är $L(s, \chi)$ analytisk i $Re(s) > 0$.

(iii)

$$L(s, \chi) = \prod_p \left(1 - \frac{\hat{\chi}(p)}{p^s}\right)^{-1}, \tag{43}$$

när båda sidor konvergerar enligt (i) eller (ii) resp.

Bevis : Beviset av (iii) följer direkt från (41) och Prop. 18. Beviset av (i) följer från jämförelse med $\zeta(s)$. För (ii) bevisar man först att, om χ är en karaktär modulo N, då är

$$\sum_{n=1}^{N} \hat{\chi}(n) = \begin{cases} \phi(N), & \text{om } \chi \text{ är trivial,} \\ 0, & \text{annars.} \end{cases} \tag{44}$$

Då tillämpar man Dirichlet's kriterium för likformig konvergens tillsammans med Weierstraβ' sats. Kom ihåg Dirichlet's kriterium (från flervariabelanalys) :

'*Serien $\sum_1^\infty f_n(x) g_n(x)$ konvergerar likformigt i en mängd M om*

(a) följden $(g_n(x))$ är avtagande för varje $x \in M$,
(b) $g_n(x) \to 0$ likformigt i M,
(c) de partiella summorna $F_N(x) := \sum_1^N f_n(x)$ är likformigt begränsade i M'.

Alltså, kvarstår det att bevisa (44). Eftersom χ är icke-trivial, finns det ett heltal y så att $(y, N) = 1$ och $0 \neq \hat{\chi}(y) \neq 1$. När n går från 1 till N då löper yn över en komplett mängd av restklasser modulo N, ty $(y, N) = 1$.

[6] Jag tror att denna L betyder 'Legendre', eftersom i de första L-serierna som studerades av Dirichlet var karaktären en Legendre symbol (se lektion 7 nedan).

Då har vi att

$$\sum_{n=1}^{N} \hat{\chi}(n) = \sum_{n=1}^{N} \hat{\chi}(yn) = \hat{\chi}(y) \cdot \sum_{n=1}^{N} \hat{\chi}(n),$$

ty $\hat{\chi}$ är multiplikativ. Men $\hat{\chi}(y) \neq 0, 1$ antyder då att summan över n måste vara noll, q.e.d.

Vi skall komma tillbaka till L-serier senare när vi diskuterar Dirichlet's sats om primtal i aritmetiska följder.

Gauss' teori av kvadratiska kongruenser

Tidigare bevisade vi följande två fakta :

(1) kongruensen $x^2 \equiv -1 \pmod{p}$ har en lösning omm $p \equiv 1 \pmod{4}$.

(2) $x^2 + y^2 = p$ har en lösning omm $p \equiv 1 \pmod{4}$.

Dessa fakta var redan välkända mot slutet av 1600-talet, när Fermat var det stora namnet inom talteori (dvs inom matematik, modulo Newton osv !!). Det dröjade över 100 år innan arbetet av tre stora matematiker - Euler, Legendre och framför allt Gauβ - ledde till en stor generalisering av dessa två resultat, och öppnade vägen till vad som kallas nuförtiden för 'algebraisk talteori'.

Ovanstående (1) och (2) är speciella fall av följande två problem resp.:

PROBLEM 1 : Lös den allmäna kvadratiska kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{n}. \tag{45}$$

PROBLEM 2 : Lös (i heltalen) den allmäna kvadratiska ekvationen i två variabler

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{46}$$

Problem 2 kallas för *representationsproblemet* för *binära kvadratiska former*. Båda problem kan, på ett naturligt sätt, ytterliggare delas upp i tre 'sub-problem', nämligen

DEL A : ange allmäna kriteria för *existens* av en lösning.

DEL B : ge effektiva algoritmer för att *hitta* en lösning.

DEL C : ge allmäna (beräknabara) formler för *antalet* lösningar. Notera att i Problem 1 räcker det att hitta alla lösningar bland en mängd av representanter för $\mathbf{Z}/n\mathbf{Z}$. Därför är antalet lösningar alltid ändligt så länge som en 'lösning' betyder en lösning modulo n. Vi adopterar denna konvention framöver.

Under kommande lektioner skall vi studera dessa två problem mycket noggrant. Vi börjar med det kvadratiska kongruens problemet (Problem 1) och framför allt existens frågan (Del A). Men först, är det bra att satisfiera oss att vi förstår linjära kongruenser

Proposition 20. *Kongruensen $ax \equiv b \ (mod\ n)$ har en lösning omm (a, n) delar b.*

I nästa två propositionerna reducerar vi den allmäna kvadratiska kongruensen till en mer hanterlig form.

Proposition 21. *Kongruensen (45) är ekvivalent med kongruensen*

$$y^2 \equiv d \ (mod\ 4an), \tag{47}$$

där $y = 2ax + b$ och $d = b^2 - 4ac$.

Denna prop. säger att det räcker att betrakta kongruenser av formen $x^2 \equiv a \pmod n$. Nu kommer huvud reduktionssteget. Det är ganska tekniskt, men det är resultatet som är viktigt :

Proposition 22. *(i) $x^2 \equiv a \ (mod\ n)$ har en lösning omm $x^2 \equiv a \ (mod\ p^\alpha)$ har en lösning för varje $p^\alpha \| n$.*

(ii) Om $a = p^i a_1$ för något $i < \alpha$ och $(a_1, p) = 1$, ett nödvändigt villkor för existens av en lösning till $x^2 \equiv a \ (mod\ p^\alpha)$ är att $2 \mid i$. I så fall ges lösningarna av $x = p^{i/2} x_1$ där $x_1^2 \equiv a_1 \ (mod\ p^{\alpha - i})$.

(iii) Om $p > 2$ och $(a, p) = 1$ då har $x^2 \equiv a \ (mod\ p^\alpha)$ en lösning omm

$x^2 \equiv a \ (mod\ p)$ *har en lösning. Antalet lösningar är antingen* 0 *eller* 2.

(iv) $x^2 \equiv 1 \ (mod\ 2)$ *har den enda lösningen* $x = \{\bar{1}\}$.

(v) $x^2 \equiv 1 \ (mod\ 4)$ *har lösningarna* $x = \bar{1}, \bar{3}$ *och* $x^2 \equiv 3 \ (mod\ 4)$ *har inga lösningar.*

(vi) Om $\alpha \geq 3$ *och* $2 \nmid a$, *då har* $x^2 \equiv a \ (mod\ 2^\alpha)$ *en lösning omm* $a \equiv 1 (mod\ 8)$, *dvs omm* $a \equiv 5^{2\lambda} \ (mod\ 2^\alpha)$ *för något* $\lambda \geq 0$. *I så fall finns det exakt 4 lösningar, nämligen* $\pm x_0, \pm 5^{2^{\alpha-3}} x_0$ *där* $x_0 \equiv 5^\lambda \ (mod\ 2^\alpha)$.

Lektion 7 (15/11/00)

Bevis av prop. 22 : Man använder CRT och Sats 12, och det hela är elementär gruppteori.

Nu har vi reducerat Problem 1 (Del A,B och C !) till att lösa kongruensen

$$x^2 \equiv a \pmod{p}, \tag{48}$$

där p är ett udda primtal och $(a,p) = 1$. Notera att Del C av problemet nu är trivialt - det finns antingen 0 eller 2 lösningar.

Notation : Låt p vara ett udda primtal och $(a,p) = 1$. Vi sätter

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{om (48) har en lösning,} \\ -1, & \text{annars.} \end{cases} \tag{49}$$

Symbolen $\left(\frac{a}{p}\right)$ kallas för en *Legendre symbol*.

Anmärkning : $\chi : a \to \left(\frac{a}{p}\right)$ är en karaktär modulo p av ordning 2, en så-kallad *kvadratisk karaktär*.

Del A av Problem 1 frågar efter ett kriterium för existensen av en lösning till (48). Det enda som jag känner till är det nästan triviala

Euler's kriterium. $\left(\frac{a}{p}\right) \equiv a^{p-1/2}$ *(mod p)*.

Bevis : $\left(\frac{a}{p}\right) = 1 \Leftrightarrow \bar{a}$ är en kvadrat i $(\mathbf{Z}/p\mathbf{Z})^{\times}$.

Från den teoretiska synpunkten är detta kriterium ganska ointeressant, men från den praktiska vinkeln ger det ett effektiv sätt att lösa existens-frågan : det räcker att kunna beräkna $a^{p-1/2}$ och det finns snabba algoritmer för att beräkna potenser av ett heltal (den klassiska använder en bas-2 utveckling av potensen).

Nu kommer vi till Gauβ' reciprocitets lag. Den leder också till ett mycket effektivt sätt att lösa existens frågan för (48), men dess största interesse är teoretiskt. Först, är det klart att det är ett mycket vackrare och djupare resultat än Euler's kriterium, men historien slutar inte där. Idag vet vi att

Gauβ' lag är ett specialt fall av en 'reciprocitets lag' av Artin (1927) som gäller för godyckliga abelska talkropps utvidningar L/K[7]. I fallet $K = \mathbf{Q}$ och $[L : \mathbf{Q}] = 2$ får man Gauβ' lag. Artin's reciprocitets lag är ett av de stora resultaten i den del av algebraisk talteori som kallas för *class field theory*, eller mer precist *abelian class field theory*[8].

Under 1900-talet har flera olika formuleringar av 'class field theory' utvecklats och vilken formulering du lär dig beror på vilken bok du läser. För en formulering i termer av så-kallade *adèles* och *idèles* (kanske den mest kända) se t.ex. [3]. För en alternativ formulering i termer av *grupp kohomologi* se t.ex. [4]. Den senare har också en kapitel om historien av 'class field theory'.

Okej, tillbaka till jorden. Här är 'what all the fuss has been about' !

Sats (Gauss' reciprocitets lag). *Låt p, q vara udda primtal. Då är*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}. \tag{50}$$

BEVIS : Som i boken, s.28-30. Notera att beviset använder ett resultat av Gauβ som är interessant i sig själv, nämligen

Gauss' lemma. *Låt p vara ett udda primtal. För varje $n \in \mathbf{Z}$, låt $[n]$ beteckna det unika talet som satisfierar $[n] \equiv n \ (mod\ p)$ och $-\frac{1}{2}p < [n] < \frac{1}{2}p$.*

Låt nu $(a, p) = 1$ och sätt $a_j = [aj]$ för varje $j \in \mathbf{Z}$. Då är

$$\left(\frac{a}{p}\right) = (-1)^l$$

där

$$l = \text{ antalet } j \text{ så att } 1 \leq j \leq \tfrac{p-1}{2} \text{ och } a_j < 0.$$

ANMÄRKNING : Bokens bevis är ganska elementärt och mycket snyggt, och är ganska nära Gauβ' ursprunlgiga idéer eftersom det använder hans lemma. Under sitt liv upptäckte Gauβ minst 8 olika bevis av sitt lag[9]. Några av

[7]En kropp som är en ändlig utvidning av $\mathbf{Q}$ kallas för en *talkropp*. En utvidning av talkroppar L/K kallas för *abelsk* om den är Galois och Galois gruppen av L/K är abelsk.

[8]There is also a class field theory for non-abelian number field extensions, but it is much more difficult and highly incomplete.

[9]Moderna böcker betraktas innehålla ungefär 40 olika bevis. Men Urban Larsson påstår att det finns 196 stycken på nätet. Isn't technology wonderful !

dessa har en lite mer analytisk inriktning, och beror på beräkningen av en typ av ändlig summa som kallas för en *Gauß summa*. Summor av denna typ har visat sig uppstå i många olika sammanhang inom talteori (både algebraisk och analytisk), t.ex. i beviset av Dirichlet's sats som kommer senare under kursen. Vi skall diskutera dem nästa gång.

References

[3] S. Lang, ALgebraic number theory, Springer.

[4] J. Cassels and A. Fröhlich eds., Algebraic number theory, Academic Press 1967.

A little Fourier analysis

We will only state the bare minimum of information that we will require. People who have not taken a course in Fourier analysis may wish to consult a textbook on that subject for proofs and a fuller treatment, though I don't believe it's really necessary. Also, you have all already seen the basic Theorem A in flervariabelanalys, though without a proof (it is Sats 3.11 in the GLO kompendium).

DEFINITION : A function $f : \mathbf{R} \to \mathbf{R}$ is said to be C^1 if f is differentiable and both f and f' are continuous.

DEFINITION : A function $f : \mathbf{R} \to \mathbf{R}$ is said to be *piecewise* C^1 if in every bounded open interval f is C^1 except perhaps at a finite number of points where both f and f' have both left- and right-hand limits.

The right- and left- hand limits of a function g at a point x are denoted $g(x+)$ and $g(x-)$ respectively. Hence g is continuous at x iff both limits exist and are equal.

DEFINITION : A function $f : \mathbf{R} \to \mathbf{R}$ satisfying $f(x+1) = f(x)$ shall be called $[0,1]$-*periodic*.

DEFINITION : Let f be a $[0,1]$-periodic Riemann integrable function. The *Fourier series* of f is the series

$$\frac{1}{2}a_0 + \sum_{n=1}^{\infty} \left(a_n \cos 2\pi nx + b_n \sin 2\pi nx\right), \tag{51}$$

where

$$\frac{1}{2}a_0 = \int_0^1 f(x)\, dx, \tag{52}$$

$$\frac{1}{2}a_n = \int_0^1 f(x) \cos 2\pi nx\, dx \qquad (n > 0), \tag{53}$$

$$\frac{1}{2}b_n = \int_0^1 f(x) \sin 2\pi nx\, dx. \tag{54}$$

The fundamental result in Fourier analysis (first proved rigorously by Dirichlet in 1829) is the following

Theorem A. *Suppose f is piecewise C^1 and $[0,1]$-periodic. Then the Fourier series of f converges pointwise to $\frac{1}{2}[f(x+)+f(x-)]$.*

We are interested in an application of Theorem A. So now consider any piecewise C^1 function $f(x)$. Let $f_1(x)$ be the unique $[0,1]$-periodic function which coincides with $f(x)$ for $0 \le x < 1$. Note that f_1 is also piecewise C^1 because it may only pick up extra discontinuities at the integers. Applying Theorem A to the function f_1 and evaluating at $x=0$ we obtain

$$\frac{1}{2}\left[f(0)+f(1)\right] = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n = \sum_{n=-\infty}^{\infty} \int_0^1 f(x)\cos 2\pi n x \, dx = \sum_{n=-\infty}^{\infty} \int_0^1 f(x) e^{2\pi i n x} \, dx, \tag{55}$$

where, to get the 2nd last equality, we have used the evenness of the cosine function, and to get the last equality oddness of the sine function.

If, for some integer t, we replace $f(x)$ by $f(x+t)$ and repeat the above argument, then we obtain

$$\frac{1}{2}\left[f(t)+f(t+1)\right] = \sum_{n=-\infty}^{\infty} \int_t^{t+1} f(x) e^{2\pi i n x} \, dx. \tag{56}$$

Now let A, B be integers with $A < B$. Adding together both sides of (56) for $n = A, A+1, ..., B-1$ we obtain

$${}^{*}\sum_{t=A}^{B} f(t) = \sum_{n=-\infty}^{\infty} \int_A^B f(x) e^{2\pi i n x} \, dx, \tag{57}$$

where ${}^{*}\sum$ means that the end terms of the sum, corresponding to $t = A$ and $t = B$, are to be replaced by $\frac{1}{2}f(A)$ and $\frac{1}{2}f(B)$.

We shall use (57) in the evaluation of a Gauβ sum next time. It is also worth remarking that (57) is a special case of the well-known *Poisson summation formula.*

Lektion 8 (17/11/00)

Först noterar vi en snygg konsekvens av Gauβ' lemma :

Proposition 23. *Låt p vara ett udde primtal. Då är*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)} = \begin{cases} 1, & om\ p \equiv \pm 1\ (mod\ 8), \\ -1, & om\ p \equiv \pm 3\ (mod\ 8). \end{cases} \quad (58)$$

Bevis : Som i boken, s.29.

Målet är nu att beskriva ett nytt effektivt sätt att beräkna Legendre symboler (dvs ett alternativ till Eulers kriterium), samt införa en bekväm (convenient) notation. Idéen är att utviga Legendre symbolen, på ett 'formelt' sätt, till udda, icke-prima moduli, så att en analog av reciprocitetslagen fortfarande stämmer.

Definition : Låt n vara ett udda positivt heltal, $n = \prod_i p_i^{\alpha_i}$, och a ett heltal med $(a, n) = 1$. Då definierar vi den så kallade *Jacobi symbolen* $\left(\frac{a}{n}\right)$ genom

$$\left(\frac{a}{n}\right) := \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}. \quad (59)$$

Notera följande :

(i) Om n är ett primtal, då får vi tillbaka den vanliga Legendre symbolen.
(ii) $\chi : a \mapsto \left(\frac{a}{n}\right)$ är en karaktär modulo n av ordning 2. Speciellt kan vi utvidga symbolen till en multiplikativ funktion på $\mathbf{Z}$ genom att sätta

$$\left(\frac{a}{n}\right) := 0, \qquad \text{om } (a, n) > 1. \quad (60)$$

(iii) För godtyckliga n, a med $(a, n) = 1$, om $\left(\frac{a}{n}\right) = -1$ då är $x^2 \equiv a\ (n)$ ej lösbar. Detta generaliserar motsvarande egenskapen hos Legendre symboler.
(iv) MEN, om $\left(\frac{a}{n}\right) = 1$ det betyder INTE nödvändigtvis att $x^2 \equiv a\ (n)$ är lösbar. Exempel : $\left(\frac{-1}{9}\right) = 1$ men $x^2 \equiv -1\ (9)$ har ingen lösning. Alltså är det bäst att tänka på Jacobi symbolen som en 'formel' utvidning av Legendres symbol. Dess användbarhet kommer från följande fakta :

Sats. *Låt m, n vara udda tal, med $n > 0$ och $(m, n) = 1$. Då har vi*

(i)

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)} = \begin{cases} 1, & om\ n \equiv 1\ (mod\ 4), \\ -1, & om\ n \equiv 3\ (mod\ 4). \end{cases} \quad (61)$$

(ii)

$$\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} = \begin{cases} 1, & om\ n \equiv \pm 1\ (mod\ 8), \\ -1, & om\ n \equiv \pm 3\ (mod\ 8). \end{cases} \quad (62)$$

(iii)

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}. \quad (63)$$

Notera att denna sats generaliserar motsvarande fakta då m, n är primtal.

Bevis : Som i boken, s.32. Man använder följande lemma

Lemma : Om $n_1, ..., n_k$ är udda tal, $n = \prod_i n_i$, då är

$$\frac{1}{2}(n-1) \equiv \sum_{i=1}^{k} \frac{1}{2}(n_k - 1) \text{ (mod 2)}. \quad (64)$$

Bevis av lemma : Induktion på k efter ett direkt bevis för $k = 2$ med hjälp av identiteten

$$n_1 n_2 - 1 = (n_1 - 1)(n_2 - 1) + (n_1 - 1) + (n_2 - 1).$$

Denna sats ger en effektiv algoritm för att beräkna Jacobi symboler (och speciellt, Legendre symboler). Repeterad tillämpning av (63) och disivion algoritmen reducerar beräkningen av $(\frac{m}{n})$, efter ändligt många steg, till en symbol av formen $\left(\frac{-1}{n_1}\right)$ eller $\left(\frac{2}{n_1}\right)$, som kan beräknas direkt med (61), resp. (62).

Gauss summor

Definition : Låt $q > 0$, χ en karaktär modulo q. Summan

$$G(\chi) := \sum_{m=1}^{q-1} \chi(m) e^{2\pi i m/q} \quad (65)$$

kallas för en *Gauß summa (modulo q).*

Gauß summor, eller ändliga summor av mer allmän ‘exponentiell typ’, uppstår i många olika sammanhang inom talteori. Vi skall se några exempel så småningom. Exakta beräkningar av sådana summor är i stortsett omöjliga och man måste nöja sig med ganska bra uppskattningar. Men det finns en viktig situation där summan kan beräknas exakt, nämligen när q är ett primtal och χ en kvadratisk karaktär modulo q, dvs en Legendre symbol. Nu koncentrerar vi oss på denna situation.

NOTATION : $e_q(m) := e^{2\pi i m/q}$. Notera då att $e_q(m_1 + m_2) = e_q(m_1)e_q(m_2)$.

Fixera nu ett udda primtal q. Vi är interesserade av att beräkna summan

$$G := \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e_q(m). \tag{66}$$

Det visar sig vara mycket lättare att i stället beräkna G^2. Vi har

Proposition 24. *Låt G ges av (66). Då är*

$$G^2 = \begin{cases} q, & om\ q \equiv 1\ (mod\ 4), \\ -q, & om\ q \equiv 3\ (mod\ 4). \end{cases} \tag{67}$$

BEVIS : Se kap.2 av den utdelade stencilen från Davenports bok [5].

Ekv. (67) räcker för att skaffa ett alternativt bevis av Gauß’ reciprocitetslag - se den utdelade stencilen från Koblitz’ bok. Notera att den ger $|G| = \sqrt{q}$ och G själv upp till ett tecke. Men det finns tillämpningar - t.ex. i Dirichlets bevis av sin sats om primtal i aritmetiska följder - där kunskapen av tecken är viktig, och detta visar sig faktiskt vara mycket svårare att reda ut. Det är här man kan använda lite fourieranalys. Resultatet är

Sats 25 (Gauss/Dirichlet).

$$G = \begin{cases} \sqrt{q}, & om\ q \equiv 1\ (mod\ 4), \\ i\sqrt{q}, & om\ q \equiv 3\ (mod\ 4). \end{cases} \tag{68}$$

BEVIS : Se kap.2 av samma stencil från Davenports bok.

References

[5] H. Davenport, Multiplicative number theory, Springer 1980.

Lektion 9 (20/11/00)

Dirichlet's theorem

In today's class we began the proof of the following fantastic result :

Theorem (Dirichlet 1837). *Let $a, q > 0$ with $(a, q) = 1$. Then there are infinitely many primes p such that $p \equiv a \ (mod\ q)$. Moreover,*

$$\sum_{p \equiv a \ (mod\ q)} p^{-1} = +\infty. \tag{69}$$

Here I'm going to outline the main steps in the proof of this theorem. More details can be found on the handout I gave from Davenport's book.

Step 1. Some time around 1800, Euler gave an 'analytic' proof of Euclid's ancient theorem that there are infinitely many primes. More precisely, he proved

Theorem 26. *There are infinitely many primes and the sum of their reciprocals diverges.*

Proof : The starting point is the infinite product for the ζ-function (see p.21), valid when $\mathrm{Re}(s) > 1$, namely

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{70}$$

Taking log of both sides[10] we get, for $\mathrm{Re}(s) > 1$,

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right). \tag{71}$$

Next recall that the Taylor series for the log function, valid when $|z| < 1$, is given by

$$-\log(1 - z) = \sum_{m=1}^{\infty} \frac{1}{m} z^m. \tag{72}$$

[10] At all times, unless otherwise stated, we are using the principal branch of the log function.

Substituting (72) into (71) we get, also for $\mathrm{Re}(s) > 1$,

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}. \tag{73}$$

Now group the terms on the rhs into two groups, those with $m = 1$ and those with $m > 1$. Note that we are changing the order of summation here, but that is okay because the series is absolutely convergent when $\mathrm{Re}(s) > 1$[11]. We obtain

$$\log \zeta(s) = \sum_p p^{-s} + \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{ms}}. \tag{74}$$

The idea now is to look at what happens when $s \to 1^+$. The sum over $m \geq 2$ does not blow up - in fact, it's value at $s = 1$ can easily be shown to be less than, for example, $2\zeta(2) = \pi^2/3$. On the other hand, we all know from envariabelanalys (use, say, the integral test) that $\zeta(s) \to +\infty$ as $s \to 1^+$. This means that the lhs of (74) goes to infinity as $s \to 1^+$. It follows that the same is true of the rhs, and hence that

$$\lim_{s \to 1^+} \sum_p p^{-s} = \infty. \tag{75}$$

In particular, the sum must contain infinitely many terms (i.e.: there are infinitely many primes) and $\sum p^{-1}$ diverges. This proves Theorem 26.

Step 2. Now enter Dirichlet. Theorem 26 is the case $q = a = 1$ of his theorem. For a fixed $q > 1$ Dirichlet suggested to consider the L-series (see p.24)

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \tag{76}$$

where χ is a Dirichlet character modulo q. The series defines an analytic function in the half-plane $\mathrm{Re}(s) > 1$. It generalises the usual ζ-function, since the latter corresponds to $q = 1$ and $\chi = \chi_0$, the trivial character. These functions also have Euler products (p.28), namely

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{77}$$

[11]Recall from envariabelanalys (or see p.42 of my notes on flervariabelanalys from last year) that the sum of an absolutely convergent series is independent of the ordering of the terms. This is not true for conditionally convergent series (Riemann's theorem).

As above, take log of both sides of (77) and expand the rhs in a Taylor series to obtain, for $\mathrm{Re}(s) > 1$,

$$\log L(s,\chi) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{mp^{ms}}. \tag{78}$$

The difference between this and the previous situation is that now we are only interested in those primes $p \equiv a \pmod q$, for some a with $(a,q) = 1$. So how do we isolate these primes in the sum (78) ? The trick is to use the following lemma (Dav. p.31, ekv. (4)) :

Lemma 27. *Let $a, n, q > 0$ with $(a,q) = (n,q) = 1$. Then*

$$\sum_{\chi} \bar{\chi}(a)\chi(n) = \begin{cases} \phi(q), & \text{if } n \equiv a \pmod q, \\ 0, & \text{otherwise}, \end{cases} \tag{79}$$

where the sum is taken over all characters modulo q.

Proof : We'll talk about this on Wednesday. The thing to note is that Lemma 27 is the 'dual' result to eq. (44) on p.28, i.e.: it's the same result, but applied to the dual group of $(\mathbf{Z}/q\mathbf{Z})^{\times}$ - see ex.6 of the supplementary exercises.

From (78) and (79) we obtain, by a simple calculation,

$$\frac{1}{\phi(q)} \sum_{\chi} \bar{\chi}(a) \log L(s,\chi) = \sum_{m=1}^{\infty} \sum_{p^m \equiv a \ (\mathrm{mod}\ q)} \frac{1}{mp^{ms}}. \tag{80}$$

Here we're still assuming that $\mathrm{Re}(s) > 1$, and the sum is taken over all characters modulo q. Next, as in the proof of Theorem 26, we split the terms of the sum into two groups, those with $m = 1$ and those with $m > 1$. We observe that the latter sum is bounded as $s \to 1$ and conclude that

$$\lim_{s \to 1^+} \frac{1}{\phi(q)} \sum_{\chi} \bar{\chi}(a) \log L(s,\chi) = \lim_{s \to 1^+} \sum_{p \equiv a \ (\mathrm{mod}\ q)} p^{-s} + O(1). \tag{81}$$

Dirichlet's theorem is (as in the case of Theorem 26) precisely the statement that the limit of the right-hand sum is $+\infty$. Hence we have reduced the proof of the theorem to showing that

$$\lim_{s \to 1^+} \frac{1}{\phi(q)} \sum_{\chi} \bar{\chi}(a) \log L(s,\chi) = +\infty. \tag{82}$$

Step 3. If $\chi = \chi_0$, the trivial character, then it's easy to see that

$$L(s, \chi_0) = \prod_{p|q} \left(1 - \frac{1}{p^s}\right) \cdot \zeta(s). \tag{83}$$

Since the product is finite and different from zero, and $\zeta(s) \to +\infty$ as $s \to 1^+$, it follows that also $L(s, \chi_0) \to +\infty$ as $s \to 1^+$. Hence, (82) would be proven if we could show that $\log L(s, \chi)$ were bounded, as $s \to 1^+$, for every $\chi \neq \chi_0$.

But we know (Sats 19, p.28) that if $\chi \neq \chi_0$, then $L(s, \chi)$ is analytic in the range $\mathrm{Re}(s) > 0$. In particular, $L(s, \chi)$ is bounded as $s \to 1$. Hence the same is true of $\log L(s, \chi)$ UNLESS $L(1, \chi) = 0$. So we have reduced the proof of Dirichlet's theorem to showing the following :

Theorem 28. *Let $q > 1$ and χ be a non-trivial character modulo q. Then*

$$L(1, \chi) \neq 0. \tag{84}$$

Step 4. All known proofs of Theorem 28 (as far as I know, anyway !) start by dividing it into two cases.

DEFINITION : A character χ is called *complex* if $\chi(m) \notin \mathbf{R}$ for some $m \in \mathbf{Z}$. Otherwise the character is called *real.*

Note that if χ is real then $\chi(m) = \pm 1$ for all m. If the modulus q is a prime power, say $q = p^m$, then one easily shows that the only non-trivial real character is the Legendre symbol $\chi(m) = \left(\frac{m}{q}\right)$.

As suggested by the definition, we divide the proof of Theorem 28 according as to whether χ is real or complex. The easier part seems to be

Proposition 29. *If χ is complex then $L(1, \chi) \neq 0$.*

PROOF : If χ is any character modulo q, then so is $\bar{\chi}$ defined by $\bar{\chi}(m) := \overline{\chi(m)}$. The point is that, if χ is complex, then $\chi \neq \bar{\chi}$. Why is this useful ? Well, suppose that $L(1, \chi) = 0$. Then $L(1, \bar{\chi}) = 0$ also, since $L(s, \bar{\chi}) = \overline{L(s, \chi)}$ for all real s. Since $L(s, \chi)$ and $L(s, \bar{\chi})$ are analytic functions in a neighbourhood of $s = 1$, it follows from elementary complex analysis that there exist functions $A(s), B(s)$ analytic in a neighbourhood U of $s = 1$ so that

$$L(s,\chi) = (s-1)A(s) \quad \text{and} \quad L(s,\bar{\chi}) = (s-1)B(s) \quad \text{for all } s \in U. \tag{85}$$

The proof of Proposition 29 now follows quickly from the following two results, the second of which is of sufficient interest in itself that we list it as a theorem in its' own right (we will also need it later in the treatment of real characters) :

Lemma 30. *If Re$(s) > 1$ then*

$$\prod_{\chi} L(s,\chi) > 1, \tag{86}$$

where the product is taken over all characters modulo q.

