Introduction to Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Algebraic Number Fields

Algebraic Number Fields

- Let α be an algebraic number with degree n.
- Let P be the minimal polynomial for α.
- By the **conjugates** of α we mean the zeros $\alpha_1, \ldots, \alpha_n$ of P.
- The **algebraic number field** k **generated by** α over the rationals $\mathbb{Q}$ is defined as the set of numbers $Q(\alpha)$, where $Q(x)$ is any polynomial with rational coefficients.
- The set can be regarded as being embedded in the complex number field $\mathbb{C}$ and, thus, its elements are subject to the usual operations of addition and multiplication.

Algebraic Number Fields (Cont'd)

Proposition

The algebraic number field k generated by α over the rationals $\mathbb{Q}$ is indeed a field.

- We have to show that every non-zero element $Q(\alpha)$ has an inverse.
  If P is the minimal polynomial for α, then P, Q are relatively prime.
  So, there exist polynomials R, S, such that $PS + QR = 1$, for all x.
  On putting $x = \alpha$, this gives $R(\alpha) = \frac{1}{Q(\alpha)}$, as required.
- The field k is said to have **degree** n over Q, if α has degree n.
  The notation $[k : \mathbb{Q}] = n$ means that the degree of k over $\mathbb{Q}$ is n.

Iteration of the Construction

- The construction can be continued to furnish, for every algebraic number field k and every algebraic number β, a field $K = k(\beta)$, with elements given by polynomials in β with coefficients in k.
- The **degree** $[K : k]$ **of** K **over** k is defined in the obvious way as the degree of β over k.
- In abstract algebra, one shows that K is also algebraic over $\mathbb{Q}$ and

$$[K : \mathbb{Q}] = [K : k][k : \mathbb{Q}].$$

Algebraic Integers

- An algebraic number is said to be an **algebraic integer** if the coefficient of the highest power of x in the minimal polynomial P is 1.
- The algebraic integers in an algebraic number field k form a ring R.
- The ring has an integral basis:

  There exist elements $\omega_1,\ldots,\omega_n$ in R, such that every element in R can be expressed uniquely in the form

  $$u_1\omega_1+\cdots+u_n\omega_n,$$

  for some rational integers $u_1,\ldots,u_n$.
- We write $\omega_i=p_i(\alpha)$, where p_i denotes a polynomial over $\mathbb{Q}$.
- The number $(\det(p_i(\alpha_j)))^2$, where $\alpha_1,\ldots,\alpha_n$ are the conjugates of α, is a rational integer independent of the choice of basis.

  It is called the **discriminant** of k.

Divisibility, Units, Associates and Irreducibles

- An algebraic integer α is said to be **divisible** by an algebraic integer β if $\frac{\alpha}{\beta}$ is an algebraic integer.
- An algebraic integer ε is said to be a **unit** if $\frac{1}{\varepsilon}$ is an algebraic integer.
- Suppose that R is the ring of algebraic integers in a number field k.

  Two elements α, β of R are said to be **associates** if $\alpha = \varepsilon\beta$, for some unit ε.

  This is an equivalence relation on R.
- An element α of R is said to be **irreducible** if every divisor of α in R is either an associate or a unit.

Unique Factorization Domains

- One calls R a **unique factorization domain** if every element of R can be expressed essentially uniquely as a product of irreducible elements.
- The fundamental theorem of arithmetic asserts that the ring of integers in $k = \mathbb{Q}$ has this property; but it does not hold for every k.
- It is known due to Kummer and Dedekind that a unique factorization property can be restored by the introduction of ideals, and this forms the central theme of algebraic number theory.

Subsection 2

The Quadratic Field

Quadratic Fields, Norms and Conjugates

- Let d be a square-free integer, positive or negative, but not 1.
- The **quadratic field** $\mathbb{Q}(\sqrt{d})$ is the set of all numbers of the form

$$u + v\sqrt{d},\ u, v \in \mathbb{Q},$$

  subject to the usual operations of addition and multiplication.
- For any element $\alpha = u + v\sqrt{d}$ in $\mathbb{Q}(\sqrt{d})$, the **norm** of α is the rational number

$$N(\alpha) = u^2 - dv^2.$$

- For any element $\alpha = u + v\sqrt{d}$ in $\mathbb{Q}(\sqrt{d})$, the **conjugate** of α is

