8.2. **Unique factorisation of ideals.** We review operations of ideals from Algebra 2B.

Let R be a commutative ring with identity 1. Let I and J be ideals of R, then the *sum* of I and J is define to be

$$I + J = \{a + b \in R \mid a \in I, b \in J\},$$

and the *product* of I and J is defined to be

$$IJ = \left\{ \sum_{i=1}^{k} a_i b_i \in R \mid k \in \mathbb{Z}^+, a_i \in I, b_i \in J \text{ for all } 1 \leqslant i \leqslant k \right\}.$$

The sum $I + J$ and product IJ are both ideals of R. This fact is Lemma 2.4 (2013) or Lemma 2.20 (2014) in Algebra 2B.

In particular, for any $\alpha \in R$ and ideal I, we can easily verify that $(\alpha)I = \{\alpha a \mid a \in I\}$.

It is easy to check that under the assumption that R is commutative, both operations are commutative and associative. Namely, for ideals I and J of R, we have $I + J = J + I$ and $IJ = JI$; for ideals I_1, I_2 and I_3 of R, we have $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$ and $(I_1 I_2)I_3 = I_1(I_2 I_3)$. Therefore, we can simply write $I_1 + I_2 + I_3$ or $I_1 I_2 I_3$ without specifying the order of the operations.

The building blocks in the factorisation of integers are prime numbers. To study factorisation of ideals, we also need to understand the building blocks first.

Definition 8.10. Let R be a commutative ring with 1. An ideal I of R is a *proper ideal* if $I \neq R$. An ideal $\mathfrak{p}$ of R is a *prime ideal* if $\mathfrak{p}$ is proper, and $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. An ideal $\mathfrak{m}$ of R is a *maximal ideal* if $\mathfrak{m}$ is proper, and there is no ideal I strictly between $\mathfrak{m}$ and R; i.e. $\mathfrak{m} \subseteq I \subseteq R$ implies $I = \mathfrak{m}$ or $I = R$.

Example 8.11. Let $R = \mathbb{Z}$. (6) is not a prime ideal because $2 \cdot 3 \in (6)$ but $2 \notin (6)$ and $3 \notin (6)$. It is not a maximal idea because $(6) \subsetneq (2) \subsetneq \mathbb{Z}$. But (2) is a prime ideal, because if $ab \in (2)$, then ab is even, hence either a or b is even. (2) is also a maximal ideal because any ideal of $\mathbb{Z}$ has the form (d). If $(2) \subseteq (d) \subseteq \mathbb{Z}$, then $d \mid 2$, hence $(d) = (1)$ or (2).

The notions of prime ideals and maximal ideals lie in the heart of the study of algebraic number theory and algebraic geometry. In general they are distinct notions, but in the context of number fields, we have the following nice agreement.

Proposition 8.12. *Let K be a number field, $\mathcal{O}_K$ its ring of integers, and I a non-zero ideal in $\mathcal{O}_K$. Then I is a prime ideal iff I is a maximal ideal.*

Sketch of Proof. This is a standard fact in commutative ring theory. For any commutative ring R with 1, one can prove that I is a prime ideal iff R/I is an integral domain, and I is a maximal ideal iff R/I is a field. A field is always an integral domain, hence a

maximal ideal is a prime ideal. This direction holds for any R. The other direction requires $R = \mathcal{O}_K$. But by Proposition 8.4, $\mathcal{O}_K/I$ is a finite commutative integral domain, hence a field. This shows a non-zero prime ideal is also a maximal ideal. □

We study the unique factorisation of ideals in the ring of integers $\mathcal{O}_K$ of a number field K and its consequences.

Proposition 8.13. *Let I be a non-zero ideal in $\mathcal{O}_K$. Then there exists an ideal J such that IJ is a non-zero principal ideal.*

Proof. This proof is omitted and non-examinable due to the limitation of time. It is technical but does not use anything beyond what have learned so far. □

We have the following two useful consequences. The first one is the cancellation law for ideals in $\mathcal{O}_K$. The second one can be phrased as "to contain is to divide".

