Comprehensive and Self-Contained Number Theory

Shin-Eui Song

Part I

Preliminaries

Chapter 1

Construction of Numbers

1.1 Peano Axioms

Peano axioms are a set of axioms for the natural numbers presented by 19th century Italian mathematician Giuseppe Peano.

1. $0 \in \mathbb{N}$
2. $=$ defines an equivalence relation.
3. For all a, b, $a = b$ with $b \in \mathbb{N}$ implies that $a \in \mathbb{N}$, i.e. $\mathbb{N}$ is closed under equality.
4. There exists a sucessor function $S : \mathbb{N} \to \mathbb{N}$

Peano's original formulation of the axioms used 1 instead of 0 as the "first" natural number. However, since 1 does not endow the constant 0 with any additional properties, this choice is *arbitrary*.

5. S is injective, i.e. $S(n) = S(m)$ implies $n = m$ for any natural numbers $n, m \in \mathbb{N}$.
6. $S^{-1}(0) = \varnothing$, i.e. there is no natural number whose successor is 0.

The above axioms require $\{0, S(0), S(S(0)), \ldots\} \subset \mathbb{N}$ with $0, S(0), S(S(0)), \ldots$ distinct elements. However, we need to show the reversed set inclusion, i.e. $\mathbb{N} \subset \{0, S(0), S(S(0)), \ldots\}$. We define $1 = S(0)$, $2 = S(S(0))$, and so on. Hence we add an additional axiom which is called the *axiom of induction*

7. If K is a set such that
   (a) $0 \in K$,
   (b) For every $n \in \mathbb{N}$, if $n \in K$, then $S(n) \in K$, then K contains every natural number.

The axiom of induction can be written in the following form:

8. If φ is a *unary predicate* such that
   (a) $\varphi(0)$ is true,
   (b) For every $n \in \mathbb{N}$, if $\varphi(n)$ is true, then $\varphi(S(n))$ is true, then $\varphi(n)$ is true for every natural number.

Peano axioms can be augmented with the operations of addition and multiplication and the usual total ordering on $\mathbb{N}$. The respective functions and relations are constructed in "second-order logic", and are shown to be unique using the Peano Axiom.

Addition

Addition is a function $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, and is defined *recursively* as:

$$a + 0 = a,$$
$$a + S(b) = S(a + b)$$

where we use the notation $+(a, b) = a + b$ for convenience. The structure $(N, +)$ is a commutative *semigroup* with identity element 0, or simply a commutative *monoid*. It is also a *cancellative magma*, and thus embeddable in a *group*, and the smallest group embedding $\mathbb{N}$ is $\mathbb{Z}$ which is the integers.

Multiplication

Let $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the notation $\times(a, b) = a \times b$ which is also defined recursively as

$$a \times 0 = a,$$
$$a \times S(b) = a + (a \times b)$$

then we can easily verify that 1 is an multiplicative identity because

$$a \times 1 = a \times S(0) = a + (a \times 0) = a + 0 = a$$

Moreover, multiplication *distributes over* addition:

$$a \times (b + c) = (a \times b) + (a \times c)$$

Thus $(N, +, \times)$ is a commutative *semiring*.

Inequalities

The usual *total order* relation $\leq$ on natural numbers can be defines as follows.

For all, $a, b \in \mathbb{N}$, $a \leq b$ if and only if there exists some $c \in \mathbb{N}$ such that $a + c = b$

This relation is stable under addition and multiplication, that is for every $a, b, c \in \mathbb{N}$, if $a \leq b$, then

1. $a + c \leq b + c$, and
2. $a \times c \leq b \times c$,

Thus, the structure $(N, +, \times)$ is an *ordered semiring*, and because there is no natural number between 0 and 1, there is no natural number between $n, n + 1$, hence becomes a *discrete ordered semiring*. Then we state the axiom of induction in its strong form: For any predicate φ

1. $\varphi(0)$ is true,
2. For every $n, k \in \mathbb{N}$ and $k \leq n$, if $\varphi(k)$ is true, then $\varphi(S(n))$ is true. Then $\varphi(n)$ is true for all natural numbers n.

This form of the induction axiom is a simple consequence of the standard formulation, but it is often more suited for reasoning about the order. Now we show that the naturals are *well-ordered*: every nonempty subset of $\mathbb{N}$ has a least element. Let $X \subset \mathbb{N}$, a nonempty subset with X no least element.

1. 0 is a least element of $\mathbb{N}$, hence $0 \notin X$.

2. If for every $k \leq n$, $k \notin X$ implies that $S(k) \notin X$, as if it were, then it would be the least element of X.