Theorem 31. *The ζ-function can be continued to a meromorphic function in the half-plane Re$(s) > 0$ which has a simple pole at $s = 1$ and no other poles.*

Before we prove these two results, let us see how they give Proposition 29. If $L(1,\chi) = 0$ for a complex χ then, as shown above, the characters χ and $\bar{\chi}$ together contribute at least a double zero at $s = 1$ to the product on the lhs of (86). But since the product is > 1 whenever $s > 1$ it must also be > 1 in the limit as $s \to 1^+$. This means that the remaining factors in the left-hand product must contribute at least a double pole at $s = 1$. But the factor $L(s,\chi_0)$ contributes only a simple pole, by (83) and Theorem 31, and the remaining factors are bounded. This is a contradiction, and completes the proof of Prop. 29.

Proof of Lemma 30 : One uses (80). The rhs of this equation is, at the very least, real and positive for Re$(s) > 1$. Now put $a = 1$, multiply across by $\phi(q)$ and finally exponentiate both sides to get (86).

Proof of Theorem 31 : The argument is classic and is given at the bottom of p.32 of the handout. Note the use of Abel's partial summation formula at the outset.

Step 5. We have reduced Dirichlet's theorem to proving

Proposition 32. *If χ is real and non-trivial, then $L(1, \chi) \neq 0$.*

This will be done next time.

Lektion 10 (22/11/00)

I denna lektion löste vi övningar från den 1:a inlämningsuppgiften.

Lektion 11 (24/11/00)

In this lecture we complete the proof of Dirichlet's theorem by proving Proposition 32[12]. Dirichlet's original proof has the benefit of being very interesting but the disadvantage of being quite complicated. Below we give his proof for prime moduli $q \equiv 3 \pmod 4$. You should read my handouts for proofs of the remaining cases - it won't be examined ! Since Dirichlet's time, several 'easier', but uniformly less interesting, proofs have been proposed. We will first of all present one such proof, due to de la Vallée Poussin (1896). For yet another 'easy' proof see, for example, [6], Band I, s.93ff.

DE LA VALLÉE POUSSIN'S PROOF : The proof is given on p.33-34 of the handout. But I'll write it here anyway, with perhaps a few more details. The proof is by contradiction. We thus assume that $L(1,\chi) = 0$, where χ is a fixed real, non-trivial character modulo q, for some $q > 0$. One considers

[12] Those who have read my spiel on elliptic curves, buried amongst the solutions to inlämningsuppgft 1, may be interested to know that there is a corresponding OPEN problem about the L-series attached to elliptic curves $E/\mathbf{Q}$. As I stated there, the Euler product defining $L(E,s)$ can be shown directly to converge and give an analytic function when $\mathrm{Re}(s) > 3/2$. It is conjectured that, as in the case of ordinary Dirichlet L-functions, $L(E,s)$ has an analytic continuation to the whole s-plane, and furthermore that it satisfies a functional equation relating the values at s and $2-s$. In fact, this conjecture is now a theorem if one believes the recent complete proof of the Shimura-Taniyama conjecture, since it has long been known that the conjecture holds for modular elliptic curves. In any case, assuming the conjecture holds, we may investigate the value $L(E,1)$. One of the outstanding open problems in the theory of elliptic curves is the so-called *Birch and Swinnerton-Dyer conjecture*. Before we state this, we have to explain another theorem : Recall from my spiel that the set of points on any elliptic curve E has the structure of an abelian group. Now suppose E is defined over $\mathbf{Q}$ and let $E(\mathbf{Q})$ denote the set of points $(x,y) \in E$ s.t. both x and y are rational numbers. One can show that $E(\mathbf{Q})$ is a subgroup of E - in fact, the same is true of $E(K)$ for any extension field K of $\mathbf{Q}$. A famous theorem from the 1920s, the so-called *Mordell-Weil theorem*, asserts that $E(\mathbf{Q})$ is always a finitely generated group, hence isomorphic to the direct sum of a finite group and a finite number, r say, of copies of $\mathbf{Z}$. The number r is called the *rank* of E (by the way, a generalisation of the Mordell-Weil theorem to abelian varieties of arbitrary dimension was proven by Faltings in 1984, for which he won the Fields medal !). We are now in a position to state a weak form of the Birch and Swinnerton-Dyer conjecture : it says that $L(E,s)$ has a zero at $s=1$ of order equal to the rank of E (in particular $L(E,1) \neq 0$ iff the group $E(\mathbf{Q})$ is finite). Note that this is more or less the complete opposite of the corresponding result for Dirichlet L-series. Finally, we remark that a special case of the conjecture was established by Wiles and Coates as part of the former's doctoral thesis, and it was this result which first established Wiles as a big name in number theory !

the function

$$\psi(s) := \frac{L(s,\chi)L(s,\chi_0)}{L(2s,\chi_0)}. \tag{87}$$

We claim that $\psi(s)$ is analytic in $\mathrm{Re}(s) > 1/2$ and that $\psi(s) \to 0$ as $s \to \frac{1}{2}^{+}$.

To see this, first note that Sats 19(ii), eq. (83) and Theorem 31 guarantee that $\psi(s)$ is at least meromorphic in the range $\mathrm{Re}(s) > 1/2$. The only possible poles are at the poles of $L(s,\chi_0)$ and at the zeroes of $L(2s,\chi_0)$. Theorem 31 implies that the former has only a single simple pole at $s = 1$, but by assumption this is cancelled by the zero of $L(1,\chi)$. From the Euler product for the ζ-function, one sees directly that $\zeta(s) \neq 0$ whenever $\mathrm{Re}(s) > 1$ - in fact, this property is equivalent to convergence of the product. Hence, from (83), the function $L(2s,\chi_0)$ is never zero in the region $\mathrm{Re}(s) > 1/2$. This proves analyticity of $\psi(s)$ in this region[13]. That $\psi \to 0$ as we approach $s = 1/2$ follows from the fact that $L(2s,\chi_0)$ has a pole at $s = 1/2$.

The next step is to restrict attention to the range $\mathrm{Re}(s) > 1$, where we can write each L-function as an Euler product. Note that all Euler factors corresponding to prime divisors p of q are equal to 1, because $\chi(p) = \chi_0(p) = 0$ for such primes. Thus we have

$$\begin{aligned} L(s,\chi) &= \prod_{p\nmid q}(1-\chi(p)p^{-s})^{-1}, \\ L(s,\chi_0) &= \prod_{p\nmid q}(1-p^{-s})^{-1}, \\ L(2s,\chi_0) &= \prod_{p\nmid q}(1-p^{-2s})^{-1}. \end{aligned}$$

Now we use the fact that the character χ is real. This implies that $\chi(p) = \pm 1$ for all primes p not dividing q. A direct calculation shows that, for any p such that $\chi(p) = -1$, the Euler factor of ψ at p is just 1, because the factors coming from the three L-functions cancel each other out. We are thus left with the factors for primes for which $\chi(p) = 1$, and another direct calculation shows that

$$\psi(s) = \prod_{\chi(p)=1} \frac{1+p^{-s}}{1-p^{-s}}, \qquad (\mathrm{Re}(s) > 1). \tag{88}$$

[13] Note that, if the Riemann hypothesis were true, we would know that $\zeta(s)$ had no zeroes for $\mathrm{Re}(s) > 1/2$, hence that $L(2s,\chi_0)$ had no zeroes for $\mathrm{Re}(s) > 1/4$, so that $\psi(s)$ would be analytic in this larger region.

Using the binomial theorem in the form $(1-p^{-s})^{-1} = \sum_{m=0}^{\infty} p^{-ms}$, we may expand (88) in a Dirichlet series

$$\psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad (\mathrm{Re}(s) > 1). \tag{89}$$

The only properties we will require of the coefficients a_n are that they are all non-negative real numbers and that $a_1 = 1$. These are seen to hold by direct inspection.

The next and final step is to use (89) to derive a contradiction to the fact that $\psi(s) \to 0$ as $s \to \frac{1}{2}^{+}$. I won't give the details because I don't think any are left out in the handout, except perhaps for the remark that Weierstraβ' theorem allows us to differentiate (89) termwise at $s = 2$[14]

Dirichlet's proof for prime moduli : I followed exactly the proof given on the handout, starting near the bottom of p.7. Observe that the

[14]If one examines (80) and (81) closely, then one can convince oneself that we have actually proven a stronger form of Dirichlet's theorem.

Definition : Let $\mathcal{A}$ be a subset of the set of primes $\mathcal{P}$. The *(analytic) Dirichlet density* of $\mathcal{A}$ is defined as

$$d_D(\mathcal{A}) = \lim_{s \to 1} \left(\sum_{p \in \mathcal{A}} \frac{1}{p^s} \right) / \left(\log \frac{1}{s-1} \right),$$

provided this limit exists. Then we've actually proved

Theorem 32.A *Let $a, q > 0$ with $(a,q) = 1$. Let P_a be the set of primes $p \equiv a$ (mod q). Then $d_D(P_a) = 1/\phi(q)$.*

The definition of 'density' given above seems rather technical. A much simpler notion is

Definition : Let $\mathcal{A} \subseteq \mathcal{P}$. The *natural density* of $\mathcal{A}$ is given by

$$d_N(\mathcal{A}) = \lim_{n \to \infty} \frac{\#\{p \in \mathcal{A} : p \leq n\}}{\#\{p \in \mathcal{P} : p \leq n\}},$$

provided the limit exists. It can be proven that $d_N = d_D$ for sets of the form P_a above, which is reassuring. In general, it can be shown that, for a set $\mathcal{A}$ of primes, $d_N(\mathcal{A}) = d_D(\mathcal{A})$ whenever the former exists. However, there are (weird) sets $\mathcal{A}$ having a Dirichlet density but not a natural density. An example is the set $\mathcal{A}$ of primes whose first decimal digit is one ! See p.76 of Serre's 'A course in arithmetic' for further comment.

appearance of the Gauβ sum G in the formula for $L(1,\chi)$ in the middle of p.8, together with the fact that $L(1,\chi)$ is a real number (χ being a real character), leads one, because of Sats 25, to distinguish the cases $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$. We only had time to finish discussing the former case. Here, I just wish to note for the record two corollaries of the proof which are very beautiful in themselves and for which to this day, as Davenport notes, no proofs are known which avoid the use of L-functions. They are

Korollarium 33. *If q is a prime, $q \equiv 3$ (mod 4), then*

$$\sum_{m=1}^{q-1} m \left(\frac{m}{q}\right) < 0. \tag{90}$$

Korollarium 34. *If q is a prime, $q \equiv 3$ (mod 4), then there are more quadratic residues than non-residues modulo q amongst the numbers $1, 2, ..., \frac{q-1}{2}$.*

REMARK : These two corollaries are amongst the oldest results concerning a problem which to this day is the subject of much research, namely that of the distribution of the quadratic residues modulo p, for a given prime number p. Since even the precise formulation of some of these problems is rather difficult, I will shy away from it, and content myself with mentioning a conjecture of Vinogradov which says that, for each $\epsilon > 0$ there esists $n_\epsilon > 0$ such that there exists a quadratic non-residue $n < p^\epsilon$ for all primes $p > n_\epsilon$. See supplementary exercise no. 7 for something much weaker.

REFERENCES

[6] E. Landau, Vorlesungen über Zahlentheorie, Leipzig 1927.

Lektion 12 (27/11/00)

Idag börjar vi studiet av kvadratiska ekvationer över $\mathbf{Z}$, dvs ekvationer av formen

$$f(x_1, ..., x_n) = 0, \tag{91}$$

där f är ett polynom av grad 2 med heltals koefficienter. Vi söker heltalslösningar till (91).

För $n = 1$ är allting klart. Ekvationen

$$ax^2 + bx + c = 0 \qquad (a \neq 0) \tag{92}$$

har lösningar i $\mathbf{C}$ som ges av

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{93}$$

Alltså, har ekvationen en lösning i $\mathbf{Q}$ omm $b^2 - 4ac = d_1^2$ är en perfekt kvadrat, och en lösning i $\mathbf{Z}$ omm $2a \mid -b \pm d_1$. Antalet lösningar i $\mathbf{Z}$ är då $0, 1$ eller 2.

För $n = 2$ blir situationen redan mycket mer komplicerad att analysera. I den här kursen ska vi koncentrera mest på detta fall (för en mer allmän diskussion kom till min doktorandkurs !).

Det var framför allt Gauβ som utvecklade en allmän teori för kvadratiska ekvationer i två variabler. Den större delen av hans klassiskt arbete *Disquisitiones Arithmeticae* handlar om denna teori. I vår presentation ska vi, till en början, följa Gauβ, innan vi reformulerar våra resultat i mer modern algebraisk talteoretiskt språk.

Vi studerar då den allmäna kvadratiska ekvationen i två variabler, dvs en ekvation av formen

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{94}$$

där koefficienterna $a, b, c, d, e, f \in \mathbf{Z}$ och $(a, b, c) \neq (0, 0, 0)$. Polynom som på vänster sidan av (94) ska betecknas framöver med $f(x, y), g(x, y)$ mm. Det är ofta passande att använda en matris notation. Om vi låter

$$A := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}, \quad g := \begin{pmatrix} d \\ e \end{pmatrix}, \quad X := \begin{pmatrix} x \\ y \end{pmatrix}, \tag{95}$$

då kan (94) skrivas i formen

$$f(x,y) = f(X) = X^T AX + g^T X + f = 0. \tag{96}$$

För att simplificerar formen av ekvationen lite, betraktar man koordinat bytningar av typen $X \to X'$ där

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = X' := UX + V, \qquad \exists\, U \in GL_2(\mathbf{Q}),\ V \in \mathbf{Q}^2. \tag{97}$$

Om $\det(A) \neq 0$ då kontrollerar man lätt att transformationen $U = I, v = -\frac{1}{2}(A^T)^{-1}g$ skaffar en ekvation av formen

$$f'(x',y') = ax'^2 + bx'y' + cy'^2 = n. \tag{98}$$

Här är kanske n inte ett heltal, men då behöver man bara klara nämnarna.

Fallet $\det(A) = 0$ är speciellt. Här ser man, efter en kvadrat komplettering (se (104) nedan), att det finns en koordinat bytning som tar (94) till formen

$$x'^2 + e'y' + f' = 0. \tag{99}$$

Denna ekvation är tämligen ointeressant eftersom det är klart att det finns två heltalslösningar för varje y' så att $-e'y' - f'$ är en perfekt kvadrat.

Alltså, i fortsättningen ska vi ägna oss åt att studera ekvationer av formen (98), där $b^2 - 4ac \neq 0$.

Definition 1 : En funktion $f : \mathbf{Z}^2 \to \mathbf{Z}$ som ges av

$$f(x,y) = ax^2 + bxy + cy^2, \qquad a,b,c \in \mathbf{Z}, \tag{100}$$

kallas för en *(integral) binär kvadratisk form.* I matris form, ges f av

$$f(X) = X^T AX, \quad X = \begin{pmatrix} x \\ y \end{pmatrix}, \ A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}. \tag{101}$$

Definition 2 : Kvantiteten $d := b^2 - 4ac$ kallas för *diskriminanten* av formen f. Notera att

$$d_f = -4\det(A_f). \tag{102}$$

Proposition 35. *An integer d is the discriminant of some binary quadratic form iff $d \equiv 0$ or 1 (mod 4).*

Proof : The definition of d immediately implies the necessity. For sufficiency, it suffices to write down explicit forms, and we choose

$$\begin{array}{ll} x^2 - \frac{1}{4}dy^2, & \text{if } d \equiv 0 \pmod 4, \\ x^2 + xy - \frac{1}{4}(d-1)y^2, & \text{if } d \equiv 1 \pmod 4. \end{array} \tag{103}$$

The forms in (103) are called the *principal forms.*

Definition 3 : En form kallas för *degenererad* om $d = 0$; annars kallas den för *icke-degenererad.* En form med $d < 0$ kallas för *definit* : *positiv definit* i fallet $a > 0$ och *negativ definit* i fallet $a < 0$. En form med $d > 0$ kallas för *indefinit.* Slutligen, kallas formen för *faktoriserbar* om d är en perfekt kvadrat.

Notera att f är positiv definit omm $-f$ är negativ definit. Då får vi strunta i negativa former framöver.

Definition 4 : Låt $n \in \mathbf{Z}$. En form f sägs *representera* n om $f(x,y) = n$ för något $(x,y) \in \mathbf{Z}^2$. En sådan representation av n kallas för *egentlig (proper)* om $\gcd(x,y) = 1$.

Problemet av att lösa (98) i heltalen kallas för *representationsproblemet* för binära kvadratiska former. Det är det grundläggande problemet som motiverar alla idéerna som vi skall nu presentera.

Först förklarar vi terminologin i Definition 3. Kvadratkomplettering i (100) leder till uttrycket

$$4af(x,y) = (2ax + by)^2 - dy^2. \tag{104}$$

Då ser vi direkt att representationsproblemet är tämligen ointeressant för faktoriserbara former, eftersom det reducerar till att faktorisera $4an$ och då att lösa par av simultana LINJÄRA ekvationer. I fortsättningen, alltså, antar vi alltid följande

'*f är en kvadratisk form vars diskriminant d inte är en perfekt kvadrat, och om $d < 0$ då är f positiv definit*'.

Nu leder (104) direkt till följande resultat som förklarar vår terminologi :

Proposition 36. *(i) f positiv definit $\Leftrightarrow$ f representerar bara positiva tal.* *(ii) f indefinit $\Leftrightarrow$ f representerar både positiva och negativa tal.*

Gauβ' approach to the representation problem can be divided up into the following main steps :

STEP 1 : Divide up all the forms according to their discriminant.

STEP 2 : Define an equivalence relation on the set of forms of a given discriminant so that equivalent forms need not be distinguished as regards the representation problem, i.e.: equivalent forms represent (properly) the same integers and there is a canonical 1-1 correspondence between their (proper) representations of a given integer.

STEP 3 : Show that the number of equivalence classes for a given discriminant is finite and that each class contains at least one 'nice' form.

STEP 4 : Find a formula for the total number of representations of an integer by a representative collection of forms of a given discriminant.

We shall carry out this program. But first, some remarks are in order :

1. The process described in Steps 2-3 is called *reduction theory.* It turns out that a satisfactory reduction theory is far easier to obtain for definite forms than for indefinite forms. We will only present detailed proofs of the results in the former case. In both cases, the theory gives an algorithm for deciding whether two forms of a given discriminant are equivalent. The procedure is simpler in the definite case.

2. With regard to Step 4, the formula in question will be seen to be quite simple and elegant. In the case of indefinite froms, where any given integer may have infinitely many representations as we'll see below, the formula counts representations of a certain type, called *primary.* It is important to note that there seems to be no such simple formula for the number of (primary) representations of an integer by a single form of a given discriminant. However, we will see that there exist, in principle, algorithms for deciding

whether (98) has a solution, and for counting the number of (primary) solutions. For definite forms, this is in fact a trivial result, since $f(x,y) = n$ implies that x and y are bounded explicitly. But for indefinite forms, this is not the case and something more clever must be done. Also, the algorithms for definite forms got by explicitly bounding x, y are obviously very slow. Finally, we observe that our algorithms here will in turn depend on those for deciding equivalence of forms, as just mentioned above.

DEFINITION : The binary quadratic forms f and f' are said to be *equivalent*, denoted $f \sim f'$, if there exists a matrix $M \in SL_2(\mathbf{Z})$ such that

$$M^T A_f M = A_{f'}. \tag{105}$$

It is readily checked that (105) does indeed define an equivalence relation on the set of all binary forms, and that equivalent forms have the same discriminant. The importance of the relation relies in the following fact :

Proposition 37. *If $f \sim f'$, then for each integer n, there is a 1-1 correspondence between the (proper) representations of n by f and f'.*

It is convenient to write down, once and for all, the explicit relationship between the coefficients of equivalent forms. If $f = \{a, b, c\}$, $f' = \{a', b', c'\}$ and $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is a matrix taking f to f', then (105) gives

$$\begin{aligned} a' &= f(p,r) = ap^2 + bpr + cr^2, \\ c' &= f(q,s) = aq^2 + bqs + cs^2, \\ b' &= 2apq + b(ps + qr) + 2crs. \end{aligned} \tag{106}$$

Lektion 13 (29/11/00)

Reduction theory

Definition : The form $\{a, b, c\}$ is said to be *reduced* if either

$$-|a| < b \leq |a| \leq |c| \quad \text{or} \quad 0 \leq b \leq |a| = |c|. \tag{107}$$

The main result of reduction theory is

Theorem 37 (Lagrange/Gauss). *(i) Every binary form is equivalent to a reduced form.*
(ii) There are only finitely many reduced forms of a given discriminant.
(iii) Every positive definite form is equivalent to precisely one reduced form.

Proof : A condensed version of the proof we gave in class is found on ps. 36-7 of Baker's book.

Important remark 1 : The proof of (i) gives an algorithm for producing a reduced form equivalent to a given form (in class I considered the example of the form $f(x, y) = 22x^2 - 108xy + 133y^2$, which I reduced to the form $f'(x, y) = 2x^2 + 5y^2$). Because of (iii) this gives, in the case of positive definite forms, an algorithm for deciding whether two given forms are equivalent.

However, for indefinite forms, things get much more complicated. It can happen that a single equivalence class of indefinite forms contains more than one reduced member. In particular, the above algorithm for deciding equivalence of forms does not work in general. In fact, one needs a whole new (and rather different !) reduction theory in order to be able to find such an algorithm[15].

[15] We will not have time to describe this theory, but here are the main results. For detailed proofs, see my handout from Zagier's book, 'Zetafunktionen und quadratische Körper'.

In this new theory, a form $\{a, b, c\}$ is called *reduced* if $a > 0, c > 0$ and $a + c < b$. We consider a special type of transformation (105). If f is the form $\{a, b, c\}$, set $n = \lceil \frac{b+\sqrt{d}}{2a} \rceil$ and define $T(f)$ to be the form obtained by transforming, as in (105), with the matrix $M_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix}$. Then the main result of the theory is

Theorem. (i) The number of reduced forms of a given discriminant is finite.

Important remark 2 : Motivated by Theorem 38, we define $H(d)$ to be the number of equivalence classes of binary forms of discriminant d. The theorem says that $H(d)$ is finite, and because of the principal forms, we conclude that $H(d)$ is a non-zero positive integer. For positive definite forms, part (iii) of the theorem implies that, in order to compute $H(d)$, it suffices to compute the number of reduced forms of discriminant d. This can be done because, from (107) and the equation $d = b^2 - 4ac$, we can easily derive explicit bounds for the coefficients of a reduced form of discriminant d, namely

$$\begin{aligned} 0 < |a| \le \sqrt{-d/3}, &\quad \text{for a reduced definite form,} \\ 0 < |a| \le \sqrt{d/4}, &\quad \text{for a reduced indefinite form.} \end{aligned} \tag{108}$$

For indefinite forms, this procedure only gives, in general, an upper bound for $H(d)$. One of the classical results of algebraic number theory is

Theorem 39 (Baker/Stark 1966.)[16] *There are only finitely many $d < 0$ for which $H(d) = 1$, and these are given explicitly by* $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$.

Likewise, one of the outstanding open problems in algebraic number theory is

Open problem. *Do there exist infinitely many $d > 0$ for which $H(d) = 1$?*

(ii) For any given form f, there exists a positive integer k, depending on f, such that $T^k(f)$ is reduced.
(iii) The operator T maps reduced forms to reduced forms.
(iv) Every equivalence class of reduced forms is acted upon transitively by T.

Note that the theorem does not say that each class of forms contains a unique reduced form (this is false !), hence does not provide an algorithm for computing class numbers (see important remark no. 2 above). On the other hand, it is easy to see that (ii),(iii) and (iv) give an algorithm for deciding equivalence of any 2 given forms.

[16] This result is usually phrased in terms of which imaginary quadratic number fields have unique factorisation. We will explain what this means later. Likewise, the open problem following Theorem 39 is usually phrased in terms of unique factorisation for real quadratic fields.

Lektion 14 (01/12/00)

DEFINITION : En matris $M \in SL_2(\mathbf{Z})$ sägs vara en *automorfism* av formen f om

$$M^T A_f M = A_f. \tag{109}$$

Notera att automorfismerna av f utgör en delGRUPP av $\mathrm{SL}_2(\mathbf{Z})$. Denna grupp betecknas $\mathrm{Aut}(f)$. Ordningen av gruppen betecknas med $w(f)$.

Proposition 40. *(i) Om $X \in \mathbf{Z}^2$ och $M \in Aut(f)$, då är*

$$f(MX) = f(X). \tag{110}$$

(ii) Om $f \sim g$, och P är en matris så att $P^T A_f P = A_g$, då har vi en 1-1 korrespondens

$$\begin{array}{ccc} Aut(f) & \leftrightarrow & Aut(g) \\ M & \leftrightarrow & P^{-1}MP. \end{array} \tag{111}$$

Notera att del (i) av propositionen säger att när vi räknar antalet representationer av ett heltal n med f, så måste vi inte glömma automorfiska representationer.

Del (ii) av propositonen säger att ekvivalenta former har samma antalet automorfismer.

Det viktiga begreppet för att studera automorfism frågan är

DEFINITION : En form $f = \{a, b, c\}$ kallas för *primitiv* om $\gcd(a, b, c) = 1$.

Proposition 41. *Låt $f = \{a, b, c\}$ vara en form med $gcd(a, b, c) = r$. Då är formen $f' = \{a/r, b/r, c/r\}$ primitiv och $Aut(f) = Aut(f')$.*

BEVIS : Klart.

Denna proposition reducerar beräkningen av automorfismgrupper till den för primitiva former. Det visar sig nu att automorfismgrupperna av primitiva former kan beskrivas helt explicit. Vi har

Sats 42. *Låt $f = \{a, b, c\}$ vara en primitiv form av diskriminant d. Då består*

Aut(f) precist av alla matriser

$$M = \begin{pmatrix} \frac{1}{2}(t-bu) & -cu \\ au & \frac{1}{2}(t+bu) \end{pmatrix}, \tag{112}$$

där $(t,u) \in \mathbf{Z}^2$ *är en lösning av ekvationen*

$$t^2 - du^2 = 4. \tag{113}$$

Bevis : Satz 202 i Landaus bok (se utdelad stencil).

Ekvation (113) kallas för *Pells ekvation.* I fallet $d < 0$ kan lösningarna ses direkt, och de är

$$\begin{array}{rc} (\pm 2, 0), (0, \pm 1), & \text{om } d = -4, \\ (\pm 2, 0), \pm(1,1), \pm(1,-1), & \text{om } d = -3, \\ (\pm 2, 0), & \text{annars.} \end{array} \tag{114}$$

Då följer det från Sats 42 att

Korollarium 43. *Låt* $f = \{a,b,c\}$ *vara en primitiv positiv definit form av diskriminant* $d < 0$. *Då har vi att*

$$\begin{array}{rlr} Aut(f) = \{\pm M_1, \pm M_2\}, & w(f) = 4, & \textit{om } d = -4, \\ Aut(f) = \{\pm M_1, \pm M_3, \pm M_3^2\}, & w(f) = 6, & \textit{om } d = -3, \\ Aut(f) = \{\pm M_1\}, & w(f) = 2, & \textit{annars,} \end{array} \tag{115}$$

där

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}. \tag{116}$$

För indefinita former, är läget mycket mer interessant. Man får följande resultat

Sats 44. *(i) (*Lagrange *1768) Låt d vara ett positivt heltal som inte är en perfekt kvadrat. Då har Pells ekvation (113) oändligt många lösningar. Om* (t_0, u_0) *är den lösning med* $t_0, u_0 > 0$ *och* u_0 *minimal, då ges alla lösningar av*

$$\frac{1}{2}(t + u\sqrt{d}) = \pm \left[\frac{1}{2}(t_0 + u_0\sqrt{d})\right]^m, \tag{117}$$

där $m \in \mathbf{Z}$.

(ii) (Gauss) *Om f är en primitiv form av diskriminant d, då är $w(f) = \infty$ och $Aut(f) \cong \mathbf{Z}$, en oändlig cyklisk grupp.*

Bevis : Kommer senare. Nuförtiden, genomförs beviset bäst i sättningen av algebraiska talkropper. Naturligtvis kan man undvika denna teori, som Lagrange tvingades göra - för en sådan synvinkel, se t.ex. Landaus Vorlesungen, Satz 111.

Vi vill säga lite mer om primitiva former innan vi går vidare.

Proposition 45. *Om f är primitiv och $f \sim g$, då är g också primitiv.*

Definition : Vi betecknar med $h(d)$ antalet ekvivalens klasser av primitiva former av diskriminant d. Notera att detta är väl-definierad enligt Prop. 45.

Definition : Ett heltal $d \equiv 0$ eller 1 (mod 4) kallas för en *fundamental diskriminant* om varje form av diskriminant d är primitiv.

Proposition 46. *Låt $d \equiv 0$ eller 1 (mod 4).*
(i) $H(d) = h(d) \Leftrightarrow d$ är en fundamental diskriminant.
(ii)

$$H(d) = \sum_{t^2|d} h\left(\frac{d}{t^2}\right). \tag{118}$$

(iii) d är en fundamental diskriminant omm

$$\begin{aligned} d \text{ är kvadratfri}, \quad & \text{om } d \equiv 1 \ (mod\ 4), \\ d/4 \text{ är kvadratfri och} \equiv 2 \text{ eller } 3 \ (mod\ 4), \quad & \text{om } d \equiv 0 \ (mod\ 4). \end{aligned} \tag{119}$$

Bevis : (i) följer direkt från definitionen av en fundamental diskriminant. För (ii) och (iii) se supplementär övning nr. 12.