$$\overline{\alpha} = u - v\sqrt{d}.$$

Properties of Quadratic Fields

- If $\alpha \in \mathbb{Q}(\sqrt{d})$, then $N(\alpha) = \alpha\overline{\alpha}$.
  Suppose $\alpha = u + v\sqrt{d}$.
  Then
  $$\begin{aligned} \alpha\overline{\alpha} &= (u+v\sqrt{d})(u-v\sqrt{d}) = u^2 - (v\sqrt{d})^2 \\ &= u^2 - dv^2 = N(\alpha). \end{aligned}$$
- If $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, then $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.
  Suppose $\alpha = u + v\sqrt{d}$ and $\beta = w + z\sqrt{d}$.
  Then
  $$\begin{aligned} \overline{\alpha}\overline{\beta} &= \overline{(uw+vzd)+(uz+vw)\sqrt{d}} = (uw+vzd)-(uz+vw)\sqrt{d} \\ &= (u-v\sqrt{d})(w-z\sqrt{d}) = \overline{\alpha}\overline{\beta}. \end{aligned}$$
- If $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, then $N(\alpha)N(\beta) = N(\alpha\beta)$.
  $$N(\alpha)N(\beta) = \alpha\overline{\alpha}\beta\overline{\beta} = \alpha\beta\overline{\alpha\beta} = N(\alpha\beta).$$

Quadratic and Gaussian Fields

Proposition

$\mathbb{Q}(\sqrt{d})$ is a field.

- Let $\alpha = u + v\sqrt{d}$ be a non-zero element of $\mathbb{Q}(\sqrt{d})$.
  We saw that $\alpha\overline{\alpha} = N(\alpha) \in \mathbb{Q}$.
  So, the inverse of α is $\frac{\overline{\alpha}}{N(\alpha)}$.
- The special field $\mathbb{Q}(\sqrt{-1})$ is called the **Gaussian field**.
  It is customary to express its elements in the form $u + iv$.
  In this case we have $N(\alpha) = u^2 + v^2$.

Algebraic Integers in $\mathbb{Q}(\sqrt{d})$

- Suppose that $\alpha = u + v\sqrt{d}$ is an integer in $\mathbb{Q}(\sqrt{d})$.
- α and $\overline{\alpha}$ are zeros of

$$\begin{aligned} P(x) &= (x-\alpha)(x-\overline{\alpha}) = (x-(u+v\sqrt{d}))(x-(u-v\sqrt{d})) \\ &= x^2 - 2ux + (u^2 - dv^2) = x^2 - ax + c, \end{aligned}$$

  where $a = 2u$ and $c = N(\alpha)$.
- This shows that the rational numbers a, c must in fact be integers.
- Letting $b = 2v$, we also have

$$a^2 - db^2 = (2u)^2 - d(2v)^2 = 4(u^2 - dv^2) = 4N(\alpha) = 4c.$$

- Since d is square-free, it follows that also b is a rational integer.

Algebraic Integers in $\mathbb{Q}(\sqrt{d})$ (First Case)

- We have $P(x) = x^2 - ax + c$, with $a = 2u$, $b = 2v$ and $c = N(\alpha)$ integers.
  - Suppose $d \equiv 2$ or $3 \pmod 4$.
    By $a^2 - db^2 = 4c$, $a^2 \equiv 2b^2$ or $a^2 \equiv 3b^2 \pmod 4$.
    But a square is congruent to 0 or 1 (mod 4).
    So, a, b are even.
    Thus, u, v are rational integers.
    We can write any algebraic integer $u + v\sqrt{d}$ as

$$u + v\sqrt{d} = u \cdot 1 + v \cdot \sqrt{d}.$$

    Hence, an integral basis for $\mathbb{Q}(\sqrt{d})$ is $\omega_1 = 1$, $\omega_2 = \sqrt{d}$.
    Since $\alpha = \sqrt{d}$, we get $p_1(x) = 1$ and $p_2(x) = x$.
    Now we can compute the discriminant:

$$D = \begin{vmatrix} p_1(\alpha) & p_1(\overline{\alpha}) \\ p_2(\alpha) & p_2(\overline{\alpha}) \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

Algebraic Integers in $\mathbb{Q}(\sqrt{d})$ (Second Case)

