Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

An Example

- Consider a world where the only positive integers are

$$1, 4, 7, 10, \ldots, 3n+1, \ldots.$$

- Suppose that, in this world, a *prime number* is an integer which cannot be factored further.
- The numbers $4, 7, 10$, and 13 are all prime (since we only have integers of the form $3n+1$).
- On the other hand, $16 = 4 \cdot 4$ is not prime.
- The integer 100 may be written as a product of primes in two different ways,

$$100 = 10 \cdot 10 = 4 \cdot 25.$$

All of the factors, 4, 10 and 25, are prime in this world.

Moreover, the two factorizations are genuinely different.

Observations

- The problem in this world is that we do not have enough integers.
- We have to enlarge our set of integers.
- Suppose we also include the integers of the form $3n+2$.
- Then in this larger world the factors are no longer prime.
- We can factorize them further

$$4 = 2 \cdot 2, \quad 10 = 2 \cdot 5, \quad 25 = 5 \cdot 5.$$

- Using these factorizations, our apparent lack of unique factorization is resolved

$$100 = (2 \cdot 5) \cdot (2 \cdot 5) = (2 \cdot 2) \cdot (5 \cdot 5).$$

Subsection 1

Uniqueness of Factorization Revisited

Remarks on Uniqueness of a Factorization

- We saw that $\mathbb{Z}$ has unique factorization.
- In defining uniqueness, expressions such as $6 = 2 \cdot 3 = (-3) \cdot (-2)$ should really be counted as equivalent factorizations.
- Here the factors are simply permuted and multiplied both by -1.
- In general, suppose we have a factorization

$$r = a \cdot b$$

in some ring R.
- Mostly, R will be the ring of integers in some number field.
- Suppose u and v in R satisfy $uv = 1$.
- Then $r = a \cdot b = (ua) \cdot (vb)$ should be considered equivalent.

Units and Associates

Definition

Let R be a ring, and let $u \in R$. The element u is a **unit** in R if there exists an element $v \in R$ with

$$uv = 1.$$

Definition

Two elements $r_1, r_2 \in R$ are **associate** if there is a unit $u \in R$, such that

$$r_2 = ur_1.$$

This relation is symmetric, i.e., if $r_2 = ur_1$, then $r_1 = vr_2$, where $uv = 1$.

Equivalent Factorizations

- Given one factorization, we want to consider another as "equivalent" if it can be got from the first by:
  (a) Multiplying by units;
  (b) Rearranging the factors.

Definition

We say that two factorizations

$$r = a_1 a_2 \ldots a_n = b_1 b_2 \ldots b_n$$

are **equivalent** if, for some permutation π of $\{1, \ldots, n\}$,

$$b_i \text{ is an associate of } a_{\pi(i)}, \text{ for all } i.$$

Irreducible Elements and Prime Elements

- There are two possible generalizations of prime numbers to more general rings.

Definition

1. Let $p \in R$. Then p is **irreducible** if:
   (a) p is not a unit;
   (b) If $p = ab$, then either a or b is a unit.
2. Let $p \in R$. Then p is a **prime element** if, whenever $p \mid ab$ (in the sense that $ab = pr$, for some $r \in R$), then $p \mid a$ or $p \mid b$.

- When $R = \mathbb{Z}$, these two are equivalent.
- However, we will see that they are different in general.

  This phenomenon is a consequence of failure of unique factorization.

Subsection 2

Non-unique Factorization in Quadratic Number Fields

Examples of Non-Unique Factorizations

- Suppose that d is squarefree.
- Assume, for simplicity, $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$.
- In this case, the ring of integers in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$.

  Example: When $d = 10$, one has the equalities

  $$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

  For an example with d negative, consider, for $d = -5$,

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

  We can check (with some effort) that:
  - These factors are all irreducible, in the sense that they cannot be factored further;
  - The factorizations are different.

"Conjugation" and Norms

- We follow the prototype of the Gaussian integers.
- For $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, we define

$$\overline{a} = a - b\sqrt{d}.$$

- This will play the role of complex conjugation.
- Next, we define the **norm**

$$N(a + b\sqrt{d}) = N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

- If $\alpha \in \mathbb{Z}[\sqrt{d}]$, then $N(\alpha) \in \mathbb{Z}$, by a preceding result.
- If we are given two elements $\alpha_1 = a_1 + b_1\sqrt{d}$ and $\alpha_2 = a_2 + b_2\sqrt{d}$, we see that

$$N(\alpha_1\alpha_2) = \alpha_1\alpha_2\overline{\alpha_1\alpha_2} \stackrel{\overline{\alpha_1\alpha_2} = \overline{\alpha_1}\,\overline{\alpha_2}}{=} \alpha_1\overline{\alpha_1}\alpha_2\overline{\alpha_2} = N(\alpha_1)N(\alpha_2).$$

Units in $\mathbb{Z}[\sqrt{d}]$

Lemma

Suppose that $u \in \mathbb{Z}[\sqrt{d}]$. Then u is a unit if and only if $N(u) = \pm 1$.

- Suppose u is a unit.

  Then, there exists v, such that $uv = 1$.

  So $N(u)N(v) = N(uv) = N(1) = 1$.

  But $N(u)$ and $N(v)$ are integers whose product is 1.

  So $N(u)$ and $N(v)$ must both be ± 1.

  Conversely, suppose $N(u) = \pm 1$.

  Then $u\overline{u} = \pm 1$.

  Define $v = \pm \overline{u}$.

  Then $uv = 1$. So u is a unit.

Non-Equivalence of Factorizations

Lemma

1. In $\mathbb{Z}[\sqrt{10}]$, the two factorizations $6 = 2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$ are not equivalent.
2. In $\mathbb{Z}[\sqrt{-5}]$, the two factorizations $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are not equivalent.

- Suppose α_1 and α_2 are associate.

  Then, there is a unit u, such that $\alpha_2 = u\alpha_1$.

  It follows that

  $$N(\alpha_2) = N(u\alpha_1) = N(u)N(\alpha_1) = \pm N(\alpha_1).$$

  So, if two factorizations are equivalent, the norms of the factors on both sides are the same (up to sign).

Non-Equivalence of Factorizations (Cont'd)

- Consider, first, $\mathbb{Z}[\sqrt{10}]$.

$$\begin{array}{ll} N(2) = 2^2 - 10 \cdot 0^2 = 4, & N(3) = 3^2 - 10 \cdot 0^2 = 9, \\ N(4+\sqrt{10}) = 4^2 - 10 \cdot 1^2 = 6, & N(4-\sqrt{10}) = 4^2 - 10 \cdot (-1)^2 = 6. \end{array}$$

So the norms on the two sides are different.