Representationsproblemet

We now finally come to what we've really been building up to all this time, namely the analysis of the equation

$$f(x, y) = ax^2 + bxy + cy^2 = n, \tag{120}$$

where everything in sight is an integer. Any such problem has both a theoretical and a practical aspect. From the theoretical viewpoint, one seeks some 'nice formulas' for the numbers $R(n, f)$ of solutions to (120). From the practical viewpoint, one is interested in having fast algorithms for computing all solutions explicitly[17]. Obviously, these two issues are inextricably linked.

Keeping in mind what people have actually succeeded in doing with the problem, we will follow the following program :

STEP 1 : As we've described earlier, the problem is uninteresting when the discriminant d is a perfect square. So we'll alawys assume this is not the case. Also, we lose nothing, in the case $d < 0$, by assuming that f is positive definite, i.e.: that $a, c > 0$.

STEP 2 : Right at the outest, a clear distinction presents itself between the definite and indefinite cases. In the former case, the number $R(n, f)$ is always finite, and the coefficients (x, y) of a representation are explicitly bounded by

$$|x| \leq \sqrt{4nc/|d|}, \qquad |y| \leq \sqrt{4na/|d|}. \tag{121}$$

These bounds follow easily from completion of squares, as in (104). Note that we hereby immediately obtain a (slow) algorithm for finding all solutions of (120) in the definite case - just check all pairs x, y up to the bounds in (121).

In the indefinite case, it follows immediately from Sats 44 that $R(n, f)$ is always either 0 or ∞. That is, each solution gives rise to an infinity of others by the application of the automorphisms of the form (see Prop. 40). It turns out that there is a fairly natural way of selecting, from each such infinite set of automorphic representations, one which is called *primary*. The number of primary representations then turns out to be finite, and we adopt the notation $R(n, f)$ for this number instead. The remarkable and wonderful fact is that, with this new convention, the indefinite and definite cases become 'unified' : more precisely we get explicit formulas valid in both cases (see Step 3).

With regard to the algorithmic question of finding explicit (primary) representations, it should not surprise you that this reduces to finding gen-

[17]The results we present in this course will only be to the extent of showing that algorithms exist. I have no idea what the state of the art is in regard to 'fast' algorithms, and hence will make no attempt to go into this matter.

erating solutions of Pell's equation. This is an instance of a problem in *Diophantine approximation* theory, and so we'll be lead to roam into this area. However, this will be postponed until the very end of the course, after we have done some algebraic number theory.

STEP 3 : It is convenient to first of all count proper representations. The number of proper representations of n by f is denoted $r(n, f)$, with the extra condition that the representations be primary in the indefinite case. Observe that

$$R(n, f) = \sum_{t^2 | n} r\left(\frac{n}{t^2}, f\right). \tag{122}$$

We now come to the crucial point :

As indicated in Step 2, there are algorithms for computing the numbers $r(n, f)$, for any given n and f. However, there seems to be NO SIMPLE FORMULAS for them. But if we sum over the forms of a fixed discriminant, then we get REALLY NICE formulas. More precisely, define, for each discriminant d,

$$R_d(n) := \sum_f R(n, f), \qquad r_d(n) := \sum_f r(n, f), \tag{123}$$

where the sum runs over a representative set of forms of discriminant d, one from each equivalence class. By Prop. 37, the sums are then well-defined.

The number $r_d(n)$ can be expressed in terms of the number of solutions to a certain quadratic congruence (Theorems 47,50 and 51 below). But solving quadratic congruences is a relatively simple matter, as discussed earlier in this course (see, in particular, Prop. 22). In particular, this already takes care of the algorithmic issues. The resulting 'formulas' are simplest in the case when d is a fundamental discriminant (basically, this is because all forms of discriminant d then have the same number of automorphisms - see Korollarium 43) and $(n, d) = 1$. The central result, Theorem 53, is due to Dirichlet. Dirichlet was led to this result by a rather circuitous route, during his investigations concerning his theorem on arithmetic progressions. Theorem 53 was his starting point for the proof of his so-called *class number formula*, which relates the class number $h(d)$ of a fundamental sicriminant d, to the value $L(1, \chi)$ of the L-function of some real character χ modulo d. The formula implies, in particular, that $L(1, \chi) \neq 0$, which you will remember was an essential ingredient in the proof of Dirichlet's theorem.

From a deeper, historical perspective, the class number formula is the starting point of two important theories :

(a) the analytic theory of number fields. Dirichlet's formula can be formulated in terms of quadratic number fields, and is then a special case of a class number formula valid for all number fields, which was first discovered by Hecke in the early 20th century. The basic analytical ingredient here is the notion of the ζ-function of a number field. Since Hecke, there has been an explosion of research into exploring the connections between analytic and algebraic aspects of number theory which, on the analytical side, usually relies on being able to extend the notion of a ζ-function to the particular realm of interest - the case of elliptic curves (see solutions to inlmningsuppgift nr. 1) being an excellent example.

(b) the analytic theory of quadratic forms. The state of the art in this area are the works of Siegel, from the 1930s and 40s, culminating in a formula which expresses the number of representations (in the indefinite case, something generalising primary representations) of an integer n by a representative set of forms Q in a given genus as an infinite product of terms over the primes (including infinity), each of which can be computed. This formula applies to quadratic forms in any number of variables. Come to my doktorandkurs if you want to learn more about this !

Representationsproblemet : the results !!

First, let's give the basic connection between proper representations and quadratic congruences :

Theorem 47. *The number n is properly represented by some binary quadratic form of discriminant d iff the congruence*

$$h^2 \equiv d \ (mod\ 4n) \tag{124}$$

is solvable.

PROOF : As in Baker, p.37-8.

APPENDIX 1

Positive definite binary quadratic forms over R and linear fractional transformations

Linear fractional transformations

Definition 1 : Let $M \in SL_2(\mathbf{R})$, say $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Let $H = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$. The map $\gamma_M : H \to H$ defined by

$$\gamma_M(z) = \frac{pz+q}{rz+s} \tag{125}$$

is called a *linear fractional transformation (of H)*.

It is well-known (and proven in every complex analysis course) that every holomorphic automorphism of H is given by a linear fractional transformation.

Definition 2 : Let G be a group which is also a topological space. If the maps

$$\begin{array}{rcccc} \mu & : & G \times G & \to & G \\ \mu & : & (x,y) & \mapsto & xy \end{array} \qquad \text{and} \qquad \begin{array}{rcccc} i & : & G & \to & G \\ i & : & x & \mapsto & x^{-1} \end{array}$$

are continuous (where $G \times G$ has the product topology), then G is called a *topological group*.

Definition 3 : A topological group G is said to *act (continuously)* on a topological space S if there is a continuous map

$$\begin{array}{ccc} G \times S & \to & S \\ (g,s) & \mapsto & gs \end{array}$$

(where $G \times S$ has the product topology) with the following properties :

(I) $\forall\, g, h \in G$, $\forall\, s \in S$, $gh(s) = g[h(s)]$.
(II) $\forall\, s \in S$, $es = s$.

Proposition 1. *Definition 1 defines a continuous action of $SL_2(\mathbf{R})$ on H.*

DEFINITION 4 : Let G act on S. For a point $s \in S$, the set

$$Gs := \{gs : g \in G\} \tag{126}$$

is called the *G-orbit* of s. Clearly, S is the disjoint union of its' G-orbits. Points in the same orbit are said to be *G-equivalent*. If there is just one G-orbit, we say that G acts *transitively* on S.

Proposition 2. *$SL_2(\mathbf{R})$ acts transitively on H.*

DEFINITION 5 : A subgroup Γ of a topological group G is called a *discrete subgroup* if the induced topology of Γ is discrete.

Proposition 3. *$\Gamma(1) := SL_2(\mathbf{Z})$ is a discrete subgroup of $SL_2(\mathbf{R})$.*

DEFINITION 6 : Let G act on S as before. A subset $\mathcal{F} \subseteq S$ is called a *fundamental domain* for the action of G if

(i) $\mathcal{F}$ is a connected Borel subset of S.
(ii) No two points of $\mathcal{F}$ are G-equivalent.
(iii) Every point of S is equivalent to some point in the closure of $\mathcal{F}$.

Theorem 4. *(i) Every discrete subgroup of $SL_2(\mathbf{R})$ has a fundamental domain in H.*
(ii) A fundamental domain for $\Gamma(1)$ is given explicitly by

$$\mathcal{F} = \left\{ z \in H : |z| > 1 \textit{ and } -\frac{1}{2} \leq Re(z) < \frac{1}{2} \right\} \quad \cup$$
$$\left\{ z \in H : |z| = 1 \textit{ and } -\frac{1}{2} \leq Re(z) \leq 0 \right\}. \tag{127}$$

DEFINITION 7 : Let G act on S as before. Let $s \in S$. The subgroup G_s of G given by

$$G_s := \{g \in G : gs = s\} \tag{128}$$

is called the *isotropy group* of s.

Theorem 5. *Let $z \in H$ and $\Gamma = \Gamma(1)$. Then*

$$\begin{aligned} \Gamma_z &= \{\pm M_1, \pm M_2\}, \quad |\Gamma_z| = 4, \quad \textit{if } z \in \Gamma i, \\ \Gamma_z &= \{\pm M_1, \pm M_3, \pm M_3^2\}, \quad |\Gamma_z| = 6, \quad \textit{if } z \in \Gamma \rho, \\ \Gamma_z &= \{\pm M_1\}, \quad |\Gamma_z| = 2, \quad \textit{otherwise}, \end{aligned} \tag{129}$$

where

$$\rho = e^{2\pi i/3}, \quad M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}. \tag{130}$$

Positive definite binary quadratic forms

We consider quadratic forms with REAL coefficients !!!!

Let $f = \{a, b, c\}$ be a positive definite binary quadratic form of discriminant $d < 0$. We associate to f the point $z_f \in H$ given by

$$z_f = \frac{-b + \sqrt{d}}{2a}. \tag{131}$$

Then the basic results of the reduction theory of positive definite forms can be phrased as follows

Theorem 6. *Fix an integer $d < 0$.*

(i) Eq. (131) describes a 1-1 correspondence between positive-definite binary forms over $\mathbf{R}$ *of discriminant d and points of H.*

(ii) If $M \in \Gamma(1)$, then $z_{M(f)} = Mz_f$, where $M(f)$ is the form with matrix $A_{M(f)} = M^T A_f M$, and Mz_f is the point of H given by (125). In particular, the group $Aut(f)$ is isomorphic to the isotropy subgroup of z_f.

(iii) Forms f and g are equivalent iff z_f and z_g lie in the same $\Gamma(1)$-orbit in H.

(iv) A form f is reduced in the sense of (107) iff the point z_f lies in the fundamental domain (127).

(v) The point $i \in \mathcal{F}$ corresponds to the reduced form f_{-4} with $b = 0, a = c = \frac{1}{2}\sqrt{-d}$. Hence, $Aut(f_{-4}) = \{\pm M_1, \pm M_2\}$ and $w(f_{-4}) = 4$.

(vi) The point $\rho \in \mathcal{F}$ corresponds to the reduced form f_{-3} with $a = b = c = \sqrt{-d/3}$. Hence, $Aut(f_{-3}) = \{\pm M_1, \pm M_3, \pm M_3^2\}$ and $w(f_{-3}) = 6$.

(vii) If the reduced form f corresponds to any other point of $\mathcal{F}$, then $Aut(f) = \{\pm M_1\}$ and $w(f) = 2$.

References

For proofs of most of the results listed here, see for example my handout from the book 'Topics in number theory, Vol. II', by W.J. LeVeque. For a (much !) more advanced discussion of the action of $SL_2(\mathbf{R})$ and its' discrete subgroups on H, and its' importance in number theory, see for example the book 'Intorduction to the arithmetic theory of automorphic functions', by G. Shimura.

Lektion 15 (04/12/00)

Vi börjar med en tillämpning av Sats 47.

Proposition 48. *(i) Låt p vara ett udda primtal. Då finns det en form av diskriminant d som representerar p omm antingen $4p|d$ eller $\left(\frac{d}{p}\right) = 1$.*

(ii) Låt p vara ett udda primtal. Då har ekvationen $x^2 - 2y^2 = p$ en lösning $(x, y) \in \mathbf{Z}^2$ omm $p \equiv \pm 1 \ (mod\ 8)$.

BEVIS : (i) Enligt Sats 47, finns det en form av diskriminant d som representerar p omm kongruensen $h^2 \equiv d \pmod{4p}$ är lösbar. Om $4p \mid d$ då är $h = 0$ en lösning. Annars finns det en lösning omm d är en kvadrat modulo $4p \Leftrightarrow d$ är en kvadrat modulo p (Prop. 22) $\Leftrightarrow \left(\frac{d}{p}\right) = 1$.

(ii) Formen $x^2 - 2y^2$ har diskriminant 8 och m.h.a. (107), (108) visar man lätt att den är den unika reducerade formen av diskriminant 8. Enligt Sats 37 finns det då precis en klass av former av diskriminant 8, så att i detta fall Sats 47 och del (i) antyder att $x^2 - 2y^2$ representerar udda primtalet p omm antingen $4p \mid 8$, som är omöjligt, eller $\left(\frac{8}{p}\right) = 1 \Leftrightarrow \left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$, enligt Sats (ii), s.38.

Under resten av lektionen, koncentrerar vi på representationsproblemet för positiv definita former. Vi skall indikera hur resultaten kan utvidgas till det indefinita fallet (där man betraktar bara primära representationer) och referera till Landaus Vorlesungen för bevis, och till och med för definitionen av en primär representation, som är lite krånglig.

Det första målet är att ge en mer precis version av Sats 47.

NOTATION : Låt $d < 0, n > 0$. Låt $h \in \mathbf{Z}$ satisfiera $h^2 \equiv d \pmod{4n}$, säg $h^2 = d + 4nk$. Den kvadratiska formen $nx^2 + hxy + ky^2$ ska betcknas med $f_{n,h}$. Notera att $d(f_{n,h}) = d$.

Lemma 49. *Låt f, g vara ekvivalenta binära former. Då finns det precist $w(f)$ matriser $M \in SL_2(\mathbf{Z})$ så att $M^T A_f M = A_g$.*

BEVIS : Eftersom $f \sim g$, finns det minst en matris N så att $N^T A_f N = A_g$.

Om N_1, N_2 är två sådana matriser, sätt $M = N_1 N_2^{-1}$ och kontrollera att $M^T A_f M = A_f$, dvs att $M \in \mathrm{Aut}(f)$. Därför, $\{MN : M \in \mathrm{Aut}(f)\}$ är mängden av alla matriser som tar f till g. Denna mängd har $w(f)$ element.

Sats 50. *Låt $f = \{a, b, c\}$ vara en positiv definit form av diskriminant $d < 0$. Låt $n > 0$. Sätt*

$$H_f(n) \overset{def}{=} \#\{h : 0 \le h < 2n,\ h^2 \equiv d\ (mod\ 4n),\ f_{n,h} \sim f\}. \tag{132}$$

Då är

$$r(n, f) = w(f) H_f(n). \tag{133}$$

Bevis : Låt X vara mängden av alla former $f_{n,h}$ så att h satisfierar villkoren i definitionen av $H_f(n)$. Denna mängd innehåller då $H_f(n)$ former. Enligt Lemma 49 finns det, för varje form $f_{n,h} \in X$, precis $w(f)$ matriser $M \in SL_2(\mathbf{Z})$ som tar f till $f_{n,h}$. Då finns det totalt $w(f)H_f(n)$ matriser som tar f till någon form i X. Låt mängden av dessa matriser betecknas med Y. För att bevisa (133), räcker det nu att etablera an 1-1 korrespondens mellan matriserna i Y och egentliga representationer av n med f.

$\Rightarrow$ Först, välj $M \in Y$, säg $M = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$. Låt $M(f) = f_{n,h} = nx^2 + hxy + ky^2$. Från transformationsformlerna (106) ser vi att

$$f(\alpha, \beta) = n. \tag{134}$$

Eftersom $\det(M) = 1$ måste $\gcd(\alpha, \beta) = 1$, så att (134) är en egentlig representation av n med f.

$\Leftarrow$ Vi måste visa att ovanstående korrespondensen har en invers, dvs vi måste bevisa följande :

Påstående : Låt $f(x, y) = n$ vara en egentlig representation av n med f. Då finns det en unik matris $M = \begin{pmatrix} x & * \\ y & * \end{pmatrix} \in SL_2(\mathbf{Z})$ så att $M \in Y$.

För att bevisa detta, först betrakta på hur många olika sätt en matris med första kolonn $\begin{pmatrix} x \\ y \end{pmatrix}$ kan kompletteras till ett element av $SL_2(\mathbf{Z})$. Euclids algoritm antyder att det finns minst ett sätt, dvs att det finns minst ett par

(u, v) av heltal så att $xu - yv = 1$. Låt $(\bar{u}, \bar{v})$ vara ett annat sådant par. Då har vi att

$$xu - yv = 1,$$
$$x\bar{u} - y\bar{v} = 1.$$

Subtraktion ger $x(\bar{u} - u) = y(\bar{v} - v)$. Men $\gcd(x, y) = 1$, så det måste finnas $t \in \mathbf{Z}$ så att $\bar{u} - u = ty$, $\bar{v} - v = tx$.

Alltså ges alla matriser i $SL_2(\mathbf{Z})$ med första kolonn $\begin{pmatrix} x \\ y \end{pmatrix}$ av $M_t = \begin{pmatrix} x & v + tx \\ y & u + ty \end{pmatrix}$, där $t \in \mathbf{Z}$.

Nu säger påståendet att det finns precist ett t så att $M_t \in Y$.

Vi har redan sett i beviset av Sats 47 i fredags att varje matris M_t tar f till en form av typen $nx^2 + hxy + ky^2$, där $h^2 \equiv d \pmod{4n}$, och $h^2 = d + 4nk$. Målet nu är att bevisa att det finns ett unikt t så att denna h också satisfierar villkoret $0 \leq h < 2n$.

Från transformationsformlerna (106) får vi att

$$\begin{array}{rcccc} h & = 2ax(v + tx) + b[x(u + ty) + y(v + tx)] + 2cy(u + ty) \\ & = & 2t(ax^2 + bxy + cy^2) & + & (2axv + bxu + byv + 2cyu) \\ & = & 2tf(x, y) & + & K \\ & = & 2nt & + & K, \end{array}$$

där konstanten K är oberoende av t. Då ser vi att det finns ett unikt t så att $0 \leq h < 2n$, q.e.d.

Anmärkning 1 : Om f är en primitiv, indefinit form av diskriminant $d > 0$, då stämmer (133) fortfarande om vi tar $w(f) = 1$. Se Vorlesungen, Satz 203, för ett bevis.

Anmärkning 2 : Ekv. (133) ger en ny algoritm för att beräkna $r(n, f)$. Först, beräknar man $w(f)$, som är lätt pga Prop. 41 och Korollarium 43. Då lösar man kongruensen $h^2 \equiv d \pmod{4n}$, och för varje lösning kontrollerar om $f_{n,h} \sim f$. Man använder reduktionsteorin för denna sista del. Notera att samma algoritm funkar i det indefinita fallet, även om reduktionsteorin är ganska mer komplicerad.

Det följer direkt från (133) att

$$r_d(n) = \sum w(f) H_f(n), \tag{135}$$

där summan är över en mängd av representanter för ekvivalensklasserna av former av diskriminant d. Eftersom $\sum H_f(n)$ är antalet lösningar till en kvadratisk kongruens, misstänker man att det borde finnas en snygg formel för $r_d(n)$ om $w(f)$ är en konstant i summan (135). Från Korollarium 43 ser vi att det är så, t.ex. när d är en fundamental diskriminant[18]. Då har vi bevisat

Sats 51. *Låt $d < 0$ vara en fundamental diskriminant. Då är*

$$r_d(n) = wN_d(n), \tag{136}$$

där

$$w = \begin{cases} 2, & om\ d < -4, \\ 4, & om\ d = -4, \\ 6, & om\ d = -3, \end{cases} \tag{137}$$

och

$$N_d(n) = \#\{h : h^2 \equiv d\ (mod\ 4n),\ 0 \le h < 2n\}. \tag{138}$$

Anmärkning : Resultatet gäller fortfarande för $d > 0$, om vi tar $w = 1$.

Vi har ett steg kvar i vår historia, nämligen att få en formel för $N_d(n)$, när $(n, d) = 1$, i termer av så kallade *Kronecker symboler* (se utdelad stencil - Satz 97 von Vorlesungen). Denna formel var startpunkten för Dirichlet i beviset av hans berömda *klasstals formel* (se utdelad stencil från Davenports bok). Detaljerna kommer på onsdag.

[18]För en komplett karakterisering av vilka d satisfierar denna egenskap, se supplementär övning nr. 13.

Lektion 16 (06/12/00)

First, we wish to describe an extension of the Jacobi symbol $\left(\frac{d}{n}\right)$ to arbitrary $n > 0$. We will assume at all times that $d \equiv 0$ or $1 \pmod 4$ and is not a perfect square[19]. We then define $\left(\frac{d}{n}\right)$ in several steps as follows :

Step 1 : $\left(\frac{d}{p}\right) := 0$ if the prime $p|d$.

Step 2 : For odd d,

$$\left(\frac{d}{2}\right) := \begin{cases} 1, & \text{if } d \equiv 1 \pmod 8, \\ -1, & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

Observe that $\left(\frac{d}{2}\right)$ equals the Jacobi symbol $\left(\frac{2}{|d|}\right)$. This follows from Sats, p.38.

Step 3 : For an odd prime p, $\left(\frac{d}{p}\right) :=$ Legendre symbol.

Step 4 : For a general $n = \prod_i p_i^{\alpha_i}$, we set

$$\left(\frac{d}{n}\right) := \prod_i \left(\frac{d}{p_i}\right)^{\alpha_i}. \tag{139}$$

REMARK : For a given d, the function $\chi(n) := \left(\frac{d}{n}\right)$ is a real character modulo d[20].

---

[19] Obviously, the reason for doing this is because we'll be interested in applications to quadratic forms, in which case d will be the discriminant of the form. In principle, the definitions we give make perfectly good sense for all $d \in \mathbf{Z}$. However, there seems to be no application for the remaining d. See also the next footnote.

[20] A character χ modulo d is called *primitive* if there does not exist a proper divisor d_1 of d and a character χ_1 modulo d_1 such that $\chi(n) = \chi_1(n)$ for all n prime to d. One also says that χ is not an *induced* character. It can be shown (see, for example, Chapter 5 of Davenport) that a real primitive character exists to the modulus d iff d is a fundamental discriminant, and that all such characters are given by the Kronecker symbols $\left(\frac{d}{n}\right)$. Recall now that, in the proof of Dirichlet's theorem, one reduces to showing that $L(1,\chi) \neq 0$ for real characters χ. In Dirichlet's original proof he first reduces further to real, primitive characters (this is easy), in other words, to Kronecker symbols. He then shows that $L(1,\chi) \neq 0$ for such characters, by relating the value of $L(1)$ to the class number $h(d)$. This is his so-called class number formula, given below in (143).

Lemma 52. *Let $d \equiv 0$ or $1 \pmod 4$, not a perfect square, and $n > 0$ with $(n,d)=1$. Then the number $N_d(n)$, as defined in (138), is given by*

$$N_d(n) = \sum_{m|n,\, m \text{ squarefree}} \left(\frac{d}{m}\right). \tag{140}$$

Bevis : Satz 97, Vorlesungen (see handout).

From Sats 51, Lemma 52 and (122) we immediately get

Theorem 53 (Dirichlet). *Let $n > 0$, and d be a fundamental discriminant with $(n,d)=1$. Then*

$$r_d(n) = w \sum_{m|n,\, m \text{ squarefree}} \left(\frac{d}{m}\right), \tag{141}$$

and

$$R_d(n) = w \sum_{m|n} \left(\frac{d}{m}\right), \tag{142}$$

where $w = 2, 4, 6, 1$ according as $d < -4, d = -4, d = -3, d > 0$ respectively.

Remark : Formula (142) was the starting point for Dirichlet's proof of his class number formula (see handout no. 10). The formula says that

$$h(d) = \begin{cases} \frac{w\sqrt{|d|}}{2\pi} L(1,\chi), & \text{if } d < 0, \\ \frac{\sqrt{d}}{\log \epsilon} L(1,\chi), & \text{if } d > 0, \end{cases} \tag{143}$$

where d is a fundamental discriminant, χ is the character $\left(\frac{d}{n}\right)$ and $\epsilon = \frac{1}{2}[t_0 + u_0\sqrt{d}]$ is a fundamental solution of Pell's equation. Note that the formula immediately implies that $L(1,\chi) > 0$.

Additional remark : Nowadays, (143) is recognised as a special case of a general class-number formula in algebraic number theory. Let K be a number field. Then the formula says that

$$h = \frac{2^{r_1}(2\pi)^{r_2} R}{w\sqrt{d}} \mathrm{Res}_{s=1} \zeta_K(s). \tag{144}$$

Here h, R, d are the *class number, regulator* and *discriminant* of K resp., r_1 (resp. $2r_2$) is the number of real (resp. complex) imbeddings of K, w is the number of roots of unity in K and ζ_K is the *Dedekind ζ-function* of K. This last object is defined, for $\mathrm{Re}(s) > 1$, as

$$\zeta_K(s) = \sum_{\mathbf{a}} \frac{1}{(N\mathbf{a})^s}, \tag{145}$$

where $\mathbf{a}$ is an ideal in O_K and $N : K \to \mathbf{Q}$ is the *norm* map. By the end of the course, you will hopefully understand what all these things mean ! Note that, if $K = \mathbf{Q}$, then $\zeta_K = \zeta$, the ordinary Riemann zeta-function[21].

Quadratic forms in more than two variables

The general theory of quadratic forms over $\mathbf{Z}$ is very hard. Over $\mathbf{Q}$ however, things are pretty much understood (here the problem of counting representations is rather meaningless, but there is still an existence question, coupled with the problem of classifying forms up to equivalence). The methods in this latter case are algebraic. The classic *Hasse-Minkowski theorem* essentially reduces the study of forms over $\mathbf{Q}$ to the study of quadratic congruences. The methods carry over in part to arbitrary fields, and the recently proved *Milnor conjecture* (1996 ?) describes this procedure precisely (it is rather abstract). Over $\mathbf{Z}$, we only get partial analogues of these results. These are most satisfying in the case of indefinite forms. The representation problem, though very hard, has essentially been solved by Siegel. But the problem of classification, for positive definite forms, remains an active

[21] In this course, we will not have time to discuss the analytic theory of the Riemann ζ-function and its' generalisations. OK, we did a little analysis in proving Dirichlet's theorem, but that's just the beginning ! That one can really do full-blooded complex analysis with ζ follows from the facts, first proven by Riemann, that ζ has a meromorphic continuation to the whole s-plane and satisfies a functional eq. relating the values at s and $1 - s$ - see (6). These facts lead to the prime number theorem. They can be generalised to Dirichlet L-functions (for primitive characters) : this was done by Hurwitz (1872) for quadratic characters and in full by de la Vallée Poussin (1896). Hecke was the first (1910s) to extend these facts to L-functions for general number fields, in particular to the Dedekind ζ-function. He also considered more general types of 'L-functions', but his methods became very complicated. Around 1940, Chevalley introduced adèles and idèles into class field theory as a method of incorporating all the diverse results into a general framework. In 1947 Tate, in his thesis, defined zeta-functions as abstract integrals over idèle groups, and proved analytic continuation and a functional equation for these. In so doing, he incorporated all the results of his predecessors, from Riemann to Hecke.

A final remark : Dirichlet's theorem on arithmetic progressions, in its' strong form as a density statement (Theorem 32.A), extends naturally to all number fields. This is proven as in the classical case, and does not require the full analytic continuation of the Dedekind L-functions.

research area. Even for positive, integral forms of discriminant 1, the situation seems to be generally hopeless. For certain dimensions, there are well-known connections to the classical sphere-packing problem and to finite simple group theory. See, for example, Serre's 'A course in arithmetic', or come to my doktorandkurs.

Here I just want to state two classical facts, and prove one of them.

Theorem 54 (Legendre/Gauss). *A positive integer n is the sum of three squares if and only if it is not of the form $4^j(8k+7)$, for some $j, k \geq 0$.*

PROOF : Serre, Ch. IV, Appendix.

Theorem 55 (Lagrange 1770). *Every positive integer is the sum of four squares.*

PROOF : Following Baker, p.39-40.

REMARK : As with most (all ?) proofs of this theorem, Baker begins by reducing to primes via the identity in the middle of p.39. To understand where this identity really comes from, one should look at Hamilton's *quaternions* H. Recall that these are defined by

$$H := \{\mathbf{R}+\mathbf{R}i+\mathbf{R}j+\mathbf{R}k : i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j\}. \quad (146)$$

H is thus a vector space of dimension 2 over $\mathbf{C}$ (or 4 over $\mathbf{R}$), which can be proven to be a (non-commutative) division algebra. A classic theorem of Frobenius ([7], Theorem 7.3.1) states that every division ring, algebraic over $\mathbf{R}$, is isomorphic to $\mathbf{R}$, $\mathbf{C}$ or H.

Let $\alpha = x + yi + zj + wk := (x, y, z, w) \in H$. The *conjugate* of α, denoted α^*, is defined by $\alpha^* := (x, -y, -z, -w)$. The following properties are easily verified :

$$[\alpha^*]^* = \alpha \quad (147)$$

$$\alpha\alpha^* = x^2 + y^2 + z^2 + w^2 \in \mathbf{R} \quad (148)$$

$$(\alpha\beta)^* = \beta^*\alpha^*. \quad (149)$$

Because of (148) we have a map $N : H \to \mathbf{R}$, called the *norm* map, given by $N(\alpha) := \alpha\alpha^*$. Eqs. (147) - (149) then easily imply that

$$N(\alpha\beta) = N(\alpha)N(\beta), \tag{150}$$

which is equivalent to the identity used in the proof of the four-squares theorem.