- We have $P(x) = x^2 - ax + c$, with $a = 2u$, $b = 2v$ and $c = N(\alpha)$ integers.
  - Suppose $d \equiv 1 \pmod 4$, (the only other possibility).
    Then $a \equiv b \pmod 2$.
    Thus, $u - v$ is a rational integer.
    We can write any algebraic integer $u + v\sqrt{d}$ as

$$u + v\sqrt{d} = (u - v) \cdot 1 + 2v \cdot \frac{1}{2}(1 + \sqrt{d}).$$

Hence, an integral basis for $\mathbb{Q}(\sqrt{d})$ is $\omega_1 = 1$, $\omega_2 = \frac{1}{2}(1 + \sqrt{d})$.
Since $\alpha = \sqrt{d}$, we get $p_1(x) = 1$ and $p_2(x) = \frac{1}{2}x + \frac{1}{2}$.
Now we can compute the discriminant:

$$D = \begin{vmatrix} p_1(\alpha) & p_1(\overline{\alpha}) \\ p_2(\alpha) & p_2(\overline{\alpha}) \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 \\ \frac{1}{2}\sqrt{d} + \frac{1}{2} & -\frac{1}{2}\sqrt{d} + \frac{1}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d.$$

Quadratic Fields and Binary Quadratic Forms

- The discriminant D of $\mathbb{Q}(\sqrt{d})$ is congruent to 0 or 1 $\pmod{4}$.

  So D is also the discriminant of a binary quadratic form.

  If α is any algebraic integer in $\mathbb{Q}(\sqrt{d})$, then, for some rational integers x, y, we have

  $$\alpha = \begin{cases} x + y\sqrt{d}, & \text{when } d \equiv 2 \text{ or } 3 \pmod{4} \\ x + \frac{1}{2}y(1+\sqrt{d}), & \text{when } d \equiv 1 \pmod{4} \end{cases}.$$

  Thus, we see that $N(\alpha) = F(x,y)$, where F denotes the principal form with discriminant D, that is,

  $$F(x,y) = \begin{cases} x^2 - dy^2, & \text{when } D \equiv 0 \pmod{4} \\ (x+\frac{1}{2}y)^2 - \frac{1}{4}dy^2, & \text{when } D \equiv 1 \pmod{4} \end{cases}.$$

Subsection 3

Units

Characterization of the Units in $\mathbb{Q}(\sqrt{d})$

- By a **unit** in $\mathbb{Q}(\sqrt{d})$ we mean an algebraic integer ε in $\mathbb{Q}(\sqrt{d})$, such that $\frac{1}{\varepsilon}$ is an algebraic integer.

Proposition

An algebraic integer ε in $\mathbb{Q}(\sqrt{d})$ is a unit if and only if $N(\varepsilon) = \pm 1$.

- If ε is a unit, then $N(\varepsilon)$ and $N(\frac{1}{\varepsilon})$ are rational integers, since they are the constant terms of the corresponding minimal polynomials.

  By multiplicativity of N, $N(\varepsilon)N(\frac{1}{\varepsilon}) = 1$.

  Therefore, $N(\varepsilon) = \pm 1$.

  Conversely, suppose $N(\varepsilon) = \pm 1$. Then $\varepsilon\overline{\varepsilon} = \pm 1$, whence, ε is a unit.
- Recalling that $N(\alpha) = F(x, y)$, we see that the units in $\mathbb{Q}(\sqrt{d})$ are determined by the integer solutions x, y of the equation $F(x, y) = \pm 1$.

Units in $\mathbb{Q}(\sqrt{d})$ (Imaginary Case)

- Suppose $d < 0$.
- The quadratic field $\mathbb{Q}(\sqrt{d})$ is said to be **imaginary**.

Proposition

In an imaginary quadratic field there are only finitely many units.

- We distinguish cases:
  - If $d < -3$, then, the equation $F(x,y) = \pm 1$ has only the solutions $x = \pm 1$, $y = 0$. So the only units in $\mathbb{Q}(\sqrt{d})$ are ± 1.
  - For $d = -1$, that is, for the Gaussian field, we have $F(x,y) = x^2 + y^2$. The equation $F(x,y) = \pm 1$ has four solutions, namely $(\pm 1, 0)$, $(0, \pm 1)$. In this case $\alpha = x + y\sqrt{d}$. So there are four units $\pm 1, \pm i$.
  - For $d = -3$, we have $F(x,y) = x^2 + xy + y^2$. The equation $F(x,y) = \pm 1$ has six solutions, namely $(\pm 1, 0)$, $(0, \pm 1)$, $(1, -1)$ and $(-1, 1)$. In this case $\alpha = x + \frac{1}{2}y(1 + \sqrt{d})$. Thus, the units of $\mathbb{Q}(\sqrt{-3})$ are ± 1 and $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$.

