Math 154. Homework 6

1. Let A be a Dedekind domain, F its fractional field, and $\mathscr{I}_A$ denote the group of fractional ideals of A.

(i) A fractional ideal ideal I of A is *principal* if $I = Ax$ for some $x \in F^\times$. Prove that the set P_A of principal fractional ideals of A is a subgroup of $\mathscr{I}_A$, and that every class in the quotient group $\mathrm{Cl}(A) = \mathscr{I}_A/P_A$ (the *class group* of A) is represented by a nonzero ordinary ideal of A. Deduce that $\mathrm{Cl}(A) = 1$ if and only if A is a PID.

(ii) For a fractional ideal J of A, let $[J]$ denote the class of J in $\mathrm{Cl}(A)$. If J and J' are two fractional ideals of A, prove that any A-linear map $J \to J'$ is multiplication by some $x \in F$, and deduce that $[J] = [J']$ in $\mathrm{Cl}(A)$ if and only if $J \simeq J'$ as A-modules.

Remark. In case $A = \mathscr{O}_K$ for a quadratic field K with discriminant D, there is a close connection between $\mathrm{Cl}(A)$ and the set of binary quadratic forms $q(x, y) = ax^2 + bxy + cy^2$ for which $b^2 - 4ac = D$ (with q taken up to invertible linear change of variables over $\mathbf{Z}$). This is explained in the handout on quadratic forms and class groups, which you may wish to read if so inclined. (We will never use it in this course.)

2. Let $K = \mathbf{Q}(\alpha)$ with $\alpha^3 = 2$. The following proves $\mathbf{Z}[\alpha] = \mathscr{O}_K$. (Recall from class that, in contrast, $\mathbf{Z}[10^{1/3}]$ is not the ring of integers of $\mathbf{Q}(10^{1/3})$.)

(i) Show $d(1, \alpha, \alpha^2) = -2^2 \cdot 3^3$, and deduce that $[\mathscr{O}_K : \mathbf{Z}[\alpha]]$ divides 6.

(ii) Prove that if $x = c_0 + c_1\alpha + c_2\alpha^2$ with $c_j \in \mathbf{Q}$ then

$$\mathrm{N}_{K/\mathbf{Q}}(x) = c_0^3 + 2c_1^3 + 4c_2^3 - 6c_0c_1c_2,$$

and deduce that $\mathrm{N}_{K/\mathbf{Q}}(x) \equiv c_0 \bmod 2$ for all $x \in \mathbf{Z}[\alpha]$.

(iii) Prove that if $x = c_0 + c_1(\alpha - 2) + c_2(\alpha - 2)^2$ with $c_j \in \mathbf{Z}$ then $\mathrm{N}_{K/\mathbf{Q}}(x) \equiv c_0 \bmod 3$. (Hint: $x = (c_0 - 2c_1 + 4c_2) + (c_1 - 4c_2)\alpha + c_2\alpha^2$).

(iv) Using (ii) and (iii), prove that $\mathscr{O}_K \cap (1/2)\mathbf{Z}[\alpha] = \mathbf{Z}[\alpha]$ and $\mathscr{O}_K \cap (1/3)\mathbf{Z}[\alpha] = \mathbf{Z}[\alpha]$, and use this with ($i$) to show that $\mathscr{O}_K = \mathbf{Z}[\alpha]$. (Hint: $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = 2$ and $\mathrm{N}_{K/\mathbf{Q}}(\alpha - 2) = -6$.)

3. (i) Compute the prime factorization of $p\mathbf{Z}[\sqrt{6}]$ for $p = 2, 3, 5, 7, 11, 13$.

(ii) Let $K = \mathbf{Q}(\alpha)$ with $\alpha^3 = 2$, so $\mathscr{O}_K = \mathbf{Z}[\alpha]$ and $\mathrm{disc}(K) = -2^2 \cdot 3^3$ by Exercise 2. Compute the prime factorization of $p\mathbf{Z}[\alpha]$ for $p = 2, 3, 5, 7, 11$, and find the least p which is totally split in $\mathbf{Z}[\alpha]$.

(iii) In $\mathbf{Z}[\sqrt{-26}]$, consider the factorizations $3 \cdot 3 \cdot 3$ and $(1 + \sqrt{-26})(1 - \sqrt{-26})$ of 27. Show that these are factorizations into irreducibles (hint: no element of $\mathbf{Z}[\sqrt{-26}]$ has norm 3). Explain this UFD counterexample in terms of the prime ideal factorizations of (3), $(1 + \sqrt{-26})$, and $(1 - \sqrt{-26})$ in $\mathbf{Z}[\sqrt{-26}]$, along the same lines as we explained the UFD counterexample $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$ in class.

4. Let $K = \mathbf{Q}(\zeta_n)$, and let $\Phi_n(X) \in \mathbf{Z}[X]$ denote the minimal polynomial of ζ_n over $\mathbf{Q}$ (so $\deg \Phi_n = \varphi(n)$).

(i) Consider the monic factorization $X^n - 1 = \Phi_n \cdot q_n$ with $q_n \in \mathbf{Z}[X]$. Show that q_n is a product of monic polynomials over $\mathbf{Z}$ that divide various $(X^d - 1)$'s in $\mathbf{Z}[X]$ (not just in $\mathbf{Q}[X]$!) for proper divisors d of n.

(ii) Using (i), prove that for any field k with $\mathrm{char}(k) \nmid n$ (so $X^n - 1$ is separable over k), the roots of Φ_n in k are precisely the primitive nth roots of unity of k (i.e., $\zeta \in k^\times$ with multiplicative order n), if any exist.

(iii) Let $p > 0$ be a prime with $p \nmid n$ and n not twice an odd integer, so $p \nmid \mathrm{disc}(K)$ and hence $p\mathbf{Z}[\zeta_n] = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ for pairwise distinct prime ideals $\mathfrak{p}_i$. Using (ii) for finite fields, show that each residue field $\mathbf{Z}[\zeta_n]/\mathfrak{p}_i$ is isomorphic to $\mathbf{F}_{p^f}$ where f is the order of p mod n (i.e., $n|(p^f - 1)$ with *minimal* f). Deduce that $g = \varphi(n)/f$, and relate the $\mathfrak{p}_i$'s to the monic irreducible factorization of Φ_n over $\mathbf{F}_p$.

(iv) Compute the prime factorization of $p\mathbf{Z}[\zeta_{12}]$ for $p = 5, 7, 11, 13$.

5. Let $R = \mathbf{Z}[\alpha]$ for $\alpha = p\sqrt{-3}$ with $p > 0$ a prime, so $X^2 + 3p^2$ is the minimal polynomial of α over $\mathbf{Q}$ and $\{1, \alpha\}$ is a $\mathbf{Z}$-basis of R. (In particular, R is not the ring of integers of its fraction field $K = \mathbf{Q}(\sqrt{-3})$ since $\sqrt{-3} \in K - R$.) Show that the ideal $\mathfrak{a} = (p, \alpha)$ in R is distinct from pR and has index p in R, but that $\mathfrak{a}^2$ has index p^3 in R. Hence, the multiplicativity of norms of nonzero ideals in integer rings of number fields is a property rather specific to those rings.