- Similarly, in $\mathbb{Z}[\sqrt{-5}]$ we have the following:

$$\begin{array}{ll} N(2) = 2^2 + 5 \cdot 0^2 = 4, & N(3) = 3^2 + 5 \cdot 0^2 = 9, \\ N(1+\sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6, & N(1-\sqrt{-5}) = 1^2 + 5 \cdot (-1)^2 = 6. \end{array}$$

Again the norms on the two sides are different.

Irreducibility of the Factors

Lemma

1. In $\mathbb{Z}[\sqrt{10}]$, all of the factors in the equality $2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$ are irreducible.
2. In $\mathbb{Z}[\sqrt{-5}]$, all of the factors in the equality $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are irreducible.

- We first see that there are no elements $\alpha \in \mathbb{Z}[\sqrt{10}]$ with $N(\alpha) = \pm 2$.
  Suppose, to the contrary, that $\alpha = a + b\sqrt{10}$ is such an element.
  Then $N(\alpha) = a^2 - 10b^2 = \pm 2$.
  This means that either $a^2 - 10b^2 = 2$ or $a^2 - 10b^2 = -2$.
  Consider these equalities modulo 5.
  We see that we would need $a^2 \equiv 2 \pmod{5}$ or $a^2 \equiv 3 \pmod{5}$.
  But both of these are impossible.
  Similarly, there are no elements $\beta \in \mathbb{Z}[\sqrt{10}]$ with $N(\beta) = \pm 3$.

Irreducibility of the Factors ($\mathbb{Z}[\sqrt{10}]$)

- Suppose that 2 factorizes as $\alpha\beta$ in $\mathbb{Z}[\sqrt{10}]$.

  Then $4 = N(2) = N(\alpha)N(\beta)$.

  If $N(\alpha) = \pm 1$, $N(\beta) = \pm 4$, then α is a unit.

  If $N(\alpha) = \pm 4$, $N(\beta) = \pm 1$, then β is a unit.

  So the only possibility of factorizing 2 into non-units occurs if $N(\alpha) = N(\beta) = \pm 2$.

  We have seen that there are no such elements.

  In the same way, if 3 were to factorize as $\alpha\beta$ into non-units, then $N(\alpha) = N(\beta) = \pm 3$. We have seen that this is not possible.

  Finally, the only way to factorize $4 \pm \sqrt{10}$ into non-units would be as the product of an element of norm ± 2 and an element of norm ± 3.

  This is impossible.

Irreducibility of the Factors ($\mathbb{Z}[\sqrt{-5}]$)

- Exactly the same argument works for $\mathbb{Z}[\sqrt{-5}]$.

  Suppose there is an element $\alpha = a + b\sqrt{-5}$ of norm ± 2.

  This would require $a^2 + 5b^2 = \pm 2$.

  So $a^2 + 5b^2 = 2$ (as $a^2 + 5b^2$ is necessarily positive).

  Arguing modulo 5, there are clearly no integral solutions.

  Nor are there any solutions to $a^2 + 5b^2 = 3$.

  So there are no elements of norm 3.

  The same argument as in the case of $\mathbb{Z}[\sqrt{10}]$ now applies to $\mathbb{Z}[\sqrt{-5}]$.

Comments on $\mathbb{Z}[\sqrt{10}]$ and $\mathbb{Z}[\sqrt{-5}]$

- We have two non-equivalent factorizations into irreducible elements.
- Therefore, factorization in these rings is not unique.
- The factors are irreducible, but they are not prime.
  - First, note that $2 \mid 6$. So $2 \mid (4+\sqrt{10})(4-\sqrt{10})$.
  - However, $2 \nmid 4 \pm \sqrt{10}$.
    Indeed,
    $$\frac{4 \pm \sqrt{10}}{2} = 2 \pm \frac{1}{2}\sqrt{10} \notin \mathbb{Z}[\sqrt{10}].$$

Subsection 3

Kummer's Ideal Numbers

Kummer's Idea of Ideal Numbers

- Kummer tried to repair the non-uniqueness of factorization in quadratic fields by enlarging the integers to include "**ideal numbers**".
- Consider, e.g., $6 = 2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$ in $\mathbb{Z}[\sqrt{10}]$.

  Kummer's idea was to invent symbols $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$, such that

  $$\begin{array}{rr} 2 = \mathfrak{a}_1 \times \mathfrak{a}_2, & 3 = \mathfrak{a}_3 \times \mathfrak{a}_4, \\ 4+\sqrt{10} = \mathfrak{a}_1 \times \mathfrak{a}_3, & 4-\sqrt{10} = \mathfrak{a}_2 \times \mathfrak{a}_4. \end{array}$$

  Then the non-unique factorization is repaired, since

  $$2 \cdot 3 = (\mathfrak{a}_1 \cdot \mathfrak{a}_2) \cdot (\mathfrak{a}_3 \cdot \mathfrak{a}_4) = (\mathfrak{a}_1 \cdot \mathfrak{a}_3) \cdot (\mathfrak{a}_2 \cdot \mathfrak{a}_4) = (4+\sqrt{10})(4-\sqrt{10}).$$

- These are fictitious symbols, without any real meaning.
- Kummer hoped that the symbols could be manipulated so that meaningful results are obtained.
- Dedekind reformulated Kummer's idea in more concrete terms.