Units in $\mathbb{Q}(\sqrt{d})$ (Imaginary Case Cont'd)

- The units in an imaginary quadratic field are all roots of unity.
- They are given by the zeros of:
  - $x^2 - 1$, when $D < -4$;
  - $x^4 - 1$, when $D = -4$;
  - $x^6 - 1$, when $D = -3$.
- Note that the number of units is the same as the number w for forms with discriminant D.

Units in $\mathbb{Q}(\sqrt{d})$ (Real Case)

- Suppose $d > 0$.
- The quadratic field $\mathbb{Q}(\sqrt{d})$ is said to be **real**.

Proposition

In a real quadratic field there are infinitely many units.

- It suffices to show that there is a unit $\eta \neq \pm 1$.
  - Then, η^m is a unit for all integers m;
  - Since the only roots of unity in $\mathbb{Q}(\sqrt{d})$ are ± 1, different m give distinct units.
- By Dirichlet's Theorem, for any integer $Q > 1$, there exist rational integers p, q, with $0 < q < Q$, such that $|\alpha| \leq \frac{1}{Q}$, where $\alpha = p - q\sqrt{d}$.

  The conjugate $\overline{\alpha} = \alpha + 2q\sqrt{d}$ satisfies $|\overline{\alpha}| \leq |\alpha| + 2q\sqrt{d} \leq Q\sqrt{d} + 2Q\sqrt{d}$ $= 3Q\sqrt{d}$. So, $|N(\alpha)| = |\alpha||\overline{\alpha}| \leq 3\sqrt{d}$.

  Further, since $\sqrt{d}$ is irrational, we obtain, as $Q \to \infty$, infinitely many α with this property.

Units in $\mathbb{Q}(\sqrt{d})$ (Real Case Cont'd)

- Now $N(\alpha)$ is a rational integer bounded independently of Q.
  Thus, for infinitely many α, it takes some fixed value, say N.
  We can select two distinct $\alpha = p - q\sqrt{d}$ and $\alpha' = p' - q'\sqrt{d}$, such that $p \equiv p' \pmod{N}$ and $q \equiv q' \pmod{N}$.
  We now put $\eta = \frac{\alpha}{\alpha'} = \frac{p-q\sqrt{d}}{p'-q'\sqrt{d}}$.
  - $N(\eta) = \frac{N(\alpha)}{N(\alpha')} = 1$;
  - $\eta \neq \pm 1$, since $\sqrt{d}$ is irrational and q, q' are positive.

  We have $\eta = x + y\sqrt{d}$, where $x = \frac{pp'-dqq'}{N}$ and $y = \frac{pq'-p'q}{N}$.
  Note that

$$\begin{aligned} pp' - dqq' &= p(p+kN) - dq(q+\ell N) = (p^2 - dq^2) + (pk - dq\ell)N; \\ pq' - p'q &= p(q+\ell N) - (p+kN)q = (p\ell - qk)N. \end{aligned}$$

  Hence, x, y are rational integers.
  It follows that η is a non-trivial unit in $\mathbb{Q}(\sqrt{d})$.

Smallest Unit Exceeding 1 in a Real Quadratic Field

- Consider the set of all units in the real field $\mathbb{Q}(\sqrt{d})$ exceeding 1.

  The set is not empty, for if η is the unit obtained in the preceding slide, then one of the numbers $\pm\eta$ or $\pm\frac{1}{\eta}$ is a member.

  Each element of the set has the form $u+v\sqrt{d}$, where u, v are integers, or, if $d \equiv 1 \pmod 4$, possibly halves of odd integers.

  u and v are positive, for $u+v\sqrt{d}$ is greater than its conjugate $u-v\sqrt{d}$, which lies between -1 and 1.

  It follows that there is a smallest element in the set, say ε.