Hence by the strong induction principle, for all $n \in \mathbb{N}$, $n \notin X$, which means that $X \cap \mathbb{N} = \varnothing$, which contradicts the fact that X is nonempty.

The following demonstrates the set-theoretic model of the natural numbers. The Peano axioms can be derived from *set theoretic* constructions of the natural numbers and axioms of set theory such as the *ZF*. Let $0 := \varnothing$, with $S(a) = a \cup \{a\}$. Then the natural number is defined to be the intersection of all sets closed under s that contains the empty set. Each natural number is equal (as a set) to the set of natural numbers less than it:

1. $0 = \varnothing$,

2. $1 = s(0) = \varnothing \cup \{\varnothing\}$,

3. $2 = s(1) = s(\{\varnothing\}) = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = \{0, 1\}$

and so on. Then $\mathbb{N}$ with 0 and the successor function s satisfies the Peano axioms. "Peano arithmetic" is *equiconsistent* with several weak systems of set theory. One such system is ZFC with the axiom of infinity replaced by its negation. We see that by Godel that a consistency proof cannot be formalized within Peano arithmetic itself. This rules out the finitistic consistency proof. However, Gentzen gave a consistency proof using transfinite induction which is arguably finitistic as transfinite ordinal can be encoded in terms of finite objects. The problem comes from not giving a precise definition of what it means to be finitistic, but both Hilbert and Gentzen could not come up with a generally accepted definition.

Citation: `https://en.wikipedia.org/wiki/Peano_axioms`, 2015-12-20, the page was last modified on 8 November 2015, at 23:39.

Chapter 2

Number Fields

2.1 Integral Extensions

We would like to show that for finitely generated $\mathcal{O}_K$-module $\mathfrak{A} \subset \mathfrak{A}'$ satisfies the following

$$d(v_1, \ldots, v_n) = [\mathfrak{A}' : \mathfrak{A}]d(w_1, \ldots, w_n)$$

then it suffices to show that the determinant of a change of basis matrix T that sends the $\mathbb{Z}$-basis of $\mathfrak{A}'$ to the $\mathbb{Z}$-basis of $\mathfrak{A}$ is equal to the index of $[\mathfrak{A}' : \mathfrak{A}]$.This follows from the well-known results from module theory, namely

1. $B_i \subset A_i$ be submodules, then $\oplus B_i \subset \oplus A_i$ is a submodule and we have the module-isomorphism
$$(\bigoplus B_i)/(\bigoplus A_i) = \bigoplus (B_i/A_i)$$

2. Let Ax be a free principal module over a principal ideal domain A. If $N \subset Ax_i$, then because we have unique representation, we may talk about the subset of A which comprises of all the "coefficients" of N which forms an ideal, and denote it $\mathfrak{A}$. Then because A is a principal ideal domain, $\mathfrak{A} = (d)$ for some $d \in A$. Hence $N = A(dx)$.

3. Let $M = M_1 \oplus \cdots \oplus M_n$ be a free A-module, then a submodule N of M is of the form $N_1 \oplus \cdots \oplus N_n$ where N_i are A-submodule of M_i. If M is a free A-module of the form $Ax_1 \oplus \cdots \oplus Ax_n$, then by the above remark, we get that the submodule is of the form $Ad_1x_1 \oplus \cdots \oplus Ad_nx_n$ for some $d_i \in A$.

By 3 above, we get that $\mathfrak{A}' = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$, then $\mathfrak{A} = \mathbb{Z}d_1x_1 \oplus \cdots \oplus \mathbb{Z}d_nx_n$, then by 1, we get that

$$\mathfrak{A}'/\mathfrak{A} = \bigoplus (\mathbb{Z}x_i)/(\mathbb{Z}d_ix_i) = \bigoplus \mathbb{Z}/\mathbb{Z}d_ix_i$$

then

$$|\mathfrak{A}'/\mathfrak{A}| = \prod d_i$$

This is exactly the determinant of the change of matrix that sends $x_i \mapsto d_ix_i$, where the matrix representation of the transformation is the diagonal matrix with its entries $d_1, \ldots, d_n$.

2.2 Quadratic Extensions

We are interested in $K = \mathbb{Q}(\sqrt{D})$ where d is square-free. We want to determined the ring of integers $\mathcal{O}_K$. First we observe that $K/\mathbb{Q}$ has degree 2, so the extension is normal. Because $\mathbb{Q}$ has characteristic 0, the extension is separable, hence Galois. The reader can easily check that $K \to K$ defined by $\sqrt{D} \mapsto -\sqrt{D}$, which can be viewed as an isomorphism between the splitting fields of $x^2 - D$ over $\mathbb{Q}$ is indeed an automorphism of K fixing $\mathbb{Q}$.