Algebraic theory of number fields

For the rest of today's class, I will just list the most important prerequisites from abstract algebra which will be required subsequently. No motivation or proofs will be provided, as you should have seen everything in the algebraic structures course.

DEFINITION : An element π of an integral domain R is said to be *irreducible* if every divisor of π is of the form $u\pi$, for some $u \in R^{\times}$.

DEFINITION : An element x of a domain R is said to be *factorisable* if x can be written as a product of irreducible elements in R.

We say that the domain R has the *factorisation property* (F) if every element in R is factorisable.

DEFINITION : A ring R is said to be *principally Noetherian* if R has no infinitely ascending chain of principal ideals.

Proposition 56. *If the domain R is principally Noetherian, then it has property (F).*

DEFINITION : R is called a *unique factorisation domain* (UFD) if R has property (F), and the factorisation of each element into irreducibles is unique up to units.

REMARK : A UFD is a generalisation of $\mathbf{Z}$. That $\mathbf{Z}$ is a UFD is the fundamental theorem of artithmetic.

An important class of UFDs are given by

DEFINITION : A domain R is called *Euclidean* if there is a function

$d : R\backslash\{0\} \to \mathbf{N} \cup \{0\}$ such that

(i) $\forall\, a, b \neq 0,\ d(a) \leq d(ab)$.

(ii) $\forall\, a, b\ \exists\, !\, q, r$ such that $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$.

A Euclidean domain is also a *principal ideal domain* (PID), i.e.: every ideal is principal.

EXAMPLES : $\mathbf{Z}$ is Euclidean with $d(n) = |n|$. For any field K, the polynomial ring $K[x]$ is Euclidean with $d(f) =$ degree of f.

It can be shown that if R is a UFD, then so is the polynomial ring $R[x]$. Hence, by induction, the polynomial ring $K[x_1, ..., x_n]$ in n variables over a field K is a UFD. However, it is only Euclidean if $n = 1$.

DEFINITION : An element p of a ring R is said to be *prime* if, for any $a, b \in R$, whenever $p|ab$ then either $p|a$ or $p|b$.

Proposition 57. *In any domain R, every prime element is irreducible.*

On the other hand

Proposition 58. *A domain R is a UFD if and only if R has property (F) and every irreducible element is prime.*

The following result gives an alternative ring-theoretic characterisation of the difference between the concepts of 'prime' and 'irreducible' :

Proposition 59. *(i) An element x in a ring R is prime iff $R/<x>$ is a domain.*
(ii) An element $x \in R$ is irreducible $\Leftrightarrow$ $<x>$ is a maximal principal ideal. In particular, if R is a PID, then $x \in R$ is irreducible $\Leftrightarrow$ $<x>$ is a maximal ideal $\Leftrightarrow$ $R/<x>$ is a field.

An important result now is

Theorem 60. *Every PID is a UFD.*

Proof : This is something you may not have seen before. Let R be a PID. By Prop. 58, it suffices to show that R has property (F) and that every irreducible element is prime. The latter follows immediately from Prop. 59. The former is more tricky. By Prop. 56, it suffices to show that R is principally Noetherian. This will be proven later in the context of something more general (Prop. 77(ii)).

The basic difficulty in the algebraic study of number fields is

Proposition 61. *The ring of integers in a number field is not always a UFD.*

Proof : Without explaining the term 'ring of integers' (this will come later), consider the following well-known ring :

$R = \mathbf{Z}[\sqrt{-5}]$. It can be shown that R is the ring of integers O_K in $K = \mathbf{Q}(\sqrt{-5})$. In R we have two alternative factorisations of the number 6, namely

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}). \tag{151}$$

One must check that all four numbers in these factorisations are irreducible in R. This is most easily done by considering the *norm* of each number. The norm is the function $N : R \to \mathbf{Z}$ given by

$$N[a + b\sqrt{-5}] = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2. \tag{152}$$

One checks readily that $N(xy) = N(x)N(y)$ for all $x, y \in R$. Using this, one shows irreducibility of all four numbers. It follows that all four numbers are irreducible but not prime (see Prop. 58).

Note also that R is not a PID ; for example, the ideal $< 2, 1 + \sqrt{-5} >$ is easily shown to be not principal (see supplementär övning nr. 15).

This completes the list of prerequisites.

Remark 1 : Although a ring of integers R need not be either a UFD or a PID, it is always in some sense close to being both.

First, every such R has a property called *unique factorisation of ideals*. This is because R is a *Dedekind domain*, a type of abstract commutative ring which always has this property. We will prove these facts in this course.

Second, associated to each number field K is a positve integer h_K called its *class number*. The fraction of the ideals in O_K which are principal is precisely $1/h_K$. In fact one can prove (and we will do so) that

$$O_K \text{ is a UFD} \Leftrightarrow O_K \text{ is a PID} \Leftrightarrow h_K = 1.$$

The hardest part of the theory is in fact the proof that h_K is finite, for every number field K. We will probably not have time to do this.

Remark 2 : In 1847, Lamé gave a notorious wrong proof of Fermat's Last Theorem[22]. His proof assumed implicitly that one had unique factorisation in the cyclotomic fields $\mathbf{Q}(\zeta_p)$ where p is an odd prime. It was subsequently shown that $p = 23$ is the first odd prime for which $h(\mathbf{Q}(\zeta_p)) \neq 1$[23]. Soon after, Kummer gave a correct proof of FLT for so-called *regular* prime exponents. A prime p is said to be *regular* if $p \dagger h(\mathbf{Q}(\zeta_p))$. Intuitively, it is a prime for which $\mathbf{Q}(\zeta_p))$ does not fail to be a UFD 'too badly'. There seem to be many regular primes : the only irregular ones less than 100 are 37,59,67. Nevertheless, the following remains open to this day

Conjecture. *There are infinitely many regular primes.*

Remark 3 : The main tool for computing class numbers is the analytic class number formula (144). Of course, this formula also implies that h is finite, but the usual way of proving this is by using geometric ideas developed by Minkowski (see, for example, Stewart and Tall, Ch. 6 ff). Actually, Minkowksi's motivation for developing these ideas was in order to have a 'geometric' reduction theory for (positive definite) quadratic forms of arbitrary rank $n > 2$ (see Appendix 1).

References

[22] Unlike most of the modern-day wrong proofs of FLT, this one was not the work of a nutcase amateur. Lamé was a professional mathematician working alongside such famous people as Cauchy at the Académie in Paris.

[23] I am not quite certain of the timing or sequence of events here. In one book I read that Kummer proved the failure of unique factorisation for $p = 23$ and published his proof for regular primes in 1847. In another book, I read that Cauchy did the former, and that Kummer's paper came in 1850. I also read in one place that Lamé gave a correct proof of FLT for $p = 7$ in 1839, but somewhere else that his proof had errors which were corrected by Lebesgue in 1840. The one thing which does not seem to be in any doubt is that the main breakthrough was Kummer's.

[7] I.N. Herstein, Topics in algebra, Wiley 1975.

Lektion 17 (08/12/00)

NOTATION : Under kommande lektioner ska följande notationer användas :

A,B,C,R,S,... ska beteckna ringar.
a,b,c,I,J ska beteckna (fraktionella) idéal.
p,q,... ska beteckna prima idéal.
F,K,L,... ska beteckna kroppar.
L,M,N,... ska beteckna moduler.
V,W,... ska beteckna moduler över kroppar, dvs vektor rum.
Små bokstaver, i vanlig font, ska beteckna element i dessa objekt.

KONVENTION : Alla ringar är kommutativa och har ettor.

DEFINITION : Låt R vara en ring, M en abelsk grupp. M kallas för en *modul* över R, eller en R*-modul*, om det finns en avbildning

$$\begin{array}{ccc} R \times M & \to & M \\ (r,m) & \mapsto & rm, \end{array}$$

som satisfierar följande villkor

$$\begin{array}{ll} (i) & r(m_1+m_2) = rm_1 + rm_2,\ \forall\, r \in R,\ \forall\, m_1, m_2 \in M. \\ (ii) & (rs)m = r(sm),\ \forall\, r,s \in R,\ \forall\, m \in M. \\ (iii) & (r+s)m = rm + sm,\ \forall r,s \in R,\ \forall\, m \in M. \\ (iv) & 1 \cdot m = m,\ \forall\, m \in M. \end{array}$$

EXEMPEL : (i) $R = K$ en kropp. Då kallas M för ett *vektor rum* över K.

(ii) $R = \mathbf{Z}$. En $\mathbf{Z}$-modul är just en vanlig abelsk grupp.

(iii) Låt $A \subseteq B$ vara ringar. Då kan B betraktas som en A-modul.

(iv) Låt M vara en R-modul, N en delmängd till M som är sluten under modul operationerna. Då kallas N för en R*-delmodul* till M.

Om $N \subseteq M$ är en delmodul, då får kvotgruppen M/N också strukturen av en R-modul genom att sätta

$$r(N+m) := N + rm, \qquad \forall\, r \in R,\ \forall\, m \in M.$$

Den kallas för *kvotmodulen* av M genom N.

(v) Låt A vara en ring, En delmängd $I \subseteq A$ som är en A-delmodul under ring operationerna i A kallas för ett *idéal.* Kvotet A/I är då också en A-modul. Den är också en ring.

(vi) Låt M, N vara R-moduler. Deras *direkt summa* $M \oplus N$ är, som en mängd, den kartesiska produkten $M \times N$, och den blir en R-modul genom att definiera

$$\begin{aligned} (m_1, n_1) + (m_2, n_2) &:= (m_1 + m_2, n_1 + n_2), \quad \forall\, m_1, m_2 \in M,\ \forall\, n_1, n_2 \in N, \\ r(m, n) &:= (rm, rn) \quad \forall\, r \in R,\ \forall\, m \in M,\ \forall\, n \in N. \end{aligned}$$

NOTATION : Om M är en R-modul, då skriver man ibland M/R, när detta kan inte misstolkas som en kvotmodul.

DEFINITION : Låt M vara en R-modul. Låt $X = \{x_\lambda\}_{\lambda \in \Lambda}$ vara en delmängd till M. Man säger att X *genererar* M om varje element av M kan skrivas som en ändlig linjär kombination av element från X ; dvs för varje $m \in M$, finns det $\lambda_1, ..., \lambda_n \in \Lambda$ och $r_1, ..., r_n \in R$ så att

$$m = r_1 x_{\lambda_1} + \cdots + r_n x_{\lambda_n}.$$

Man säger att M/R är *ändligt genererad* om den kan genereras av en ändlig delmängd.

EXEMPEL : (i) Ett vektor rum V/K är en ändligt genererad K-modul omm $\dim_K V < \infty$.

(ii) $\mathbf{Q}/\mathbf{Z}$ är inte ändligt genererad. För låt $p_1/q_1, ..., p_n/q_n \in \mathbf{Q}$, där $(p_i, q_i) = 1$. Antag att talet r kan skrivas som en $\mathbf{Z}$-linjär kombination av dessa, där $r = p/q$ i lägsta termer. Då finns det $t_1, ..., t_n \in \mathbf{Z}$ så att

$$\begin{aligned} &\tfrac{p}{q} = \tfrac{t_1 p_1}{q_1} + \cdots + \tfrac{t_n p_n}{q_n}, \\ &\Rightarrow \tfrac{p}{q} = \tfrac{z}{\prod_{i=1}^{n} q_i}, \text{ för något } z \in \mathbf{Z}, \\ &\Rightarrow q | \textstyle\prod_{i=1}^{n} q_i. \end{aligned}$$

Då kan p/q ej skrivas som en $\mathbf{Z}$-linjär kombination av $\{p_i/q_i\}$ om q är tillräckligt stor.

DEFINITION : En mängd $X = \{x_\lambda\}_{\lambda\in\Lambda}$ kallas för en *bas* till R-modulen M om varje element av M har ett unikt uttryck som en R-linjär kombination av element från X.

Ekvivalent, X är en bas till M om X genererar M och, för alla $\lambda_1, ..., \lambda_k \in \Lambda$,

$$r_1 x_{\lambda_1} + \cdots + r_k x_{\lambda_k} = 0 \Rightarrow r_1 = \cdots = r_k = 0. \tag{153}$$

DEFINITION : Låt M, N vara R-moduler. En avbildning $\phi : M \to N$ kallas för en R-modul *homomorfism* om

$$\forall r \in R,\ \forall m_1, m_2 \in M, \quad \phi[r(m_1 + m_2)] = r[\phi(m_1) + \phi(m_2)]. \tag{154}$$

Om ytterligare ϕ är surjektiv då kallas det för en R-modul *epimorfism*. Om ϕ är bijektiv då kallas det för en R-modul *isomorfism*. I så fall, skriver man $M \cong_R N$.

1:a isomorfism sats för moduler. *Låt M, N vara R-moduler, $\phi : M \to N$ en R-modul homomorfism. Då,*

(i) $Im(\phi)$ är en R-delmodul till N.

(ii) $Ker(\phi)$ är en R-delmodul till M.

(iii) ϕ inducerar en R-modul isomorfism $M/ker(\phi) \cong_R im(\phi)$.

BEVIS : Övning.

DEFINITION : En R-modul M sägs vara *fri* av *rang* $n \geq 0$ om $M \cong_R R^n$, den direkta summan av n kopior av R (notera att vi menar isomorfism av moduler här, trots att R^n också har en ring struktur).

Proposition 62. *(i) En R-modul M är ändligt genererad omm det finns $n \geq 0$ och en R-delmodul $I \subseteq R^n$ så att $M \cong_R R^n/I$ (här menar vi bara isomorfism av moduler igen).*

(ii) M är fri av rang n omm den har en bas som består av n element.[24]

[24] I allmänhet, låt $\aleph$ vara en kardinal. Då sägs en R-modul M vara fri av rang $\aleph$ om M har en bas av kardinalitet $\aleph$; ekvivalent, är $M \cong_R R^{\aleph}$, den direkta summan av $\aleph$ kopior av R. Notera att man tillåter bara ändliga summor av bas elementen i den direkta summan så att det är inte samma sak som den direkta produkten $\bar{R}^{\aleph}$, om $\aleph$ är en oändlig kardinal (kom ihåg att den direkta produkten $\bar{R}^{\aleph}$ är, som en mängd, den kartesiska produkten av

OBS! Modulen I i denna proposition är en R-modul, INTE ett ideal i R^n, dvs en R^n-modul.

EXEMPEL : (i) Ett vektor rum V/K är fri av rang n omm $\dim_K V = n$[25].

(ii) En modul M/R kallas för *torsion-fri* om, för alla $r \in R, m \in M$, $rm = 0 \Rightarrow m = 0$. En fundamental sats i abstrakt algebra är att, om R är en huvudidéal domän, då är varje ändligt genererad torsion-fri R-modul faktiskt fri. Det viktigaste fallet är när $R = \mathbf{Z}$[26]. Till exempel, ska vi se senare att heltalsringen i en algebraisk talkropp är ändligt genererad som en abelsk grupp, alltså en fri $\mathbf{Z}$-modul (som en delmängd till en kropp av karakteristisk noll, måste den vara torsion-fri). Men vi skall kunna bevisa frihet på ett alternativt sätt som undvikar denna allmäna satsen.

Proposition 63. *Låt A, B, C vara ringar, $A \subseteq B \subseteq C$. Om både B/A och C/B är ändligt genererade, då gäller detsamma för C/A.*

BEVIS : Låt $b_1, ..., b_m$ generera B/A, och $c_1, ..., c_n$ generera C/B. Då bevisar man lätt att $\{b_i c_j\}$ genererar C/A.

ANMÄRKNING : Om A, B, C är kroppar eller, mer allmänt, om både B/A och C/B är fria moduler, då är C/A också fri och

$$[C : A] = [C : B][B : A], \tag{155}$$

där $[M : N]$ betecknar rangen av M som en fri N-modul. Idéen av beviset är att välja baser för B/A och C/B och använda samma argument som ovan. Man måste bevisa att produkterna $\{b_i c_j\}$ är linjärt oberoende över A. Jag hoppas att ni har sett formel (155) och dess bevis för kroppar i algebraiska strukturer !

$\aleph$ kopior av R, och addition och multiplikation definieras komponentvis. Som en R-modul är den aldrig fri om $\aleph \geq \aleph_0$ (en övning !)).

Mer allmänt, kan M genereras av en delmängd X av kardinalitet $\aleph$ omm $M \cong_R R^{\aleph}/I$ för någon R-delmodul $I \subseteq R^{\aleph}$.

[25]Det kan bevisas att varje vektor rum över en kropp har en bas och att alla baser har samma kardinalitet, som kallas för *dimensionen* av rummet. Det krävs *Valaxiomet*, i formen av *Zorns lemma*, för att bevisa detta i allmänhet.

[26]Läget är mycket mer komplicerad för oändligt genererade moduler, till och med över $\mathbf{Z}$. En oändligt genererad torsion-fri abelsk grupp behöver inte ens ha en icke-trivial direkt faktor. Det finns också det notoriska exemplet av en abelsk grupp A så att $A \cong A \oplus A \oplus A$, men $A \ncong A \oplus A$. Se en godtycklig algebra bok på doktorandsnivån för vidare diskussion.

Integrala utvidningar

DEFINITION : Låt $A \subseteq B$ vara ringar. Ett element $x \in B$ kallas för *integral över A* om x satisfierar ett moniskt polynom med koefficienter från A ; dvs,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \tag{156}$$

för något $n > 0,\ a_0, ..., a_{n-1} \in A$.

Proposition 64. *Låt $A \subseteq B$ och $x \in B$. Då är följande ekvivalenta :*

(i) x är integral över A.
(ii) $A[x]/A$ är ändligt genererad.
(iii) Det finns en delring $C \subseteq B$ så att $A[x] \subseteq C$ och C/A är ändligt genererad.

BEVIS : Gavs i föreläsningen. Den svåraste delen är (iii) $\Rightarrow$ (i). Man tar en mängd av generatorer $x_1, ..., x_k$ för C/A och introducerar element $a_{ij} \in A$ genom $xx_i = \sum a_{ij}x_j$. Då har man en matris ekvation

$$(xI_k - M)\begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ x_k \end{pmatrix} = 0, \tag{157}$$

där $M = (a_{ij})$. Sätt $N = xI_k - M$, och multiplicera båda sidor av (157) med adj N, så att man får att $(\det N)c = 0$ för alla $c \in C$. Speciellt, kan man ta $c = 1$, som betyder att $\det N = 0$. Detta ger ett moniskt polynom över A som satisfieras av x.

DEFINITION : (i) Låt $A \subseteq B$. Mängden av element i B som är integrala över A kallas för det *integrala höljet av A i B* och betecknas $\bar{A}^B$.
(ii) B sägs vara en *integral utvidning av A*, eller *integral över A*, om $\bar{A}^B = B$.
(iii) A sägs vara *integralt sluten i B* om $\bar{A}^B = A$.
(iv) En domän A kallas helt enkelt för *integralt sluten* om $\bar{A}^K = A$, där K är kvotkroppen av A.

VIKTIGT EXEMPEL : $\mathbf{Z}$ är integralt sluten (kvotkroppen är $\mathbf{Q}$). För låt

$x \in \mathbf{Q}$ vara integral över $\mathbf{Z}$. Säg att $x = p/q$ i lägsta termer, och att x satisfierar det moniska polynomet

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0, \text{ där } a_i \in \mathbf{Z}.$$

Multiplicera båda sidor med q^{n-1} och man får att $p^n/q \in \mathbf{Z} \Rightarrow q = 1$ (ty $(p,q) = 1) \Rightarrow x \in \mathbf{Z}$.

Nästa resultat följer (med något arbete !) från Prop. 63 och 64 :

Sats 65. *(i) Låt $A \subseteq B \subseteq C$. Om B/A och C/B är integrala, då gäller detsamma för C/A.*
(ii) Låt $A \subseteq B$. Då är $\bar{A}^B$ en ring som innehåller A. Dessutom är $\bar{A}^B$ integralt sluten i B.

Mängden som består av alla lösningar till alla möjliga moniska polynom över en ring A kallas för DET *integrala höljet* av A och betecknas med $\overline{A}$. Det följer från Sats 65 att $\bar{A}$ har en väl-definierad ring struktur.

Exempel : $\overline{\mathbf{C}} = \mathbf{C}$. Detta är Algebrans Fundamentalsats.

Kroppar

När man betraktar kroppsutvidningar $K \subseteq L$, brukar man använda man ordet '*algebraisk*' i stället för 'integral'. Alltså används termerna *algebraisk utvidning, algebraiskt hölja, algebraiskt sluten* i stället för motsvarande termerna ovan.

Proposition 66. *Låt $K \subseteq L$ vara kroppar. Då är $\bar{K}^L$ en delKROPP av L.*

Bevis : (se också Lemma 80) Vi vet redan från Sats 65(ii) att $\bar{K}^L$ är en delring till L. Låt $0 \neq x \in \bar{K}^L$. Det kvarstår att bevisa att $x^{-1} \in \bar{K}^L$. Låt

$$x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0 = 0$$

vara ett moniskt polynom över K av minimal grad som satisfieras av x. Vi måste ha $k_0 \neq 0$ - annars skulle x vara en faktor av den vänstra sidan, som kunde tas ut för att få ett moniskt polynom av mindre grad som satisfieras av x. Dela nu båda sidor med $k_0 x^n$ så får man att

$$(x^{-1})^n + \frac{k_1}{k_0}(x^{-1})^{n-1} + \cdots + \frac{k_{n-1}}{k_0}x^{-1} + \frac{1}{k_0} = 0,$$

som antyder att $x^{-1} \in \bar{K}^L$, v.s.v.

Definition : Om $K/\mathbf{Q}$ är en kroppsutvidning med $[K : \mathbf{Q}] < \infty$, då kallas K för en *talkropp*. Ett element av en talkropp kallas för ett *algebraiskt tal*.

Algebrans fundamentalsats antyder att $\overline{\mathbf{Q}} \subseteq \mathbf{C}$, och är faktiskt en delkropp av $\mathbf{C}$ enligt Prop. 66. Ett komplext tal $z \in \mathbf{C}$ är ett algebraiskt tal omm

$$z \in \overline{\mathbf{Q}} = \bigcup_{K \text{ en talkropp}} K.$$

Definition : Ett komplext tal z som inte är algebraiskt kallas för *transcendental*. Vi skall diskutera transcendentala tal senare. Under kommande lektioner blir algebraiska tal vårt största intresse.

Lektion 18 (11/12/00)

NOTATION : $K(x)$ denotes the field obtained by adjoining an indeterminate x to the field K. That is,

$$K(x) = \left\{ \frac{p(x)}{q(x)} : p, q \in K[x], \ q \neq 0 \right\}. \tag{158}$$

In other words, $K(x)$ is the quotient field of $K[x]$.

First, we need to recall some general facts which you learned in algebraic structures :

Let $K \subseteq L$ be fields, $\alpha \in L$ which is algebraic over K. Let

$$\mathcal{I} = \{p(x) \in K[x] : p(\alpha) = 0\}. \tag{159}$$

Then $\mathcal{I}$ is an ideal in $K[x]$, hence a principal ideal. Hence there exists a unique monic polynomial $p_0(x) \in K[x]$ which is irreducible over K and generates the ideal $\mathcal{I}$. It is called the *minimal polynomial* of α over K. We have

$$K[\alpha] = K(\alpha) \cong K[x]/\mathcal{I}. \tag{160}$$

Moreover, if $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ are the roots of $p_0(x)$ in some extension field of K over which p_0 splits, then all α_i are distinct and each has minimal polynomial p_0.

Okay, that's enough facts. An important technical result about number fields[27] is the following :

Theorem 67. *Let $K \subseteq L$ be number fields. Then there exists $\alpha \in L$ such that $L = K(\alpha)$.*

REMARK : In other words, there exists $\alpha \in L$ such that the minimal polynomial of α over K has degree $[L : K]$.

PROOF : Since L/K is a finite-dimensional vector space, there certainly exists a finite set of elements $\alpha_1, ..., \alpha_n \in L$ such that $L = K(\alpha_1, ..., \alpha_n)$ - for

[27] In fact, the result applies to any pair of infinite fields, as long as one is a finite extension of the other. In particular, it applies to fields of characteristic zero (since these contain a copy of $\mathbf{Q}$). This will become clear from the proof.

example, choose a basis of L/K. Hence, it suffices to prove the result when $L = K(\alpha, \beta)$, for some PAIR of elements α, β, because we then just proceed by induction on the number of elements in a generating set.

Let $p(x), q(x)$ be the minimal polynomials of α, β resp. over K, say of degrees n, m resp. Over $\mathbf{C}$ we have splittings

$$p(x) = \prod_{i=1}^{n} (x - \alpha_i), \quad \alpha = \alpha_1, \ \alpha_i \text{ distinct},$$

$$q(x) = \prod_{j=1}^{m} (x - \beta_j), \quad \beta = \beta_1, \ \beta_j \text{ distinct}.$$

For each pair of indices $(i, j) \neq (1, 1)$, there is at most one solution $x \in L$ to the equation

$$\alpha_i + x\beta_j = \alpha + x\beta. \tag{161}$$

As K is an infinite field, we can pick $\gamma \in K$ which does not satisfy any of these equations. Put $\theta = \alpha + \gamma\beta$. We claim that $L = K(\theta)$.

To prove this, it suffices to prove that $\beta \in K(\theta)$, because then $\alpha = \theta - \gamma\beta \in K(\theta)$ and so $L = K(\alpha, \beta) \subseteq K(\theta)$. To prove that $\beta \in K(\theta)$ it suffices to show that the minimal polynomial of β over $K(\theta)$ has degree one.

So consider the polynomials $q(t), r(t) \in K(\theta)[t]$ defined by

$$q(t) := q(x)|_{x=t},$$
$$r(t) := p(\theta - \gamma t).$$

Observe that $q(\beta) = r(\beta) = 0$. Hence the minimal polynomial of β over $K(\theta)$ must be a common divisor of $q(t)$ and $r(t)$. We claim that the gcd of these polynomials has degree one ; equivalently, they have no common root in $\mathbf{C}$ other than β.

So suppose that $q(\xi) = r(\xi) = 0$ with $\xi \neq \beta$:

On the one hand, ξ is a root of $q(t)$ so

$$\xi = \beta_j, \quad \text{for some } j, \ 2 \leq j \leq m. \tag{162}$$

On the other hand, $r(\xi) = p(\theta - \gamma\xi) = 0$, so

$$\theta - \gamma\xi = \alpha_i, \quad \text{for some } i, \ 1 \leq i \leq m. \tag{163}$$

From (162) and (163) we deduce that γ satisfies one of the equations (161), a contradiction. This completes the proof.

EMBEDDINGS

DEFINITION : Let K be a number field. An injective field homomorphism $\phi : K \to \mathbf{C}$ is called an *embedding* of K.

NOTATION : Let $\phi : K \to \mathbf{C}$ be an embedding. The *fixed field* of ϕ, denoted F_ϕ, is defined by

$$F_\phi = \{x \in K : \phi(x) = x\}. \tag{164}$$

That F_ϕ IS a field follows immediately from the fact that ϕ is a field homomorphism.

Proposition 68. *Let K be any number field. Then*

$$\mathbf{Q} = \bigcap_{\phi \text{ an embedding of } K} F_\phi. \tag{165}$$

PROOF : First we prove that $\mathbf{Q} \subseteq$ r.h.s. Let ϕ be an embedding of K. Then $\phi(1) = 1$ since ϕ is injective. Since ϕ is additive, we thus have $\phi(n) = n$ for all $n \in \mathbf{Z}$. Finally, $\phi\left(\frac{m}{n}\right) = \frac{\phi(m)}{\phi(n)} = \frac{m}{n}$.

The proof of the reverse inclusion is postponed until after the next result, which characterises all embeddings of K.

Proposition 69. *Let K be a number field, say $[K : \mathbf{Q}] = n$. Pick $\alpha \in K$ so that $K = \mathbf{Q}(\alpha)$. Let $p(x)$ be the minimal polynomial of α over $\mathbf{Q}$. Over $\mathbf{C}$, let $p(x)$ split as*

$$p(x) = \prod_{i=1}^{n}(x - \alpha_i), \quad \alpha = \alpha_1, \ \alpha_i \text{ distinct.}$$

Let ϕ be an embedding of K. Then $\phi(\alpha) = \alpha_i$ for some i, and this choice completely determines ϕ. In particular, K has precisely n embeddings.

PROOF : That $\phi(\alpha) =$ some α_i follows from the fact that

$$\phi(0) = 0 = \phi(p(\alpha)) = p(\phi(\alpha)),$$

which implies that $\phi(\alpha)$ is a root of $p(x)$. Now suppose $\phi(\alpha)$ is given. Any element of K has a unique representation as a polynomial in α of degree $< n$, with coefficients in $\mathbf{Q}$. Since $\mathbf{Q} \subseteq F_\phi$ and ϕ is a field homomorphism, we have that

$$\phi\left(\sum a_i \alpha^i\right) = \sum a_i (\phi(\alpha))^i, \qquad (a_i \in \mathbf{Q}),$$

which proves that ϕ is completely determined by $\phi(\alpha)$.

Definition : An embedding ϕ of the number field K is called *real* if $\phi(K) \subset \mathbf{R}$. Otherwise, ϕ is called *complex*.

