Math 80220 Algebraic Number Theory
Problem Set 3

Andrei Jorza

due Wednesday, February 26 (you have 2 weeks to complete this set)

Almost half of the problems in this set (problems 3e, 4, 5b, 6 and 7c) are optional. You also have 2 weeks to complete this set.

1. This exercise gives an algorithm for decomposing primes under finite extensions. Let L/K be number fields, $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$ and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ such that the rational prime p lying below $\mathfrak{p}$ does not divide the integer $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Let f be the minimal polynomial of α over K, f necessarily monic.

   (a) Show that $f \in \mathcal{O}_K[X]$. [Hint: what are the roots of f?]

   (b) For a polynomial $h \in \mathcal{O}_K[X]$ let $\overline{h} \in k_{\mathfrak{p}}[X]$ be the image mod $\mathfrak{p}$. Since $k_{\mathfrak{p}}[X]$ is a UFD one may find monic polynomials $g_i \in \mathcal{O}_K[X]$, of degree f_i, such that $\overline{f}(X) = \prod \overline{g}_i(X)^{e_i}$ is the decomposition into distinct irreducible polynomials $\overline{g}_i$. Let $\mathfrak{q}_i = (\mathfrak{p}, g_i(\alpha)) = \mathfrak{p}\mathcal{O}_L + (g_i(\alpha))\mathcal{O}_L$. Show that $\mathcal{O}_L = \mathcal{O}_K[\alpha] + p\mathcal{O}_L$ and deduce that $\mathcal{O}_L = \mathcal{O}_K[\alpha] + \mathfrak{q}_i$ for all i. [Hint: p is invertible in $\mathcal{O}_L/\mathcal{O}_K[\alpha]$.]

   (c) Show that $\mathcal{O}_K[X]/(\mathfrak{p}, g_i(X)) \cong k_{\mathfrak{p}}[X]/(\overline{g}_i)$ under the natural $\mod \mathfrak{p}$ map.

   (d) Show that $\mathcal{O}_K[X] \to \mathcal{O}_L/\mathfrak{q}_i$ under the map $X \mapsto \alpha$ is surjective. Show that it yields a map $\mathcal{O}_K[X]/(\mathfrak{p}, g_i(X)) \to \mathcal{O}_L/\mathfrak{q}_i$.

   (e) Deduce that $\mathfrak{q}_i$ is either $\mathcal{O}_L$ or a prime ideal. In the former case show that $f_{\mathfrak{q}_i/\mathfrak{p}} = f_i$.

   (f) Use the fact that for $i \neq j$ the polynomials $\overline{g}_i$ and $\overline{g}_j$ are distinct irreducibles in $k_{\mathfrak{p}}[X]$ to show that $\mathfrak{q}_i + \mathfrak{q}_j = \mathcal{O}_L$. [Hint: lift to $\mathcal{O}_K[X]$ the relation $\overline{g}_i\overline{u} + \overline{g}_j\overline{v} = 1$ which comes from the Euclidean algorithm in $k_{\mathfrak{p}}[X]$.]

   (g) Show that $\prod g_i(\alpha)^{e_i}\mathcal{O}_L \subset \mathfrak{p}\mathcal{O}_L$ and that $\mathfrak{p}\mathcal{O}_L + \prod g_i(\alpha)^{e_i}\mathcal{O}_L \mid \prod \mathfrak{q}_i^{e_i}$. Deduce that $\mathfrak{p}\mathcal{O}_L \mid \prod \mathfrak{q}_i^{e_i}$.

   (h) Reorder the ideals $\mathfrak{q}_i$ such that $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime ideals of $\mathcal{O}_L$ and $\mathfrak{q}_{s+1}, \ldots = \mathcal{O}_L$. Show that $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{s} \mathfrak{q}_i^{d_i}$ with $d_i \leq e_i$. Show that $[L : K] = \sum_{i=1}^{s} d_i f_i$ and $[L : K] = \sum e_i f_i$ and deduce that $\mathfrak{q}_i$ are all prime ideals and that $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$ with $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg g_i$ and $e_{\mathfrak{q}_i/\mathfrak{p}} = e_i$.