The Ring of Integers $R=\mathbb{Z}[\sqrt{10}]$ of $\mathbb{Q}(\sqrt{10})$

- Consider again the factorizations into "ideal numbers"
$$2=\mathfrak{a}_1\times\mathfrak{a}_2,\quad 4+\sqrt{10}=\mathfrak{a}_1\times\mathfrak{a}_3.$$
- Then 2 would be a multiple of $\mathfrak{a}_1$.
- So any multiple of 2 would also be a multiple of $\mathfrak{a}_1$.
- Similarly, $4+\sqrt{10}$ is also a multiple of $\mathfrak{a}_1$.
- So any multiple of $4+\sqrt{10}$ is a multiple of $\mathfrak{a}_1$.
- Combining these, any $\mathbb{Z}[\sqrt{10}]$-linear combination of 2 and $4+\sqrt{10}$ should be a multiple of $\mathfrak{a}_1$.
- Let R denote the ring of integers $\mathbb{Z}[\sqrt{10}]$ of $\mathbb{Q}(\sqrt{10})$.
- The set of multiples of 2, namely $2R$, must be contained in the set of multiples of $\mathfrak{a}_1$. Thus, $2R\subseteq\mathfrak{a}_1R$.
- Similarly, $(4+\sqrt{10})R\subseteq\mathfrak{a}_1R$.
- Thus,
$$2R+(4+\sqrt{10})R\subseteq\mathfrak{a}_1R.$$

The Ring of Integers $R = \mathbb{Z}[\sqrt{10}]$ (Cont'd)

- We show the inclusion $2R + (4+\sqrt{10})R \subseteq \mathfrak{a}_1 R$ ought to be an equality.
- First, note that $\mathfrak{a}_1 R = R$ implies $\mathfrak{a}_1$ would be invertible.
- So $\mathfrak{a}_1$ would be a unit.
- But we do not want our factors to be units.
- A calculation gives

$$2R + (4+\sqrt{10})R = \{m + n\sqrt{10} : m, n \in \mathbb{Z},\ 2 \mid m\}.$$

- This set has index 2 in R (informally, half of the elements of R are in this set).
- There is no room for anything between R and $2R + (4+\sqrt{10})R$.
- But $\mathfrak{a}_1 R$ is strictly contained in R and contains $2R + (4+\sqrt{10})R$.
- So we must have $\mathfrak{a}_1 R = 2R + (4+\sqrt{10})R$.

Dedekind's Ideals

- Instead of thinking of $\mathfrak{a}_1$ as an "ideal number", Dedekind's idea was to work with the set $\mathfrak{a}_1 R$.
- Now $\mathfrak{a}_1$ is not actually an element.
- We shall simply write $\mathfrak{a}_1$ for the set, i.e.,

$$\mathfrak{a}_1 = 2R + (4 + \sqrt{10})R.$$

- In this viewpoint, even the symbol 2, which we would normally think of as a number, should be viewed as the set $2R$ of all multiples of 2.

Dedekind's Ideals (Cont'd)

- In $\mathbb{Z}$, suppose a divides b.
- Then b is a multiple of a.
- Any multiple of b is also a multiple of a.
- Symbolically, $b\mathbb{Z} \subseteq a\mathbb{Z}$.
- Thus, $a \mid b$ if and only if $b\mathbb{Z} \subseteq a\mathbb{Z}$.
- In the example above, since $\mathfrak{a}_1$ contains all multiples of 2, one could say that $\mathfrak{a}_1$ is a **divisor** of 2.
- Similarly, $\mathfrak{a}_1$ is also a divisor of $4 + \sqrt{10}$, as one would hope.
- There are no *elements* of R which divide 2 and $4 + \sqrt{10}$ except units.
- However, there are certain *subsets* of R which contain $2R$ and $(4 + \sqrt{10})R$ and are strictly contained in $1R$.

Subsection 4

Ideals

Ideals of a Ring

- The prototype for Dedekind's sets are all the multiples of a given element of R, or, more generally (when unique factorization fails), all the linear combinations of some set of elements.

Definition

An **ideal** I of a commutative ring R is a subset of R, such that:

1. $0_R \in I$;
2. If i and $i' \in I$, then $i - i' \in I$;
3. If $i \in I$ and $a \in R$, then $ai \in I$.

- The second requirement here is equivalent to I being closed under both addition and additive inverses.
- These conditions are the same as those needed for I to be a **module**.
- The only difference is that ideals are subsets of the ring.

Examples

1. Any ring R is an ideal in itself.
2. For any ring R, $\{0_R\}$ is an ideal in R.
3. Let R be any ring, and let $r \in R$.

   Let $I = rR$, all the multiples of r.

   Then I is an ideal in R.

   - The element 0 is a multiple of r;
   - The difference of any two multiples of r is again a multiple of r;
   - Any multiple of a multiple of r is certainly a multiple of r.

- The last example gives a large class of ideals.
- In some rings, all ideals are of this form.

Ideals in $\mathbb{Z}$

Lemma

In $\mathbb{Z}$, every ideal is of the form $n\mathbb{Z}$, for some integer n.

- Let I be an ideal of $\mathbb{Z}$.

  First suppose $I \neq \{0\}$.

  I contains a non-zero integer.

  Then it will contain a positive integer.

  Indeed, suppose $k \in I$, and $k < 0$.

  By the definition of ideal, $(-1)k = -k \in I$ also.

  Let n be the smallest positive integer contained in I.

  Clearly I then contains all multiples of n.

  So $I \supseteq n\mathbb{Z}$.

Ideals in $\mathbb{Z}$ (Cont'd)

- If $a \in I$, we can write, by the division algorithm,

$$a = qn + r, \quad 0 \leq r < n.$$

  As a and $n \in I$, we conclude that $r \in I$.

  As n was the smallest positive integer in I, we conclude that $r = 0$.

  So a is a multiple of n.

  Thus, $I = n\mathbb{Z}$.

  On the other hand, suppose $I = \{0\}$.

  We can regard it as $0\mathbb{Z}$.

  So I is again of the required form.

- For a general ring R, not every ideal in R is of the form rR.
- The reason that it holds in $\mathbb{Z}$ is because of Euclid's algorithm.

Operations on Ideals

Lemma

Let R be a ring.

1. If I and J are ideals of R, then so is $I \cap J$.
2. More generally, if $\{I_\alpha\}_{\alpha \in A}$ is any family of ideals of R, then so is their intersection $\bigcap_{\alpha \in \Lambda} I_\alpha$.
3. If I and J are both ideals of R, then so is
$$IJ = \{\text{finite sums of elements of the form } ij : i \in I \text{ and } j \in J\}.$$
and $IJ \subseteq I \cap J$.
4. If I and J are both ideals of R, then so is
$$I + J = \{i + j : i \in I \text{ and } j \in J\}.$$

Operations on Ideals (Cont'd)

1. We check the axioms.

   By hypothesis, I and J are ideals.

   So $0_R \in I$ and $0_R \in J$.

   Therefore, $0_R \in I \cap J$.

   Suppose i and $j \in I \cap J$.

   Then i and j each lie in both I and J.

   As these are ideals, $i - j \in I$ and $i - j \in J$.

   Thus, $i - j \in I \cap J$.

