Assignment 3 – All 4 parts – Math 661

Due in class: Thursday, Feb. 27, 2020

(1) The Chinese Remainder Theorem in Dedekind Domains. Let $\mathcal{O}$ be a Dedekind Domain.

(a) Let I be an ideal of $\mathcal{O}$ and suppose

$$I = \prod_{i=1}^{r} \mathfrak{p}^{e_i}$$

is the prime factorization of I (with the $\mathfrak{p}_i$ distinct). Fix an $\alpha \in \mathcal{O}$. Show that some $\beta \in \mathcal{O}$ is such that $\beta \equiv \alpha \pmod{I}$ if and only if $\beta \equiv \alpha \pmod{\mathfrak{p}_i^{e_i}}$ for all i.

(b) For $i = 1, \ldots, r$, let $\mathfrak{p}_i$ be distinct non-zero prime ideals of $\mathcal{O}$, let $e_i \in \mathbf{Z}_{\geq 1}$, and fix $\alpha_i \in \mathcal{O}$. Show that there is an element $\alpha \in \mathcal{O}$ such that

$$\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{e_i}}, \text{ for } i = 1, 2, \ldots, r.$$

(Hint: you can adapt the proof for $\mathbf{Z}$ given what we know about the divisibility theory of ideals of a Dedekind domain.)

(c) Explain how this proves the following (called the Chinese Remainder Theorem): For $j = 1, \ldots, r$, let I_j be pairwise relatively prime ideals of $\mathcal{O}$ and let α_j be fixed elements of $\mathcal{O}$. Then there is an element $\alpha \in \mathcal{O}$ such that

$$\alpha \equiv \alpha_j \pmod{I_j}, \text{ for } j = 1, 2, \ldots, r.$$

(2) (a) Let R be a (commutative) ring and suppose I and J are ideals of R generated by S and T, respectively. Show that IJ is generated by $\{st : s \in S, t \in T\}$.

(b) Let $K = \mathbf{Q}(\sqrt{79})$ so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{79}]$. We saw in class that every ideal of $\mathcal{O}_K$ can be generated by 2 elements. Let $I = (3, 2+\sqrt{79})$. Show that $I^2 = (9, 5+\sqrt{79})$.

(c) With K and I as in part (b), let $J = (3, 1+\sqrt{79})$. Show that IJ is principal!

(d) Bonus: show that the ideals I, J, and I^2 are not principal. (Hint: try looking at their norms and the possible norms of elements of $\mathcal{O}_K$.)

(3) Let K be a number field and let I be an ideal of $\mathcal{O}_K$. Show that if there is an $\alpha \in I$ with $N(I) = |N_{K/F}(\alpha)|$, then $I = (\alpha)$.

(4) Let A be a Dedekind domain, F its field of fractions, K/F a finite separable extension, and $\mathcal{O}$ the integral closure of A in K. Let $\alpha \in \mathcal{O}$.

(a) Show that $\alpha \in \mathcal{O}^\times$ if and only if $N_{K/F}(\alpha) \in A^\times$.

(b) Show that if $N_{K/F}(\alpha)$ is irreducible in A, then α is irreducible in $\mathcal{O}$.

(5) Let A be a Dedekind domain, F its field of fractions, K a finite, separable extension of F, and $\mathcal{O}$ the integral closure of A in K. Let $\mathfrak{p}$ be a non-zero prime ideal of A with

$$\mathfrak{p}\mathcal{O} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

and f_i the residue degree of $\mathfrak{P}_i$. Recall that in class we defined the 'decomposition type' of $\mathfrak{p}$ to be the symbol $(f_1^{e_1}\ f_2^{e_2}\ \cdots\ f_g^{e_g})$. Write down the possible decomposition types when K/F has degree 4.

(6) (a) For the primes $p = 2, 3, 5$ and $\mathcal{O} = \mathbf{Z}[\sqrt{-5}]$, find the prime factorizations of $p\mathcal{O}$. Which of these p are ramified in $\mathbf{Q}(\sqrt{-5})/\mathbf{Q}$?

(b) Let $K = \mathbf{Q}(\sqrt[3]{2})$. Find the factorization types of $p = 2, 3, 5$, and 7 in K.

(7) Let $p \in \mathbf{Z}$ be a prime number, let $f(x) \in \mathbf{Z}[x]$ be a monic polynomial of degree $n \geq 2$ that is Eisenstein at p, and let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(x)$. Show that p is totally ramified in K, i.e. that $p\mathcal{O}_K = \mathfrak{p}^n$.

(8) Recall from class that quadratic reciprocity states the following: if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$

Recall also that the Legendre symbol satisfies the following properties:

- for any $a, b \in \mathbf{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
- for any $a, k \in \mathbf{Z}$, $\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$,
- $\left(\frac{-1}{p}\right) \equiv p \pmod 4$.

Prove the following: suppose d is an odd squarefree integer (possibly negative) and $p \nmid d$ is an odd prime, show that $\left(\frac{d}{p}\right)$ only depends on p modulo $4d$, and if $d \equiv 1 \pmod 4$ then it only depends on p modulo d.

(9) Suppose that $K/\mathbf{Q}$ is a degree 3 number field in which 2 splits completely. Show that for all $\alpha \in \mathcal{O}_K \setminus \mathbf{Z}$, we have that $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. (Hint: otherwise, Dedekind's theorem applies to $p = 2$.) (Remark: there are infinitely many such fields; one of them is obtained by adjoining a root of $x^3 - x^2 - 2x - 8$.)