Algebraic Number Theory, Math 421
Instructor: Sreekar M. Shastry
Final Examination Solutions

- ⋆ There are 8 problems. Each problem is worth 5 points. The maximum score is 40 points.
- ⋆ Clearly state the results which you invoke; you may invoke without proof results from the textbook and other problems on this exam.

1. Recall the following theorem from the book:
Let $\mathscr{O}_K$ be the ring of integers of a number field K with $[K:\mathbb{Q}] = n$ and let $\alpha \in \mathscr{O}_K$ be of degree n over $\mathbb{Q}$. Then there is an integral basis

$$\left\{1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right\}$$

of $\mathscr{O}_K$ where $d_i \in \mathbb{Z}$ satisfy $d_1|d_2|\cdots|d_{n-1}$, the $f_i \in \mathbb{Z}[x]$ are monic, and $\deg f_i = i$. The d_i are uniquely determined.

(a) Let $a_1, \dots, a_n$ and $b_1, \dots, b_n$ be elements of K such that $\langle a_i \rangle = \langle b_i \rangle$ where $\langle S \rangle :=$ the additive subgroup of K generated by $S \subset K$. Show that

$$\mathrm{disc}(a_1, \dots, a_n) = \mathrm{disc}(b_1, \dots, b_n).$$

(b) Show that

$$\mathrm{disc}(\alpha) = (d_1 d_2 \cdots d_{n-1})^2 \mathrm{disc}(\mathscr{O}_K)$$

where $\mathrm{disc}(\alpha) := \mathrm{disc}(1, \alpha, \dots, \alpha^{n-1})$.

(c) Show that

$$\#(\mathscr{O}_K/\mathbb{Z}[\alpha]) = d_1 d_2 \cdots d_{n-1}.$$

Solution. (a) (case 1) $\mathrm{disc}(a_i) = 0 \Rightarrow$ the a_i are $\mathbb{Q}$-linearly dependent by Theorem 7 on page 25 of Marcus. Writing the b_i as $\mathbb{Z}$-linear combinations of the a_i shows that the b_i are $\mathbb{Q}$-linearly independent and thus $\mathrm{disc}(b_i) = 0$.

(case 2) $\mathrm{disc}(a_i) \neq 0$. Then $b_i = \sum_j c_{ij} a_j$ with the matrix $C = (c_{ij}) \in GL_n(\mathbb{Z})$ i.e. $\det C = \pm 1$. This is because $\langle a_i \rangle = \langle b_i \rangle$ w.r.t. the addition in K which is induced from the addition in $\mathbb{C}$, which is a characteristic zero field; such points can easily lead one astray in positive characteristic. Returning to the proof, we have

$$\mathrm{disc}(b_i) = (\det C)^2 \mathrm{disc}(a_i)$$

because the $c_{ij} \in \mathbb{Z}$ and therefore the matrix made from the Galois embeddings which defines the discriminant of $\{b_i\}$ factors in terms of C and the matrix defining the discriminant of the $\{a_i\}$.

(b) The subgroups of K generated by $1, \alpha, \dots, \alpha^{n-1}$ and $\{1, f_1(\alpha), \dots, f_{n-1}(\alpha)\}$ coincide because $\deg f_i = i$ and each f_i is monic; compare with Theorem 2 on page 15. Now use (a).

(c) The integral basis gives a direct sum decomposition of the additive group $\mathscr{O}_K$; on the other hand, the new basis $\{1, f_1(\alpha), \dots, f_{n-1}(\alpha)\}$ of the group generated by $1, \alpha, \dots, \alpha^{n-1}$ makes said group into a direct sum w.r.t. the same basis as for $\mathscr{O}_K$; the result follows.

2. Show that $\mathrm{Cl}(\mathbb{Q}[\sqrt{-3}])$ is trivial. (Hint: $(4/\pi)^2 < 9/5$, a fact which you may take for granted.)

Solution. I made a mistake in the statement of the hint. We have $n = r + 2s = 2$ so that $s = 1$, and the hint should have been an estimate on $4/\pi$ not on $(4/\pi)^2$. I wrote the hint erroneously thinking that $s = 2$. However, even with the hint I gave the solution is possible without recourse to a calculator. To wit:

Recall that the discriminant of $\mathbb{Q}[\sqrt{-3}]$ is -3 because $-3 \equiv 1 \pmod 4$ (see page 33 of the book).

We seek to apply corollary 2 on page 136. We have: $(4/\pi)^2 < 9/5 < 9/4 \Rightarrow 4/\pi < 3/2$. Thus, given an ideal class, it contains an ideal J such that

$$\|J\| < \frac{1}{2}\frac{3}{2}\sqrt{3} < \frac{3\sqrt{4}}{4} = \frac{6}{4} < 2$$

so that J is a principal ideal.

