MA40238 NUMBER THEORY 2013/14 SEMESTER 1
WEEK 7 OVERVIEW

Recap

Last week we introduced the notions of algebraic numbers, algebraic integers and (algebraic) number fields. We know that every element in a number field is an algebraic number but not necessarily an algebraic integer. This is the starting point of this week.

Monday Lecture

Topic 1. Given a number field K, how can we find all algebraic integers in K?

We have at least three tools to prove a certain number is an algebraic integer. But to answer the above question we will also need to prove some elements in K are not algebraic integers. This is where the trace and norm come into play. (Do you remember that the trace and norm of an algebraic integer in K must be a rational integer?)

We study this question in explicit examples, namely, number fields of degrees 1 and 2.

Topic 2. For a number field K of degree n over $\mathbb{Q}$, we will define the *discriminant* of any n elements in K.

The discriminant will be defined as the determinant of a certain $n \times n$ matrix. We will also see three properties of the discriminant. A lot of examples can be found in exercises (Exercises 7.1, 7.3 and 7.4).

Tuesday Lecture

We know that every number field K is a vector space over $\mathbb{Q}$. There are many choices for a $\mathbb{Q}$-basis for K, but we will see some choices are much more preferred than others.

Topic. For every non-zero ideal I in $\mathcal{O}_K$, we will show that we can find a $\mathbb{Q}$-basis for K which consists of elements in I, such that every element in I is an integral linear combination of elements of this basis. Such a basis is called an *integral basis* for I.

We can use the integral basis to define the *discriminant of the ideal* I and the *discriminant of the number field* K. We will see their examples on quadratic fields.

Date: November 10, 2014.

Preparing for Next Week

Some concepts in Algebra 2B will be important for next week. The following is a partial list. It will be helpful if you can review the notion of the quotient ring, the addition and multiplication of two ideals. The following questions could be used as an outline. You should be able to find answers to questions (1) and (3) in Algebra 2B notes. Questions (2) and (4) help you think about them from a slightly different point of view. It does not matter if you cannot answer them all – we will still recall them when we use them.

Assume R is a commutative ring with 1.

(1) Let I be a non-zero ideal of R. How can you describe the quotient ring R/I? (The quotient ring R/I is the collection of all cosets of I in R, with a well-defined addition and multiplication.)

(2) Write down you favourite example of a ring (e.g. $R = \mathbb{Z}$). Write down two ideals of this ring such that one contains the other (e.g. $I = (3)$, $J = (6)$, then $I \supseteq J$). Compare the two quotient rings. Which quotient ring is larger? (In this example, R/I has 3 elements, while R/J has 6 elements. The larger ideal corresponds to a smaller quotient ring.) Can you explain this phenomenon using the notion of cosets? (Every coset of J is contained in a coset of I, but every coset of I contains more than 1 coset of J, hence I has fewer cosets in R.)

(3) Let I_1 and I_2 be two non-zero ideals of R. What is their sum $I_1 + I_2$? What is their product $I_1 I_2$?

(4) Do commutativity and associativity hold for addition of ideals? (i.e. Is it true that $I_1 + I_2 = I_2 + I_1$? Is it true that $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$?) Do they hold for multiplication of ideals? (i.e. Is it true that $I_1 I_2 = I_2 I_1$? Is it true that $(I_1 I_2) I_3 = I_1 (I_2 I_3)$?)

An Extra Hint

Here is an extra hint for **Exercise 6.4 (3)**: you can assume α is a root of the monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree m. If you write $f(x) = x^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_{m-1} x + c_m$, then all entries of the matrix in question can be expressed in terms of the coefficients of $f(x)$. More precisely, the matrix for L_α under the given basis is

$$M = \begin{pmatrix} D & & & \\ & D & & \\ & & \ddots & \\ & & & D \end{pmatrix}, \quad \text{where each block} \quad D = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -c_m \\ 1 & 0 & 0 & \cdots & 0 & -c_{m-1} \\ 0 & 1 & 0 & \cdots & 0 & -c_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & 0 & \cdots & 1 & -c_1 \end{pmatrix}.$$

It follows that all entries of M are integers and so are $T(\alpha)$ and $N(\alpha)$. Can you see why?