   Finally, suppose $i \in I \cap J$ (so $i \in I$ and $i \in J$) and $r \in R$.

   Then $ri \in I$ as I is an ideal, and similarly $ri \in J$.

   So $ri \in I \cap J$.

   This shows that $I \cap J$ is an ideal.
2. Similar to the first assertion.

Operations on Ideals (Cont'd)

3. We have $0_R \in I$ (or J).

   So $0_R \in IJ$.

   Suppose given two finite sums of terms of the form ij.

   Their difference is clearly again a finite sum of terms of the same form.

   So IJ is closed under addition.

   Finally, suppose given a sum $\sum_k i_k j_k \in IJ$ and an element $r \in R$.

   We see that

   $$r\left(\sum_k i_k j_k\right) = \sum_k (r i_k) j_k.$$

   As I is an ideal, all the bracketed terms $r_i k \in I$.

   So this is again a finite sum of products of elements of I with elements of J.

Operations on Ideals (Cont'd)

- For the inclusion, an element of IJ is a finite sum of elements of the form ij, with $i \in I$ and $j \in J$.

  As $J \subseteq R$, we have $j \in R$.

  So, by definition of ideals, $ij \in IR = I$.

  Similarly, $I \subseteq R$.

  So $i \in R$.

  Hence, $ij \in RJ = J$.

  It follows that all terms $ij \in I \cap J$.

  So $IJ \subseteq I \cap J$.

Operations on Ideals (Conclusion)

4. We have $0_R \in I$ and $0_R \in J$.
   So $0_R = 0_R + 0_R \in I + J$.
   Next, we take $i_1 + j_1$ and $i_2 + j_2 \in I + J$.
   Their difference is
   $$(i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J,$$
   as $i_1 - i_2 \in I$ and $j_1 - j_2 \in J$.
   Finally, suppose $i + j \in I + J$, and $r \in R$.
   Since I and J are ideals, $r(i + j) = ri + rj \in I + J$.
   We conclude that $I + J$ is an ideal.

The Union of Ideals May Not Be An Ideal

- If I and J are ideals, *it is not generally true that* $I \cup J$ *is an ideal.*
- Consider the ring $R = \mathbb{Z}$.

  Take the ideals $I = 2\mathbb{Z}$ and $J = 3\mathbb{Z}$.

  We have:
  - $2 \in I \subset I \cup J$;
  - $3 \in J \subset I \cup J$;
  - However, their sum, 5, is not in $I \cup J$.

  Thus $I \cup J$ is not an ideal.

Ideals and Units

Lemma

Suppose that R is a ring, and that I is an ideal of R. If I contains a unit of R, then $I = R$.

- Suppose $u \in I$ is a unit in R.

  Then, there exists $v \in R$, such that $uv = 1_R$.

  Thus $1_R \in I$.

  Now, for all $a \in R$, $a \cdot 1_R = a$ must lie in the ideal.

  Thus, $a \in I$.

  So $R \subseteq I$.

Principal Ideals and Associates

Lemma

Suppose that R is an integral domain (i.e., has no zero divisors). Suppose that $a, b \in R$. Then $aR = bR$ if and only if a and b are associate.

- Suppose that $aR = bR$.

  We have
  $$a = a \cdot 1_R \in aR = bR.$$

  So $a = bu$, for some element $u \in R$.

  Similarly, $b = av$, for some element $v \in R$.

  Then
  $$a = bu = (av)u = a(vu).$$

  As R is an integral domain, this only happens if $vu = 1$.

  So u and v are units.

Principal Ideals and Associates (Cont'd)

- Conversely, if a and b are associate, then:
  - $a = bu$, for some unit u;
  - $b = av$, for the unit v, with $uv = 1$.

  Thus, any multiple $br \in bR$ of b can also be written avr.

  So it lies in aR.

  Then $bR \subseteq aR$.

  The reverse inclusion is similar.
- We are going to prove that ideals in rings of integers of number fields factorize uniquely into "prime ideals".
- The lemma then shows that the units no longer play any role.

Characterization of Fields in terms of Ideals

Lemma

R is a field if and only if the only ideals in R are $\{0_R\}$ and R itself.

- If R is a field, then every non-zero element is a unit.
  Suppose I is an ideal of R.
  Suppose I contains a non-zero element.
  Then I contains a unit. So $I = R$, by a previous lemma.
  Conversely, suppose R is not a field.
  Then there exists some non-zero element r which is not a unit.
  Then the collection
  $$rR = \{ra : a \in R\}$$
  is an ideal in R.
  It is non-zero as it contains $r = r \cdot 1_R \neq 0$.
  Nor is there $a \in R$, such that $ra = 1_R$, as r is not a unit.
  So rR is not all of R either.

Subsection 5

Generating Sets for Ideals

Ideals Generated by Sets

Definition

Let X be a (possibly infinite) subset of R.
Then the intersection of all ideals containing X is an ideal of R.
It is clearly contained in all ideals containing X.
This ideal is denoted by $\langle X\rangle$ and called the **ideal generated by** X.

Proposition

Let X be a subset of R. Then

$$\langle X\rangle = \{\text{all finite sums of elements of the form } rx, \text{ with } r\in R,\ x\in X\}.$$

- Define

$$I = \{\text{all finite sums of elements of the form } rx, \text{ with } r\in R,\ x\in X\}.$$

We want to show that $I = \langle X\rangle$.

Ideals Generated by Sets (Cont'd)

- One inclusion is clear from the definition.
  I is an example of an ideal containing X.
  So the intersection $\langle X\rangle$ of all such ideals must be a subset of I.
  We need to check $I \subseteq \langle X\rangle$.
  Let J be any ideal containing all $x \in X$.
  For any $r \in R$, as $x \in J$ and J is an ideal, $rx \in J$.
  So all elements $r_1x_1,\ldots,r_nx_n$, with $r_i \in R$ and $x_i \in X$ lie in J.
  But J is also closed under addition.
  So $r_1x_1+\cdots+r_nx_n$ is also in J.
  But any element of I is of this form.
  So each element of I lies in J.
  This shows that, if J is any ideal containing all $x \in X$, then $J \supseteq I$.
  However, $\langle X\rangle$ is an ideal containing every element of X.
  So $\langle X\rangle \supseteq I$.