The number of real (resp. complex) embeddings of K is denoted by r_1 (resp. $2r_2$). From Prop. 69 we see that

$$\begin{aligned} r_1 &= \#\text{ real embeddings} = \#\{i : \alpha_i \in \mathbf{R}\}, \\ 2r_2 &= \#\text{ complex embeddings} = \#\{i : \alpha_i \notin \mathbf{R}\}. \end{aligned} \tag{166}$$

Proof of prop. 68 (ctd.) : Let $[K : \mathbf{Q}] = n$, say $K = \mathbf{Q}(\alpha)$. Let $\theta \in K$. Then θ has a unique expression as a polynomial in α, of degree $< n$, with rational coefficients, say

$$\theta = f(\alpha) = \sum_{i=0}^{r} a_i \alpha^i, \qquad \text{where } r < n.$$

Let ϕ be an embedding of K, and suppose that $\phi(\theta) = \theta$. In the notation of Prop. 69, there is some i, $1 \le i \le n$, such that $\phi(\alpha) = \alpha_i$. Hence,

$$f(\alpha) = \theta = \phi(\theta) = \phi(f(\alpha)) = f(\phi(\alpha)) = f(\alpha_i). \tag{167}$$

Now let $g(x) := f(x) - \theta$, so that g is polynomial of degree r with coefficients in K. From (167) we see that, if θ is fixed by every embedding of K, then $g(\alpha_i) = 0$ for $i = 1, ..., n$. Thus g has at least n distinct roots, but as g is of degree $r < n$, this is only possible if $g \equiv 0$, the zero polynomial. Thus $f(x) = \theta$ is a constant polynomial with rational coefficients, so that $\theta \in \mathbf{Q}$. This completes the proof.

Definition : A number field K is said to be *Galois* over $\mathbf{Q}$ if $\phi(K) = K$ for every embedding ϕ of K.

If $K/\mathbf{Q}$ is Galois, then the embeddings of K form a group of field automorphisms of K under composition. This group is called the *Galois group* of K over $\mathbf{Q}$ and is denoted $\mathrm{Gal}(K/\mathbf{Q})$.

THE DISCRIMINANT

DEFINITION : Let K be a number field, $[K : \mathbf{Q}] = n$. Let $\phi_1, ..., \phi_n$ be the embeddings of K, in some order. Let $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ be a basis for K as a vector space over $\mathbf{Q}$. The *discriminant of the basis* $\mathcal{B}$ is defined and denoted by

$$\Delta(\alpha_1, ..., \alpha_n) := [\det(\phi_i(\alpha_j))]^2 . \tag{168}$$

Proposition 70. *The discriminant of a basis is well-defined, i.e.: it does not depend on the ordering of the ϕ_i or of the α_i.*

PROOF : Choosing a different ordering of the ϕ's corresponds to a permutation π of the rows of the matrix $A = (\phi_i(\alpha_j))$. If A^π denotes the permuted matrix, then we all know from linear algebra that

$$\det A^\pi = (-1)^{\mathrm{sgn}\pi} \det A. \tag{169}$$

Since, for Δ, we take the square of the determinant, we see that the result is independent of the permutation π. The same argument applies to a permutation of the α_i - this corresponds to a permutation of the columns in A, q.e.d.

Theorem 71. *The determinant of any basis is a non-zero rational number.*

PROOF : First, we show that $\Delta \in \mathbf{Q}$. We will only do this under the extra assumption that $K/\mathbf{Q}$ is Galois[28]. In this case, the proof is easy. By Prop. 68, it suffices to show that $\phi(\Delta) = \Delta$ for every embedding ϕ of K. But in the Galois case, application of ϕ serves only to reorder the rows of the matrix defining Δ. The argument used to prove Prop. 70 implies that Δ is thereby left unchanged.

The second part is to show that $\Delta \neq 0$. This part involves two steps :

[28]In the general case, one first notes that the determinant (170) is a symmetric polynomial in the θ_i. One then applies a result on symmetric polynomials to conclude that this determinant is a rational number (see handout nr. 12). Finally, one uses (173) to conclude that the discriminant of ANY basis is rational.

Step 1 : We show that $\Delta \neq 0$ for a special type of basis. We pick $\theta \in K$ such that $K = \mathbf{Q}(\theta)$ and consider the basis $\{1, \theta, ..., \theta^{n-1}\}$. Let $\theta = \theta_1, \theta_2, ..., \theta_n$ be the (distinct) roots of the minimal polynomial of θ over $\mathbf{Q}$. Let ϕ_i be the unique embedding (see Prop. 69) such that $\phi_i(\theta) = \theta_i$. Then

$$\Delta(1, \theta, ..., \theta^{n-1}) = \begin{vmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{vmatrix}^2 . \tag{170}$$

But this determinant is of Vandermonde type and so we have that

$$\Delta(1, \theta, ..., \theta^{n-1}) = \left[\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right]^2 \neq 0, \tag{171}$$

since the θ_i are distinct.

Step 2 : We give a formula relating the discriminants of two different bases. So let $\mathcal{B}_1 = \{\alpha_1, ..., \alpha_n\}$, $\mathcal{B}_2 = \{\beta_1, ..., \beta_n\}$ be two different bases for $K/\mathbf{Q}$. Let $M = (m_{ij}) \in GL_n(\mathbf{Q})$ be the change of basis matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$, i.e.:

$$\beta_i = \sum_{j=1}^{n} m_{ij} \alpha_j .$$

Applying an embedding ϕ_i we obtain that

$$\phi_i(\beta_j) = \phi_i \left(\sum_{k=1}^{n} m_{jk} \alpha_k \right) = \sum_{k=1}^{n} m_{jk} \phi_i(\alpha_k). \tag{172}$$

From (172) we see that the matrices $B = (\phi_i(\beta_j))$ and $A = (\phi_i(\alpha_j))$ are related by

$$B = AM^T.$$

From this, it follows immediately that

$$\Delta(\beta_1, ..., \beta_n) = (\det M)^2 \Delta(\alpha_1, ..., \alpha_n). \tag{173}$$

In particular, since $\det M \neq 0$, we see that one discriminant is non-zero if and only if the other is. Since we have in Step 1 produced at least one basis with a non-zero discriminant, it follows that the discriminant of any basis is non-zero. This completes the proof of Theorem 71.

REMARK : The discriminant of a basis need not be a POSITIVE rational number. For example, let d be an integer which is not a perfect square, and take $K = \mathbf{Q}(\sqrt{d})$. Then $[K : \mathbf{Q}] = 2$ since the minimal polynomial of $\sqrt{d}$ over $\mathbf{Q}$ is $x^2 - d = 0$. The roots of this equation are $\pm\sqrt{d}$, so K has two embeddings completely determined by

$$\phi_1(\sqrt{d}) = \sqrt{d}, \qquad \phi_2(\sqrt{d}) = -\sqrt{d}.$$

In particular, $K/\mathbf{Q}$ is Galois. Now consider the basis $\{1, \sqrt{d}\}$ of K as a $\mathbf{Q}$-vector space. The discriminant of this basis is given by

$$\Delta(1, \sqrt{d}) = \begin{vmatrix} \phi_1(1) & \phi_1(\sqrt{d}) \\ \phi_2(1) & \phi_2(\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d, \tag{174}$$

which is > 0 iff $d > 0$.

THE RING OF INTEGERS

DEFINITION : Let K be a number field. The integral closure of $\mathbf{Z}$ in K is called the *ring of integers of* K, and is denoted O_K. To avoid confusion, elements of $\mathbf{Z}$ (i.e.: ordinary integers) are often called *rational integers* in algebraic number theory.

Proposition 72. *(i) O_K IS a subring of K containing $\mathbf{Z}$.*
(ii) $O_K \cap \mathbf{Q} = \mathbf{Z}$.
(iii) Let $\alpha \in K$. Then there exists $0 \neq n \in \mathbf{Z}$ such that $n\alpha \in O_K$.

PROOF : (i) Follows from the more general Sats 65(ii).

(ii) Follows from the fact that $\mathbf{Z}$ is integrally closed (proven last day).

(iii) α is algebraic over $\mathbf{Q}$, hence satisfies some polynomial with rational coefficients, hence (by clearing denominators) some polynomial with integer coefficients, say

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0, \qquad a_i \in \mathbf{Q}, a_n \neq 0.$$

Multiply through by a_n^{n-1} and you will get an equation of the form

$$(a_n\alpha)^n + b_{n-1}(a_n\alpha)^{n-1} + \cdots + b_1(a_n\alpha) + b_0 = 0,$$

for some integers b_i. This says that $a_n\alpha$ satisfies a monic polynomial over $\mathbf{Z}$, hence lies in O_K.

REMARK : From (iii) of Prop. 72, it follows that there exist bases of $K/\mathbf{Q}$ consisting of elements of O_K. Any such basis of $K/\mathbf{Q}$ is called an *integral basis*[29].

The main result of today's lecture is the following theorem giving the structure of O_K as an additive group.

Theorem 73. *O_K is a free abelian group of rank $[K : \mathbf{Q}]$.*

PROOF : Let $[K : \mathbf{Q}] = n$. Let $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ be an integral basis for K. Let ϕ be an embedding of K. Since each α_i satisfies a monic polynomial over $\mathbf{Z}$, by the usual type of argument the same is true of each $\phi(\alpha_i)$. It follows that $\Delta(\mathcal{B}) \in \overline{\mathbf{Z}}$, the integral closure of $\mathbf{Z}$ in $\mathbf{C}$. But Theorem 71 says that $\Delta(\mathcal{B}) \in \mathbf{Q}^\times$. Hence, $\Delta(\mathcal{B}) \in \mathbf{Q}^\times \cap \overline{\mathbf{Z}} = \mathbf{Z}^\times$.

It follows that there exists an integral basis $\mathcal{B}_0 = \{\theta_1, ..., \theta_n\}$ for which $|\Delta(\mathcal{B}_0)|$ is minimal. We claim that any such $\mathcal{B}_0$ is also a $\mathbf{Z}$-basis for O_K.

First, since the θ_i form a $\mathbf{Q}$-basis of K, in particular they are linearly independent over $\mathbf{Q}$, hence over $\mathbf{Z}$ also. It remains to show that they generate the $\mathbf{Z}$-module O_K.

We argue by contradiction. So suppose there exists $w \in O_K$, $w \notin \mathbf{Z}\theta_1 \oplus \cdots \oplus \mathbf{Z}\theta_n$. Since $\mathcal{B}_0$ is a $\mathbf{Q}$-basis for K, there must exist rational numbers $r_1, ..., r_n$ such that

$$w = r_1\theta_1 + \cdots + r_n\theta_n.$$

WLOG, $r_1 \notin \mathbf{Z}$. Let $z_1 := \lfloor r_1 \rfloor$, $r_1 = z_1 + r$, where $0 < r < 1$. Define a new integral basis $\mathcal{B}_1 = \{\psi_1, ..., \psi_n\}$ by

$$\psi_1 = w - r_1\theta_1, \qquad \psi_i = \theta_i, \;\; i = 2, ..., n.$$

It is easily verified that $\mathcal{B}_1$ IS, in fact, an integral basis for K. The change

[29]Do not confuse an integral basis with a basis for O_K as a free $\mathbf{Z}$-module (see Theorem 73). A basis of the latter type is always an integral basis, but not conversely. In fact, Prop. 74 gives the precise condition for an integral basis to be a $\mathbf{Z}$-basis of O_K.

of basis matrix from $\mathcal{B}_0$ to $\mathcal{B}_1$ is given by

$$M = \begin{pmatrix} r & r_2 \cdots r_n \\ \vdots & \\ 0 & I_{n-1} \\ \vdots & \end{pmatrix},$$

so that $\det M = r$. By (173), we see that $\Delta(\mathcal{B}_1) = r^2\Delta(\mathcal{B}_0)$, which contradicts the minimality of $|\Delta(\mathcal{B}_0)|$. This completes the proof of the theorem.

Definition : The positive integer given by the minimum absolute value of the discriminant of an integral basis is called, quite simply, the *discriminant of* K, and is denoted d_K.

The discriminat of a number field is an important invariant. Some of its' properties will be discussed in due course, either in the main text or in the form of footnotes.

Proposition 74. *Let* $\{\alpha_1, ..., \alpha_n\}$ *be an integral basis for* K*. Then* $|\Delta(\alpha_1, ..., \alpha_n)| = d_K$ *if and only if* $\{\alpha_1, ..., \alpha_n\}$ *is a* $\mathbf{Z}$*-basis for* O_K*.*

Proof : The 'only if' part follows from the proof of Theorem 73.

For the 'if' part, let $\mathcal{B}_0$ be any integral basis which is also a $\mathbf{Z}$-basis for O_K. Let $\mathcal{B}_1$ be a $\mathbf{Z}$-basis for O_K for which $|\Delta(\mathcal{B}_1)| = d_K$.

Since $\mathcal{B}_0$ and $\mathcal{B}_1$ are both $\mathbf{Z}$-bases for O_K, the change of basis matrix M from $\mathcal{B}_0$ to $\mathcal{B}_1$ must have integer entries, and the same is true of M^{-1}. It follows that $\det M = \pm 1$. From (173), it now follows that $|\Delta(\mathcal{B}_1)| = |\Delta(\mathcal{B}_0)| = d_K$. q.e.d.

Lektion 20 (15/12/00)

Ideal

Notation : Låt R vara en ring. Mängden av alla ideal i R ska betecknas med $I(R)$. Mängden av prima ideal (se definitionen nedan) i R ska betecknas $\mathrm{Spec}(R)$, och kallas för *spektrum av R*. Denna terminologi är mest vanlig i algebraisk geometri.

Definition : Låt $\mathbf{a},\mathbf{b} \in I(R)$. Sätt

$$\mathbf{ab} := \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathbf{a}, b_i \in \mathbf{b} \right\}. \tag{175}$$

Detta är också ett ideal som kallas för *produkten* av idealen $\mathbf{a}$ och $\mathbf{b}$.

Proposition 75. *(i) Ideal multiplikation ger $I(R)$ strukturen av en kommutativ monoid med enhet (unity) R själv.*
(ii) $\mathbf{ab} \subseteq \mathbf{a} \cap \mathbf{b}$.

Bevis : Del (i) säger att

1. $\mathbf{ab} = \mathbf{ba}$.
2. $(\mathbf{ab})\mathbf{c} = \mathbf{a}(\mathbf{bc})$.
3. $R\mathbf{a} = \mathbf{a}R = \mathbf{a}$.

Alla tre egenskaper följer lätt från definitionen. Detsamma gäller för del (ii).

Ett av våra stora mål är att utvidga $I(R)$ till en grupp, dvs att införa 'inverser' av ideal, i fallet där $R = O_K$ för någon talkropp K. Vi återkommer till detta.

Definition : (i) Ett ideal I i en ring R kallas för *prim* om, för alla $x, y \in R$, $xy \in I \Rightarrow x \in I$ eller $y \in I$.
(ii) Idealet I kallas för *maximalt* om $I \neq R$ och, för varje ideal J så att $I \subseteq J \subseteq R$, antingen $J = I$ eller $J = R$.

Proposition 76. *(i) I prim $\Leftrightarrow$ R/I är en domän. Speciellt, R är en*

domän omm $\{0\}$ är ett primt ideal.
(ii) I maximal $\Leftrightarrow R/I$ är en icke-trivial kropp. Speciellt, R är en icke-trivial kropp omm $\{0\}$ är ett maximalt ideal.
(iii) Om $\mathbf{p}$ är ett primt ideal och $\mathbf{a}_1,...,\mathbf{a}_n$ är godtyckliga ideal så att $\mathbf{p} \supseteq \mathbf{a}_1 \cdots \mathbf{a}_n$, då måste $\mathbf{p} \supseteq \mathbf{a}_i$ för något i.

Bevis : (i) och (ii) är triviala. För (iii), antag att ingen av $\mathbf{a}_1, ..., \mathbf{a}_{n-1} \subseteq \mathbf{p}$. Välj $x_i \in \mathbf{a}_i - \mathbf{p}$. Låt nu $y \in \mathbf{a}_n$. Eftersom $x_1 \cdots x_{n-1} y \in \mathbf{a}_1 \cdots \mathbf{a}_n \subseteq \mathbf{p}$, så måste minst en av termerna i produkten vara i $\mathbf{p}$, enligt definitionen av ett prim idéal. Därför måste faktiskt $y \in \mathbf{p}$, v.s.v.

Propositionen säger speciellt att varje maximalt ideal är prim. Existens av maximala ideal (och därför prima ideal) i en godtyclkig ring följer från Zorn's Lemma - efterom om $I_1 \subseteq I_2 \subseteq \cdots$ utgör en växande följd av ideal, då är deras union $\cup I_n$ också ett ideal.

Definition : En ring R kallas för *Noetersk* om R innehåller ingen oändlig strängt växande kedje av ideal.

Alternativt, säger man att R är Noetersk om varje växande kedje av ideal i A *stabiliserar.* Dvs, om $I_0 \subseteq I_1 \subseteq \cdots$ utgör en växande kedje av ideal i R, då måste det finnas $N > 0$ så att $I_m = I_n$ för alla $m, n \geq N$.

Definition : *Dimensionen* av en Noetersk ring R är längden n av den längsta strängt växande kedjen $\mathbf{p}_0 \subset \mathbf{p}_1 \subset \cdots \subset \mathbf{p}_n$ av prima ideal i R.

Exempel : (i) Låt R vara en domän. $\mathrm{Dim}(R) = 0 \Leftrightarrow A$ är en kropp.

(ii) Låt R vara en domän igen. $\mathrm{Dim}(R) = 1 \Leftrightarrow$ varje icke-noll primt ideal i A är maximalt.

(iii) Dim $K[x_1, ..., x_n] = n$ (se suppl. öv. nr. 17). Terminologin 'dimension' kommer från algebraisk geometri. Dimensionen av ett affint varietet V över en kropp K, som en hyperyta, är lika med den algebraiska dimensionen av sin koordinat ring $K[V]$. Detta är faktiskt definitionen av $\dim(V)$ för kroppar utom $\mathbf{R}$ eller $\mathbf{C}$.

Definition : En integralt sluten, Noetersk domän av dimension ett kallas för en *Dedekind domän.*

Viktigt exempel : $\mathbf{Z}$ är en Dedekind domän.

Definition : Låt R vara en ring och M en R-modul. Då kallas M för en *Noetersk R-modul* om varje växande följd $M_1 \subseteq M_2 \subseteq \cdots$ av R-delmoduler till M stabiliserar.

Obs! EN ring R är Noetersk omm den är en Noetersk R-modul.

Proposition 77. *(i) Låt A vara en ring. En A-modul M är Noetersk omm varje delmodul till M är ändligt genererad.*
(ii) Speciellt, en ring A är Noetersk omm varje ideal i A är ändligt genererad.

Bevis : Vi bevisar (i) ; då följer (ii) direkt.

$\Rightarrow$ Antag att M är Noetersk och att $L \subseteq M$ är en delmodul som inte är ändligt genererad. Välj $x_0 \in L$. Då genereras inte L av x_0 så välj $x_1 \in L - (x_0)$. På samma sätt, genereras L inte av x_0, x_1, så vi kan välja $x_2 \in L - (x_0, x_1)$. Om vi fortsätter den här processen, då får vi en oändlig, strängt växande följd

$$(x_0) \subset (x_0, x_1) \subset (x_0, x_1, x_2) \subset \cdots$$

av delmoduler till M - motsägelse.

$\Leftarrow$ Antag att varje delmodul till M är ändligt genererad, och låt

$$L_0 \subseteq L_1 \subseteq \cdots \tag{176}$$

vara en växande följd av delmoduler till M. Låt $L = \cup L_i$. Då är L också en delmodul till M, alltså måste vara ändligt genererad. Låt $x_1, ..., x_n$ vara en mängd av generatorer. Det måste finnas ett $N > 0$ så att alla $x_i \in L_N$. I så fall stabiliserar kedjan (176) vid L_N.

Exempel : En PID är alltid Noetersk eftersom varje ideal genereras av ett enda element. Med detta i hand, kan vi avsluta beviset av Sats 60.

Proposition 78. *Låt A vara en ring, M en A-modul, N en A-delmodul till M. Då är M Noetersk omm både N och M/N är Noeterska.*

Bevis : $\Rightarrow$ Antag först att M är Noetersk.

Steg 1 : M/N är Noetersk.

Låt $L_0 \subseteq L_1 \subseteq \cdots$ vara en växande kedje av delmoduler till M/N. Då utgör $\pi^{-1}(L_0) \subseteq \pi^{-1}(L_1) \subseteq \cdots$ en växande kedje av delmoduler till M, där $\pi : M \to M/N$ är den naturliga projektionen. Eftersom M är Noetersk, måste den senare kedjen stabilisera. Men $\pi(\pi^{-1}(L_n)) = L_n$ för varje n, så att den ursprunliga kedjen i M/N stabiliserar också.

Steg 2 : N är Noetersk.

Låt $L_0 \subseteq L_1 \subseteq \cdots$ vara en växande kedje av delmoduler till N. Men varje L_n är också en delmodul till M, så kedjan måste stabilisera.

$\Leftarrow$ Antag nu att både N och M/N är Noeterska.

Låt $L_0 \subseteq L_1 \subseteq \cdots$ vara en växande kedje av delmoduler till M. Vi måste visa att kedjen stabiliserar. Sätt $\mathbf{a}_k = L_k \cap N$ och $\mathbf{b}_k = \pi(L_k)$. Då utgör $\mathbf{a}_0 \subseteq \mathbf{a}_1 \subseteq \cdots$ och $\mathbf{b}_0 \subseteq \mathbf{b}_1 \cdots$ växande kedjor av delmoduler i N och M/N respektivt. Eftersom båda dessa moduler är Noeterska så måste båda kedjor stabilisera, dvs det finns $N_1, N_2 > 0$ så att

$$\mathbf{a}_m = \mathbf{a}_n \ \forall\, m, n \geq N_1, \quad \mathbf{b}_m = \mathbf{b}_n \ \forall\, m, n \geq N_2.$$

Vi påstår nu att $L_m = L_n$ för alla $m, n \geq \max\{N_1, N_2\}$.

Så låt $m > n \geq \max\{N_1, N_2\}$. Låt $x \in L_m$; vi måste visa att $x \in L_n$.

Först har vi att $\pi(x) \in \mathbf{b}_m = \mathbf{b}_n$. Därför finns det $y \in L_n$ så att $\pi(y) = \pi(x)$, som antyder att $x - y \in \mathbf{a}_m$. Men $\mathbf{a}_m = \mathbf{a}_n$, så $x - y = z$ för något $z \in \mathbf{a}_n \subseteq L_n$. Därför är $x = y + z \in L_n$, som behövdes. Detta avslutar beviset.

Korollarium 79. *(i) Låt A vara en Noetersk ring, M en ändligt genererad A-modul. Då är M en Noetersk A-modul.*

Bevis : Från Prop. 62, vet vi att det finns $n > 0$ och ett A-modul $I \subseteq A^n$ så att $M \cong_A A^n/I$.

Steg 1 : A^n är en Noetersk A-modul.

Eftersom $A^n \cong A \oplus A^{n-1}$ räcker det att bevisa att, om M, N är två Noeterska A-moduler, så också är $M \oplus N$. Då skulle man göra en induktion på n.

Så låt M, N vara Noeterska A-moduler. Avbildningen $m \mapsto (m, 0)$ identifierar M med en delmodul M^* till $M \oplus N$. Det är också klart att $(M \oplus N)/M^* \cong N$. Då följer det från Prop. 78 att $M \oplus N$ är Noetersk.

Steg 2 : Så A^n är Noetersk, och vår ändligt genererad modul M är isomorfisk med A^n/I, för någon A-delmodul I. Då följer det från Prop. 78 att M är också Noetersk.

Lemma 80. *Låt $A \subseteq B$ vara domäner, B integral över A. Då är B en kropp $\Leftrightarrow$ A är en kropp.*

Bevis : $\Rightarrow$ Antag att B är en kropp, och låt $0 \neq x \in A$. Vi vet att $x^{-1} \in B$; vi måste visa att $x^{-1} \in A$. Efterom B/A är integral, då satisfierar x^{-1} ett moniskt polynom med koefficienter i A, säg

$$x^{-n} + a_{n-1}x^{-(n-1)} + \cdots + a_1 x^{-1} + a_0 = 0.$$

Multiplicera båda sidor med x^{n-1}. Då får vi att

$$x^{-1} = \sum_{i=1}^{n} a_{n-i} x^{i-1} \in A.$$

$\Leftarrow$ Antag nu att A är en kropp. Låt $0 \neq y \in B$. Låt

$$y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0 \qquad (177)$$

vara ett moniskt polynom av minimal grad som satisfieras av y. Om vi hade $a_0 = 0$ då kunde vi ta ut en faktor y och få, eftersom B är en domän, en monisk ekvation av mindre grad som y satisfierar.

Alltså är $a_0 \neq 0$. Då finns $a_0^{-1} \in A$, eftersom A är en kropp. Betrakta nu

$$z := a_0^{-1}\left(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_2 y + a_1\right) \in B.$$

Man beräknar lätt att $yz = zy = 1$ så att $z = y^{-1} \in B$. Därför är B en kropp, och beviset är slut.

Sats 81. *Låt $A \subseteq B$ vara domäner, B ändligt genererad som en A-modul.*

(i) A Noetersk $\Rightarrow$ B Noetersk.
(ii) $dim(A) = 1 \Rightarrow dim(B) = 1$.

Bevis : (i) följer omedelbart från Korollarium 79.

(ii) Om $\dim(B) = 0$ då skulle $\dim(A) = 0$ enligt Lemma 80. Då är $\dim(B) > 0$. Det kvarstår att bevisa att varje icke-noll primt ideal i B är maximalt. Låt då $\mathbf{q}$ vara ett icke-noll prim ideal i B. Låt $\mathbf{p} = A \cap \mathbf{q}$. Då är $\mathbf{p}$ ett prim ideal i A. Vidare är det lätt att se att $B/\mathbf{q}$ är integral över $A/\mathbf{p}$. Antag nu att $\mathbf{p} \neq \{0\}$. Då är $\mathbf{p}$ ett maximalt ideal i A, så att $A/\mathbf{p}$ är en kropp. Då följer det från Lemma 80 att $B/\mathbf{q}$ är också en kropp, dvs att $\mathbf{q}$ är ett maximalt ideal i B, v.s.v.

Det räcker då att visa att $\mathbf{p} \neq \{0\}$. Välj $0 \neq y \in B$ och välj, som i (177), ett moniskt polynom över A av minimal grad som satisfieras av y. Som i argumentet som följer (177), får vi att $a_0 \neq 0$. Men eftersom $\mathbf{q}$ är en A-modul, får vi då att

$$0 \neq a_0 = -y^n - \sum_{i=1}^{n-1} a_i y^i \in \mathbf{q} \cap A = \mathbf{p},$$

och beviset är slut.

Korollarium 82. *Låt K vara en talkropp. Då är O_K en Dedekind domän.*

Huvudsatsen om Dedekind domäner (svag version). *I en Dedekind domän har varje icke-noll ideal $\mathbf{a}$ en unik decomposition som en produkt*

$$\mathbf{a} = \mathbf{p}_1^{\alpha_1} \cdots \mathbf{p}_r^{\alpha_r} \qquad \alpha_i \geq 0, \tag{178}$$

av prima ideal.

Definition : Låt A vara en domän med kvotkropp K. En A-delmodul I till K kallas för ett *fraktionellt ideal* till A om $I \neq \{0\}$ och det finns $0 \neq a \in A$ så att $aI \subseteq A$.

Om $I \subseteq K$ är en A-modul, så också är aI för varje $a \in A$. Därför, om I är ett fraktionellt ideal och $a \neq 0$ är så att $aI \subseteq A$, då måste aI vara ett ideal i A. Vi har då bevisat

Proposition 83. *Låt A vara en domän med kvotkropp K. Då är en delmängd $I \subseteq K$ en fraktionell A-ideal omm det finns ett ideal $\mathbf{a} \subseteq A$ och $0 \neq c \in A$ så att $I = c^{-1}\mathbf{a}$.*

Vi kan multiplicera fraktionella ideal på samma sätt som ideal, dvs

$$\left(c^{-1}\mathbf{a}\right)\left(d^{-1}\mathbf{b}\right) := (cd)^{-1}\mathbf{ab}. \tag{179}$$

Nu har vi äntligen

Huvudsatsen om Dedekind domäner (stark version). *Låt A vara en Dedekind domän med kvotkropp K. De fraktionella idealen till A i K utgör en abelsk grupp under multiplikation. Varje element $\mathbf{a}$ av denna grupp har en unik decomposition*

$$\mathbf{a} = \mathbf{p}_1^{\alpha_1} \cdots \mathbf{p}_r^{\alpha_r} \qquad \alpha_i \in \mathbf{Z}, \tag{180}$$

som en produkt av prima ideal i A och deras inverser.

Lektioner 21,22,23 (18,20,22/12/00)

The goal is to prove the main theorem about Dedekind domains referred to in the previous lecture. The method we will adopt is perhaps not the simplest one, but I think it is the most fruitful, in that it illustrates a type of approach common to more advanced treatments of algebraic number theory, which also involves ideas fundamental to algebraic geometry. We will christen it the 'local-global' approach. Further general discussion of what this involves is postponed until after presentation of the main results.

In what follows, the ring R is always a domain and K denotes its' quotient field. We will indicate whenever we wish to restrict to a smaller class of rings. A fractional R-ideal I will be referred to simply as a fractional ideal (no R !) when it is clear to which ring R it refers.

DEFINITION : Let I, J be any two R-submodules of K. Their *product* IJ is defined by

$$IJ := \left\{ x \in K : x = \sum_{t=1}^{n} a_t b_t, \text{ where } a_t \in I, \ b_t \in J \right\}. \tag{181}$$

This generalises the idea of multiplying ideals in R. It is clear that IJ is also an R-submodule of K.

DEFINITION : Let I be an R-submodule of K. We define

$$I^{-1} := \{x \in K : xI \subseteq R\}, \tag{182}$$

$$R(I) := \{x \in K : xI \subseteq I\}. \tag{183}$$

Proposition 84. *Both I^{-1} and $R(I)$ are R-submodules of K. In fact, $R(I)$ is a ring. Furthermore, we have*

(i) $R(I) \supseteq R \supseteq II^{-1}$.