Units in Relation to Smallest Unit Exceeding 1

- If ε' is any positive unit in the field, then there is a unique integer m, such that $\varepsilon^m \leq \varepsilon' < \varepsilon^{m+1}$.

  Hence
  $$1 \leq \frac{\varepsilon'}{\varepsilon^m} < \varepsilon.$$

  But $\frac{\varepsilon'}{\varepsilon^m}$ is also a unit in the field.

  It follows from the definition of ε, that $\varepsilon' = \varepsilon^m$.

  This shows that all the units in the field are given by
  $$\pm\varepsilon^m, \quad m = 0, \pm 1, \pm 2, \ldots.$$

Subsection 4

Primes and Factorization

Primes in the Ring of Algebraic Integers

- Let R be the ring of algebraic integers in a quadratic field $\mathbb{Q}(\sqrt{d})$.
- A **prime** π in R is an element of R that is neither 0 nor a unit and which has the property that, if π divides $\alpha\beta$, where α, β are elements of R, then either π divides α or π divides β.

Proposition

A prime π is irreducible.

- Suppose π is prime and $\pi = \alpha\beta$.

  By primality $\frac{\alpha}{\pi}$ or $\frac{\beta}{\pi}$ is an element of R.

  But the first implies that β is a unit and the second that α is a unit.

  Therefore, π is irreducible.

Irreducibles Need Not Be Primes

Claim: An irreducible element need not be a prime.

Consider the number 2 in the quadratic field $\mathbb{Q}(\sqrt{-5})$.

- It is irreducible: Suppose $2 = \alpha\beta$. Then $4 = N(\alpha)N(\beta)$. But $N(\alpha)$ and $N(\beta)$ have the form $x^2 + 5y^2$, for some integers x, y. Note that the equation $x^2 + 5y^2 = \pm 2$ has no integer solutions. So, either $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$. Thus, either α or β is a unit.
- On the other hand, 2 is not a prime in $\mathbb{Q}(\sqrt{-5})$:
  - 2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$;
  - 2 does not divide either $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$.

    Taking norms to verify that each of the latter is irreducible.

Decomposition into a Product of Irreducibles

Proposition

Every element α of R that is neither 0 nor a unit can be factorized into a finite product of irreducible elements.

- If α is irreducible, there is nothing to prove.

  Otherwise, $\alpha = \beta\gamma$, for some β, γ in R, neither of which is a unit.

  If β were not irreducible, then it could be factorized likewise, and the same holds for γ.

  The process must terminate, for if $\alpha = \beta_1 \cdots \beta_n$, where none of the β's is a unit, then, since $|N(\beta_j)| \geq 2$, we see that $|N(\alpha)| \geq 2^n$.

Unique Factorization Domains

- A finite product of irreducible elements is **essentially unique** if it is unique except for:
  - the order of the factors;
  - the possible replacement of irreducible elements by their associates.
- The ring R is said to be a **unique factorization domain** if the expression for α as a finite product of irreducible elements is essentially unique.

Characterization of Unique Factorization Domains

Theorem

R is a unique factorization domain if and only if every irreducible element of R is also a prime in R.

- Suppose factorization in R is unique.
  Let π be an irreducible element such that π divides $\alpha\beta$, with α, β in R.
  Then π is an associate of one of the irreducible factors of α or β.
  So π divides α or β, as required.
  Conversely, suppose that every irreducible element is also a prime.
  We argue as in the proof of the fundamental theorem of arithmetic.
  Suppose $\alpha = \pi_1 \cdots \pi_k$ as a product of irreducible elements, and π' is an irreducible element occurring in another factorization.
  Then π' must divide π_j, for some j. So, π' and π_j are associates.
  Assuming by induction that the result holds for $\frac{\alpha}{\pi'}$, the required uniqueness of factorization follows.

Subsection 5

Euclidean Fields

Euclidean Fields

- A quadratic field $\mathbb{Q}(\sqrt{d})$ is said to be **Euclidean** if its ring of integers R has the property that, for any elements α, β of R with $\beta \neq 0$, there exist elements γ, δ of R, such that $\alpha = \beta\gamma + \delta$ and $|N(\delta)| < |N(\beta)|$.

  Claim: A Euclidean quadratic field has a Euclidean algorithm.