Remarks

- The typical element of $\langle X \rangle$ is
$$r_1 x_1 + r_2 x_2 + \cdots + r_k x_k,$$
for some $k \in \mathbb{N}$.
- In particular, suppose $X = \{x_1, \ldots, x_n\}$ is a finite set.
- The ideal $\langle X \rangle$, in this case, is also denoted by
$$\langle x_1, \ldots, x_n \rangle.$$
- It consists of all sums of the form
$$\sum_{i=1}^{n} r_i x_i, \quad \text{with } r_i \in R.$$
- In other words, we have
$$\langle x_1, \ldots, x_n \rangle = x_1 R + \cdots + x_n R.$$

Minimal Generating Sets

- Consider the ideal $\langle 2,3\rangle$ in $\mathbb{Z}$.
- This consists of every integer n which can be written as

$$2a+3b, \quad \text{for integers } a,b.$$

- But every integer may be written in this way $(n=2\cdot(-n)+3\cdot n)$.
- So $\mathbb{Z}=\langle 2,3\rangle=\langle 1\rangle$.
- Note that $\langle 2\rangle$ and $\langle 3\rangle$ are both proper subsets of $\mathbb{Z}$.
- So this shows that $\{2,3\}$ is a minimal set of generators.
- This means that no proper subset generates the whole ideal.
- Now, both $\{1\}$ and $\{2,3\}$ are minimal generating sets.
- So ideals may have minimal generating sets of different sizes (in contrast to vector spaces).

Principal Ideals

Definition

Ideals of the form $\langle r \rangle$, with one generator, are called **principal**.

Example: Rings exist where not every ideal is principal.

Consider, e.g., the ring $\mathbb{Z}[X]$.

Let I be the set of polynomials whose constant term is divisible by 2.

I is an ideal of $\mathbb{Z}[X]$.

It is not of the form $r\mathbb{Z}[X]$, for any r.

Both 2 and X would have to be multiples of r.

This means that r would have to be ± 1.

But ± 1 does not belong to I.

So this is also not possible.

Principal Ideals (Cont'd)

- In fact, we have $I = \langle 2, X \rangle$.
  Suppose
  $$f(X) = \sum_{n=0}^{d} a_n X^n \in I.$$
  We can write it as
  $$f(X) = a_0 + X \sum_{n=1}^{d} a_n X^{n-1},$$
  where $a_0 \in 2\mathbb{Z} \subseteq 2\mathbb{Z}[X]$.
  Clearly
  $$X \sum_{n=1}^{d} a_n X^{n-1} \in X \cdot \mathbb{Z}[X].$$
  It follows that every polynomial in I can be written as the sum of something in $2\mathbb{Z}[X]$ and something in $X\mathbb{Z}[X]$.
  So $I \subseteq \langle 2, X \rangle$. The opposite inclusion is clear.

Example

- Suppose that $R = \mathbb{Z}[\sqrt{10}]$.
  Consider the set
  $$\mathfrak{a}_1 = 2R + (4+\sqrt{10})R = \langle 2, 4+\sqrt{10}\rangle.$$
  It is an ideal in R.
  It is not possible to write $\mathfrak{a}_1$ as $\langle\alpha\rangle$, for any $\alpha \in R$.
  Suppose every element of $\mathfrak{a}_1$ is a multiple of α.
  In particular, we would have
  $$2 = \alpha\beta \quad \text{and} \quad 4+\sqrt{10} = \alpha\gamma.$$
  Taking norms,
  $$4 = N(2) = N(\alpha)N(\beta), \quad 6 = N(4+\sqrt{10}) = N(\alpha)N(\gamma).$$
  Thus, this means that $N(\alpha) = 1$ or $N(\alpha) = 2$.

Example (Cont'd)

- We know that there are no elements in $\mathbb{Z}[\sqrt{10}]$ with norm 2.

  If $N(\alpha)=1$, α would be a unit.

  So $\langle\alpha\rangle$ would equal R.

  However, every element in $\mathfrak{a}_1$ has an even number as a coefficient of 1.

  So $1 \notin \mathfrak{a}_1$.
- It is traditional to use Gothic letters $\mathfrak{a}, \mathfrak{b}$, etc., for ideals in rings of integers of number fields.
- However, we will use I, J, etc., for ideals in more general rings.

Noetherian Rings

- An ideal of R is called **finitely generated** if it has a finite generating set.
- A ring R is called **Noetherian** if every ideal in R is finitely generated.
- We shall see that rings of integers of number fields have this property.

IJ versus $I \cap J$

- In a previous lemma, we saw that $IJ \subseteq I \cap J$.
- Sometimes we can have equality.
- Consider, e.g., $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, $J = 3\mathbb{Z}$

  Then $IJ = \langle 2 \rangle \langle 3 \rangle = \langle 6 \rangle$.

  Also $I \cap J$ consists of all integers in $I \cap J$, which are those integers simultaneously divisible by 2 (so lie in I) and by 3 (so lie in J).

  So it consists of all integers that are multiples of 6.

  So $I \cap J = \langle 6 \rangle = IJ$.
- On the other hand, there are examples where $IJ \neq I \cap J$.
- Let $R = \mathbb{Z}$, $I = J = 2\mathbb{Z}$.

  Then $IJ = \langle 2 \rangle \langle 2 \rangle = \langle 4 \rangle$. But $I \cap J = \langle 2 \rangle$.
- The impression we get is that the equality of IJ and $I \cap J$ should be related to whether they are "coprime" in a certain sense.

Divisibility for Ideals

Definition

As already remarked, the notation $\alpha \mid \beta$ means that β is a multiple of α.
In particular, any multiple of β is a multiple of α. So $\langle \beta \rangle \subseteq \langle \alpha \rangle$.
We extend the notation to ideals by writing $\mathfrak{a} \mid \mathfrak{b}$ to mean $\mathfrak{b} \subseteq \mathfrak{a}$.
We may use either notation interchangeably.

- Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in the ring of integers $\mathbb{Z}_K$ of a number field K.
- We will see that $\mathfrak{b} \subseteq \mathfrak{a}$ iff there is some ideal $\mathfrak{c}$ of $\mathbb{Z}_K$, such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.
- This is another definition of division one might have come up with.

