3704 Algebraic Number Theory: a narrowly practical summary. February, 2009

We can consider a somewhat artificial division of the course into three parts:

I. Algebraic number fields and algebraic numbers.

II. Algebraic integers.

III. Factorization into ideals and ideal class groups.

As you review the material you should concentrate on

(1) how the different concepts fit together;

and (2) how to compute things.

Algebraic number theory provides in fact a perfect illustration of the process whereby theorems are developed to aid with computation. Try to detect this pattern as it runs through the course material.

I.

Review the concepts of:

-algebraic numbers;

-algebraic number fields;

-minimal polynomials;

-embeddings into $\mathbb{C}$;

-field extensions;

-degree of an extension;

-norms, traces, and discriminants.

Here are some sample questions you can try out. (Warning: these questions should not necessarily be taken as directly indicative of exam questions. They are rather things to think about. During an exam, you don't have much time to think. Put differently, you should have thought about them enough before the exam so that you can answer related question during the exam without thinking much.)

-Which theorem ties together the concept of an algebraic number field to that of an algebraic number?

-Similarly, how does the 'abstract' definition of an algebraic number field relate to the notion of algebraic numbers in $\mathbb{C}$?

-How does one typically 'give' an algebraic number field? What other ways are there? Give several examples.

-How would you write down a multiplication table for an algebraic number field? Examples.

-What are the conjugates of an algebraic number? Examples.

-In how many ways can you embed $\mathbb{Q}$ into $\mathbb{C}$?

-Explain the relationship between degree of an algebraic number field, minimal polynomials, and

embeddings into $\mathbb{C}$. Examples.

-How does the norm and trace relate to the minimal polynomial, at least for a primitive element? Examples.

-How does one regard an algebraic number as a linear map? Examples.

-If one does that, how does the minimal polynomial, norm, and trace in algebraic number theory relate to concepts of linear algebra? Examples.

-Write down all the examples where you have an efficient algorithm for computing norms.

-Write down all the examples where you have an efficient algorithm for computing discriminants of bases.

II.

Review the notions of

-rings of algebraic integers;

-Units, irreducible elements;

-integral bases;

-minimal discriminants.

Questions:

-Why do the algebraic integers inside an algebraic number field form a subring?

-If an algebraic number field were 'given' and a specific element were written down for you, would you be able to say whether or not it was an algebraic integer?

-For a few examples of quadratic fields, say $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$, try to compute just from the definition the full ring of algebraic integers.

-What is the relationship between the three notions listed above, rings of algebraic integers, integral bases, and minimal discriminants?

-When one refers just to the discriminant of an algebraic number field, what is meant?

-Review completely the theorems on algebraic integers and discriminants for quadratic fields.

-Write down at least two infinite families of cubic fields where you can completely determine the ring of algebraic integers.

-How does the problem of computing the ring of algebraic integers relate to the computational devices from part I?

-In fact, which theorems from the notes are helpful for computing rings of algebraic integers?

-Give a few examples where a simple change of variables helps in finding the ring of algebraic integers. (Say cyclotomic fields, or a field like $\mathbb{Q}(2^{1/3})$. I admit I gave a rather complicated approach to the latter in class.)

-Consider corollary 105. How is it used in the examples of the previous question?

-If you compute discriminants using proposition 73, can you interpret corollary 105 purely in terms of linear algebra?

-Recall that the sign of the discriminant is independent of the basis. Why is that?

-How does the previous question relate to a theorem on matrix representatives for quadratic forms?

-Why is the discriminant always non-zero?

-What can you say about the norm of a unit?

-Give an example of a ring with infinitely many units.

-Find all units in the rings $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-10}]$.

-Give an example of a ring R and an irreducible element $a \in R$ such that (a) is *not* an prime ideal.

-What does the previous theorem have to do with unique factorization?

III. Review the notions of

-a unique factorization domain with several examples and non-examples;

-a principal ideal domain with several examples and non-examples;

-integral domains, fields, and how they relate to quotient rings;

-norm of an ideal;

-fractional ideals;

-products of fractional ideals, inverses;

-decomposition into ideals.

Questions:

-How does one describe an ideal?

-How does the concept of an ideal relate to that of a quotient ring?

-What is the relationship between integral domains and fields?

-How does the multiplication of fractional ideals relate to multiplication of numbers?

-How does the inverse of a fractional ideal relate to the inverse of a number?

-How does the norm of an ideal relate to the norm of a number?

-How does the sum of ideals relate to the sum of numbers?

-What is the relationship between an irreducible element and a prime ideal?

-Give a few examples of fractional ideals that are not ideals.

-Give a few examples of fractional ideals that are not ideals and that are not a priori principal.

-Give a few examples of fractional ideals that are not ideals but also do not contain the ring of algebraic integers.

-What is the relationship between containment of ideals and divisibility? How does this work out for the usual integers?

-Explain precisely how ideals are used to compensate for lack of unique factorization in rings of algebraic integers.

-In fact, in the theorem on decomposition of integers into primes, the existence is pure logic while the uniqueness requires a bit of work (say, Bezout's lemma). But for the theorem on decomposition into maximal ideals, uniqueness is essentially trivial. Why is that?

-Given a maximal ideal in $\mathbb{Z}$, how many maximal ideals can there be in $\mathcal{O}_K$ lying above it?

-Given a prime number in $\mathbb{Z}$, how many numbers in $\mathcal{O}_K$ could divide it?

-For what kinds of examples do you know how to decompose ideals into maximal ideals?

-In fact, how would you go about decomposing an ideal into maximal ideals?

-What is a very simple situation where you know using norms that an ideal is maximal?

-Suppose $N(I) = 6$ can I be maximal?

-Why did I keep conflating the terms prime and maximal in class, and why was this just slightly inaccurate?

-Suppose $N(I) = 9$. Can I be prime? Can you give an example? A counter-example?

-How would you check if an ideal is principal? Do you know how to do this in general? At least for a good class of examples?

-Give a few examples of fractional ideals that are not ideals and that are not principal.

-Notice that the ideal class group can in fact be generated by the classes of ideals. What was the point of introducing fractional ideals?

-Could there be an algebraic number field with discriminant 1?

-Give an example of a class group of order bigger then 2.

-Give an example of a class group of order bigger than 5.

-Take some of the examples given in sheet 6 and the supplementary notes where there is a non-trivial class group. Write down explicit examples of non-unique factorization (of numbers into irreducibles, of course) in each case.

List of important theorems. propositions, corollaries, . . . :

Thm. 28, Prop. 34, Thm. 35, Cor. 37, Thm. 40, Thm. 69, Prop. 77, Cor. 83, Lem. 86, Cor. 87, Lem. 89, Thm. 98, Thm. 102, Prop. 105, Thm. 106, Cor. 109, Prop. 110, Thm. 111, Prop. 115, Thm. 118, Prop. 120, Prop. 121, Thm. 128, Prop. 136, Lem. 143, Thm. 150, Cor. 152, Thm. 153, Cor. 159, Thm. 164, Thm. 170.

For any given result listed, of course you are expected to have a good understanding of the background, that is, definitions, discussion, and preliminary results, leading to it.