(ii) $I \subseteq R \Leftrightarrow I^{-1} \supseteq R$.

(iii) If $I = Ra$, a principal R-module, then $I^{-1} = Ra^{-1}$. In particular, $II^{-1} = R$.

PROOF : Everything is immediate from the definitions, and the checking is left as an exercise.

Given the notation, one is tempted to call I^{-1} the *inverse* of I. However, this terminology is only used when $II^{-1} = R$. By part (iii) of the proposition, this is the case for principal modules over an arbitrary domain. More importantly, it is the case for any fractional ideal over a Dedekind domain (see Theorem 90, (iii)). A more fitting term for I^{-1} in general is the *dual module* of I (*with respect to* R).

Proposition 85. *(i) If I_1, I_2 are fractional R-ideals, then so is $I_1 I_2$.*
(ii) If I is a fractional R-ideal, then so are I^{-1} and $R(I)$.

PROOF : (i) This is just a restatement of eq. (179).

(ii) More generally, we will prove that, if I_1, I_2 are fractional R-ideals, then so is

$$J := \{x \in K : xI_2 \subseteq I_1\}.$$

First we show that $J \neq \{0\}$. Since I_2 is a fractional ideal, there exists $0 \neq a \in R$ such that $aI_2 \subseteq R$. Pick any $0 \neq b \in I_1$. Then $ba \in J$ and $ba \neq 0$, since R is a domain.

Second, we must produce $0 \neq r \in R$ such that $rJ \subseteq R$. Since I_1 is a fractional ideal, there exists $0 \neq c \in R$ such that $cI_1 \subseteq R$. Pick any $0 \neq d \in I_2 \cap R$ (such a d exists because $I_2 \neq \{0\}$, and if we pick any $0 \neq d_1 \in I_2$ then, as an element of K, its' numerator is a non-zero element of $I_2 \cap R$, since I_2 is an R-module). Then

$$cdJ = c(dJ) \subseteq c(I_2 J) \subseteq cI_1 \subseteq R,$$

and $0 \neq cd \in R$. q.e.d.

The next result is something worth keeping in mind :

Proposition 86. *(i) A non-zero, finitely-generated R-submodule of K is a fractional ideal.*
(ii) If R is Noetherian, then the converse is true.

PROOF : (i) Suppose I is a non-zero, finitely-generated R-submodule of K, with generating set $x_1, ..., x_n$. Write

$$x_i = \frac{r_i}{s_i}, \quad \text{where } r_i, s_i \in R \text{ and } s_i \neq 0.$$

Let $s = \prod_{i=1}^{n} s_i$. Then $0 \neq s \in R$ and $sI \subseteq R$.

(ii) Suppose I is a fractional ideal. There exists $0 \neq a \in R$ so that $aI \subseteq R$, and then aI is an ideal in R, by Prop. 83. By Prop. 77, aI is finitely-generated as an R-module, say by $x_1, ..., x_n$. But then $a^{-1}x_1, ..., a^{-1}x_n$ generate the R-module I. Now apply part (i).

Definition : The domain R is called a *discrete valuation ring (DVR)* if R is a PID and has exactly one non-zero prime ideal.

Proposition 87. *(i) Let R be a DVR with prime ideal (π). Then every element $x \in R$ has a unique representation as*

$$x = u\pi, \quad \text{where } u \in R^{\times} \text{ and } 0 \leq n \in \mathbf{Z}. \tag{184}$$

In particular, every ideal of R is of the form $(\pi)^n = (\pi^n)$, for some $n \geq 0$.

(ii) Every element of K also has a unique representation of the form (184), but where we allow $n \in \mathbf{Z}$, unrestricted. In particular, every fractional R-ideal is of the form $R\pi^n$, for some $n \in \mathbf{Z}$.

Proof : R is a PID, hence a UFD by Theorem 60. Hence every $x \in R$ has a decomposition as a product of irreducible elements, unique up to units. But every irreducible element $\theta \in R$ is prime (Prop. 58), hence generates a non-zero prime ideal, which must coincide with (π) since R is a DVR. Hence $\theta = u_1\pi$ for some $u_1 \in R^{\times}$. The result for R now follows, and that for K is an immediate consequence.

Let R be a DVR with prime ideal (π). By Prop. 87, there is a well-defined map $\nu : K \to \mathbf{Z} \cup \{+\infty\}$ given by

$$\nu(0) = +\infty, \tag{185}$$

$$\nu(x) = n \text{ whenever } x = u\pi^n \text{ for some } u \in R^{\times}. \tag{186}$$

The map ν has the following properties :

(i) $\nu(K^{\times}) = \mathbf{Z}$.
(ii) $\nu(xy) = \nu(x) + \nu(y)$, for all $x, y \in K^{\times}$.
(iii) $\nu(x) = +\infty \Leftrightarrow x = 0$.
(iv) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, for all $x, y \in K$.

(v) $R = \{x \in K : \nu(x) \geq 0\}$.

Now let L be any field. A map $\nu : L \to \mathbf{Z} \cup \{+\infty\}$ with properties (i) - (v) is called a *discrete valuation* (sometimes *non-archimedean valuation*) of L. Properties (i) - (v) then imply that the set $S = \{x \in L : \nu(x) \geq 0\}$ is a subring of L with quotient field equal to L. S is called the *valuation ring* of the valuation ν. The ring S is always integrally closed (see proof of Prop. 88), and has the property that, for all $x \in L$, either x or x^{-1} lies in S. For more on (discrete) valuations of fields, see the volume edited by Cassels and Fröhlich, and/or Chapter 5 of the book of Atiyah and McDonald[30].

[30]The important points are the following. Let ν be a discrete valuation on the field L, with valuation ring S. Choose a constant $c > 0$ and set, for $x \in L$,

$$||x|| := c^{-\nu(x)}.$$

The properties of a discrete valuation then imply that $||\cdot||$ is a norm on L. It is in fact an *ultra-norm* because it satisfies

$$||x + y|| \leq \max\{||x||, ||y||\}, \quad \forall\, x, y \in L,$$

which is stronger than the usual triangle inequality. The associated metric topology on L is independent of the choice of $c > 0$. It is called the *ν-adic topology* on L. The completion of L, as a metric space with this topology, is denoted L_ν. The basic theorem then is

Theorem. *(i) L_ν is a field.*

(ii) The discrete valuation ν on L can be extended in a unique manner to a discrete valuation ν^* on L_ν.

(iii) Let S_ν be the valuation ring of ν^* in L_ν. Then S_ν coincides with the completion of S w.r.t. ν.

(iv) S_ν is a discrete valuation ring.

An important problem (from the point of view of number theory) is the classification of all discrete valuations on $\mathbf{Q}$. It turns out that they are in 1-1 correspondence with the prime numbers, as follows :

Let p be a fixed prime. Every element $x \in \mathbf{Q}$ has a unique representation as $x = p^n x_1$, where x_1, when written as a fraction in lowest terms, has both its' numerator and denominator relatively prime to p. One then defines the discrete valuation ν_p of $\mathbf{Q}$ by setting

$$\nu_p(p^n x_1) := n.$$

It is easily checked that ν_p IS, in fact, a discrete valuation on $\mathbf{Q}$. It is called the *p-adic valuation*. The completion of $\mathbf{Q}$ w.r.t. ν_p is called the field of *p-adic numbers*, and denoted $\mathbf{Q}_p$. The valuation ring of ν_p^* is called the ring of *p-adic integers*, and denoted $\mathbf{Z}_p$. Note that, by the above theorem, $\mathbf{Z}_p$ is just the completion of $\mathbf{Z}$ w.r.t. the valuation ν_p. For an explicit description of the ring $\mathbf{Z}_p$, see supplementär övning nr. 18.

Proposition 88. *A domain R is a DVR iff it is Noetherian, integrally closed and possesses exactly one non-zero prime ideal.*

IMPORTANT REMARK : A ring R is called *local* if it has exactly one maximal ideal. Here, we include the case of non-trivial fields, where the maximal ideal is $\{0\}$. Hence, Prop. 88 can be reformulated as

'*A domain R is a DVR iff it is a local Dedekind domain*'.

In particular, a local Dedekind domain is a UFD. When we remove the local condition we may lose the UF property but, according to the Main Theorem, we retain unique factorisation of ideals.

PROOF OF PROP. 88 : $\Rightarrow$ Suppose R is a DVR. Then it possesses exactly one non-zero prime ideal, by our definition of a DVR. Furthermore, R is Noetherian since it is a PID (see Prop. 77). It remains to show that R is integrally closed. So let $x \in K$, the quotient field of R, and suppose x satisfies a monic polynomial over R, say

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0.$$

Consider the valuation ν on K. We have

$$\begin{array}{rcl} \nu(x^n) = n\nu(x) & = & \nu\left(-\sum_{i=0}^{n-1} r_i x^i\right) \\ & \geq & \min_{0\leq i<n}\{\nu(-r_i x^i)\} \\ & = & \min_{0\leq i<n}\{\nu(-r_i) + i\nu(x)\} \\ & \geq & \min_{0\leq i<n}\{i\nu(x)\}, \quad \text{since } \nu(r) \geq 0,\ \forall\, r \in R, \end{array}$$

from which we conclude that $\nu(x) \geq 0$, i.e.: that $x \in R$. This proves integral closure of R.

$\Leftarrow$ The proof in this direction is technical and will be accomplished in a sequence of steps. So let R denote a local Dedekind domain, with maximal ideal $\mathbf{p}$, and quotient field K.

It was proven by Ostrowski that every discrete valuation of $\mathbf{Q}$ must be one of the ν_p. Actually, Ostrowski's theorem says more, but we defer to Cassels and Fr¨hlich for details. For a comprehensive introduction to the p-adic numbers, including methods of p-adic analysis, see also the book 'P-adic numbers, p-adic analysis and zeta functions', by N. Koblitz.

NOTATION : In the following proof, $\supset$ always denotes strict containment.

Step 1 : If I is any fractional R-ideal, then $R(I) = R$.

PROOF : By Prop. 84, $R(I) \supseteq R$, so it remains to prove the converse. By Props. 85 and 86, $R(I)$ is a ring, which is finitely generated as an R-module. Let $x \in R(I)$. By definition, $xI \subseteq I$, which implies that $R[x] \subseteq R(I)$. By Prop. 64(iii), x is integral over R. Thus $x \in R$, since R is integrally closed.

Step 2 : $\mathbf{p}^{-1} \supset R$.

PROOF : A priori, $I^{-1} \supseteq R$ for any ideal I of R, by Prop. 84(ii). Pick $0 \neq a \in \mathbf{p}$ and let $I = (a)$. Since $a^{-1} \notin R$, we have that $I^{-1} \supset R$, by Prop. 84(iii).

We now consider the set $\mathcal{A}$ of non-zero ideals I in R such that $I^{-1} \supset R$. We've just shown that the set $\mathcal{A}$ is non-empty. Since R is Noetherian, $\mathcal{A}$ has a maximal element[31], J say. We claim that $J = \mathbf{p}$. Since $\mathbf{p}$ is the unique non-zero prime ideal of R, it suffices to show that J is a prime ideal.

So let $x, y \in R$ such that $xy \in J$, $x \notin J$. We must show that $y \in J$. Pick $z \in J^{-1} - R$. Then $zy(xR + J) \subseteq R$, i.e.: $zy \in (xR + J)^{-1}$. Since $x \notin J$, we have $xR + J \supset J$, so maximality of J implies that $zy \in R$. But then $z(yR + J) \subseteq R$, i.e.: $z \in (yR + J)^{-1}$. Again, maximality of J implies that $yR + J = J$, i.e.: that $y \in J$. q.e.d.

Step 3 : $R = \mathbf{p}\mathbf{p}^{-1}$.

PROOF : By Prop. 84(ii), we have $R \supseteq \mathbf{p}\mathbf{p}^{-1} \supseteq \mathbf{p}R = \mathbf{p}$. Hence, $\mathbf{p}\mathbf{p}^{-1}$ is an ideal of R containing $\mathbf{p}$, hence must be either $\mathbf{p}$ or R.

But $\mathbf{p}\mathbf{p}^{-1} = \mathbf{p}$ would imply that $\mathbf{p}^{-1} \subseteq R(\mathbf{p})$, which contradicts *Steps 1* and *2*.

Step 4 : $\cap_{n=0}^{\infty} \mathbf{p}^n = \{0\}$.

PROOF : If $x \in \mathbf{p}$ and $y \in \mathbf{p}^{-1}$, then $yx \in R$. It follows that, for each

[31] Here the Noetherian hypothesis is essential, since we cannot use Zorn's lemma. In an arbitrary domain, the ideal which is the union of the members of an ascending chain of ideals in $\mathcal{A}$ will in general not be in $\mathcal{A}$

$n > 0$, if $x \in \mathbf{p}^n$ then $yx \in \mathbf{p}^{n-1}$. It follows in turn that $\mathbf{p}^{-1} \subseteq R\,(\cap_{n=0}^{\infty}\mathbf{p}^n)$. But this contradicts *Steps 1* and *2* unless $\cap_{n=0}^{\infty}\mathbf{p}^n = \{0\}$. q.e.d.

We can now complete the proof that R is a DVR. By *Step 3*, there exists $\pi \in \mathbf{p}$ such that $\mathbf{p}^{-1}\pi \not\subseteq \mathbf{p}$. Since $\mathbf{p}^{-1}\pi$ is an ideal of R, we must therefore have $\mathbf{p}^{-1}\pi = R$. In particular, $1 \in \mathbf{p}^{-1}\pi$, so that $\pi^{-1} \in \mathbf{p}^{-1}$.

Let $x \in \mathbf{p}$. Then $\pi^{-1}x \in R$ so that $x \in (\pi)$, the principal ideal of R generated by π. Thus $\mathbf{p} \subseteq (\pi)$. But the reverse inclusion is trivial, so we must have that $\mathbf{p} = (\pi)$. Consequently, $\mathbf{p}^n = (\pi)^n = (\pi^n)$, for all $n \geq 0$, where $\pi^0 = 1$.

Finally, we claim that each $r \in R$ has a unique expression as $r = u\pi^n$, for some $u \in R^\times$ and $n \geq 0$. Clearly, this would imply that R is a DVR. By *Step 4*, there is a maximal $n \geq 0$ such that $r \in \mathbf{p}^n$. Since $\mathbf{p}^n = (\pi^n)$, we thus have $r = u\pi^n$ for some $u \in R$. But we must have that $u \in R^\times$, as otherwise $u \in \mathbf{p} = (\pi)$, which would imply that $r \in (\pi^{n+1}) = \mathbf{p}^{n+1}$, a contradiction.

This completes the proof of Prop. 88.

Definition : Let R be a domain with quotient field K, $\mathbf{p}$ a prime ideal of R. We set

$$R_{\mathbf{p}} := \left\{ a \in K : a = \frac{r}{s}, \text{ where } r, s \in R \text{ and } s \notin \mathbf{p} \right\}. \tag{187}$$

$R_{\mathbf{p}}$ is called the *local ring of fractions of R w.r.t.* $\mathbf{p}$, or simply the *localisation of R at* $\mathbf{p}$.

Proposition 89. *(i) $R_{\mathbf{p}}$ is a subring of K.*
(ii) $R_{\mathbf{p}}$ is a local ring. If $\mathbf{m}$ *is its' unique maximal ideal, then*

$$\mathbf{m} = \mathbf{p}R_{\mathbf{p}} = \left\{ \frac{r}{s} \in R_{\mathbf{p}} : r \in \mathbf{p} \right\}.$$

(iii) $\mathbf{m} \cap R = \mathbf{p}$.
(iv) If I is any ideal in $R_{\mathbf{p}}$ then $I = (I \cap R)R_{\mathbf{p}}$.

Proof : All parts of this proposition are quite simple, but a notational nightmare to write down. So look in your lecture notes !

Theorem 90. *The following three conditions are equivalent on an integral domain R which is not a field :*

(i) R is Dedekind.
(ii) R is Noetherian and, for each non-zero prime ideal $\mathbf{p}$ of R, the local ring $R_{\mathbf{p}}$ is a DVR.
(iii) For each fractional ideal I of R, $II^{-1} = R$.

PROOF : (i) $\Rightarrow$ (ii) Suppose R is Dedekind. Then R is Noetherian. Let $\mathbf{p}$ be a non-zero prime ideal of R. By Prop. 88, it suffices to show that $R_{\mathbf{p}}$ is Noetherian, integrally closed, and has exactly one non-zero prime ideal.

Step (a) : $R_{\mathbf{p}}$ is Noetherian.

Let I be an ideal in $R_{\mathbf{p}}$. By Prop. 89(iv), $I = (I \cap R)R_{\mathbf{p}}$. But $I \cap R$ is an ideal in R, hence finitely-generated, since R is Noetherian. But any generating set for $I \cap R$ as an R-module will also be a generating set for I as an $R_{\mathbf{p}}$-module. Hence, every ideal of $R_{\mathbf{p}}$ is finitely-generated, which proves that $R_{\mathbf{p}}$ is Noetherian.

Step (b) : $R_{\mathbf{p}}$ is integrally closed.

Suppose $x \in K$ is integral over $R_{\mathbf{p}}$, say

$$x^n + \frac{r_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{r_1}{s_1}x + \frac{r_0}{s_0} = 0, \tag{188}$$

where $r_i, s_i \in R$ and $s_i \notin \mathbf{p}$. Let $s = \prod_{i=0}^{n-1} s_i$. Multiply (188) through by s and we obtain

$$sx^n + t_{n-1}x^{n-1} + \cdots + t_1 x + t_0 = 0,$$

for some $t_i \in R$. Multiplying through further by s^{n-1}, we obtain a monic polynomial over R satisfied by sx. That is, sx is integral over R. But R, being Dedekind, is integrally closed, hence $sx \in R$, say $sx = r$. But then $x = \frac{r}{s} \in R_{\mathbf{p}}$, since $s \notin \mathbf{p}$.

Step (c) : $R_{\mathbf{p}}$ has exactly one non-zero prime ideal.

From Prop. 89(ii), we know that $R_{\mathbf{p}}$ has at least one non-zero prime ideal, namely its' maximal ideal $\mathbf{m}$. Now let I be any non-zero prime ideal of $R_{\mathbf{p}}$; we must show that $I = \mathbf{m}$.

One sees immediately that $I \cap R$ is a prime ideal in R, and at the very least it is non-zero (since I is), by Prop. 89(iv). But $I \subseteq \mathbf{m} = \mathbf{p}R_{\mathbf{p}}$, so we must have that $I \cap R \subseteq \mathbf{p}$. But $\dim(R) = 1$, so therefore $I \cap R = \mathbf{p}$ and $I = \mathbf{m}$ by Prop. 89(ii).

(ii) $\Rightarrow$ (iii) Let I be a fractional ideal of R. A priori, II^{-1} is an ideal of R, by Prop. 84(i). It suffices to show that, for each non-zero prime ideal $\mathbf{p}$ of R, $II^{-1} \not\subseteq \mathbf{p}$.

So fix such a $\mathbf{p}$. Let ν denote the discrete valuation of K corresponding to the DVR $R_{\mathbf{p}}$. Since R is Noetherian we know, by Prop. 86, that I is finitely-generated as an R-module, say by $a_1, ..., a_n \in K$. Order the a_i so that $\nu(a_1)$ is minimal. Then, for each i, we have that $\nu(a_1^{-1}a_i) = \nu(a_i) - \nu(a_1) \geq 0$, so that $a_1^{-1}a_i \in R_{\mathbf{p}}$, the valuation ring of ν. Let

$$a_1^{-1}a_i = \frac{r_i}{s_i}, \quad \text{where } r_i, s_i \in R \text{ and } s_i \notin \mathbf{p}.$$

Set $s = \prod s_i$. Then, for each i, $sa_1^{-1}a_i \in R$. Since the a_i generate I as an R-module, we may conclude that $sa_1^{-1} \in I^{-1}$. But then $s = (sa_1^{-1})a_1 \in I^{-1}I$ and $s \notin \mathbf{p}$. q.e.d.

(iii) $\Rightarrow$ (i) We have to show that R is Noetherian, integrally closed and of dimension 1.

Step (a) : R is Noetherian.

Let I be an ideal of R. We'll show that I is finitely-generated. Since $II^{-1} = R$ we can find $a_1, ..., a_n \in I$, $b_1, ..., b_n \in I^{-1}$ such that

$$1 = \sum_{i=1}^{n} a_i b_i.$$

Let $x \in I$. Then

$$x = 1 \cdot x = \left(\sum_{i=1}^{n} a_i b_i \right) x = \sum_{i=1}^{n} a_i (b_i x). \tag{189}$$

Since each $b_i \in I^{-1}$, we have that each $b_i x \in R$. Hence, (189) expresses x as an R-linear combination of $a_1, ..., a_n$. This shows that $a_1, ..., a_n$ generate the ideal I.

Step (b) : R is integrally closed.

Let $x \in K$ be integral over R. We must show that $x \in R$. Set $S = R[x]$. By Prop. 64(ii), S is a finitely-generated R-module, hence a fractional ideal of R, by Prop. 86. Thus $SS^{-1} = R$. However, S is also a ring, so that $SS = S$. Now we have

$$S = SR = S(SS^{-1}) = (SS)S^{-1} = SS^{-1} = R.$$

This shows that $x \in R$, as required.

Step (c) : $\dim(R) = 1$.

dim $(R) > 0$ since R is not a field. It remains to show that any non-zero prime ideal is maximal. So let $\mathbf{p}$ be a non-zero prime ideal, $\mathbf{m}$ a maximal ideal containing it. Then $\mathrm{pm}^{-1} \subseteq \mathbf{mm}^{-1} = R$ is an ideal of R and $\mathbf{p} = \mathbf{p}R = \mathbf{p}(\mathbf{m}^{-1}\mathbf{m}) = (\mathbf{pm}^{-1})\mathbf{m}$. By Prop. 76(iii), we have that either $\mathbf{m} \subseteq \mathbf{p}$, exactly as required, or $\mathbf{pm}^{-1} \subseteq \mathbf{p}$. So suppose the latter holds. Then

$$R = \mathbf{mm}^{-1} = \mathbf{m}R\mathbf{m}^{-1} = \mathbf{m}(\mathbf{p}^{-1}\mathbf{p})\mathbf{m}^{-1} = \mathbf{mp}^{-1}(\mathbf{pm}^{-1}) \subseteq \mathbf{mp}^{-1}\mathbf{p} = \mathbf{m}R = \mathbf{m},$$

i.e.: $R \subseteq \mathbf{m}$, which is absurd.

The proof of Theorem 90 is now complete.

Proof of Main Theorem on Dedekind domains : Let R be Dedekind. Combining Prop. 75 and Theorem 90(iii), we have already shown that the fractional ideals of R generate an abelian group under multiplication. It remains to show that each element of this group has a unique expression as a product of prime ideals and their inverses. In fact, by Theorem 90(iii), it suffices to show that every non-zero IDEAL has a unique expression as a product of prime ideals. There are two things to show here : existence and uniqueness of the expression.

Existence : Let $\mathcal{A}$ denote the set of non-zero ideals which cannot be written as a product of prime ideals. We claim that the set $\mathcal{A}$ is empty. Suppose it isn't. Then, since R is Noetherian, $\mathcal{A}$ must have a maximal element, I say. Then I cannot itself be prime, so let $\mathbf{p}$ be a prime ideal properly containing I. Consider $I\mathbf{p}^{-1}$. It is an ideal of R containing I. In fact, it properly contains I since, if we assumed that $I\mathbf{p}^{-1} \subseteq I$, then multiplying both sides by $I^{-1}\mathbf{p}$ would give the contradiction that $R \subseteq \mathbf{p}$. Hence, by maximality of I in $\mathcal{A}$, it must be possible to write $I\mathbf{p}^{-1}$ as a product of prime ideals. But then multiplying both sides by $\mathbf{p}$ gives an expression for I as a product of prime ideals, contradiction.

Uniqueness : Same idea as in the proof of the FTA, making use of Prop. 76(iii). You are left to fill in the details for yourselves.

Ramification in number fields

From now on, let K be a number field with ring of integers O_K. Let p be a prime number. By the Main Theorem, the principal ideal pO_K can be written as a product of prime ideals in O_K, say

$$pO_K = \mathbf{q}_1^{e_1} \cdots \mathbf{q}_r^{e_r}. \tag{190}$$

The prime ideals $\mathbf{q}_i$ are said to *lie above* p. The numbers e_i are called *ramification indices*. The prime p is said to be *ramified* in K if some $e_i > 1$; otherwise, it is said to be *unramified*. If $r = e_1 = 1$, we say that p *remains prime* in K.

Pick some $\mathbf{q}_i$ lying over p, and consider the quotient $O_K/\mathbf{q}_i$. It is a field, containing $\mathbf{Z}/p\mathbf{Z}$ as a subfield. The degree of the field extension is denoted f_i, and is called the *residue class degree* at $\mathbf{q}_i$. This means that $O_K/\mathbf{q}_i$ is a finite field of order p^{f_i}.

Theorem 91. *In the above notation,*

$$\sum_{i=1}^{r} e_i f_i = [K : \mathbf{Q}]. \tag{191}$$

For the proof of this, we will require two lemmas :

Lemma 92 (real CRT !). *Let R be a ring, $I_1, ..., I_n$ ideals of R such that $I_k + I_l = R$ for any $k \neq l$. Then we have an isomorphism of rings*

$$R/\cap_{k=1}^{n} I_k \cong \prod_{k=1}^{n} R/I_k. \tag{192}$$

PROOF : Same idea as in the proof of the ordinary CRT (see Lektion 3). There is a natural ring homomorphism from the lhs to the rhs of (192), and the hard part is showing it is surjective. Surjectivity is equivalent to the statement that, for any $x_1, ..., x_n \in R$, there exists $x \in R$ with $x - x_k \in I_k$, for $k = 1, ..., n$.

Lemma 93. *Let R be a Dedekind domain, $\mathbf{p}$ be a non-zero prime ideal of R. Then, for each $i \geq 0$, $\mathbf{p}^i/\mathbf{p}^{i+1}$ is a one-dimensional $R/\mathbf{p}$ vector space.*

PROOF : Let $\mathbf{m}$ be the maximal ideal in $R_{\mathbf{p}}$. By Theorem 90(ii), $\mathbf{m}$ is principal, and WLOG it is generated by some element $\pi \in R$. Then, for each $n \geq 0$, $\mathbf{m}^n$ is generated by π^n and one easily checks that $\mathbf{m}^n \cap R = \mathbf{p}^n$. One now easily checks that multiplication by π^n induces an isomorphism of vector spaces from $R/\mathbf{p}$ to $\mathbf{p}^n/\mathbf{p}^{n+1}$.

PROOF OF THEOREM 91 : Let $[K : \mathbf{Q}] = n$. Since O_K is a free $\mathbf{Z}$-module of rank n (Theorem 73), O_K/pO_K is a free $\mathbf{Z}/p\mathbf{Z}$-module of rank n. In particular, it is a ring of order p^n. Suppose pO_K factors as in (190). By Lemma 91, there is a ring isomorphism

$$O_K/pO_K \cong \prod_{i=1}^{r} O_K/\mathbf{q}_i^{e_i}. \tag{193}$$

But from Lemma 92 it follows immediately that $|O_K/\mathbf{q}_i^{e_i}| = |O_K/\mathbf{q}_i|^{e_i}$. Since $|O_K/\mathbf{q}_i| = p^{f_i}$, comparing the orders of both sides of (193) now gives the desired result.

By Theorem 91, there are at most $[K : \mathbf{Q}]$ prime ideals in K lying above any given prime number p. If there are exactly $[K : \mathbf{Q}]$ such ideals, we say that p *splits completely* in K. In this case $e_i = f_i = 1$ for $i = 1, ..., n$. On the other hand, if $r = f = 1$ and $e = n$ we say that p is *totally ramified* in K.

Proposition 94. *Suppose $K/\mathbf{Q}$ is Galois. Let p be a prime number, which factors in K as in (190). Then all e_i are equal, to e say, all f_i are equal, to f say, and $efr = [K : \mathbf{Q}]$.*

PROOF : It clearly suffices to show that the Galois group G of K over $\mathbf{Q}$ acts transitively on the primes lying over p. Suppose the contrary, i.e.: suppose there are two primes $\mathbf{q}_1$ and $\mathbf{q}_2$ lying over p such that $\sigma\mathbf{q}_1 \neq \mathbf{q}_2$ for all $\sigma \in G$. Equivalently, since G is a group, $\sigma\mathbf{q}_1 \neq \tau\mathbf{q}_2$ for all $\sigma, \tau \in G$. By

Lemma 92, there thus exists $x \in O_K$ such that

$$x \equiv 0 \pmod{\sigma \mathbf{q}_1} \quad \forall\, \sigma \in G, \tag{194}$$

$$x \equiv 1 \pmod{\sigma \mathbf{q}_2} \quad \forall\, \sigma \in G. \tag{195}$$

Consider

$$n := \prod_{\sigma \in G} \sigma x.$$

Since n is invariant under all elements of G, we must have that $n \in \mathbf{Q}$, by Prop. 68. But $x \in \mathbf{q}_1$, by (194), so $n \in \mathbf{Q} \cap \mathbf{q}_1$. By the argument in the proof of Lemma 80, this intersection must be $p\mathbf{Z}$. The same is true of $\mathbf{Q} \cap \mathbf{q}_2$. But, by (195), $\sigma x \notin \mathbf{q}_2$ for all $\sigma \in G$, so that $n \notin \mathbf{q}_2$ either, since $\mathbf{q}_2$ is a prime ideal. This is a contradiction, which completes the proof.