Subsection 6

Ideals in Quadratic Fields

Non-Uniqueness of Factorization

- We saw that $\mathbb{Q}(\sqrt{d})$ does not always have unique factorization.
- E.g., let $d = -5$.
  Consider the ring of integers is $\mathbb{Z}[\sqrt{-5}]$.
  Then
  $$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$
- In terms of ideals, we can consider the ideal $\langle 6 \rangle \subset \mathbb{Z}[\sqrt{5}]$.
  Then the above factorizations correspond to factorizations of ideals,
  $$\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle,$$
  where $\langle a \rangle$ denotes the principal ideal generated by a, namely $a\mathbb{Z}[\sqrt{-5}]$.
- We saw 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{-5}]$.
  This means that the ideal $\langle 3 \rangle$, say, cannot be written as the product of principal ideals (if $3 = \alpha \cdot \beta$, then $\langle 3 \rangle = \langle \alpha \rangle \langle \beta \rangle$).
- But $\langle 3 \rangle$ may be factored as a product of non-principal ideals.

Repairing Non-Uniqueness of Factorization

- The obstruction to unique factorization is coming from the fact that not every ideal in $\mathbb{Z}[\sqrt{-5}]$ is principal.
- Indeed, consider the two ideals

$$\begin{aligned} \mathfrak{a}_1 &= \langle 3, 1+\sqrt{-5}\rangle; \\ \mathfrak{a}_2 &= \langle 3, 1-\sqrt{-5}\rangle. \end{aligned}$$

- We work out the product $\mathfrak{a}_1\mathfrak{a}_2$,

$$\begin{aligned} \mathfrak{a}_1\mathfrak{a}_2 &= \langle 3\cdot 3, 3(1-\sqrt{-5}), 3(1+\sqrt{-5}), (1+\sqrt{-5})(1-\sqrt{-5})\rangle \\ &= \langle 9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6\rangle. \end{aligned}$$

- That is, every element of the product $\mathfrak{a}_1\mathfrak{a}_2$ is of the form

$$9\alpha + (3-3\sqrt{-5})\beta + (3+3\sqrt{-5})\gamma + 6\delta,$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$.

Repairing Non-Uniqueness of Factorization (Cont'd)

- It is clear that the collection of such elements must be contained in the set
$$\{A+B\sqrt{-5} : 3 \mid A, 3 \mid B\}.$$
- Conversely, consider an element $3A+3B\sqrt{-5}$.
- It lies in $\mathfrak{a}_1\mathfrak{a}_2$ on taking, e.g.,
$$\alpha = A+B\sqrt{-5}, \quad \beta=\gamma=0, \quad \delta=-\alpha.$$
- It follows that
$$\mathfrak{a}_1\mathfrak{a}_2 = \{A+B\sqrt{-5} : 3 \mid A, 3 \mid B\}.$$
- That is, $\mathfrak{a}_1\mathfrak{a}_2$ consists of all multiples of 3.
- Thus, $\mathfrak{a}_1\mathfrak{a}_2 = \langle 3\rangle$.

Repairing Non-Uniqueness of Factorization (Conclusion)

- Similarly, let $\mathfrak{b} = \langle 2, 1+\sqrt{-5}\rangle$.
- Then a typical element of $\mathfrak{b}^2$ is given by

$$4\alpha + (2+2\sqrt{-5})\beta + (1+\sqrt{-5})^2\gamma.$$

- An easy check shows that $\mathfrak{b}^2 = \langle 2\rangle$.
- We may also verify that:
  - The ideal $\langle 1+\sqrt{-5}\rangle$ is given by $\mathfrak{a}_1\mathfrak{b}$;
  - The ideal $\langle 1-\sqrt{-5}\rangle$ is given by $\mathfrak{a}_2\mathfrak{b}$.
- Now the two distinct factorizations $6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ actually become the same factorization in terms of the ideals,

$$\langle 6\rangle = \mathfrak{b}^2\mathfrak{a}_1\mathfrak{a}_2 = (\mathfrak{a}_1\mathfrak{b})(\mathfrak{a}_2\mathfrak{b}).$$

- By introducing ideals, we have repaired the non-uniqueness of factorization in this case.

Subsection 7

Unique Factorization Domains and Principal Ideal Domains

Unique Factorization Domains

Definition

A ring R is a **unique factorization domain** (**UFD**) if it is an integral domain in which every non-zero $a \in R$ may be written

$$a = up_1 \cdots p_n,$$

where u is a unit and each p_i is irreducible (i.e., factorization into irreducibles exists). Further, if $a = vq_1 \cdots q_m$ is another such factorization, then $n = m$ and p_i is an associate of $q_{\pi(i)}$, for some permutation of $\{1, \ldots, n\}$ (i.e., factorization into irreducibles is unique).

Example: We have seen that:

- $\mathbb{Z}$ and $\mathbb{Z}[i]$ both have unique factorization, and are therefore UFDs;
- Neither $\mathbb{Z}[\sqrt{10}]$ nor $\mathbb{Z}[\sqrt{-5}]$ are UFDs.

Principal Ideal Domains

- Recall that a **principal ideal** is one of the form aR.
- For some rings, such as $\mathbb{Z}$, these are the only ideals.

Definition

Let R be an integral domain. Then R is a **principal ideal domain** (abbreviated **PID**) if every ideal of R is principal.

Example: Examples of integral domains which are not PIDs:

- $\mathbb{Z}[X]$ has an ideal $\langle 2, X\rangle$ which we saw is not principal;
- $\mathbb{Z}[\sqrt{10}]$ has an ideal $\langle 2, \sqrt{10}\rangle$ which is not principal.

- Every field K is a PID.

  Its only ideals are:

  - $\langle 0_K\rangle$;
  - K itself, which may be written as $\langle 1_K\rangle$.

Euclidean Domains

- We have already seen that $\mathbb{Z}$ is a PID.
- The proof that $\mathbb{Z}$ is a PID relies on Euclid's algorithm.

Definition

An integral domain R is a **Euclidean domain** if there is a function

$$\phi : R - \{0_R\} \to \mathbb{Z}_{>0},$$

such that:

1. $a \mid b \Rightarrow \phi(a) \leq \phi(b)$;
2. If $a \in R$, $b \in R - \{0_R\}$, then there exist q and r in R, such that

$$a = bq + r$$

and either $r = 0$ or $\phi(r) < \phi(b)$.

ϕ is called a **Euclidean function** on R.

Examples

- We know that $\mathbb{Z}$ is a Euclidean domain.
  To see this, define $\phi(n) = |n|$.
- We also know that, for any field K, $K[X]$ is a Euclidean domain.
  In this case, we define $\phi(f) = \deg f$.
- We also saw that there is also a Euclidean algorithm in $\mathbb{Z}[i]$.
  Here, we define $\phi(a + ib) = a^2 + b^2$.

