Dr. Marques Sophie
Office 519

Algebraic number theory

Spring Semester 2014
marques@cims.nyu.edu

FINAL EXAM (1h50)

Show ALL steps and make sure I understand how you get the answer to have full credit! No material allowed!

Problem 1: Show that if $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$.

Solution: *Let $r = c/d$, $(c, d) = 1$ be an algebraic integer. Then r is the root of a monic polynomial in $\mathbb{Z}[x]$, say $f(x) = x^n + b_{n-1}x^{n-1} + ... + b_0$.*
So

$$\begin{array}{c} f(r) = \left(\frac{c}{d}\right)^n + b_{n-1}\left(\frac{c}{d}\right)^{n-1} + ... + b_0 = 0 \\ \Leftrightarrow c^n + b_{n-1}c^{n-1}d + ... + b_0 d^n = 0 \end{array}$$

This implies that $d|c^n$, which is true only when $d = \pm 1$. So $r = \pm c \in \mathbb{Z}$.

Problem 2:

1. Let $f(x) = x^n + a_n x^{n-1} + ... + a_1 x + a_0$ and assume that $p|a_i$ for $0 \leq i < n$ and $p^2 \nmid a_0$. Show that $f(x)$ is irreducible. (Hint: By contradiction, suppose that $f(x)$ is reducible.)
2. Let p be a prime number and define the **cyclotomic polynomial** Φ_p **of order** p by
$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1 \in \mathbb{Z}[x]$$
Show that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$. (Hint: Compute $\Phi_p(x + 1)$.)

Solution:

1. *By contradiction, if $p(x)$ factors as a product of two rational polynomials having integer coefficients. Thus if we assume that $p(x)$ is reducible, then*
$$p(x) = (b_0 + b_1 x + ... + b_r x^r)(c_0 + c_1 x + .. + c_s x^s),$$
where the b's and the c's are integers and where $r > 0$ and $s > 0$. Reading off the coefficient we first get $a_0 = b_0 c_0$. Since $p|a_0$, p must divide one of b_0 or c_0. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Suppose that $p|b_0$, $p \nmid c_0$. Not all the coefficients b_0, ... , b_r can be divisible by p; otherwise since $p \nmid a_n$. Let b_k be the first b not divisible by p, which manifestly false since $p \nmid a_n$. Let b_k be the first b not divisible by p, $k \leq r < n$. Thus, $p|b_{k-1}$ and earlier b's. But $a_k = b_k c_0 + b_{k-1}c_1 + b_{k-2}c_2 + ... + b_0 c_k$, which conflicts with $p|b_k c_0$. This contradiction proves that we could not have factored $p(x)$ and so $p(x)$ is indeed irreducible.

2. Note first that

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$$

We have that $p | \binom{p}{i}$ *for all* $i \in \{1, 2, ..., p-1\}$ *and* $p^2 \nmid \binom{p}{1} = p$. *Therefore by Eisenstein's Criterion, we have that* $\Phi_p(x+1)$ *is irreducible over* $\mathbb{Q}$ *and hence over* $\mathbb{Z}$.

Lastly, note that if $\Phi_p(x)$ *were reducible, then* $\Phi_p(x+1)$ *is also irreducible over* $\mathbb{Z}$.

Problem 3:

1. Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Show that $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$.
2. Show that every nonzero prime ideal in $\mathcal{O}_K$ contains exactly one integer prime.

Solution:

1. *Let* α *be a nonzero algebraic integer in* $\mathfrak{a}$ *satisfying the minimal polynomial* $x^r + a_{r-1}x^{r-1} + ... + a_0 = 0$ *with* $a_i \in \mathbb{Z}$, *for any* i *and* a_0 *not zero. Then* $a_0 = -(\alpha^r + ... + a_1\alpha)$. *The left hand side of this equation is in* $\mathbb{Z}$, *while the right-hand side is in* $\mathfrak{a}$.
2. *By the previous question, if* $\mathfrak{p}$ *is a prime ideal of* $\mathcal{O}_K$, *then certainly it contains an integer. By the definition of a prime ideal, if* $ab \in \mathfrak{p}$, *either* $a \in \mathfrak{p}$ *or* $b \in \mathfrak{p}$. *So* $\mathfrak{p}$ *must contain some rational prime. Now, if* $\mathfrak{p}$ *contain their greatest common denominator which is* 1. *But this contradict the assumption of non triviality. So every prime ideal of* $\mathcal{O}_K$ *contains exactly one integer prime.*