3. (a) Let $f \in \mathbb{Z}[x]$ be nonconstant. Show that f has a root mod p for infinitely many primes p. (Hint: prove this first under the assumption $f(0) = 1$ by considering prime divisors of $f(n!)$. Then reduce to this case by setting $g(x) = f(xf(0))/f(0)$.)

(b) Let $K/\mathbb{Q}$ be a finite Galois extension. Show that there are infinitely many primes P of K such that $f(P/p) = 1$ where $p \in \mathbb{Z}$ lies under P (the notation $f(P/p)$ indicates the degree of the residual extension).

Solution. (a) Recall a classical proof that there are infinitely many primes: if there were only finitely many, the largest of which was less than N, then $1 + N!$ would be divisible by none of them, and thus would be a prime larger than N, a contradiction.

In our case, first suppose that $f(0) = 1$ so that $f(x) = 1 + a_1x + \cdots + a_mx^m$. Suppose that f has a root mod p for only finitely many p, the largest of which is less than N. Let q be a prime divisor of $f(N!) = 1 + a_1N! + \cdots a_m(N!)^m$. If $q < N$ then $f(N!) \equiv 1 \pmod{q}$. Thus $q > N$ and f has a root mod q, a contradiction.

Now, write $f(x) = a_0 + a_1x + \cdots + a_mx^m$ with $a_0 \neq 0$ no longer taken to be 1. Then $f(0) = a_0$ and $g(x) = f(a_0x)/a_0 = 1 + a_1x + \cdots a_ma_0^{m-1}x^m$. Then $g(x)$ has a root mod p for infinitely many p by the above. Fix p and suppose that $g(\alpha) = 0$ for some $\alpha \in \mathbb{F}_p$. Then $x := \alpha/a_0$ is a zero of $f(x)$ mod p.

The case where $a_0 = 0$ is automatic since then 0 is a root mod p for all p.

(b) Write $K = \mathbb{Q}[\alpha]$ and let g be the minimal polynomial of α. We use Theorem 27 on page 79. Let $N := \#(\mathscr{O}_K/\mathbb{Z}[\alpha])$. Fix a prime $p \nmid N$ of which of course there are infintely many. The splitting of p in K is then given by the factorization of $g \pmod{p}$. In greater detail, we have

$$p.\mathscr{O}_K = P_1^{e_1} \cdots P_r^{e_r}$$

with $P_i = (p, g_i(\alpha))$ (= the ideal generated in $\mathscr{O}_K$ by p and $g_i(\alpha)$) where

$$g \equiv g_1^{e_1} \cdots g_r^{e_r} \pmod{p}$$

with the $g_i \in \mathbb{Z}[x]$ monic. Moreover we have $f(P_i/p) = \deg(g_i)$. Thus, part (a) gives us a linear factor of the minimal polynomial for infinitely many p, and the solution is complete.

4. (a) Let $K \subset L \subset M$ be a tower of finite Galois extensions of number fields (i.e. M/L is Galois and so is L/K). Let P, Q, U be a primes of K, L, M with U above Q above P. Suppose that P is unramified in M. Show that

$$\mathrm{Fr}_{U/Q} = \mathrm{Fr}_{U/P}^{f(Q/P)}$$

and that

$$\mathrm{Fr}_{Q/P} = \mathrm{Fr}_{U/P}|L.$$

(b) Let $\omega := e^{2\pi i/m}$ and $K \subset \mathbb{Q}[\omega]$. Identify $(\mathbb{Z}/m)^\times$ with $\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ and write $H = \mathrm{Gal}(\mathbb{Q}[\omega]/K)$. Suppose moreover that $(\mathbb{Z}/m)^\times$ is a cyclic group (this is the case, for instance, if m is the power of an odd prime). For $p \in \mathbb{Z}$ s.t. $p \nmid m$, let f be the least positive integer such that the residue class $p^f \in H \subset (\mathbb{Z}/m)^\times$ (f exists by the cyclicity assumption). Show that f is $f(P/p)$ for any prime P of K lying over p. (Hint: use part (a).)

Solution. (a) Consider the extensions of finite fields

$$k(P) \overset{f(Q/P)}{\subset} k(Q) \overset{f(U/Q)}{\subset} k(U)$$

of the indicated degree. Write $\sigma_{U/P}, \sigma_{U/Q}, \sigma_{Q/P}$ for the generator of the Galois group of $k(U)/k(P)$, $k(U)/k(Q)$, $k(Q)/k(P)$, respectively. By what we know about finite fields, we have

$$\sigma_{U/Q} = \sigma_{U/P}^{f(Q/P)} \text{ and } \sigma_{Q/P} = \sigma_{U/P}|k(Q).$$

We may identify the decomposition groups with the Galois groups of the respective finite fields because P is unramified in M. Lifting the previous equations to the level of the decomposition group completes the proof.

