Algebraic Number Theory, Math 421
Instructor: Sreekar M. Shastry
Solutions to the Mid Semester Examination

- ⋆ Choose any 5 problems. Each problem is worth 5 points.
- ⋆ The maximum score is 25 points.
- ⋆ It is not permitted to submit partial solutions to more than 5 problems; you must choose the 5 that you want to be graded.
- ⋆ Clearly state the results which you invoke.

1. Let $K := \mathbb{Q}[\sqrt{m}]$ where m is squarefree and suppose that p is an odd prime. Write $\left(\frac{m}{p}\right)$ for the Legendre symbol. Show that

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & \text{if } p.\mathscr{O}_K = \text{ product of distinct primes of } \mathscr{O}_K \\ 0 & \text{if } p.\mathscr{O}_K = \text{ the square of a prime of } \mathscr{O}_K \\ -1 & \text{if } p.\mathscr{O}_K = \text{ a prime in } \mathscr{O}_K \end{cases}$$

Solution. We will use Theorem 27 on page 79 of Marcus which relates the factorization of $p.\mathscr{O}_K$ to the reduction mod p of the polynomial $X^2 - m \in \mathbb{Z}[X]$. This theorem is sometimes called Kummer's theorem.

First of all, note that $\mathscr{O}_K = \mathbb{Z}[\alpha]$ with $\alpha = \sqrt{m}$ or $(1+\sqrt{m})/2$ according as $m \equiv -1, 2 \pmod 4$ or $m \equiv 1 \pmod 4$ (see page 30 of Marcus).

We are considering in all cases the ring $\mathbb{Z}[\sqrt{m}]$ and we must check that p is prime to $\#\mathscr{O}_K/\mathbb{Z}[\sqrt{m}]$ (quotient of additive abelian groups) when $m \equiv 1 \pmod 4$. We have that $\mathbb{Z}[\sqrt{m}] = \mathbb{Z}[1+\sqrt{m}]$ which makes it clear that the quotient group in question is of order 2; p is an odd prime and so we may proceed.

Now, $\left(\frac{m}{p}\right) = 1 \iff X^2 - m \pmod p$ is reducible $\iff p.\mathscr{O}_K$ is a product of distinct primes by the Theorem; $e = f = 1, r = 2$.

Next, $\left(\frac{m}{p}\right) = -1 \iff X^2 - m \pmod p$ is irreducible $\iff f(Q/p) = 2, e = r = 1$ so that $p.\mathscr{O}_K = Q$ is a prime. Again we have used the theorem.

Finally, $\left(\frac{m}{p}\right) = 0 \iff p|m \iff X^2 - m \equiv X^2 \pmod p$ is the square of the prime $(X) \subset \mathbb{F}_p[X]$.

2. The objective of this problem is to show that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.
(a) Use the fact that $(\mathbb{Z}/p)^\times$ is cyclic to show that if $p \equiv 1 \pmod 4$ then $n^2 \equiv -1 \pmod p$ for some $n \in \mathbb{Z}$.
(b) Show that p cannot be irreducible in $\mathbb{Z}[i]$. (Hint: use (a).)
(c) Prove that p is a sum of two squares. (Hint: use (b).)

Solution. (a) The group $(\mathbb{Z}/p)^\times$ is cyclic of order $p-1$ and $p-1$ is divisible by 4, and thus we consider the homomorphism $x \mapsto x^{\frac{p-1}{4}}$ from $(\mathbb{Z}/p)^\times$ to itself. Let $y = x_0^{\frac{p-1}{4}}$ be in the image of this homomorphism. Then $y^2 \equiv -1 \pmod 4$ since $(y^2)^2 = x_0^{p-1} = 1$ and on the other hand $-1 \in (\mathbb{Z}/p)^\times$ is the unique element g such that $g^2 = 1$. Here we have used the cyclicity. Now choose $n \in \mathbb{Z}$ to be any lift of y.

(b) This follows from $p|n^2 + 1 = (n+i)(n-i)$ in $\mathbb{Z}[i]$. Here we must use the fact that $\mathbb{Z}[i]$ is a UFD.

(c) Recall that $\mathbb{Z}[i]$ is a Euclidean domain hence PID hence UFD. We have $p = (a+bi)(c+di)$ with neither factor a unit, by (b) — if no such expression was possible, i.e. if in every such factorization one of the factors was a unit, then p would still be a prime in $\mathbb{Z}[i]$ — that shows that p has at least two non unit factors; that there are at most two follows since the norm of each nonunit factor is a nontrivial divisor of $\mathrm{N}(p) = p^2$. On the other hand, the ideal $p.\mathbb{Z}[i]$ is principle and generated by a nonzero element $\alpha + \beta i$ of minimal norm. The norm of this element is a proper and nontrivial divisor of $\mathrm{N}(p) = p^2$, hence p, and we have $\mathrm{N}(\alpha + \beta i) = p = \alpha^2 + \beta^2$.