Problem 4: Find an integral basis for $\mathbb{Q}(\sqrt{2}\sqrt{-3})$.
Solution: *If* $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{-3})$, *then* $d_K = 8$, $d_L = -3$ *which are coprime. So that, a* $\mathbb{Z}$*-basis for the ring of integers of* $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ *is given by*

$$\{1, \sqrt{2}, \frac{1+\sqrt{-3}}{2}, \sqrt{2}(\frac{1+\sqrt{-3}}{2})\}$$

Problem 5: Show that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, but not a principal ideal domain.

Solution: $\mathbb{Z}[\sqrt{-5}]$ *is not a unique factorization domain by taking* $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, *and so cannot be a principal domain.*
To see that it is a Dedekind domain, it is enough to show that it is the set of algebraic integers of the algebraic number field $K = \mathbb{Q}(\sqrt{-5})$.

Problem 6: Show that a finite integral domain is a field.

Solution: *Let* R *be a finite integral domain. Let* $x_1, x_2, ..., x_n$ *be the elements of* R. *Suppose that* $x_ix_j = x_ix_k$, *for some* $x_i \neq 0$. *Then* $x_i(x_j - x_k) = 0$. *Since* R *is an integral domain* $x_j = x_k$, *so* $j = k$. *Thus, for any* $x_i \neq 0$,

$$\{x_ix_1, x_ix_2, ..., x_ix_n\} = \{x_1, x_2, ..., x_n\}$$

Since $1 \in R$, there exists x_j such that $x_i x_j = 1$. Therefore, x_i is invertible. Thus all nonzero elements are invertible, so R is a field.

Problem 7: Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathcal{O}_K$, then $\mathfrak{b}|\mathfrak{a}$ if and only if there is an ideal $\mathfrak{c}$ of $\mathcal{O}_K$ with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Solution: *If $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}_K$. Thus, $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, with $\mathfrak{c}$ an ideal of $\mathcal{O}_K$.*
If $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ with $\mathfrak{c} \subseteq \mathcal{O}_K$, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c} \subseteq \mathfrak{b}$.

Problem 8: Find a prime ideal factorization of $7\mathcal{O}_K$ in $\mathbb{Z}[(1+\sqrt{-3})/2]$.

Solution: *We now consider $f(x) (mod\ 7)$. We have*

$$x^2 - x + 1 \equiv x^2 + 6x + 1 \equiv (x+2)(x+4) \ (mod\ 7)$$

so 7 splits and its factorization is

$$(7) = (7, \frac{5+\sqrt{-3}}{2})(7, \frac{9+\sqrt{-3}}{2})$$

Problem 9: Show that

$$\sum_{a=1}^{p-1} (\frac{a}{p}) = 0$$

for any fixed prime p.

Solution: *Follows directly from the far that the number of residues equals the number of non residues.*

Problem 10: Show that W_K, the group of roots of unity in a number field K is cyclic, of even order.

Solution: *Let $\alpha_1, ..., \alpha_l$ be the roots of unity in K. For $j = 1, ..., l$, $\alpha_j^{q_j} = 1$ for some q_j which implies that $\alpha_j = e^{2\pi p_j} q_j$, for some $0 \le p_j \le q_j - 1$. Let $q_0 = \prod_{i=1}^{l} q_j$. Then clearly, each $\alpha_i \in (e^{\frac{2\pi i}{q_0}})$ so W_K is a subgroup of the cyclic group $(e^{\frac{2\pi i}{q_0}})$ and is, thus cyclic. Moreover, since $\{\pm 1\} \subseteq W_K$, W_K has even order.*

Problem 11: Show that, for any real quadratic field $K = \mathbb{Q}(\sqrt{d})$, where d is a positive square free integer, $U_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. That is, there is a fundamental unit $\epsilon \in U_K$ such that $U_K = \{\pm\epsilon^k : k \in \mathbb{Z}\}$.

Solution: *Since $K \subseteq \mathbb{R}$, the only roots of unity in K are $\{\pm 1\}$ so $W_K = \{\pm 1\}$. Moreover, since there are $r_1 = 2$ real and $2r_2 = 0$ non real*