(b) The Galois group G is isomorphic to $(\mathbb{Z}/m)^\times$ with $\sigma \in G$ corresponding to $k \in (\mathbb{Z}/m)^\times$ iff $\sigma(\omega) = \omega^k$. We may consider Fr_p for all unramified primes, i.e. for all primes $p \nmid m$ (the primes dividing the discriminant are exactly the primes dividing m). We have

$$\mathrm{Fr}_p(x) \equiv x^p \pmod{p.\mathbb{Z}[\omega]}$$

for all $x \in \mathbb{Z}[\omega]$. Since the automorphism $\sigma_p : \omega \mapsto \omega^p \in G$ satisfies this congruence, and since G is abelian so that the Frobenius automorphism is uniquely determined as an element of G, we must have that $\sigma_p : \omega \mapsto \omega^p \in G$ coincides with Fr_p.

Thus we see that taking powers of the Frobenius corresponds to taking powers of the residue class of p in the multiplicative group $(\mathbb{Z}/m)^\times$. Combining with part (a) solves the problem. For more along these lines, see the discussion on page 110 of the book.

5. Let p be a prime not dividing m and suppose that $(\mathbb{Z}/m)^\times$ is a cyclic group. Determine how p splits in $\mathbb{Q}[\omega+\omega^{-1}]$ where $\omega := e^{2\pi i/m}$. Express your answer in terms of how p splits in $\mathbb{Q}[\omega]$. (Hint: use part (b) of problem 4.)

Solution. The splitting of p in $K := \mathbb{Q}[\omega]$ is given by Theorem 26 on page 76 of Marcus. Namely, p is unramified in K since $p \nmid m$, p splits into r primes in K where

$$r := \frac{\#(\mathbb{Z}/m)^\times}{f}$$

and the degree of the residual extension $f = f(Q/p)$ for one (and hence any since $K/\mathbb{Q}$ is Galois) prime Q of K lying over p coincides with the multiplicative order of $p \in (\mathbb{Z}/m)^\times = \mathrm{Gal}(K/\mathbb{Q}) =: G$.

Now, put $K^+ := \mathbb{Q}[\omega+\omega^{-1}]$ and $H := \mathrm{Gal}(K/K^+)$. We claim that K/K^+ is a quadratic extension. Clearly $K \neq K^+$. On the other hand, ω satisfies the monic polynomial with coefficients in K^+

$$f(X) := X^2 - aX + 1 \text{ where } a := \omega + \omega^{-1}.$$

To see this easily, observe that $a\omega = \omega^2 + 1$. Thus, $H \subset (\mathbb{Z}/m)^\times$ is of order 2.

Invoking 4(b) solves the problem: the splitting of p in K^+ is determined by the order, 1 or 2, of p^f in H, where f is as in the statement of 4(b).

6. Let $\omega := e^{2\pi i/m}$ and fix a prime $p \in \mathbb{Z}$. Write $m = p^k n$ with $p \nmid n$. We have

$$\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \simeq (\mathbb{Z}/m)^\times \simeq (\mathbb{Z}/p^k)^\times \times (\mathbb{Z}/n)^\times.$$

Describe the decomposition and inertia groups associated to p in terms of this direct product.

Solution. The splitting of p in $K := \mathbb{Q}[\omega]$ is given by Theorem 26 on page 76 of Marcus. Namely, $e = \varphi(p^k) = \#(\mathbb{Z}/p^k)^\times$ is the ramification index. Furthermore, p splits into r primes in K where

$$r := \frac{\#(\mathbb{Z}/m)^\times}{f}$$

and the degree of the residual extension $f = f(Q/p)$ for one (and hence any since $K/\mathbb{Q}$ is Galois) prime Q of K lying over p coincides with the multiplicative order of $p \in (\mathbb{Z}/m)^\times = \mathrm{Gal}(K/\mathbb{Q}) =: G$. (The difference with the previous problem is that we do not assume $p \nmid m$.)

Writing H for the subgroup of $(\mathbb{Z}/n)^\times$ generated by the residue class of p modulo n, we have that $I \simeq (\mathbb{Z}/p^k)^\times$ and $D/I \simeq H$ lands in the second factor of the direct product. Finally, $D \simeq I \times H \simeq (\mathbb{Z}/p^k)^\times \times H$.