Euclidean Domains are PIDs

Proposition

Every Euclidean domain is a principal ideal domain.

- Let I be an ideal of the Euclidean domain R, and suppose $I \neq \{0\}$.

  Consider the set of all values taken by the Euclidean function ϕ on the nonzero elements of the ideal I,

  $$D = \{\phi(i) : i \in I, i \neq 0\} \subseteq \mathbb{Z}_{>0}.$$

  Choose $b \in I$, such that $\phi(b)$ is the minimal value in D.

  Now $b \in I$.

  So I contains all multiples of b.

  Hence, $I \supseteq \langle b \rangle$.

Euclidean Domains are PIDs (Cont'd)

- Conversely, take $a \in I$.

  We can write
  $$a = qb + r,$$
  where either $r = 0$ or $\phi(r) < \phi(b)$.

  As $a, b \in I$, we conclude that $r = a - qb \in I$.

  But b is an element of I with the least possible value of ϕ.

  So it cannot be that $\phi(r) < \phi(b)$.

  Hence, $r = 0$.

  Thus, every element of I is a multiple of b.

  This shows that $I \subseteq \langle b \rangle$.
- Not every PID is a Euclidean domain.
- It is known that, for $\rho = \frac{1+\sqrt{-19}}{2}$, $\mathbb{Z}[\rho]$ is a PID, but not Euclidean.

Highest Common Factors

Definition

Let R be a PID, and let a and b be in R.
The ideal $\langle a, b\rangle = aR + bR$ is principal.
So it can be written $\langle d\rangle = dR$, for some element $d \in R$.
Then d is a **highest common factor** of a and b.
Highest common factors are unique up to multiplication by a unit.

- This agrees with the usual notion in $\mathbb{Z}$.
- The difference between PIDs and Euclidean domains is not in the essential point that highest common factors exist, but rather that there is a good way to compute them in Euclidean domains.
- Euclidean domains have a Euclidean algorithm, which may be absent in more general PIDs.

PIDs are UFDs

Theorem

Every PID is a UFD.

- Suppose first that there exists an element a without any factorization.

  Call such elements "bad", and other elements "good".

  Then a is not a unit, nor an irreducible.

  So we must have $a = a_1 b_1$, for some a_1, b_1.

  At least one of a_1 and b_1 must be bad (otherwise the product of the factorizations for a_1 and b_1 gives a factorization of a).

  Suppose a_1 is bad.

  Then, in the same way, $a_1 = a_2 b_2$, with a_2 bad.

  Continuing in this way, we get a sequence of bad elements $a_1, a_2, \ldots$.

  Further, as a_i is a multiple of a_{i+1}, we see that $\langle a_{i+1} \rangle \supset \langle a_i \rangle$.

  Moreover, these are different as no b_{i+1} is a unit.

PIDs are UFDs (Cont'd)

- Define
$$I = \bigcup_{i=1}^{\infty} \langle a_i \rangle.$$
It is easy to check that this is an ideal.
Therefore, $I = \langle c \rangle$, for some $c \in R$.
Thus $c \in I$.
So c lies in some $\langle a_n \rangle$.
Then
$$I = \langle c \rangle \subseteq \langle a_n \rangle \subset \langle a_{n+1} \rangle \subseteq I.$$
This is a contradiction.
So no bad elements exist.
It follows that every element has some factorization.

PIDs are UFDs (Claim)

Claim: Every irreducible element $p \in R$ satisfies $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Let p be an irreducible element.

Suppose $p \mid ab$.

If $p \nmid a$, we show that $p \mid b$.

Consider the ideal $\langle p, a \rangle = pR + aR$.

As R is a PID, $\langle p, a \rangle = \langle d \rangle$.

Then $d \mid p$ and $d \mid a$.

As p is irreducible, either d is a unit or d is an associate of p.

The latter is impossible, as $p \nmid a$.

Thus $\langle p, a \rangle$ is generated by a unit d.

So $\langle p, a \rangle = R$.

Thus, we can find $r, s \in R$, such that $pr + as = 1_R$.

Multiply by b to get $p(br) + (ab)s = b$.

We see that b is a multiple of p, as $p \mid ab$.

PIDs are UFDs (Uniqueness)

- We finally show uniqueness of factorization.

  Suppose we had an element n with two factorizations:

  $$n = up_1 \cdots p_r = vq_1 \cdots q_s,$$

  where u and v are units, and the p_i, q_j are irreducible.

  Then p_1 divides n and therefore the right-hand side.

  By the Claim, p_1 divides some q_i, q_1 say (permute the q_i if not).

  But both p_1 and q_1 are irreducible.

  So we must have $q_1 = u_1 p_1$ where u_1 is a unit.

  Cancel p_1 and q_1 from the factorizations (R is an integral domain).

  We can continue in this way until all prime factors on the left-hand side are paired off with factors on the right-hand side, and only units are left.

Remarks

- Note that the proof that every element has some factorization (i.e., there are no bad elements) would work given only the weaker statement that every ideal (in particular, the ideal I) has a finite generating set, so that $I = \langle d_1, \ldots, d_k \rangle$.
- This is the defining property of a **Noetherian ring**.
- We will see in the next subsection that rings of integers of number fields are always Noetherian.

Remarks (Cont'd)

- We will show later that for rings of integers in number fields, the converse to this theorem is true.

  Such a ring is a PID if and only if it is a UFD.

- This is false in a general ring.
- It is known that, if R is a UFD, then so is the polynomial ring $R[X]$.
- This shows that $\mathbb{Z}[X]$ is a UFD.
- We have already seen that it is not a PID.

  E.g., the ideal $\langle 2, X\rangle$ is not principal.

Subsection 8

The Noetherian Property

Noetherian Rings

- The property of unique factorization in a number field is equivalent to the ring of integers having the property that every ideal is principally generated, i.e., has one generator.
- Many number fields do not have unique factorization, and therefore do not have this property.
- However, there is a weaker property that they all satisfy:

Definition

A **Noetherian ring** is a ring R in which every ideal is finitely generated.

- We saw that $\mathbb{Z}_K$ has an integral basis, and that this is equivalent to the property that $\mathbb{Z}_K$ is a free abelian group of rank $[K:\mathbb{Q}]$.
- We will show that this implies that $\mathbb{Z}_K$ is Noetherian.