Terminology : If p is a prime, and $K/\mathbf{Q}$ is Galois, then p is said to be *tamely ramified* in K if $p \nmid e$; otherwise, p is said to be *wildly ramified.*

Norms

Let $\mathbf{q}$ be any non-zero prime ideal of O_K. As just indicated above (see also the proof of Lemma 80), there is a prime number $p \in \mathbf{N}$ such that $\mathbf{Q} \cap \mathbf{q} = p\mathbf{Z}$. Then $\mathbf{q}$ lies above p. Let f be the associated residue class degree. We define the *norm* $N(\mathbf{q})$ of $\mathbf{q}$ by

$$N(\mathbf{q}) := p^f. \tag{196}$$

This defines the norm of a prime ideal. We extend the definition to an arbitrary fractional O_K-ideal by multiplication, i.e.:

$$N(\mathbf{q}_1^{n_1} \cdots \mathbf{q}_k^{n_k}) := \prod_{i=1}^{k} N(\mathbf{q}_i)^{n_i}. \tag{197}$$

For any non-zero $x \in K$, we define the *norm of* x, $N(x)$, by

$$N(x) := N[(x)], \tag{198}$$

Where $(x) = xO_K$ is the principal fractional ideal generated by x.

Notice that, by Theorem 91, if p is a prime number, then

$$N(p) = p^{[K:\mathbf{Q}]}. \tag{199}$$

Hence, by multiplicativity, we have

$$0 \neq r \in \mathbf{Q} \Rightarrow N(r) = |r|^{[K:\mathbf{Q}]}. \tag{200}$$

More generally, we have

Theorem 95. *Let $[K:\mathbf{Q}] = n$.*
(i) Let $\mathbf{a}$ be a non-zero ideal in O_K. Then

$$N(\mathbf{a}) = |O_K/\mathbf{a}|. \tag{201}$$

(ii) Let $a \in O_K$. Considering O_K as a $\mathbf{Z}$-module with a fixed basis, let $A \in M_n(\mathbf{Z})$ be the matrix of the linear transformation $x \mapsto ax$ from O_K to O_K. Then $N(a) = |\det A|$.
(iii) For any $0 \neq a \in K$ we have

$$N(a) = \left| \prod_{i=1}^{n} \sigma_i(a) \right|, \tag{202}$$

where $\sigma_1, ..., \sigma_n$ are the distinct embeddings of K.
(iv) More generally, if $K/\mathbf{Q}$ is Galois, and $\mathbf{a}$ is any fractional ideal of O_K, then

$$(N(\mathbf{a})) = \prod_{i=1}^{n} \sigma_i(\mathbf{a}), \tag{203}$$

where the lhs denotes the principal O_K-fractional ideal generated by the rational integer $N(\mathbf{a})$.
(v) Let $\epsilon \in O_K$. Then $\epsilon \in O_K^{\times}$ iff $N(\epsilon) = 1$.
(vi) Let $\mathbf{a}$ be a non-zero ideal in O_K. Then $\mathbf{a}$ is a free $\mathbf{Z}$-module of rank n. If $\alpha_1, ..., \alpha_n$ is any $\mathbf{Z}$-basis for $\mathbf{a}$ then

$$\Delta(\alpha_1, ..., \alpha_n) = N(\mathbf{a})^2 d_K. \tag{204}$$

Obs! The product on the rhs of (202) is taken, in some books, as the definition of the norm of an element. Let us denote it by $n(a)$. As (202) indicates, it only coincides with our definition up to a sign. However, it is also multiplicative, i.e.:

$$n(a)n(b) = n(ab), \quad \forall\, a, b \neq 0. \tag{205}$$

PROOF : (i) For a non-zero prime ideal $\mathbf{q}$ of O_K, we have $N(\mathbf{q}) = |O_K/\mathbf{q}|$ by definition. The result for a general ideal now follows from multiplicativity (eq. (197)) and Lemma 92.

(ii) Follows immediately by application of (i) to the principal ideal aO_K.

(iii) First suppose that $a \in O_K$. $K = \mathbf{Q}(a)$. Consider the characteristic equation

$$\det(A - \lambda I_n) = 0, \tag{206}$$

of the matrix A in part (ii). Notice that $Aa = a \cdot a$, so that $\lambda = a$ is an eigenvalue. Now let σ be any embedding of K. Applying σ to (206) and remembering that the matrix A has rational integer entries, we find that $\sigma(\lambda)$ is an eigenvalue whenever λ is. Now since $K = \mathbf{Q}(a)$, the complex numbers $\sigma_1(a), ..., \sigma_n(a)$ are all distinct. Hence, we've produced n distinct eigenvalues of A, and these must be all its' eigenvalues, since A is an $n \times n$ matrix. But for any square matrix A, det A is equal to the product of its' eigenvalues which, together with part (ii), implies (202).

For a general $0 \neq a \in K$, the result follows by an extension of this argument which we skip over.

(iv) Because of the multiplicativity of the norm (eq. (197)), it suffices to prove this when $\mathbf{a}$ is a prime ideal. But then it follows from the ideas used in the proof of Theorem 91 and Prop. 94.

(v) Fix a $\mathbf{Z}$-basis of O_K and let $A \in M_n(\mathbf{Z})$ be the matrix of ϵ, as in part (ii). Then A^{-1} is the matrix of ϵ^{-1}, and hence $\epsilon^{-1} \in O_K$ iff A^{-1} also has integer entries. This is the case iff det $A = \pm 1$. Now (v) follows from (ii).

(vi) O_K is a free $\mathbf{Z}$-module of rank n, by Theorem 73. By part (i), $\mathbf{a}$ is a subgroup of this group of finite index. Hence it must also be free of rank n (see suppl. öv. nr. 16). The statement about the discriminant of a $\mathbf{Z}$-basis for $\mathbf{a}$ follows from part (ii) and eq. (173).

Note that (204) allows us to define the *discriminant of an ideal* $\{0\} \neq \mathbf{a} \subseteq O_K$ by

$$d(\mathbf{a}) := N(\mathbf{a})^2 d_K. \tag{207}$$

The multiplicativity of the norm implies the same property for the discriminant, i.e.:

$$d(\mathbf{ab}) = d(\mathbf{a})d(\mathbf{b}), \quad \forall\, \mathbf{a},\mathbf{b} \neq \{0\}. \tag{208}$$

We mention one more result in this connection :

Proposition 96. *The prime number p ramifies in the number field K if and only if $p|d_K$, the discriminant of K.*

PROOF : Skipped over.

Two classical results

We wish to state two of the most important results of algebraic number theory. Proofs may be found in, for example, Stewart and Tall.

The first result is about ideals. So let K be a number field. By the main theorem on Dedekind domains, the fractional ideals of O_K comprise a group under ideal multiplication. Call this group $\mathcal{I}(K)$. It is clear that the principal fractional ideals form a subgroup, since

$$\begin{aligned}(a)(b) &= (ab),\\ (a)^{-1} &= (a^{-1}).\end{aligned} \tag{209}$$

This subgroup is denoted $\mathcal{P}(K)$. Then we have

Class number theorem. *$\mathcal{I}(K)/\mathcal{P}(K)$ is a finite group.*

This quotient group is called the *(ideal) class group* of K. Its' order is denoted h_K and called the *(ideal) class number* of K. One important property of the class number is the following

Proposition. *Let K be a number field. Then*

$$h_K = 1 \Leftrightarrow K \textit{ is a PID} \Leftrightarrow K \textit{ is a UFD.}$$

PROOF : The first equivalence follows from the definition of h_K. From Sats 60, we know that if K is a PID then it is a UFD. It remains to show that if K is a UFD, then it is a PID.

So assume K is a UFD. Since every ideal in O_K is a product of prime ideals, it suffices to show that every prime ideal is principal. So let $\mathbf{p}$ be a prime ideal. Pick any $x \in \mathbf{p}$. Since K has the factorisation property (F), we can factorise x as a product of irreducible elements of O_K, say

$$x = \pi_1 \cdots \pi_k.$$

Since $\pi_1 \cdots \pi_k \in \mathbf{p}$, there is at least one index i such that $\pi_i \in \mathbf{p}$. But since K is a UFD, the principal ideal (π_i) is prime (Prop. 58). Hence, (π_i) is a non-zero prime ideal of O_K contained in $\mathbf{p}$. Since O_K has dimension 1, we conclude that $\mathbf{p} = (\pi_i)$.

The second classical result relates to the units in O_K.

Dirichlet's units theorem. *The multiplicative group $O_K^\times$ is a finitely-generated abelian group. It is of the form*

$$T \times F$$

where T is a finite group consisting of all the roots of unity in K, and F is a free abelian group of rank $r_1 + r_2 - 1$ (see eq. (166)).

REMARK : A basis for the group F above is called a *system of fundamental units* for the field K.

The *regulator* R of a number field K is defined as follows. Let $[K : \mathbf{Q}] = n$. Suppose K has real embeddings $\sigma_1, ..., \sigma_{r_1}$ and complex embeddings $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, ..., \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$, in any order. Let $\epsilon_1, ..., \epsilon_{r_1+r_2-1}$ be a system of fundamental units for K. Then

$$R := \left|\det\left[\sigma_i(\epsilon_j)\right]\right|, \quad 1 \le i, j \le r_1 + r_2 - 1. \tag{210}$$

It's an easy exercise to show that the definition of R is independent of the choice of a system of fundamental units, and of the ordering of the embeddings σ_i - for the latter, use Theorem 95 (iii),(v).

Kvadratiska kroppar

DEFINITION : En algebraisk talkropp K kallas för en *kvadratisk kropp* om $[K : \mathbf{Q}] = 2$.

Under resten av kursen ska vi koncentrera på dessa kroppar, och ska se hur föregående idéer och resultat om allmäna talkroppar specialiserar till denna situation. Vi ska dela upp vår analys i fem delar :

DEL 1 : Klassificiering av kvadratiska kroppar.
DEL 2 : Heltalsringen i en kv. kropp, och diskriminanten.
DEL 3 : Ramificiering och sambandet med Legendre symboler.
DEL 4 : Enheter och sambandet med Pells ekvation. Detta ledar till ett nytt stort område inom talteori, nämligen Diophantisk approximation.
DEL 5 : Sambandet mellan idéal klasser i kv. kroppar och binära kvadratiska former.

DEL 1 : KLASSIFICIERING

Sats 97. *Det finns en 1-1 korrespondens mellan kvadratiska kroppar och heltal d som är kvadratfria. Korrespondensen ges explicit av $d \leftrightarrow \mathbf{Q}(\sqrt{d})$.*

BEVIS : Först är det klart att om d är ett kvadratfritt heltal då är $\mathbf{Q}(\sqrt{d})$ en kvadratisk kropp.

Näst antag att d_1, d_2 är två kvadratfria heltal och att $\mathbf{Q}(\sqrt{d_1}) = \mathbf{Q}(\sqrt{d_2})$. Vi måste visa att $d_1 = d_2$. Från föregående likhet vet vi att det finns $x, y, z, w \in \mathbf{Q}$ så att

$$x + y\sqrt{d_1} = z + w\sqrt{d_2}. \tag{211}$$

Efter uttagning av en gemensam nämnare och kryss multiplikation får vi antaga att $x, y, z, w \in \mathbf{Z}$. Tag nu z till vänstra sidan av (211) och kvadrera båda sidor, så får man att

$$(x-z)^2 + y^2 d_1 + 2y(x-z)\sqrt{d_1} = w^2 d_2.$$

Därför är $2y(x-z)\sqrt{d_1} \in \mathbf{Q} \Rightarrow y(x-z) = 0 \Rightarrow y = 0$ eller $x = z$.

Om $y = 0$ då skulle (211) säga att $\sqrt{d_2} \in \mathbf{Q}$, en motsägelse.

Om $x = z$ då säger (211) att $y^2 d_1 = w^2 d_2$. Men eftersom både d_1 och d_2 är kvadratfria, så följer det att $d_1 = d_2$, v.s.v.

För att avsluta beviset, måste vi visa att varje kvadratisk kropp ges av $\mathbf{Q}(\sqrt{d})$ för något kvadratfritt heltal d. Alltså. låt K vara en kvadratisk kropp. Enligt Sats 67 är $K = \mathbf{Q}(\alpha)$ för något $\alpha \in K$. Eftersom K har grad 2 över $\mathbf{Q}$, så måste mimimal polynomet av α över $\mathbf{Q}$ ha grad 2. Då satisfierar α också något polynom av grad 2 över $\mathbf{Z}$, säg

$$a\alpha^2 + b\alpha + c = 0, \qquad \text{där } a, b, c \in \mathbf{Z},\ a \neq 0.$$

Från formeln för lösningarna till en kvadratisk ekvation får vi då att

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{212}$$

Sätt $d_1 = b^2 - 4ac$. Heltalet d_1 har en unik representation i formen $d_1 = w^2 d$, där $w \in \mathbf{N}$ och d är kvadratfritt. Då kan (212) skrivas om som

$$\alpha = \frac{-b}{2a} \pm \frac{w}{2a}\sqrt{d}.$$

Det följer att $K = \mathbf{Q}(\sqrt{d})$, och beviset av Sats 97 är avklarat.

Korollarium 98. *Varje kvadratisk kropp är Galois över* $\mathbf{Q}$.

Del 2 : Heltalsringen

I detta avsnitt ska element av $\mathbf{Z}$ kallas för 'rationella heltal'.

Sats 99. *Låt d vara ett kvadratfritt rationellt heltal och $K = \mathbf{Q}(\sqrt{d})$ vara en kvadratisk kropp.*

(i) Om $d \equiv 2, 3 \pmod 4$, då är

$$O_K = \mathbf{Z} \oplus \mathbf{Z}\sqrt{d}. \tag{213}$$

(ii) Om $d \equiv 1 \pmod 4$, då är

$$O_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1 + \sqrt{d}}{2}. \tag{214}$$

Anmärkning : Vi vet a priori från Sats 73 att O_K är en fri abelsk grupp av rang 2.

Bevis : $O_K \cap \mathbf{Q} = \mathbf{Z}$, eftersom $\mathbf{Z}$ är integralt sluten (Prop. 72(ii)). Låt nu $\alpha \in O_K - \mathbf{Q}$. Då måste α satisfiera ett moniskt polynom av grad 2 över $\mathbf{Z}$, säg

$$\alpha^2 + a\alpha + b = 0, \qquad a, b \in \mathbf{Z}. \tag{215}$$

α kan skrivas (på ett unikt sätt) i formen

$$\alpha = x + y\sqrt{d},$$

för några $x, y \in \mathbf{Q}$. Substituera i (215), så får man att

$$(x^2 + y^2 d + ax + b) + (2xy + ay)\sqrt{d} = 0,$$

som antyder att

$$x^2 + y^2 d + ax + b = 0 \tag{216}$$

och

$$2xy + ay = 0. \tag{217}$$

Från (217) får vi att antingen $y = 0$ eller $2x + a = 0$. Men $y = 0$ betyder att $\alpha \in \mathbf{Q}$, som säger emot hypotesen. Därför måste

$$x = -\frac{a}{2}. \tag{218}$$

Substituera (218) i (216) och vi får att

$$y = \pm\sqrt{\frac{a^2 - 4b}{4d}}.$$

Men $y \in \mathbf{Q}$ och d är ett kvadratfritt rationellt heltal, så det måste finnas $w \in \mathbf{N}$ så att

$$a^2 - 4b = dw^2, \tag{219}$$

och då att

$$y = \pm\frac{w}{2}. \tag{220}$$

Om $d \equiv 2, 3 \pmod 4$, då har (219) en lösning omm både a och w är jämna. Då följer (213) från (218) och (220).

Om $d \equiv 1 \pmod 4$, då har (219) en lösning om antingen (i) både a och w är jämna eller (ii) både a och w är udda. Alltså, följer (213) från (218) och (220) i detta fall också.

Korollairum 100. *Låt d vara ett kvadratfritt rationellt heltal och $K = \mathbf{Q}(\sqrt{d})$ vara en kvadratisk kropp.*

(i) Om $d \equiv 2, 3 \ (mod\ 4)$, då är

$$d_K = 4d. \tag{221}$$

(ii) Om $d \equiv 1 \ (mod\ 4)$, då är

$$d_K = d. \tag{222}$$

Speciellt, finns det precist en kvadratisk kropp av diskriminant D för varje heltal D som är en fundamental diskriminant, i meningen av binära kvadratiska former.

Bevis : Följer från Prop. 74, Sats 99 och faktumet att de två imbäddningarna ϕ_1, ϕ_2 av kroppen $\mathbf{Q}(\sqrt{d})$ ges av

$$x + y\sqrt{d} \overset{\phi_1}{\mapsto} x + y\sqrt{d}, \quad x + y\sqrt{d} \overset{\phi_2}{\mapsto} x - y\sqrt{d}.$$

Lektion 24 (08/01/01)

Del 3 : Ramificiering

Låt K vara en kvadratisk kropp och $p \in \mathbf{Z}$ ett primtal. Från Prop. 94 och Kor. 98, finns det precis tre möjligheter för prim decompositionen av huvudidéalet pO_K, nämligen

(I) $e = f = 1, r = 2 : pO_K = \mathbf{q}_1\mathbf{q}_2$ och p splittrar komplett i K.
(II) $e = r = 1, f = 2 : pO_K = \mathbf{q}$ och p kvarstår prim i K.
(III) $f = r = 1, e = 2 : pO_K = \mathbf{q}^2$ och p är totalt ramifierad i K.

Vilket av de tre fallen gäller för ett givet p kan ges explicit i termer av Kronecker symboler. Vi har

Sats 101. *Låt d vara ett kvadratfritt heltal, $K = \mathbf{Q}(\sqrt{d})$. Låt $p \in \mathbf{Z}$ vara ett primtal. Då*

(i) p splittrar komplett i $K \Leftrightarrow p \dagger d_K$ och $\left(\frac{d}{p}\right) = 1$.
(ii) p kvarstår prim i $K \Leftrightarrow p \dagger d_K$ och $\left(\frac{d}{p}\right) = -1$.
(iii) p är totalt ramifierad i $K \Leftrightarrow p | d_K$.

Obs! För udda p är Kronecker symbolen samma sak som Legendre symbolen. Alltså i del (i) (resp. del (ii)) är $\left(\frac{d}{p}\right) = 1$ (resp. $= -1$) omm $x^2 \equiv d \pmod{p}$ är lösbar (resp. ej lösbar).

För $p = 2$, då $2 \dagger d_K$ omm $d \equiv 1 \pmod{4}$, enligt Kor. 100. Alltså, i del (i) (resp. del (ii)) är $\left(\frac{d}{2}\right) = 1$ (resp. $= -1$) omm $d \equiv 1 \pmod{8}$ (resp. $d \equiv 5 \pmod{8}$).

Alltså, det mest koncisa sättet att formulera Sats 101 är

'(i) p splittrar komplett i $K \Leftrightarrow \left(\frac{d_K}{p}\right) = 1$.
(ii) p kvarstår prim i $K \Leftrightarrow \left(\frac{d_K}{p}\right) = -1$.
(iii) p är totalt ramifierad i $K \Leftrightarrow \left(\frac{d_K}{p}\right) = 0$'.

Till slut, notera att del (iii) av satsen är ett speciellt fall av Prop. 96.

Bevis av sats 101 : Props. 13.1.3 och 13.1.4 på utdelade stencilen nr. 13. Vi bevisade bara 13.1.3 under föreläsningen.

Ett exempel av prim faktorisering

Vi avslutar detta avsnitt med ett explicit exempel av prim faktorisering av ett idéal i en kvadratisk kropp. Exempelt finns på utdelad stencil nr. 15, men metoden som presenteras där kan uppskattas mycket bättre i kontexten av våra resultat om ramificiering (Sats 101). Följande är alltså en alternativ (och mycket bättre !) presentation.

Exempel : Faktorisera huvudidéalet $< 18 >$ i $\mathbf{Z}[\sqrt{-17}]$.

Lösning : Låt $K = \mathbf{Q}(\sqrt{-17})$. Notera att $-17 \equiv 3 \pmod 4$ så att $\mathbf{Z}[\sqrt{-17}] = O_K$ och

$$d_K = 4(-17) = -68.$$

Den prima faktoriseringen av 18 i $\mathbf{Z}$ är

$$18 = 2 \cdot 3^2,$$

alltså räcker det att kunna faktorisera huvudidéalen $< 2 >$ och $< 3 >$ i O_K. För detta använder vi Sats 101 och dess bevis.

(a) $2 | d_K$ så 2 ramifierar i K och

$$< 2 > = \mathbf{q}_1^2,$$

där

$$\mathbf{q}_1 = < 2, 1 + \sqrt{-17} > .$$

(b) $3 \dagger d_K$ och $\left(\frac{-17}{3}\right) = \left(\frac{1}{3}\right) = 1$, och $1^2 \equiv -17 \pmod 3$, så att 3 splittrar i K och

$$< 3 > = \mathbf{q}_2 \mathbf{q}_3,$$

där

$$\mathbf{q}_2 = < 3, 1 + \sqrt{-17} >$$

och

$$\mathbf{q}_3 = \mathbf{q}_2' = < 3, 1 - \sqrt{-17} > .$$

Äntligen har vi då att

$$< 18 > = \mathbf{q}_1^2 \, (\mathbf{q}_2 \mathbf{q}_3)^2 = \mathbf{q}_1^2 \mathbf{q}_2^2 \mathbf{q}_3^2.$$

Del 4 : Enheter

Låt $K = \mathbf{Q}(\sqrt{d})$ vara en kvadratisk kropp, där d är ett kvadratfritt heltal. Enligt Sats 99 har ett element $u \in O_K$ en unik representation $u = x + y\sqrt{d}$ där

(I) $d \equiv 2, 3 \pmod 4 \Rightarrow x, y \in \mathbf{Z}$.

(II) $d \equiv 1 \pmod 4 \Rightarrow$ antingen $x, y \in \mathbf{Z}$ eller $x = x_1/2, y = y_1/2$ där $x_1, y_1 \in \mathbf{Z}$ och är udda.

Enligt Sats 95(v) ges enheterna då av alla heltalslösningarna till ekvationerna

$$x^2 - dy^2 = \pm 1, \quad \text{om } d \equiv 2, 3 \pmod 4, \tag{223}$$

$$(x + \frac{1}{2}y)^2 - \frac{1}{4}dy^2 = \pm 1, \quad \text{om } d \equiv 1 \pmod 4. \tag{224}$$

Notera också att avbildningen

$$(x, y) \mapsto (x - y, 2y) \tag{225}$$

ger en injektion från lösningarna till (223) till lösningarna till (224).

Vårt mål är att bevisa Dirichlets sats om enheter för kvadratiska kroppar, och att tillämpa resultatet till Pells ekvation (se Sats 42, ekv. (113)). I fallet $d < 0$ har kroppen $K = \mathbf{Q}(\sqrt{d})$ två komplexa och inga reella inbäddningar. Då säger Dirichlets sats att $O_K^\times$ är en ändlig grupp. Beviset av detta faktum är ganska trivialt. Vi har

Proposition 102. *Låt $d < 0$ vara kvadratfritt.*

(i) Om $d = -1$ *då har (223) fyra lösningar* $(\pm 1, 0), (0, \pm 1)$. *Alltså är* $O^{\times}_{\mathbf{Q}(i)} = \{\pm 1, \pm i\} \cong \mathbf{Z}/4\mathbf{Z}$.

(ii) Om $d = -3$ *då har (224) sex lösningar* $(\pm 1, 0), (0, \pm 1), \pm(1, -1)$. *Alltså är* $O^{\times}_{\mathbf{Q}(\sqrt{-3})} = \{\pm 1, \pm \frac{1}{2}(1 \pm \sqrt{3})\} \cong \mathbf{Z}/6\mathbf{Z}$.

(iii) Om $d \neq -1, -3$, *då har (224) bara två lösningar* $(\pm 1, 0)$, *och* $O^{\times}_{\mathbf{Q}(\sqrt{d})} = \{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$.

För $d > 0$ har $K = \mathbf{Q}(\sqrt{d})$ två reella och inga komplexa inbäddningar och Dirichlets sats säger att $O^{\times}_{K}$, modulo en ändlig grupp av enhetsrötter, är en oändlig cycklisk grupp. Beviset av detta faktum är betydligt svårare. Vår metod ska använda idéer av en annorlunda karaktär från de som träffats hittills, speciellt följande resultat av Dirichlet, som är det enklaste (och äldste) resultatet i ett område inom talteori som kallas för *Diofantisk approximation.*

Dirichlets approximationsats. *Låt* θ_1, θ_2 *vara reella tal med* $\theta_2 > 1$. *Då finns det heltal* p, q, *med* $0 < q < \theta_2$ *så att*

$$|q\theta_1 - p| \leq 1/\theta_2. \tag{226}$$

Bevis : (Se också Baker s.43). Antag först att $\theta_2 \in \mathbf{N}$. För värje q så att $0 < q \leq \theta_2$ sätt

$$r_q := q\theta_1 - [q\theta_1].$$

Detta ger θ_2 reella tal (kanske med repititoner) i intervallen $[0, 1)$. Dela upp denna intervall i θ_2 delintervaller I_t där

$$I_t = \left[\frac{t}{\theta_2}, \frac{t+1}{\theta_2}\right), \qquad t = 0, 1, ..., \theta_2 - 1.$$

Då har vi följande två möjligheter :

Fall I : Det finns $q_1 \neq q_2$ så att både $r_{q_1}, r_{q_2} \in I_t$ för något t. WLOG, $q_1 > q_2$. Då har vi att

$$|q\theta_1 - p| < 1/\theta_2,$$

där $q = q_1 - q_2$, så att $0 < q < \theta_2$, och $p = [q_1\theta_1] - [q_2\theta_2]$.

Fall II : Det finns precis en r_q i varje I_t. Då finns det $q_1 \neq q_2$ så att $r_{q_1} \in I_0$ och $r_{q_2} \in I_{\theta_2 - 1}$. Låt $q = \min\{q_1, q_2\}$. Då är $0 < q < \theta_2$ och $|q\theta_1 - p| \leq 1/\theta_2$ där $p = [q\theta_1]$.

Detta avslutar beviset när $\theta_2 \in \mathbf{N}$. För $\theta_2 \notin \mathbf{N}$, tillämpa resultatet för paret $(\theta_1, [\theta_2] + 1)$.

OBS! Det följer från ovanstående bevis att satsen stämmer med en STRÄNG olikhet i (226) om inte $\theta_1 \in \mathbf{Q}$.

En direkt, och imponerande tillämpning av Dirichlets sats är

Sats 103. *Låt d vara ett heltal som inte är en perfekt kvadrat. Då finns det oändligt många $(x, y) \in \mathbf{Z}^2$ så att $x^2 - dy^2 = 1$.*

BEVIS : Kommer nästa gång.

Lektion 25 (10/01/01)

NOTATION : Låt K vara en kvadratisk kropp, $x \in K$. Då ska x' beteckna bilden av x under den unika icke-triviala automorfismen av K. Alltså, om $K = \mathbf{Q}(\sqrt{d})$ och $x = \alpha + \beta\sqrt{d}$, där $\alpha, \beta \in \mathbf{Q}$, då är $x' = \alpha - \beta\sqrt{d}$.

BEVIS AV SATS 103 : (se Baker s.64-65). Låt $m > 0$. Tillämpa Dirichlets approximationsats till paret $\theta_1 = \sqrt{d}$, $\theta_2 = m\sqrt{d}$. Då finns det heltal p_m, q_m, med $0 < q_m < m\sqrt{d}$ så att

$$\left|p_m - q_m\sqrt{d}\right| < \frac{1}{m\sqrt{d}}. \tag{227}$$

Sätt $\alpha_m := p_m - q_m\sqrt{d}$, så att $|\alpha_m| < 1/m\sqrt{d}$. Vi har att

$$\begin{aligned} \alpha'_m = p_m + q_m\sqrt{d} = \alpha_m + 2q_m\sqrt{d} \Rightarrow |\alpha'_m| &\leq |\alpha_m| + 2q_m\sqrt{d} \\ &< \tfrac{1}{m\sqrt{d}} + 2q_m\sqrt{d} \\ &< 3q_m\sqrt{d}, \text{ säg.} \end{aligned}$$

Då har vi att

$$|n(\alpha_m)| = |\alpha_m\alpha'_m| = |\alpha_m| \cdot |\alpha'_m| < \frac{1}{m\sqrt{d}} \cdot 3q_m\sqrt{d} < 3\frac{q_m}{m} < 3\sqrt{d}.$$

Poängen är att $|n(\alpha_m)|$ är begränsad oberoende av m.

Näst, eftersom $\sqrt{d} \notin \mathbf{Q}$ då är varje $\alpha_m \neq 0$. Men $1/m\sqrt{d} \to 0$ då $m \to \infty$, så det måste finnas oändligt många olika tal bland de α_m. Eftersom deras normer är begränsade, hittar vi då oändligt många olika tal av formen $p - q\sqrt{d}$, där $p, q \in \mathbf{Z}$ och $q > 0$, vars normer är alla lika, till N säg. Vidare kan vi nu välja en oändlig delmängd av dessa tal så att alla p är kongruenta till varandra modulo N, och detsamma för alla q. Välj nu två bland dessa tal, säg $\alpha_i = p_i - q_i\sqrt{d}$, för $i = 1, 2$ och betrakta

$$\eta := \frac{\alpha_1}{\alpha_2}.$$

PÅSTÅENDE : $\eta \neq \pm 1$ och $\eta = x + y\sqrt{d}$, där $x, y \in \mathbf{Z}$ och $x^2 - dy^2 = 1$.