3. Let $\omega := e^{2\pi i/p}$ with p an odd prime. Show that $\mathbb{Q}[\omega]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$ and contains $\sqrt{-p}$ if $p \equiv -1 \pmod 4$.

Solution. We shall make use of the fact that the discriminant of the field extension $\mathbb{Q}[\omega]/\mathbb{Q}$ is $\Delta := (-1)^{\frac{p-1}{2}}p^{p-2}$. We may use the Vandermonde determinant to compute the discriminant as well:

$$\Delta = \prod_{\substack{i<j \\ \sigma_i \in \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})}} (\sigma_i(\omega) - \sigma_j(\omega))^2$$

to conclude that $\Delta = x^2 \in K$, i.e. that Δ is a square in K and hence that $\sqrt{(-1)^{\frac{p-1}{2}}p^{p-2}} \in K$. We multiply the last expression by $1/p^{\frac{p-3}{2}}$ (which is in K because p is odd) to see that $\sqrt{(-1)^{\frac{p-1}{2}}p} \in K$. This completes the proof.

4. (a) Show that if m is squarefree, $m < 0$, and $m \neq -1, -3$, then ± 1 are the only units in the ring of integers of $\mathbb{Q}[\sqrt{m}]$.
(b) What if $m = -1$ or -3?

Solution. (a) Two cases.
Case 1. $m \equiv -1, 2 \pmod 4$. In this case the integral basis of the ring of integers is given by $\{1, \sqrt{m}\}$ and the norm is $\mathrm{N}(a + b\sqrt{m}) = a^2 - b^2m = a^2 + |m|b^2$ (since $m < 0$). We set this equal to 1 and solve (no need to check the -1 case as the norm is automatically positive). We get $a = \pm 1, b = 0$.
Case 2. $m \equiv 1 \pmod 4$. The basis is $\{1, (1 + \sqrt{m})/2\}$ and a typical element is $\frac{a+b\sqrt{m}}{2}$ with $a \equiv b \pmod 2$ and we similarly reduce to solving the equation

$$a^2 + |m|b^2 = 4.$$

Solving gives $a = \pm 2, b = 0$ as required.
(b) $m = -1$. This is the fundamental example of the Gaussian integers $\mathbb{Z}[i]$. In this case, we quickly calculate with norms to see that the units are $\{\pm 1, \pm i\}$.
$m = -3$. The equation to solve is $a^2 + 3b^2 = 4$ and the units are $\{\pm 1, (\pm 1 \pm \sqrt{-3})/2\}$. (The factor of $1/2$ comes from the presentation of the ring of integers when $m \equiv 1 \pmod 4$).

5. Let α be an algebraic integer and let f be any monic polynomial in $\mathbb{Z}[x]$ such that $f(\alpha) = 0$. Show that $\mathrm{disc}(\alpha)$ divides $\mathrm{N}_{\mathbb{Q}[\alpha]/\mathbb{Q}}(f'(\alpha))$.

Solution. We shall invoke Theorem 8 on page 26 of Marcus which tells us that the discriminant of $\mathbb{Q}[\alpha]/\mathbb{Q}$ is $\pm\mathrm{N}_{\mathbb{Q}[\alpha]/\mathbb{Q}}(F'(\alpha))$ where F is the minimal polynomial of α.
In our case, f is not necessarily the minimal polynomial, and all we know is that $f(X) = F(X)g(X)$ where F is the minimal polynomial of α. Taking derivatives gives us $f'(X) = F'(X)g(X) + g'(X)F(X)$ and evaluating at α gives us

$$f'(\alpha) = F'(\alpha)g(\alpha).$$

Taking norms we have $\mathrm{N}(f'(\alpha)) = \mathrm{N}(F'(\alpha))\mathrm{N}(g(\alpha)) = \mathrm{disc}(\alpha).c$ where $c \in \mathbb{Z}$. The last assertion holds because $g(\alpha)$, being an algebraic integer, has norm in $\mathbb{Z}$.

6. Let K be a number field and $\mathfrak{a} \subset \mathscr{O}_K$ be a nonzero ideal. Show that $\#(\mathscr{O}_K/\mathfrak{a})$ divides $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ for all $\alpha \in \mathfrak{a}$, and equality holds iff $\mathfrak{a} = (\alpha)$.