Corollary 8.14. *Let I, J_1, J_2 be ideals in $\mathcal{O}_K$, $I \neq 0$. If $IJ_1 = IJ_2$, then $J_1 = J_2$.*

Corollary 8.15. *Let I_1, I_2 be ideals in $\mathcal{O}_K$. If $I_1 \subseteq I_2$, then there exists an ideal J in $\mathcal{O}_K$, such that $I_1 = I_2 J$.*

Proof of Corollaries 8.14 and 8.15. Both statements are simple consequences of Proposition 8.13. We leave them as exercises. See Exercise 8.4. □

Now we are ready to establish the unique factorisation for ideals in $\mathcal{O}_K$.

Theorem 8.16 (Unique Factorisation of Ideals in $\mathcal{O}_K$)**.** *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then every non-zero proper ideal in $\mathcal{O}_K$ can be uniquely written as a finite product of prime ideals up to reordering factors.*

Proof. The proof consists of two parts: existence and uniqueness of prime factorisations.

First we prove the existence. Let I be a non-zero proper ideal of $\mathcal{O}_K$. We claim that I is contained in some maximal ideal P_1. If I is not contained in any maximal ideal of $\mathcal{O}_K$, then in particular, I itself is not maximal. Hence there is an ideal I_1 with $I \subsetneq I_1 \subsetneq \mathcal{O}_K$. Since I_1 is not maximal, we can find I_2 with $I_1 \subsetneq I_2 \subsetneq \mathcal{O}_K$. The same procedure can be repeated to obtain a strictly increasing chain of infinitely many ideals $I \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$, which contradicts Proposition 8.8.

By Corollary 8.15, we have $I = P_1 J_1$ for some ideal J_1. It is clear that $I \subseteq J_1$. We claim $I \neq J_1$. Indeed, if $I = J_1$, then by Corollary 8.14, we have $\mathcal{O}_K = P_1$, which contradicts the properness of P_1.

If $J_1 \neq \mathcal{O}_K$, then the same argument shows that $J_1 = P_2 J_2$ for some maximal ideal P_2 and some ideal J_2 strictly larger than J_1. If $J_2 \neq \mathcal{O}_K$ then we can continue the process to get P_3 and J_3. We claim that we can get $J_r = \mathcal{O}_K$ for some r. If not, this process goes on forever and we get a strictly increasing chain of infinitely many ideals $I \subsetneq J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$, which contradicts Proposition 8.8.

Assume $J_l = \mathcal{O}_K$, then the process terminates here and we get

$$I = P_1 J_1 = P_1 P_2 J_2 = P_1 P_2 P_3 J_3 = \cdots = P_1 P_2 \cdots P_r J_r = P_1 P_2 \cdots P_r,$$

where each P_i is a maximal ideal, hence is also a prime ideal by Proposition 8.12.

Then we prove the uniqueness. Suppose $P_1 P_2 \cdots P_r = I = Q_1 Q_2 \cdots Q_s$ where P_i's and Q_j's are prime ideals. Then $P_1 \supseteq Q_1 Q_2 \cdots Q_s$. We claim that $P_1 \supseteq Q_j$ for some Q_j. If not, then for each $j = 1, 2, \cdots, s$, we can find $a_j \in Q_j \backslash P_1$. Since P_1 is a prime ideal, $a_1 a_2 \cdots a_s \notin P_1$. However $a_1 a_2 \cdots a_s \in Q_1 Q_2 \cdots Q_s \subseteq P_1$. Contradiction.

Therefore, by renumbering the Q_j's if necessary, we can assume that $P_1 \supseteq Q_1$. Since Q_1 is a maximal ideal by Proposition 8.12, we conclude that $P_1 = Q_1$.

Using Corollary 8.14 we obtain $P_2 \cdots P_r = Q_2 \cdots Q_s$. Continuing in the same way we eventually find that $r = s$ and $P_i = Q_i$ for all i after renumbering. $\square$