2. Let m be a square-free integer $\neq 1$. Let $K = \mathbb{Q}(\sqrt{m})$ and $\mathcal{O}_K$ be the ring of integers. Show that the following are prime factorizations of $(p)\mathcal{O}_K$ in $\mathcal{O}_K$:

   (a) if $p \mid m$ then $(p)\mathcal{O}_K = (p, \sqrt{m})^2$. [Hint: The ring of integers of K depends on whether $m \equiv 1, 2, 3 \pmod 4$ but in applying Problem 1 you can choose any α of degree $[L : K]$ in particular you can choose $\sqrt{m}$ independent of $m \mod 4$. You just have to verify the hypotheses of Problem 1.]

   (b) if m is odd then

$$(2)\mathcal{O}_K = \begin{cases} (2, 1+\sqrt{m})^2 & m \equiv 3 \pmod 4 \\ (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2}) & m \equiv 1 \pmod 8 \\ (2) & m \equiv 5 \pmod 8 \end{cases}$$

   [Caution: the hypothesis of Problem 1 is not always satisfied here for $\mathbb{Z}[\sqrt{m}]$.]

(c) if $p > 2$ and $p \nmid m$ then

$$(p)\mathcal{O}_K = \begin{cases} (p, a+\sqrt{m})(p, a-\sqrt{m}) & m \equiv a^2 \pmod{p} \\ (p) & m \text{ not a square mod } p \end{cases}$$

3. Let $p > 2$ be a prime and $K = \mathbb{Q}(\zeta_p)$. Let $f(X) = X^{p-1} + \cdots + X + 1$ be the minimal polynomial of ζ_p. Throughout this problem you may use Problem 1.

   (a) Show that $f(X) \equiv (X-1)^{p-1} \pmod{p}$ and conclude that $(p)\mathcal{O}_K = (p, 1-\zeta_p)^{p-1}$ with $K/\mathbb{Q}$ totally tamely ramified at $\mathfrak{p} = (p, 1-\zeta_p)$ over (p). Show that $1-\zeta_p \mid p$ and deduce that $(p, 1-\zeta_p) = (1-\zeta_p)$.

   (b) Let $q \nmid p$ be a prime and let r be the smallest positive integer such that $q^r \equiv 1 \pmod{p}$. Show that $r \mid p-1$.

   (c) For r as above show that $f(X)$ splits into a product of linear terms over $\mathbb{F}_{q^r}$ but not over any proper subfield of $\mathbb{F}_{q^r}$. [Hint: $\mathbb{F}_{q^r}^\times$ is a cyclic group of order $q^r - 1$.]

   (d) Conclude that $(q)\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_d$ where $d = (p-1)/r$ is the prime factorization of the ideal $(p)\mathcal{O}_K$ and that $K/\mathbb{Q}$ is unramified at $\mathfrak{q}_i/q$ with $f_{\mathfrak{q}_i/q} = r$. [Hint: $f(X)$ splits into linear facors over $\mathbb{F}_{q^r}$ but over no smaller finite field and so show that $f(X)$ splits over $\mathbb{F}_q$ into irreducible factors of degree r.]

   (e) (Optional since the same proof works) More generally suppose $n \geq 1$ and $L = \mathbb{Q}(\zeta_{p^n})$. Let $f(X) = (X^{p^n} - 1)/(X^{p^{n-1}} - 1)$ be the minimal polynomial of ζ_{p^n}. Show that the same decompositions hold, i.e.,

      i. $(p)\mathcal{O}_L = (p, 1-\zeta_{p^n})^{p^{n-1}(p-1)}$ and

      ii. if $q \neq p$ is a prime and r is the smallest positive integer such that $q^r \equiv 1 \pmod{p^n}$ then $(q)\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_d$ where $d = p^{n-1}(p-1)/r$ is the prime factorization of the ideal $(p)\mathcal{O}_L$ and $L/\mathbb{Q}$ is unramified at $\mathfrak{q}_i/q$ with $f_{\mathfrak{q}_i/q} = r$.