Solution. We shall use Theorem 22 (c) on page 66 of Marcus which tells us that $\#\mathscr{O}_K/(\alpha) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$.
The tower of abelian group $(\alpha) \subset \mathfrak{a} \subset \mathscr{O}_K$ gives us

$$[\mathscr{O}_K : (\alpha)] = [\mathscr{O}_K : \mathfrak{a}][\mathfrak{a} : (\alpha)]$$

and since the left hand side equals $\#\mathscr{O}_K/(\alpha)$, the problem is solved.

7. Let L/K be a Galois extension with group G. Fix a prime P of K and a prime Q of L which lies above it.
(a) Define the inertia and decomposition groups associated to Q/P. What is the relation between these groups and the Galois group of the residual extension associated to Q/P? Give a proof of your assertion.
(b) Let P be a prime of K and Q be a prime of L above it. Define $\mathrm{Fr}_{Q/P}$. If G is abelian, what more can you say? Give a proof of your assertion.
(c) Show that for all $\sigma \in G$, we have

$$\mathrm{Fr}_{\sigma Q/P} = \sigma \mathrm{Fr}_{Q/P} \sigma^{-1}.$$

Solution. The solutions to (a) and (b) may be found in the book.

For (c) we compute as follows. Let $x \in \mathscr{O}_L$, and let $k(P) := \mathscr{O}_K/P$.

(1) $\mathrm{Fr}_{Q/P}(x) \equiv x^{\#k(P)} \pmod{Q}$.

(2) $\mathrm{Fr}_{\sigma Q/P}(x) \equiv x^{\#k(P)} \pmod{\sigma Q}$.

(3) $\mathrm{Fr}_{Q/P}(\sigma^{-1}(x)) \equiv (\sigma^{-1}(x))^{\#k(P)} \pmod{Q}$.

(4) $\sigma(\mathrm{Fr}_{Q/P}(\sigma^{-1}(x))) \equiv x^{\#k(P)} \equiv \mathrm{Fr}_{\sigma Q/P}(x) \pmod{\sigma Q}$.

(5) $\mathrm{Fr}_{\sigma Q/P} = \sigma \mathrm{Fr}_{Q/P} \sigma^{-1}$.

(1), (2), (3) are just the definitions. We apply σ to (3) to get (4) and (4) is the same as (5) which is what we were looking for.

8. Let L/K be a Galois extension of number fields with group G and let P be a prime of K. By "intermediate field" we mean "intermediate field different from K and L."

(a) Show that if P is inert in L then G is cyclic. In other words, show that no prime remains inert in a non-cyclic Galois extension of number fields.

(b) Suppose that P is totally ramified in every intermediate field, but not totally ramified in L. Show that no intermediate field can exist. What can you say about the structure of G in this case?

Solution. We make use of the following theorem, written in standard notation, especially $e := e(Q/P), f := f(Q/P), I := I(Q/P), D := D(Q/P)$. We have

$$\begin{tikzcd}
L \arrow[d, dash, "e=[L:L^I]"'] & Q \arrow[d, dash, "{e(Q/Q^I)=e,\, f(Q/Q^I)=1}"] \\
L^I \arrow[d, dash, "f=[L^I:L^D]"'] & Q^I \arrow[d, dash, "{e(Q^I/Q^D)=1,\, f(Q^I/Q^D)=f}"] \\
L^D \arrow[d, dash, "r=[L^D:K]"'] & Q^D \arrow[d, dash, "{e(Q^D/P)=f(Q^D/P)=1}"] \\
K & P.
\end{tikzcd}$$

This is Theorem 28 page 100 of Marcus.

(a) The fact that P is inert gives us $e = r = 1, f = n$. Thus $L^D = L$ and $L^I = L$. Thus $I = \{1\}$ and $G = D$. But D/I is always cyclic. Thus G is cyclic.

(b) Since P totally ramifies in any intermediate field, L^I cannot be an intermediate field (since L^I is the maximal intermediate field in which P does not ramify). Thus $L^I = L$ or K. In fact $L^I = K$ because otherwise P would be unramified in L while simultaneously being totally ramified in every intermediate field. Since the ramification index is multiplicative in towers, this cannot occur.

Thus $e = n$ and P is totally ramified in L, contradicting our hypothesis.

Therefore the only way that P could be totally ramified in every intermediate field and not totally ramified in L is if there are no intermediate fields.

This means that G has no proper subgroups at all and is hence cyclic of prime order.