  We can generate the sequence of equations

$$\delta_{j-2} = \delta_{j-1}\gamma_j + \delta_j, \quad j = 1, 2, \ldots,$$

  where $\delta_{-1} = \alpha$, $\delta_0 = \beta$, $\delta_1 = \delta$, $\gamma_1 = \gamma$ and $|N(\delta_j)| < |N(\delta_{j-1})|$.

  The sequence terminates when $\delta_{k+1} = 0$, for some k.

  Then δ_k has the properties of a greatest common divisor:
  - δ_k divides α and β;
  - every common divisor of α, β divides δ_k.

  Moreover, we have $\delta_k = \alpha\lambda + \beta\mu$, for some λ, μ in R.

Euclidean Fields (Cont'd)

- This can be verified by successive substitution.
- Alternatively, consider the set of positive integers of the form $|N(\alpha\lambda+\beta\mu)|$, where $\lambda,\mu\in R$.

  This set has a least member $|N(\delta')|$, say, $\delta'=\alpha\lambda+\beta\mu$, $\lambda,\mu\in R$.

  Thus, every common divisor of α,β divides δ'.

  Note that $\alpha=\delta'\gamma+\delta''$, with $|N(\delta'')|<|N(\delta')|$.

  Therefore, $\delta''=\alpha\lambda'+\beta\mu'$, for some λ',μ' in R.

  Hence, δ' divides α. Thus, $N(\delta'')=0$ and, so, $\delta''=0$.

  Similarly, δ' divides β. Hence, we have $\delta'=\delta_k$.
- If δ_k is a unit then, by division, we obtain elements λ,μ in R, with $\alpha\lambda+\beta\mu=1$.

Euclidean Fields have Unique Factorization

Theorem

A Euclidean field has unique factorization.

- It suffices to show that every irreducible element π in R is a prime.
  Suppose that π divides $\alpha\beta$ but that π does not divide α.
  By the Euclidean Algorithm, there exist integers λ, μ in R, such that
  $$\alpha\lambda + \pi\mu = 1.$$
  This gives $\alpha\beta\lambda + \pi\beta\mu = \beta$.
  Hence, π divides β.
  Thus, π is a prime.

Euclidean Quadratic Fields: A Negative Result

Theorem

There can be no other Euclidean fields with $d<0$, apart from $d=-11,-7,-3,-2,-1$.

- We exclude two cases that cover all non-listed numbers.
  - Suppose, first, that $d\equiv 2$ or $3 \pmod 4$ and $d\leq -5$.
    We cannot have $\sqrt{d}=2\gamma+\delta$, with $|N(\delta)|<4$.
    Let $\gamma=x+y\sqrt{d}$, $\delta=x'+y'\sqrt{d}$, with x,y, x',y' rational integers.
    Note that $N(\delta)\geq x'^2+5y'^2$. So, $y'=0$.
    But $\sqrt{d}=2\gamma+\delta$ yields $2y+y'=1$, contradicting $y'=0$.
  - Suppose, next, that $d\equiv 1 \pmod 4$ and $d\leq -15$.
    We cannot have $\frac{1}{2}(1+\sqrt{d})=2\gamma+\delta$, with $|N(\delta)|<4$.
    Let $\gamma=x+y\frac{1}{2}(1+\sqrt{d})$, $\delta=x'+y'\frac{1}{2}(1+\sqrt{d})$, with x,y, x',y' integers.
    Note that $N(\delta)\geq\frac{1}{4}(2x'+y')^2+\frac{15}{4}y'^2$. So, $y'=0$ or $y'=-2x'$.
    But $\frac{1}{2}(1+\sqrt{d})=2\gamma+\delta$ yields $y+\frac{1}{2}y'=\frac{1}{2}$.
    This contradicts $y'=0$ or $y'=-2x'$.

Euclidean Quadratic Fields for $d = -2, -1, 2, 3$

Theorem

If $d = -2, -1, 2$ or 3 then $\mathbb{Q}(\sqrt{d})$ is Euclidean.