4. (Optional) Let $L, L'/K$ be number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ which splits completely in L and L'. Suppose $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$ and $\mathfrak{p}$ is coprime to $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.

   (a) Let $f(X)$ be the minimal polynomial of α over K. Show that $f \pmod{\mathfrak{p}}$ splits into linear factors.

   (b) Show that $LL' = L'(\alpha)$ and the minimal polynomial $g(X)$ of α over L divides $f(X)$ in $\mathcal{O}_{L'}[X]$.

   (c) For every prime ideal $\mathfrak{q}' \mid \mathfrak{p}$ of $\mathcal{O}_{L'}$ show that $\mathfrak{q}'\mathcal{O}_{LL'}$ splits completely.

   (d) Deduce that $\mathfrak{p}$ splits completely in the composite extension LL'.

5. (a) Show that $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is everywhere unramified over $\mathbb{Q}(\sqrt{15})$. (Remark: $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is the largest extension of $\mathbb{Q}(\sqrt{15})$ which is everywhere unramified.) [Hint: Compute the different. You may use that that $\mathcal{O}_{\mathbb{Q}(\sqrt{3}.\sqrt{5})}$ has as integral basis $1, \sqrt{3}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{3}+\sqrt{15}}{2}$].]

   (b) (Optional, since same as the first part, but more work.) For which m, n square-free, $\neq 1$ and coprime is $\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}(\sqrt{mn})$ everywhere unramified? You may use the fact that an integral basis of the ring of integers of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is given by

m	n	Integral basis
$\equiv 3 \pmod{4}$	$\equiv 3 \pmod{4}$	$1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{mn}}{2}$
$\equiv 3 \pmod{4}$	$\equiv 2 \pmod{4}$	$1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{mn}}{2}$
$\equiv 1 \pmod{4}$	$\equiv 2, 3 \pmod{4}$	$1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{mn}}{2}$
$\equiv 1 \pmod{4}$	$\equiv 1 \pmod{4}$	$1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{mn}}{4}$

6. (Optional) Let K, L be two number fields and assume that $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. In this exercise you study when $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.

(a) Suppose α_i is an integral basis of $\mathcal{O}_K$ and β_j is an integral basis of $\mathcal{O}_L$. Show that $\alpha_i\beta_j$ form an integral basis of $\mathcal{O}_K\mathcal{O}_L$. [Hint: what is the degree of KL/L?]

(b) Show that every $\alpha \in \mathcal{O}_{KL}$ is of the form

$$\alpha = \sum_{i,j} \frac{m_{i,j}}{r}\alpha_i\beta_j$$

where $r, m_{i,j} \in \mathbb{Z}$ with r coprime to $\gcd(m_{i,j})$.

(c) Recall that the embeddings of $KL \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$ are of the form $\sigma\tau$ where $\sigma : K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$ and $\tau : KL \hookrightarrow \mathbb{C}$ fixing L.

Let $x_i = \sum_j \frac{m_{i,j}}{r}\beta_j$ and $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$. Show that $\sum_i \sigma_j(\alpha_i)x_i = (\sigma_j\tau)(\alpha)$. If $d = \det((\sigma_j(\alpha_i))$ show that $x_i \in \frac{1}{d}\overline{\mathbb{Z}}$ where $\overline{\mathbb{Z}}$ is the ring of algebraic integers.

(d) Recall that $d^2 = D = \operatorname{disc}(\mathcal{O}_K) \in \mathbb{Z}$ and show that $Dx_i = \sum \frac{Dm_{i,j}}{r}\beta_j \in \mathcal{O}_L$. Deduce that $r \mid D$ and $r \mid \gcd(\operatorname{disc}(\mathcal{O}_K), \operatorname{disc}(\mathcal{O}_L))$.