Subgroups of Free Abelian Groups of Finite Rank

Proposition

Suppose H is a subgroup of a free abelian group G of rank n. Then H is also a free abelian group of rank at most n.

- By induction on n.
  For $n=1$, $G \cong \mathbb{Z}$.
  By the Euclidean algorithm, $H = k\mathbb{Z}$, for some k.
  If $k=0$, then H has rank 0.
  Otherwise, H has rank 1 and has finite index.
  Suppose the result is true for free abelian groups of rank $n-1$.
  Let G be a free abelian group of rank n.
  We can write
  $$G = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Subgroups of Free Abelian Groups of Finite Rank (Cont'd)

- Let $\pi : G \to \mathbb{Z}$ map $a_1\omega_1 + \cdots + a_n\omega_n$ to a_1.
  Let
  $$K = \ker\pi = \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n,$$
  a free abelian group of rank $n-1$.
  Then $\pi(H) \subseteq \mathbb{Z}$, and by the base, $\pi(H) = \{0\}$ or $\pi(H)$ is infinite cyclic.
  - Suppose $\pi(H) = \{0\}$.
    Then $H \subset \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$.
    This is a subgroup of a free abelian group of rank $n-1$.
    The result follows by the inductive hypothesis.
  - Suppose $\pi(H)$ is infinite cyclic.
    Choose $h_1 \in H$, such that $\pi(h_1)$ generates $\pi(H)$.
    It is easy to prove that $H = \mathbb{Z}h_1 \oplus (H \cap K)$.
    $H \cap K$ is contained in K, a free abelian group of rank $n-1$.
    The inductive hypothesis shows that $H \cap K$ is a free abelian group, say $\mathbb{Z}h_2 + \cdots + \mathbb{Z}h_r$. From this, the claim follows.

Rings of Integers are Noetherian

Theorem

If K is a number field, then $\mathbb{Z}_K$ is Noetherian.

- An ideal is an (additive) subgroup of $\mathbb{Z}_K$.
  So we can apply the proposition to conclude that every ideal is also a free abelian group of finite rank.
  Equivalently, it is finitely generated as a $\mathbb{Z}$-module.
  Thus, for some elements $\omega_1, \ldots, \omega_r \in I$,
  $$I = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_r.$$
  Since I is an ideal, $\mathbb{Z}\omega_i \subseteq I$.
  Clearly, $\mathbb{Z}_K\omega_i \supseteq \mathbb{Z}\omega_i$.
  So
  $$\mathbb{Z}_K\omega_1 + \cdots + \mathbb{Z}_K\omega_r \supseteq \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_r.$$

Rings of Integers are Noetherian (Cont'd)

- On the other hand, $\{\omega_1,\ldots,\omega_r\}$ is a generating set for I as a $\mathbb{Z}$-module. So

$$\mathbb{Z}\omega_1+\cdots+\mathbb{Z}\omega_r=I.$$

But each $\mathbb{Z}_K\omega_i\subseteq I$.

So

$$\mathbb{Z}_K\omega_1+\cdots+\mathbb{Z}_K\omega_r\subseteq I.$$

Hence,

$$I\supseteq\mathbb{Z}_K\omega_1+\cdots+\mathbb{Z}_K\omega_r\supseteq\mathbb{Z}\omega_1+\cdots+\mathbb{Z}\omega_r=I.$$

So all the inclusions are equalities.

In particular, we see that $I=\mathbb{Z}_K\omega_1+\cdots+\mathbb{Z}_K\omega_r$.

So I is finitely generated as an ideal.

The Ascending Chain Condition

Definition

A ring R is said to **satisfy the ascending chain condition** (or **ACC**) if for every chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

of ideals of R, there exists some positive integer n, such that

$$I_n = I_{n+1} = I_{n+2} = \cdots .$$

Characterization of Noetherian Rings

Proposition

A ring R is Noetherian if and only if it satisfies the ACC.

- Assume that R is Noetherian.

  Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals.

  Let $I = \bigcup_{i=1}^{\infty} I_i$.

  It is easy to check that I is an ideal.

  As R is Noetherian, I has a finite generating set, $\{r_1, \ldots, r_n\}$.

  Each element r_j of the generating set must occur in some I_{n_j}.

  Let $n = \max(n_j)$ be the largest of these numbers.

  Then each element of the generating set is already contained in I_n.

  Thus, $I_n = I_{n+1} = \cdots$.

  So the chain becomes stationary.

Characterization of Noetherian Rings (Cont'd)

- Conversely, suppose the ACC is satisfied.

  We show that every ideal must be finitely generated.

  If not, there is an ideal I which has no finite generating set.

  Pick $r_1 \in I$.

  Then $I \neq \langle r_1 \rangle$, as otherwise $\{r_1\}$ would generate I.

  So we may pick $r_2 \in I - \langle r_1 \rangle$.

  Again, $I \neq \langle r_1, r_2 \rangle$.

  So we may pick $r_3 \in I - \langle r_1, r_2 \rangle$.

  In this way, we find:

  - An infinite sequence of elements $r_1, r_2, \ldots$;
  - An infinite strictly ascending chain

  $$\langle r_1 \rangle \subsetneq \langle r_1, r_2 \rangle \subsetneq \langle r_1, r_2, r_3 \rangle \subsetneq \cdots.$$

  This contradicts the ACC.

Artinian Rings

- There is also the notion of a **descending chain condition**.
- It stipulates that every descending chain must eventually become stationary.
- Rings satisfying the DCC are said to be **Artinian**.

  Example: Note that $\mathbb{Z}$ is Noetherian (as it is a PID).

  But $\mathbb{Z}$ is not Artinian, as the descending chain

  $$\langle 2\rangle \supset \langle 4\rangle \supset \langle 8\rangle \supset \cdots$$

  never becomes stationary.
- Rings of integers in number fields are never Artinian.

Noetherian Rings and Maximal Ideals

- The Ascending Chain Condition can be used to prove various results.

Lemma

Suppose that I is a proper ideal in a Noetherian ring R.
Then I is contained in a maximal ideal.

- If I is maximal, there is nothing to prove.

  Otherwise, it is strictly contained in a larger proper ideal I_1.

  If I_1 is maximal, the result follows.

  Otherwise, it is strictly contained in a larger ideal I_2.

  Repeat this process.

  By hypothesis, there cannot be arbitrarily long chains $I \subset I_1 \subset I_2 \subset \cdots$.

  So, at some point, one of the ideals must be maximal.

  The result follows.