- Let α, β be any algebraic integers in $\mathbb{Q}(\sqrt{d})$, with $\beta \neq 0$. Then $\frac{\alpha}{\beta} = u + v\sqrt{d}$, for some rationals u, v. Select integers x, y as close as possible to u, v and set
$$r = u - x \quad \text{and} \quad s = v - y.$$
Then $|r| \leq \frac{1}{2}$ and $|s| \leq \frac{1}{2}$ and, moreover,
$$\alpha = \beta(u + v\sqrt{d}) = \beta((x + r) + (y + s)\sqrt{d}) = \beta(x + y\sqrt{d}) + \beta(r + s\sqrt{d}).$$
Now note that:
  - For $|d| \leq 2$, we have $|r^2 - ds^2| \leq r^2 + 2s^2 \leq \frac{3}{4}$;
  - For $d = 3$, we have $|r^2 - ds^2| \leq \max(r^2, ds^2) \leq \frac{3}{4}$.

  Therefore, $|N(\beta(r + s\sqrt{d}))| = N(\beta)(r^2 - ds^2) \leq N(\beta)$.

Subsection 6

The Gaussian Field

The Gaussian Field and the Gaussian Integers

- The **Gaussian field** is $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$.
- The **Gaussian integers** are the integers in the field.

  They have the form $x + iy$, with x, y rational integers.
- The **norm** of a Gaussian integer has the form $x^2 + y^2$.

  In particular, it is non-negative.
- It was noted that there are just four units ± 1 and $\pm i$.
- Moreover, the field is Euclidean and so has unique factorization.
- It follows that there is no need to distinguish between irreducible elements and primes.

  These elements are called **Gaussian primes**.

Gaussian Integers and Primes

Proposition

If α is any Gaussian integer and if $N(\alpha)$ is a rational prime, then α is a Gaussian prime.

Assume α is any Gaussian integer and $N(\alpha)$ a rational prime.

Suppose $\alpha = \beta\gamma$, for some Gaussian integers β, γ.

Then $N(\alpha) = N(\beta)N(\gamma)$.

Hence, either $N(\beta) = 1$ or $N(\gamma) = 1$.

So, either β or γ is a unit.

Gaussian and Rational Primes

Proposition

Every Gaussian prime π divides just one rational prime p.

- π certainly divides $N(\pi)$.

  So there is a least positive rational integer p, such that π divides p.

  p is a rational prime: Suppose $p = mn$, where m, n are rational integers. Then, since π is a Gaussian prime, we have either π divides m or π divides n. By the minimal property of p, either m or n is 1.

  The prime p is unique: Suppose p' is any other rational prime. Then there exist rational integers a, a', such that $ap + a'p' = 1$. Thus, if π were to divide both p and p', then it would divide 1. So π would be a unit contrary to definition.

Gaussian Primes

Theorem

A rational prime p is either itself a Gaussian prime or is the product $\pi\pi'$ of two Gaussian primes, where π, π' are conjugates.

- p is divisible by some Gaussian prime π.
  Thus, we have $p = \pi\lambda$, for some Gaussian integer λ.
  This gives $N(\pi)N(\lambda) = p^2$, whence one of the following holds:
    - $N(\lambda) = 1$. So λ is a unit and p is an associate of π;
    - $N(\lambda) = p$. So $N(\pi) = p$.

  In the first case $p \equiv 3 \pmod 4$ and in the second $p \equiv 1 \pmod 4$:
  $N(\pi)$ has the form $x^2 + y^2$. A square is congruent to 0 or 1 (mod 4).
  Suppose $p \equiv 1 \pmod 4$. Then -1 is a quadratic residue $\pmod p$.
  So p divides $x^2 + 1 = (x+i)(x-i)$, for some rational integer x.
  If p were a Gaussian prime, it would divide either $x+i$ or $x-i$.
  This contradicts the neither $\frac{x}{p} + \frac{i}{p}$ nor $\frac{x}{p} - \frac{i}{p}$ is a Gaussian integer.

Gaussian Primes (Cont'd)

- With regard to the prime 2, we have $2=(1+i)(1-i)$.
  - $1+i$ and $1-i$ are Gaussian primes;
  - $1+i$ and $1-i$ are associates.
- In conclusion, we find that the totality of Gaussian primes are given by:
  - the rational primes $p\equiv 3 \pmod 4$;
  - the factors π,π' in the expression $p=\pi\pi'$ for primes $p\equiv 1 \pmod 4$;
  - $1+i$;

  together with all the associates of the elements in this list, formed by multiplying by ± 1 and $\pm i$.
- The argument provides another proof of the result that every prime $p\equiv 1 \pmod 4$ can be expressed as a sum of two squares.