(e) Conclude that if $\operatorname{disc}(\mathcal{O}_K)$ and $\operatorname{disc}(\mathcal{O}_L)$ are coprime then $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$. In particular, show that if n is square-free then $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. (Recall that we proved this for n prime.)

(f) Show that $\frac{\sqrt{3}+\sqrt{7}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{7})} - \mathcal{O}_{\mathbb{Q}(\sqrt{3})}\mathcal{O}_{\mathbb{Q}(\sqrt{7})}$.

7. (a) If L/K is a Galois extension of number fields and $\mathcal{O}_L = \mathcal{O}_K[\alpha_1, \ldots, \alpha_r]$ show that $I_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in G_{L/K} | \sigma(\alpha_i) \equiv \alpha_i \pmod{\mathfrak{q}}, \forall i\}$ and similarly for the higher ramification groups $V_m = \{\sigma \in G_{L/K} | \sigma(\alpha_i) \equiv \alpha_i \pmod{\mathfrak{q}^{m+1}}, \forall i\}$.

(b) Consider the extension $K = \mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}$.

i. Write $\alpha = \sqrt{2+\sqrt{3}}$. Show that the roots of the minimal polynomial of α are $\pm\alpha, \pm\alpha^{-1}$ and deduce that $\alpha \in \mathcal{O}_K^\times$.

ii. Show that $K/\mathbb{Q}$ is Galois with Galois group $G_{K/\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ having generators $\sigma(\alpha) = \alpha^{-1}$ and $\tau(\alpha) = -\alpha$.

iii. Show that $(3)\mathcal{O}_K = (\sqrt{3})^2$ is the prime factorization in $\mathcal{O}_K$. Conclude that $I_{\sqrt{3}/3} = \{1, \sigma\tau\}$ but $P_{\sqrt{3}/3} = \{1\}$. (You may assume that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2+\sqrt{3}}]$.)

iv. Show that $(2)\mathcal{O}_K = \mathfrak{q}^4$ where $\mathfrak{q} = (\alpha+1)$ is the prime factorization in $\mathcal{O}_K$. Show that $I_{\mathfrak{q}/2} = P_{\mathfrak{q}/2} = G_{K/\mathbb{Q}}$, $V_2 = V_3 = \{1, \tau\}$ and $V_m = \{1\}$ for $m \geq 4$. [Hint: Check that $\alpha + 1 \mid \alpha - 1$.]

(c) (Optional) Let $p > 2$ be a prime and $K = \mathbb{Q}(\zeta_{p^n})$ for $n \geq 2$. Recall that $(p)\mathcal{O}_K = \mathfrak{q}^{p^{n-1}(p-1)}$ where $\mathfrak{q} = (p, 1-\zeta_{p^n})$ and $\mathfrak{q}/p$ is totally ramified.

i. Show that $I_{\mathfrak{q}/p} = G_{K/\mathbb{Q}}$.

ii. Let $\alpha = \zeta_{p^n} - 1$. Show that $N_{K/\mathbb{Q}}(\alpha) = p$ and deduce that $(\alpha) = (p, \alpha)$. Thus $\alpha^{p^{n-1}(p-1)}$ the is the power of α in p.

iii. For $m < n$ show that the largest power of α dividing $(\alpha+1)^{p^m\ell} - 1$ (with $p \nmid \ell$) is α^{p^m} and conclude that $(\zeta_{p^n} - 1)^{p^m} \mid \zeta_{p^n}^{p^m\ell} - 1$ but $(\zeta_{p^n} - 1)^{p^m+1} \nmid \zeta_{p^n}^{p^m\ell} - 1$. [Hint: first, do this for $\ell = 1$ using the fact that if $k \neq 0, p^m$ then $p \mid \binom{p^m}{k}$; then deduce for all ℓ.]

iv. Finally deduce that for $m \geq 1$ we have $V_m = 1 + p^m(\mathbb{Z}/p^n\mathbb{Z})$ as a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong G_{K/\mathbb{Q}}$.