We know that all elements in $\mathbb{Z}[\sqrt{D}]$ is integral because $(x-(a+b\sqrt{D}))(x-(a-b\sqrt{D})) = x^2 - 2ax + (a^2 - b^2 D)$ gives an monic irreducible with coefficient in $\mathbb{Z}$. Now we assume that $\alpha \in \mathbb{Q}(\sqrt{D}) \backslash \mathbb{Z}[\sqrt{D}]$, i.e.

$$\alpha = \frac{a}{b} + \frac{c}{d}\sqrt{D}$$

then consider the minimal polynomial f of α over $\mathbb{Q}$, then if we let $^-$ be the map $\sqrt{D} \mapsto -\sqrt{D}$, $f(\alpha) = 0 \Rightarrow \overline{f}(\overline{\alpha}) = \ f(\overline{\alpha}) = 0$. $\mathbb{Z}$ being integrally closed implies that $f \in \mathbb{Z}[x]$. In fact, as $\alpha, \overline{\alpha}$ integral implies that f has coefficients in $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. This implies that

$$\frac{2a}{b}, \frac{a^2}{b^2} - \frac{Dc^2}{d^2} \in \mathbb{Z}$$

with assuming that a, b are relatively prime and c, d are relatively prime. If $b = 1$, then we get $(Dc^2)/d^2 \in \mathbb{Z}$ which is impossible unless $d^2 | D$, but we have that D is squarefree. Hence $b \geq 2$. Let p be a odd prime dividing b, then $p | 2a \Rightarrow p | a$, which contradicts $(a, b) = 1$. Hence b is a power of 2. If $b = 2^n$ with $n \geq 2$, then $2^n | 2a \Rightarrow 2^{n-1} | a$ which again contradicts $(a, b) = 1$. We may conclude that $b = 2$.

Now we focus when

$$\frac{a^2}{4} - \frac{Dc^2}{d^2} = \frac{a^2 d^2 - 4Dc^2}{4d^2} \in \mathbb{Z}$$

Then we have that the numerator is divisible by 4. Modding out by 4, we get $a^2 d^2$ is even. Because b is even, then a has to be odd. i.e. d is even. We then have $d = 2k$ for some k, and the above transforms to

$$\frac{4a^2k^2 - 4Dc^2}{16k^2} = \frac{a^2k^2 - Dc^2}{4k^2} \in \mathbb{Z}$$

Suppose a prime p divides k, then we have that $p | a^2k^2 - Dc^2 \Rightarrow p | Dc^2$. Because $(c, d) = 1$, we have that p divides D, and because D is squarefree, p does not divide (D/p). Then we get

$$\frac{a^2k^2 - Dc^2}{4k^2} = \frac{a^2(pl)^2 - Dc^2}{4(pl)^2} = \frac{a^2pl^2 - (D/p)c^2}{4pl^2} \in \mathbb{Z}$$

then $p | 4pl^2 | a^2pl^2 - (D/p)c^2 \Rightarrow p | (D/p)c^2 \Rightarrow p | (D/p)$ which leads to a contradiction. Hence $k = 1$. We finally have the form

$$\frac{a^2 - Dc^2}{4} \in \mathbb{Z}$$

with a, c odd. Let's mod the numerator by 4, then we get $1 - D \equiv 0$, hence there exists a element $\alpha \in \mathbb{Q}(\sqrt{D}) \backslash \mathbb{Z}[\sqrt{D}]$ only if $D \equiv 1 \mod 4$. Clearly, all $\frac{1}{2}(a + b\sqrt{D})$ is generated by $\frac{1}{2}(1 + \sqrt{D})$ and 1 which are both integral, hence integral itself. To conclude we have the following,

1. $D \equiv 2, 3 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}[\sqrt{D}]$
2. $D \equiv 1 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}[\frac{1}{2}(1+\sqrt{D})]$ which is strictly larger than $\mathbb{Z}+\mathbb{Z}[\sqrt{D}]$. This gives an example of when $K/\mathbb{Q}$ a number field, then by the primitive element theorem $K = \mathbb{Q}(\theta)$, then the ring of integers is not always $\mathbb{Z}[\theta]$.

Then for the first case, we have the determinant

$$\left(det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} \right)^2 = (-2\sqrt{D})^2 = 4D$$

and for the second case,

$$\left(det \begin{pmatrix} 1 & \frac{1}{2}(1+\sqrt{D}) \\ 1 & \frac{1}{2}(1-\sqrt{D}) \end{pmatrix} \right)^2 = (-\sqrt{D})^2 = D$$