Homework set 10 - due 11/019/21

Math 5031

1. (For this exercise, read III.K on Gauss's lemma.)

   (a) Let f be a primitive polynomial in $\mathbb{Z}[x]$ and let g be any polynomial with integer coefficients. Suppose that f divides g in $\mathbb{Q}[x]$; that is, $g = fq$ with $q \in \mathbb{Q}[x]$. Show that $q \in \mathbb{Z}[x]$, hence f divides g in $\mathbb{Z}[x]$.

   (b) Let f, g be polynomials in $\mathbb{Q}[x]$, and let f_0, g_0 be the associated primitive polynomials in $\mathbb{Z}[x]$. If f divides g in $\mathbb{Q}[x]$, show that f_0 divides g_0 in $\mathbb{Z}[x]$.

   (c) Let f, g be polynomials in $\mathbb{Z}[x]$ having a common nonconstant factor in $\mathbb{Q}[x]$. Show that they have a common nonconstant factor in $\mathbb{Z}[x]$.

   (d) Show that if a nonconstant polynomial is irreducible in $\mathbb{Z}[x]$ then it is also irreducible in $\mathbb{Q}[x]$.

2. (For this exercise, review the concepts of algebraic numbers and algebraic integers.)

   (a) State the definition of *algebraic integers* in a number field.

   (b) Let α be an algebraic number and $\mathrm{ev}_\alpha : \mathbb{Q}[x] \to \mathbb{C}$, $\mathrm{ev}_\alpha(f(x)) = f(\alpha)$ the evaluation map. Show that the kernel of this ring homomorphism is the principal ideal generated by an irreducible polynomial over $\mathbb{Q}$.

   (c) Show that the kernel of the evaluation map $\mathrm{ev}_\alpha : \mathbb{Z}[x] \to \mathbb{C}$ is the principal ideal of $\mathbb{Z}[x]$ generated by the (unique up to unit) primitive irreducible polynomial for α.

   (d) Show that an algebraic number α is an algebraic integer if and only if the primitive irreducible polynomial in $\mathbb{Z}[x]$ having α as a root is monic. Said differently, α is an algebraic integer if and only if the monic irreducible polynomial for α in $\mathbb{Q}[x]$ has integer coefficients.

   (e) Let α be an algebraic integer in an number field. Show that if $\alpha \in \mathbb{Q}$ then $\alpha \in \mathbb{Z}$.

3. A *quadratic number field* $F = \mathbb{Q}[\sqrt{d}]$ consists of all (possibly complex) numbers $a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ where d is a fixed square-free integer.

   (a) Show that $\alpha = a + b\sqrt{d}$ is an algebraic integer in F if and only if $2a$ and $a^2 - b^2 d$ are rational integers (that is to say, they lie in $\mathbb{Z}$). (To get started, consider the polynomial $(x - \alpha)(x - \tilde{\alpha})$, where $\tilde{\alpha} = a - b\sqrt{d}$.)

   (b) It is easy to show by elementary calculation that the set of algebraic integers in a quadratic number field is a ring. This is not at all as easy for algebraic numbers in more general number fields. Read the beginning of Section III.L of Kerr's notes (up to Corollary III.L.2) to become acquainted with the general argument. (This is only a reading assignment.)

   (c) The following theorem is standard in the theory of quadratic number fields and it is not too difficult to prove:

   Theorem. *The algebraic integers in the quadratic field $\mathbb{Q}[\sqrt{d}]$ have the form $\alpha = a + b\sqrt{d}$ where*

   i. If $d \equiv 2$ or 3 (modulo 4), then $a, b \in \mathbb{Z}$.

ii. If $d \equiv 1$ (modulo 4), then either $a, b \in \mathbb{Z}$ or $a, b \in \mathbb{Z} + \frac{1}{2}$.

Let us denote by $\mathcal{O}_F$ the ring of algebraic integers in F. Now suppose $d < 0$. (We call $\mathbb{Q}[\sqrt{d}]$ for $d < 0$ an *imaginary quadratic number field*.) The above theorem implies that $\mathcal{O}_F$, regarded as an additive group, is isomorphic to $\mathbb{Z}^2$. Thus any ideal in $\mathcal{O}_F$ is similarly isomorphic to a subgroup of $\mathbb{Z}^2$.

Show that any non-trivial ideal of $\mathcal{O}_F$ is isomorphic, as an additive group, to $\mathbb{Z}^n$ for $n \leq 2$. (Not much to do here other than going back to Section II.K of Kerr's notes and quoting the relevant theorem.)

(d) We continue to assume $d < 0$. Let $I \subset \mathcal{O}_F$ be an ideal. Show that I is generated by no more than two elements in $\mathcal{O}_F$. (For a more general statement, read Proposition III.J.17 in Kerr's notes.)

(e) For this exercise (mainly for context), familiarize yourself with the concepts of *monoid of integral ideals*, *fractional ideals* and *invertible ideals* from Section III.L. Let I be an ideal in the imaginary quadratic number field $\mathbb{Q}[\sqrt{d}]$. Let $\tilde{I}$ be the ideal generated by the conjugates of the generators of I. Show that $I\tilde{I} = (n)$ for some $n \in \mathbb{Z}$. (Hurwitz's theorem!) This means that ideals in ring of integers in an imaginary quadratic number field are invertible in the set of fractional ideals.

(f) Read the part of Section III.L under the heading **Integral ideals**, with particular attention to Proposition III.L.14 and Corollary III.L.15. As you do, think about the following question: How does the failure of the ring of integers of a number field to have unique prime factorization gets resolved with the concept of prime ideals in the monoid of ideals (denoted $\wp \in \mathcal{I}(K)$ in the notes). You don't need to write anything down.

4. Let $\mathcal{O}_F$ denote the ring of integers in $F = \mathbb{Q}[\sqrt{d}]$, where d is a square-free negative integer (that is, an imaginary quadratic number field.) We call two ideals I, J *similar* ($I \sim J$) if there are nonzero elements $\alpha, \beta \in \mathcal{O}_F$ so that $\beta J = \alpha I$. It is easy to check that this is an equivalence relation. The equivalence classes for $\sim$ are called *ideal classes*. We denote them by $[I]$. Note that $[(1)]$ is the class of principal ideals.

(a) Show that the ideal classes form an abelian group $\mathcal{C}(F)$, with law of composition obtained from multiplication of ideals: $[I][J] = [IJ]$, and the identity $[\mathcal{O}_F] = [(1)]$. (You may take for granted the easy fact that multiplication of ideals is commutative and associative; thus you only have to show that multiplication in $\mathcal{C}(F)$ is well-defined and that elements of $\mathcal{C}(F)$ have inverses.)

(b) Read the discussion on the ideal class group in Section III.L under the heading **The ideal class group**. It is shown there how this concept is defined in the general context of number fields.