Först, $\alpha_1 \neq \alpha_2 \Rightarrow \eta \neq 1$. Att $\eta \neq -1$ följer från att både q_1 och q_2 är positiva. A priori är $\eta = x + y\sqrt{d}$ för några $x, y \in \mathbf{Q}$, och $x^2 - dy^2 = \eta\eta' =$

$n(\eta) = n\left(\frac{\alpha_1}{\alpha_2}\right) = \frac{n(\alpha_1)}{n(\alpha_2)} = 1$. Alltså, kvarstår det att bevisa att $x, y \in \mathbf{Z}$. En explicit beräkning ger

$$\eta = \frac{\alpha_1}{\alpha_2} = \frac{\alpha_1 \alpha_2'}{n(\alpha_2)} = \frac{(p_1 - q_1\sqrt{d})(p_2 + q_2\sqrt{d})}{N},$$

så att

$$x = \frac{p_1 p_2 - q_1 q_2 d}{N}, \quad y = \frac{p_1 q_2 - q_1 p_2}{N}. \tag{228}$$

Det följer nu från faktumet att $p_1 \equiv p_2$ och $q_1 \equiv q_2$ modulo N att täljarna i båda uttrycken i (228) är delbara med N, och alltså att $x, y \in \mathbf{Z}$, v.s.s.v.

Detta räcker nu för att bevisa Sats 103, eftersom α_1 och α_2 valdes från en oändlig mängd, så att det finns oändligt många möjligheter för talet η.

Viktig anmärkning : Ovanstående bevis, tillsammans med beviset av Dirichlets approximationssats, är konstruktiva, men ger en ganska krånglig algoritm för att skapa lösningar till $x^2 - dy^2 = 1$. Denna algoritm kan uppfattas på ett mycket mer elegant sätt med hjälp av *kedjebråk*. Se Lektion 26 nedan.

Vi vill ge två tillämpningar av Sats 103. Den första är avslutningen av beviset av Dirichlets sats för kvadratiska kroppar :

Sats 104. *Låt $d > 0$ vara kvadratfritt och $K = \mathbf{Q}(\sqrt{d})$. Då är $O_K^\times \cong \{\pm 1\} \times \mathbf{Z}$.*

Bevis : (se Baker, s.65). Enligt Sats 103 är $O_K^\times$ en oändlig mängd. Speciellt, finns det en enhet $\eta \neq \pm 1$. Bland de fyra enheterna $\pm\eta, \pm 1/\eta$ finns det precis en som är > 1 i den triviala inbäddningen av K i $\mathbf{R}$, dvs den inbäddningen där vi tar den positiva roten $\sqrt{d}$. Vi fixerar nu denna inbäddning och betrakta mängden

$$S = \{x \in O_K^\times : x > 1\}.$$

Ovanstående argument betyder att $S \neq \emptyset$. Låt $s \in O_K^\times$. Enligt Sats 99 är $s = u + v\sqrt{d}$ där åtminstone $2u, 2v \in \mathbf{Z}$.

Påstående : Om $s \in S$ då är $u, v > 0$.

Eftersom $s \in O'_K$ så är $u - v\sqrt{d} = s' = \pm 1/s$.

Först, eftersom $s > 1$ så måste $s > s'$, som antyder att $v > 0$. Alltså är $v \geq 1/2 \Rightarrow v\sqrt{d} \geq 1/2$.

Näst är faktiskt $|s'| = 1/|s| < 1$. Om $u < 0$ då är $u \leq -\frac{1}{2} \Rightarrow s' = u - v\sqrt{d} \leq -\frac{1}{2} - \frac{1}{2} = -1$, en motsägelse.

Till slut, om $u = 0$ då är $s = v\sqrt{d}$ och $ss' = \pm 1 = -v^2 d$ som kan satisfieras (eftersom $2v \in \mathbf{Z}$) omm $d = 1, v = \pm 1$ eller $d = 4, v = \pm\frac{1}{2}$. I båda fall har vi en motsägelse, eftersom d måste vara kvadratfritt.

Detta bevisar påståendet.

Från påståendet följer det att mängden S innehåller ett minsta element. Låt det betecknas med ϵ. Låt nu η vara en godtycklig enhet så att $\eta > 0$. Då finns det ett unikt bestämt $m \in \mathbf{Z}$ så att

$$\epsilon^m \leq \eta < \epsilon^{m+1} \Rightarrow 1 \leq \frac{\eta}{\epsilon^m} < \epsilon.$$

Valet av ϵ antyder nu att faktiskt $\eta = \epsilon^m$.

Till slut, eftersom antingen η eller $-\eta$ är > 0 för varje $\eta \in O_K^\times$, så visar ovanstående argument att

$$O_K^\times = \{\pm 1\} \times < \epsilon >,$$

och att ϵ genererar en oändlig cyklisk grupp. Detta avslutar beviset av Sats 104.

Viktig anmärkning : En enhet ϵ som genererar $O_K^\times$ modulo ± 1 kallas för en *fundamental enhet.* Ovanstående bevis är också konstruktiv, dvs ger en algoritm för att skapa en fundamental enhet. Vi har sett att en fundamental enhet ges av det minsta elementet i mängden $S = \{x \in O_K^\times : x > 1\}$. Från påståendet i mitten av beviset vet vi att varje element av S är av formen $u + v\sqrt{d}$ där $u, v > 0$. Motsatsen stämmer också, dvs om $\zeta = u + v\sqrt{d}$ är en enhet med $u, v > 0$, då är $\zeta > 1$. För $d > 1$ och $2u, 2v \in \mathbf{Z} \Rightarrow u, v \geq \frac{1}{2}$. Nu har vi följande algoritm för att skapa en fundamental enhet :

Steg 1 : Skapa en lösning $\eta = x + y\sqrt{d}$ till ekvationen $x^2 - dy^2 = 1$ $(x, y \in \mathbf{Z})$, enligt den krångliga algoritmen som nämnades i föregående anmärkning.

Steg 2 : Precis en av $\pm 1, \pm 1/\eta$ är > 1. Låt denna kallas för ζ.

Steg 3 : Vi har att $\zeta = u + v\sqrt{d}$ för några $u, v > 0$ så att $2u, 2v \in \mathbf{Z}$. Både u och v har beräknats i *Steg 1* och *2*. Det finns en fundamental enhet $\epsilon = u_0 + v_0\sqrt{d}$ så att

$$u_0, v_0 > 0, \quad 2u_0, 2v_0 \in \mathbf{Z}, \quad u_0 + v_0\sqrt{d} \leq u + v\sqrt{d}, \quad u_0^2 - v_0^2 d = \pm 1.$$

Det är klart att det finns bara ändligt många par (u_0, v_0) som satisfierar dessa fyra villkor. Det minsta av dem är en fundamental enhet.

Vår andra tillämpning av Sats 103 är till Pells ekvation. Först en teknisk lemma

Lemma 105. *Låt d vara ett kvadratfritt heltal, $K = \mathbf{Q}(\sqrt{d})$. Låt $e \in \mathbf{Z}$ och betrakta*

$$G_e = \{u + v\sqrt{d} \in O_K^\times : v = n\frac{e}{2} \text{ för något } n \in \mathbf{Z}\}.$$

Då är G_e en oändlig delgrupp till $O_K^\times$ som innehåller $\{\pm 1\}$, och därför av formen

$$G_e = \{\pm 1\} \times \ < \eta >, \tag{229}$$

där $\eta = \epsilon^m$ är någon potens av en fundamental enhet, och genererar en oändlig cyklisk grupp.

Bevis : $\pm 1 = \pm 1 + 0\sqrt{d}$ och $0 = 0 \cdot \frac{e}{2} \Rightarrow \{\pm 1\} \subseteq G_e$.

Näst visar vi att om $x \in G_e$ då är $x^{-1} \in G_e$. Låt $x = u + v\sqrt{d}$ där $v = n\frac{e}{2}$, säg. Eftersom x är en enhet, har vi då att

$$x^{-1} = \pm(u - v\sqrt{d}) \Rightarrow x^{-1} \in G_e.$$

Näst visar vi att G_e är sluten under multiplikation. Låt $x_1, x_2 \in G_e$, säg

$$x_1 = u_1 + v_1\sqrt{d}, \quad \text{där } v_1 = n_1\tfrac{e}{2},$$
$$x_2 = u_2 + v_2\sqrt{d}, \quad \text{där } v_2 = n_2\tfrac{e}{2}.$$

Då är $x_1 x_2 = u + v\sqrt{d}$, där

$$v = \frac{e}{2}\left(u_1 n_2 + u_2 n_1\right).$$

Därför måste vi visa att $u_1n_2 + u_2n_1 =: T \in \mathbf{Z}$.

Om $u_1, u_2 \in \mathbf{Z}$ då är $T \in \mathbf{Z}$. A priori (Sats 99) vet vi att $2u_1, 2u_2 \in \mathbf{Z}$. Antag WLOG att $u_1 \notin \mathbf{Z}$ så att $u_1 = z_1/2$ där z_1 är udda. Från Stas 99 måste v_1 vara av samma form, så att både e, n_1 är udda.

Fall I : n_2 udda. Då är $v_2 \notin \mathbf{Z} \Rightarrow u_2 \notin \mathbf{Z} \Rightarrow u_2 = z_2/2$ där z_2 är udda. Nu har vi att

$$T = \frac{1}{2}(z_1n_2 + z_2n_1) \in \mathbf{Z}, \text{ eftersom } z_1, z_2, n_1, n_2 \text{ är alla udda.}$$

Fall II : n_2 jämt. Då är $u_1n_2 \in \mathbf{Z}$. Oclså $v_2 \in \mathbf{Z} \Rightarrow u_2 \in \mathbf{Z} \Rightarrow u_2n_1 \in \mathbf{Z}$. Då har vi igen att $T \in \mathbf{Z}$.

Vi har nu bevisat att G_e är en delgrupp till $O_K^\times$ som innehåller $\{\pm 1\}$. Det kvarstår att bevisa att den är en oändlig mängd. Eftersom $G_e \supseteq G_{2e}$, betrakta G_{2e} i stället. Det består av alla enheter $u + v\sqrt{d}$ så att $u, v \in \mathbf{Z}$ och $e|v$. Dvs, den består av alla lösningar $(u, v_1) \in \mathbf{Z}^2$ till

$$u^2 - (de^2)v_1^2 = \pm 1.$$

Eftersom de^2 inte är en perfekt kvadrat har denna ekvation oändligt många lösningar, enligt Sats 103. Detta avslutar bevisat av lemman.

Sats 106. *Låt $d > 0$ vara ett heltal som inte är en perfekt kvadrat. Då har Pells ekvation (se (113))*

$$t^2 - du^2 = 4, \quad (t, u) \in \mathbf{Z}^2, \tag{230}$$

oändligt många lösningar. Det finns en så-kallad 'fundamental lösning' (t_0, u_0) så att alla lösningarna ges av

$$\frac{1}{2}\left(t + u\sqrt{d}\right) = \pm\left[\frac{1}{2}\left(t_0 + u_0\sqrt{d}\right)\right]^m, \quad \textit{där } m \in \mathbf{Z}. \tag{231}$$

Bevis : Antag först att d är kvadratfritt. Låt (t, u) vara en lösning till (230). Notera att $2|t \Leftrightarrow 2|u$, eftersom $4 \dagger d$. Vidare har vi att

$$\left(\frac{t}{2}\right)^2 - d\left(\frac{u}{2}\right)^2 = 1.$$

Då ser vi att (t, u) löser Pells ekvation omm $\frac{t}{2} + \frac{u}{2}\sqrt{d}$ är en enhet i $K := \mathbf{Q}(\sqrt{d})$ av norm 1. Dessa utgör en delgrupp till $O_K^\times$ av index 1 eller 2, som innehåller $\{\pm 1\}$. Nu följer resultatet från Sats 104.

Låt nu d vara ett godtyckligt positivt heltal som inte är en perfekt kvadrat. Då kan d skrivas i formen $d = e^2 d_1$ där d_1 är kvadratfritt. Att (t, u) löser (230) är ekvivalent med att

$$\left(\frac{t}{2}\right)^2 - d_1 \left(\frac{e}{2}u\right)^2 = 1.$$

Då har vi en 1-1 korrespondens mellan lösningarna till (230) och enheterna av norm 1 i delgruppen G_e till $O^\times_{\mathbf{Q}(\sqrt{d_1})}$. Resultatet följer nu från Lemma 105.

Del 5 : Idéal klasser och binära kvadratiska former

We did not reach this material during the lecture. It is not examinable.

Let K be a number field. We denote by $P_+(K)$ the collection of principal fractional ideals $\mathbf{a}$ of K such that $\mathbf{a}$ has a generator λ with $n(\lambda) > 0$.

Proposition. *(i) $P_+(K)$ is a subgroup of $P(K)$.*
(ii) $P_+(K) = P(K)$ iff either $n(x) > 0$ for all $x \in K^\times$, or there exists $\eta \in O_K^\times$ with $n(\eta) = -1$.
(iii) Otherwise $[P(K) : P_+(K)] = 2$.

Proof : (i), (ii) are obvious. For (iii), there exists by hypothesis $x \in K^\times$ with $n(x) < 0$, and every unit of K has positive norm. Hence the principal ideal (x) is not in $P_+(K)$, and we have the coset decomposition

$$P(K) = P_+(K) \sqcup P_+(K) \cdot (x).$$

Proposition. *Let $K = \mathbf{Q}(\sqrt{d})$, where d is a squarefree integer.*

(i) There exists $x \in K$ with $n(x) < 0$ iff $d > 0$.
(ii) There exists $\eta \in O_K^\times$ with $n(\eta) = -1$ iff the equation $x^2 - dy^2 = -1$ has a solution $(x, y) \in \mathbf{Z}^2$.

Proof : (i) Every $x \in K$ can be expressed as $x = a + b\sqrt{d}$ for some $a, b \in \mathbf{Q}$. Then $n(x) = a^2 - b^2 d$, and it is clear that this is negative for some choice of a, b iff $d > 0$.

(ii) There exists $\eta \in O_K^\times$ with $n(\eta) = -1$ iff there exists an integer solution to, according to the value of d, (222) or (223), with -1 on the rhs in both cases. If $d \equiv 2, 3 \pmod 4$, we are thus already done. Now suppose $d \equiv 1 \pmod 4$ and that there exists a unit η with $n(\eta) = -1$. We have to show that there exists such an η in G_2, in the notation of Lemma 105. Let $P = \{\epsilon \in O_K^\times : n(\epsilon) = +1\}$. Then $[O_K^\times : P] = 2$. Hence, it suffices to show that $[O_K^\times : G_2]$ is odd. To prove this, it suffices in turn to show that, if η is a unit and $\eta \notin G_2$, then $\eta^2 \notin G_2$.

That $\eta \notin G_2$ means that $\eta = \frac{1}{2}(x + y\sqrt{d})$, where both x, y are odd integers. Then

$$\eta^2 = \frac{x^2 + dy^2}{4} + \frac{xy}{2}\sqrt{d},$$

from which we immediately see that the same is true of η^2.

Definition : The quotient group $I(K)/P_+(K)$ is called the group of *strict ideal classes* of K.

The main result of this section now is

Theorem. *Let d be a squarefree integer, $K = \mathbf{Q}(\sqrt{d})$. Then there is a 1-1 correspondence between the strict ideal classes of K and the equivalence classes of binary quadratic forms of discriminant d_K.*

Proof : See handout 14. Chapter VII of that book is a good reference for further information on quadratic fields and binary quadratic forms.

Remarks : (i) The question of for which $d > 0$ there exists an integer solution to $x^2 - dy^2 = -1$ will be answered in the next lecture (Theorem 113).

(ii) The group structure on the set of strict ideal classes allows one, by the above theorem, to define a similar structure on the equivalance classes of binary forms of a given fundamental discriminant. Since the proof of the theorem gives an explicit description of the class of forms corresponding to a class of ideals, one may thus write down explicit formulas for 'multiplying' two forms. These are called the *composition formulas* for binary quadratic forms, and were already known to Gauβ.

Supplementär lektion 26 (15/01/01)

The material of this lecture is not examinable.

Continued fractions

There are two distinct ways to introduce the notion of a continued fraction, which illustrate an important philosophical difference :

(a) The constructive/intuitive approach : One starts with a real number and shows how to associate to it a sequence (which may be finite or infinite) of fractions, i.e.: rational numbers, which converge to it. These fractions will be called the *convergents* to the real number. Of course, there are many ways to do this, e.g.: decimal expansions, but it will be intuitively clear (I hope !) from the construction that the convergents to a real number are, in a sense we can make precise, the best approximations to it by rational numbers. Hence, continued fractions are a basic notion in the subject of *Diophantine approximation*.

(b) The abstract/formal approach : One begins with, in principle, any sequence (a_n), finite or infinite, of REAL numbers (positive if $n > 0$), and associates to it a sequence of 'fractions', which will actually be rational numbers if the terms in the sequence are integers. One then shows that under certain conditions on the a_n, the sequences of fractions converge, that different sequences converge to different real numbers, and that each real number is the limit of some sequence.

As in Baker (and most other books), I will begin with approach *(a)*, because it is obviously more natural and in agreement with the historical order, and also because it makes the connection to the whole subject of Diophantine approximation immediately clear. This is an important area of number theory, not just for its' intrinsic interest, but also because of impressive applications to, for example, (i) the theory of transcendental numbrs (ii) solution of Diophantine equations. Baker's book is actually a very good introduction to these applications.

On the other hand, the proofs of the main results will be carried out in the more formal setting of approach *(b)*.

Intuitive definition : Let $\theta \in \mathbf{R}$. We associate to θ a sequence $a_0, a_1, \ldots$ of integers, possibly finite, by the following procedure :

$$\begin{array}{l}
\theta_0 := \theta. \\
a_0 := [\theta_0]. \\
\text{If } a_0 = \theta_0 \text{ then stop,} \\
\quad \text{else} \quad 1/\theta_1 := \theta_0 - a_0. \\
\qquad\qquad a_1 := [\theta_1]. \\
\qquad\qquad \text{If } a_1 = \theta_1 \text{ then stop,} \\
\qquad\qquad\quad \text{else} \quad 1/\theta_2 := \theta_1 - a_1. \\
\qquad\qquad\qquad\qquad \vdots
\end{array}$$

Proposition 107. *(i) We have $a_n > 0$ for all $n > 0$ such that a_n is defined. (ii) The process stops if and only if θ is rational. If θ is rational, say $\theta = p/q (q > 0)$ in lowest terms, then the numbers $a_0, \ldots, a_n$ which appear are precisely the quotients which appear in the Euclidean algorithm for the pair (p, q), i.e.:*

$$\begin{aligned}
p &= a_0 q + r_0, \\
q &= a_1 r_0 + r_1, \\
&\vdots \\
r_{n-3} &= a_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} &= a_n r_{n-1} + 0.
\end{aligned}$$

Proof : (i) Clear.

(ii) $\Rightarrow$ It's clear that θ is rational if the process terminates.

$\Leftarrow$ If θ is rational, then the assertion about the numbers a_n is one of those things that's obvious when you play around with the definition, but rather messy to write down a proof of, so I'll leave it to yourselves.

We have the associated sequence $r_0, r_1, \ldots$ of rational numbers, possibly finite, given by

$$
\begin{aligned}
r_0 &:= a_0, \\
r_1 &:= a_0 + \tfrac{1}{a_1}, \\
r_2 &:= a_0 + \tfrac{1}{a_1 + \frac{1}{a_2}}, \\
&. \\
&. \\
&. \\
r_n &:= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots \cfrac{1}{a_n}}}}. \qquad (232) \\
&. \\
&. \\
&.
\end{aligned}
$$

The sequence of rational numbers (r_n) is called the *continued fraction expansion* of the real number θ. The term r_n is called the n^{th} *continued fraction* corresponding to θ. The sequence r_n converges to θ - this is intuitively obvious and will be proven shortly.

The integers a_n are called the *partial quotients* of θ, and the numbers θ_n are called the *complete quotients* of θ.

The first thing now is to satisfy the obvious need for a more concise notation. Hence the fraction r_n above will henceforth be denoted by $[a_0; a_1, ..., a_n]$. We then have the recursive formula

$$[a_0] = a_0, \quad [a_0; a_1, ..., a_n] = a_0 + \frac{1}{[a_1; a_2, ..., a_n]}, \tag{233}$$

which in turn suggests

FORMAL DEFINITION : Let $a_0, a_1, ...$ be a sequence (possibly finite) of real numbers, with $a_n > 0$ for all $n > 0$. The *continued fraction expansion* corresponding to the sequence (a_n) is the sequence of numbers $([a_0; a_1, ..., a_n])_{n \geq 0}$ defined by the equations (233). The term $[a_0; a_1, ..., a_n]$ is called the n^{th} *continued fraction* in the expansion.

OBS! : The condition that $a_n > 0$ for all $n > 0$ ensures that each continued fraction is actually a real number - that we never get $1/0$ appearing.

NOTATION/TERMINOLOGY : (i) If the sequence of continued fractions in the above definition converges, then the limit is denoted by $[a_0; a_1, a_2, ...]$.

(ii) We can expand the continued fraction $[a_0; a_1, ..., a_n]$ as a formal 'fraction' as in (232), and, collecting numerators and denominators, write it in the form p_n/q_n. Here p_n, q_n are, in general, just REAL numbers. If all a_i are integers, then each continued fraction is a rational number and p_n, q_n are integers. It's not clear that p_n, q_n are in this case always relatively prime - that is, that the continued fraction $[a_0; a_1, ..., a_n]$ is already expressed in lowest terms when we just collect numerators and denominators. This will be proven below. The numbers p_n, q_n are called the n^{th} *convergents* in the continued fraction expansion.

Theorem 108. *(i) Let $(a_n)_{n\geq 0}$ be a (finite or infinite) sequence of real numbers, with $a_n > 0$ for all $n > 0$. Suppose there exists $\epsilon > 0$ such that $a_n > \epsilon$ for all $n > 0$. Then the sequence $([a_0; a_1, ..., a_n])_{n\geq 0}$ of continued fractions converges.*
(ii) Now suppose in addition that all a_n are integers. If the continued fractions converge to the real number θ, then the a_n are precisely the partial quotients of theta, in the sense of our first, intuitive, definition of continued fractions. Morevover, the convergents p_n, q_n are relatively prime.

SKETCH PROOF (See Baker, p.45) : Directly for $n = 0, 1, 2$ and therefafter by induction on n, one shows that the convergents p_n, q_n satisfy the recurrence relations

$$p_0 = a_0, \quad q_0 = 1, \tag{234}$$

$$p_1 = a_0 a_1 + 1, \quad q_1 = a_1, \tag{235}$$

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2} \quad \text{for } n \geq 2 \tag{236}$$

and that $\gcd(p_n, q_n) = 1$ under the conditions of part (ii). From the recurrence relations one proves by a simple induction that, for all $n \geq 0$,

$$p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}, \tag{237}$$

and hence that

$$\left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \frac{1}{q_n q_{n+1}}. \tag{238}$$

One sees easily from (234),(235),(236) that, under the conditions of part (i), $q_n \to +\infty$ as $n \to \infty$, and hence (238) implies that the continued fraction expansion converges in this case.

It remains to prove that, under the conditions of part (ii), the a_n are the partial quotients of the limit number θ. Suppose $(b_n)_{n\geq 0}$ are the partial quotients of θ. To make life simpler, suppose θ is irrational, so that the sequence (b_n) is infinite, and that the sequence (a_n) is also infinite - remaining possibilities can be dealt with by trivial modifications of what follows.

Now suppose $b_n \neq a_n$ for some n, and choose the smallest such n. Observe that

$$\theta = [b_0; b_1, ..., b_{n-1}, \theta_n], \tag{239}$$

where θ_n is the n^{th} complete quotient of θ and that

$$\theta_n = [b_n; b_{n+1}, ...] = [a_n; a_{n+1}, ...].$$

Hence

$$b_n - a_n = [0; a_{n+1}, ...] - [0; b_{n+1}, ...]. \tag{240}$$

But it is clear from the definitions that each term on the rhs lies in the interval $[0,1]$. Since the lhs is a non-zero integer, the only possibility is that $|b_n - a_n| = 1$ and that one of the terms on the rhs is zero. But no continued fraction $[0; c_1, c_2, ...]$, where the c_i are all positive integers, represents zero. Indeed, it also follows quickly from the definition that

$$[0; c_1, c_2, ...] \geq \frac{1}{c_1 + 1}.$$

This completes the proof of Theorem 108.

Rational approximations

Let θ be any irrational number. Since $\mathbf{Q}$ is dense in $\mathbf{R}$, we can approximate θ arbitrarily well by rational numbers. However, as these rationals approach θ, their denominators (when written as fractions in lowest terms), will obviously get bigger and bigger. More precisely, given $N > 0$, there exists $\epsilon = \epsilon(\theta, N) > 0$ such that, if p/q is any rational number written in lowest terms (i.e.: $(p,q) = 1$ and $q > 0$), then

$$|\theta - p/q| < \epsilon \Rightarrow q > N.$$

In the theory of rational approximations, one is interested in sequences of rationals converging to θ whose denominators grow 'as slowly as possible', such sequences of approximations being considered 'good'. Hers's a precise definition (mostly just for completeness : the terminology used in it is cumbersome and will generally be avoided) :

Definition : Let $f : \mathbf{N} \to \mathbf{R}^+$ be any strictly increasing function. Let θ be an irrational number. Let $r = p/q$ be any rational number, written in lowest terms. Then r is said to *approximate θ well with respect to f* if

$$|\theta - p/q| \leq 1/f(q). \tag{241}$$

The number θ is said to be *rationally approximable to order f* if there exists a sequence (r_n) of rational numbers which converges to θ, and such that each r_n approximates θ well w.r.t. f.

For the remainder of this section all rational numbers, when presented as fractions, are assumed to be written in lowest terms.

Dirichlet's approximation theorem gives a non-trivial 'lower bound' on how well one can rationally approximate an arbitrary irrational number. We have

Theorem 109. *Let θ be any irrational number. Then there exists a sequence p_n/q_n of rational numbers converging to θ such that*

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}. \tag{242}$$

A classical result of Lindemann (1844) places upper bounds on how well one can rationally approximate an irrational algebraic number θ. This result, and its' subsequent improvements over the following century or so, have far-reaching consequences, for example in the theory of transcendental numbers and for the solution of certain Diophantine equations. In these notes, we will concentrate on presenting the intimate connection between 'good' rational approximations to an irrational number θ and the continued fraction expansion of θ.

These connections are summed up by

Theorem 110. *Let θ be an irrational number. Let p_n, q_n be the sequence of convergents in the continued fraction expansion of θ. Let (a_n) be the sequence of partial quotients.*

(i) We have the following inequalitites

$$\left|\theta - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}. \tag{243}$$

$$\left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| \leq \frac{q_n}{q_{n+1}} \left|\theta - \frac{p_n}{q_n}\right|. \tag{244}$$

$$\frac{1}{(a_{n+1}+2)q_n^2} < \left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{a_{n+1}q_n^2}. \tag{245}$$

(ii) The convergents are the 'best' rational approximations to θ in the sense that, for each $n \geq 0$, if p/q is a rational number with $q < q_{n+1}$, then

$$|q\theta - p| \geq |q_n\theta - p_n|.$$

(iii) For each n either

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad or \quad \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}. \tag{246}$$

More impressively, if p/q is any fraction such that $|\theta - p/q| < 1/2q^2$, then $p = p_n$, $q = q_n$ for some n.

Proof : The first inequality (243) follows from (238) and the fact, obvious from the definition of continued fractions, that

$$n \text{ even} \Rightarrow p_n/q_n < \theta,$$
$$n \text{ odd} \Rightarrow p_n/q_n > \theta.$$

For the rest of the proof, see Baker p.46-7. Note the importance of the equation

$$\theta = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}}, \tag{247}$$

which follows from the recurrence relations (234),(235),(236). Note further that, as Baker indicates, it is possible to strengthen part (iii) considerably. We will ignore this direction.

For more on rational approximations, in particular Lindemann's theorem, its' improvements and consequences, see Baker, sections 6.5,6.6,6.7,8.2,8.3.

Quadratic irrationals

In this and remaining sections, we only consider 'simple' continued fractions, i.e.: those satisfying the conditions of Theorem 108(ii).

We wish to state the classic theorem of Lagrange on the continued fraction expansions of quadratic irrational numbers, i.e.: irrational elements of quadratic number fields. First, the required definitions :

DEFINITION : The continued fraction $[a_0; a_1, ...]$ is said to be *ultimately periodic* if there exists $k \geq 0, m > 0$ such that $a_{l+m} = a_l$ for all $l \geq k$. The smallest such m is called the *period* of the continued fraction. If $k = 0$ we say that the continued fraction is *(purely) periodic.*

Theorem 111 (Lagrange). *Let θ be an irrational number. The continued fraction expansion of θ is ultimately periodic if and only if θ is a quadratic irrational.*

PROOF : Baker, p.48-9. Note the role of (247) again.

OBS! The proof gives an algorithm for computing, for a given θ, the least numbers k, m in the above definition.

Theorem 112. *(i) Let θ be a quadratic irrational. The continued fraction of θ is purely periodic iff $\theta > 1$ and $-1 < \theta' < 0$.*
(ii) Let d be a positive integer other than a perfect square. Then the continued fractions of $\sqrt{d} + [\sqrt{d}]$ and $1/(\sqrt{d} - [\sqrt{d}])$ are purely periodic. The continued fraction of $\sqrt{d}$ satisfies $a_{l+m} = a_l$ for all $l \geq 1$.

PROOF : Baker, p.50.

The equations $\mathbf{x^2 - dy^2 = \pm 1}$

Let $d > 0$ not be a perfect square. The solutions in positive integers x, y to the equations $x^2 - dy^2 = \pm 1$, which were studied in the previous two lectures, can be nicely characterised in terms of the continued fraction of $\sqrt{d}$. We have

Theorem 113. *Let m be the period of the continued fraction of $\sqrt{d}$. Let p_n, q_n be the convergents.*

(i) The positive integers x, y satisfy $x^2 - dy^2 = 1$ if and only if $x = p_n, y = q_n$ for some odd $n \equiv -1 \pmod{m}$.
(ii) If m is even, then there are no solutions in positive integers to $x^2 - dy^2 = -1$. If m is odd, then all solutions are given by $x = p_n, y = q_n$, where n is even and $n \equiv -1 \pmod{m}$.

PROOF : Part (i) is proved in Baker, p.75-6, and the proof of (ii) is similar.