7. Show that every finite subgroup of the unit circle is cyclic.

Solution. Let H be a finite subgroup of S^1. It is a discrete group by finiteness. Let G be the full preimage of H along the universal covering $\mathbb{R} \to S^1$ which is also a group homomorphism (provided that we choose coordinates on $\mathbb{R}$ properly). Since a covering map is a local homeomorphism, it follows that G is a discrete subgroup of $\mathbb{R}$. Thus it will suffice to show that a discrete subgroup G of $\mathbb{R}$ is (infinite) cyclic.

Let $\alpha_1 := \inf G \cap \mathbb{R}_{>0}$ so that $\alpha > 0$ since G is discrete and $\alpha \in G$ since G, being discrete, is closed in $\mathbb{R}$.

Let $\alpha_2 := \inf G \cap \mathbb{R}_{>\alpha_1}$. We have $\alpha_1 < \alpha_2 \leq 2\alpha_1$ and $\alpha_2 \in G$ by combining the facts that G is discrete and $2\alpha_1 \in G \cap \mathbb{R}_{>\alpha_1}$.

If $\alpha_2 < 2\alpha_1$ then $0 < \alpha_2 - \alpha_1 < \alpha_1$ and $\alpha_2 - \alpha_1 \in G$. This contradicts the definition of α_1. Thus $\alpha_2 = 2\alpha_1$. An identical argument shows that $\alpha_3 = 3\alpha_1, \ldots, \alpha_j = j\alpha_1, \ldots$ with the obvious notation. Thus

$$G \cap \mathbb{R}_{>0} = \mathbb{Z}_{>0}.\alpha$$

and therefore

$$G = \mathbb{Z}.\alpha$$

is cyclic.

8. (a) Let K be a number field and I be an ideal of $\mathscr{O}_K$. Show that there is a finite extension L/K in which I becomes principal, i.e. such that $I.\mathscr{O}_L$ is a principal ideal in $\mathscr{O}_L$.

(b) Show that there is a finite extension L/K in which every ideal of K becomes principal.

Solution. (a) Let $I \subset \mathscr{O}_K$ be an ideal. By the finiteness of the class group, $I^m = (\alpha) = \alpha.\mathscr{O}_K$ for some $\alpha \in \mathscr{O}_K$. Let $L := K[\alpha^{1/m}]$ and $J := I.\mathscr{O}_L$. Thus we have $J^m = (\alpha^{1/m})^m$. Then we claim that $J = (\alpha^{1/m}) = \alpha^{1/m}.\mathscr{O}_L$ is principal. If we could show this, the problem would be solved.

This statement may seem obvious; in fact it is not, and its proof relies in an essential way on the theorem on unique factorization of ideals in Dedekind domains.

Let $\mathscr{S}$ be the set of all ideals contained in $\mathscr{O}_L$. Then $\mathscr{S}$ is in a natural way an abelian monoid under multiplication of ideals (Corollary 2 page 59 of Marcus). The theorem on the unique factorization of ideals (Theorem 16 page 59) is equivalent to the statement that this monoid is the free abelian monoid generated by the prime ideals.

Let then $\mathscr{S} \to \mathscr{S}$ be the mth power map $I \mapsto I^m$. This homomorphism of monoids is injective because $\mathscr{S}$ is free. Therefore we may finally conclude

$$J^m = (\alpha^{1/m})^m \Rightarrow J = (\alpha^{1/m}).$$

This solves the problem.

(If you don't like monoids, we may consider the set of fractional ideals instead of the set of ideals. Then, by the unique factorization of fractional ideals, this set is the free abelian group generated by the prime ideals. The above argument goes through verbatim. See pages 94 and 98 of "Introduction to Commutative Algebra" by Atiyah and MacDonald. Cf. the isomorphism of groups

$$\mathbb{Q}^\times = \{\pm 1\} \cdot \prod_p p^{\mathbb{Z}} \simeq \mathbb{Z}/2 \times \bigoplus_p \mathbb{Z}$$

which comes from unique factorization, not only of ideals, but of elements of $\mathbb{Z}$.)

(b) Let $I_1, \ldots, I_t$ be ideals which represent each class of the class group. Let $n_1, \ldots, n_t$ be such that $I^{n_i} = (\alpha_i) \subset \mathscr{O}_K$ for some $\alpha_1, \ldots, \alpha_t$. Then $L = K[\alpha_1^{1/n_1}, \ldots, \alpha_t^{1/n_t}]$ is the sought extension. Of course, this only shows that all ideals of K become principal in L and says nothing about the ideals of L which do not come from K.