Math 154. Homework 5

1. (*i*) Read §1.3 of the text, and using Corollary 2 there show that $\varphi(n) > \sqrt{n}$ for all $n > 6$.

(*ii*) For a number field K, give a (crude) upper bound in terms of $[K : \mathbf{Q}]$ on n such that K contains a primitive nth root of unity.

(*iii*) Explain why the torsion subgroup of $\mathscr{O}_K^\times$ is the set of roots of unity in K, and prove it is finite.

2. Let A be a (commutative) ring, and M and N two A-modules. Define $\mathrm{Hom}_A(M, N)$ to be the set of A-linear maps $f : M \to N$, endowed with an A-module structure via $(a.f)(m) = a \cdot f(m)$.

(*i*) Show that the definition of the A-module structure makes sense. That is, prove $a.f : M \to N$ is A-linear for all $a \in A$ and that $(a, f) \mapsto a.f$ satisfies the axioms to be an A-module structure.

(*ii*) Show that this A-module structure depends "naturally" on M and N in the sense that if $T : M' \to M$ and $L : N' \to N$ are A-linear maps then the two induced maps

$$\rho_T : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N), \quad \lambda_L : \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N)$$

(note the placements of M' and N'!) respectively defined by $f' \mapsto f' \circ T$ and $f \mapsto L \circ f$ are A-linear and satisfy $\rho_{T'} \circ \rho_T = \rho_{T \circ T'}$ and $\lambda_L \circ \lambda_{L'} = \lambda_{L \circ L'}$ for A-linear maps $T' : M'' \to M'$ and $L' : N'' \to N'$.

(*iii*) If $M \simeq A^n$ is free with finite rank, construct an A-linear isomorphism $\mathrm{Hom}_A(M, N) \simeq N^n$.

(*iv*) If A is noetherian and M and N are finitely generated, prove that $\mathrm{Hom}_A(M, N)$ is finitely generated. (Hint: Choose a surjection $\pi : A^n \to M$ and show that ρ_π is injective. Then use (*iii*).)

3. This exercise uses Exercise 2 to interpret some ideal-theoretic operations in terms of module theory (especially in the Dedekind case). We fix a noetherian domain A with fraction field F.

(*i*) A *fractional ideal* of A is a nonzero finitely generated A-submodule of F. Prove that a fractional ideal of A is simply $(1/a)\mathfrak{a}$ for some nonzero $a \in A$ and some nonzero ideal $\mathfrak{a} \subseteq A$. Describe all fractional ideals when A is a PID, and construct a $\mathbf{Z}$-submodule of $\mathbf{Q}$ that is not finitely generated over $\mathbf{Z}$.

(*ii*) Let $I \subseteq F$ be a fractional ideal of A. Define $\widetilde{I} = \{x \in F \,|\, xI \subseteq A\}$. Prove $\widetilde{I} \neq 0$, and construct an A-linear isomorphism $\widetilde{I} \simeq \mathrm{Hom}_A(I, A)$. Deduce that $\widetilde{I}$ is a fractional ideal of A (in particular, *finitely generated* over A).

(*iii*) Now assume that A is *Dedekind*. Let $\mathfrak{a}$ be a nonzero ideal of A, with prime factorization $\mathfrak{a} = \prod \mathfrak{p}_i$. Prove that $\prod \widetilde{\mathfrak{p}}_i \subseteq \widetilde{\mathfrak{a}}$, and use that $\mathfrak{a}\widetilde{\mathfrak{a}} \subseteq A$ to prove that in fact $\prod \widetilde{\mathfrak{p}}_i = \widetilde{\mathfrak{a}}$ and $\mathfrak{a}\widetilde{\mathfrak{a}} = A$. (cf. Exercise 4(*ii*))

(*iv*) If I and J are fractional ideals of a Dedekind domain A, prove that so is IJ and that $\widetilde{IJ} = \widetilde{I} \cdot \widetilde{J}$. Conclude that fractional ideals of A for a commutative group under multiplication (with identity element A and inversion given by $I \mapsto \widetilde{I}$), and that as such it is a free $\mathbf{Z}$-module with basis given by the maximal ideals of A. In terms of the expression $I = \prod \mathfrak{p}_i^{e_i}$ with pairwise distinct maximal ideals $\mathfrak{p}_i$ and (possibly negative) exponents $e_i \in \mathbf{Z}$, show that $I \subseteq A$ if and only if $e_i \geq 0$ for all i.

4. Let $K = \mathbf{Q}(\sqrt{5})$ and let A be the index-2 order $\mathbf{Z}[\sqrt{5}]$ in $\mathscr{O}_K = \mathbf{Z}[(1 + \sqrt{5})/2]$.

(*i*) Rigorously prove that the ideal $\mathfrak{p} = (2, 1 + \sqrt{5})A$ in A is maximal, with $A/\mathfrak{p} = \mathbf{F}_2$.

(*ii*) Prove that $\mathfrak{p}^2 = 2\mathfrak{p}$ and $\widetilde{\mathfrak{p}} = (1/2)\mathfrak{p}$, so $\mathfrak{p}\widetilde{\mathfrak{p}} = \mathfrak{p}$.

(*iii*) Although $2A \subseteq \mathfrak{p}$, show that $\mathfrak{p} \nmid 2A$ in the sense of ideals; that is, $2A \neq \mathfrak{p}\mathfrak{b}$ for any ideal $\mathfrak{b}$ of A. (Hint: if $2A = \mathfrak{p}\mathfrak{b}$ for some $\mathfrak{b}$, show $\widetilde{\mathfrak{p}} = (1/2)\mathfrak{b}$ and deduce that $\mathfrak{p}\widetilde{\mathfrak{p}} = A$, contradicting (*ii*).)

5. This exercise uses the Chinese Remainder Theorem from HW3, Exercise 2. Let A be Dedekind.

(*i*) For nonzero ideals $\mathfrak{a}, \mathfrak{b} \subseteq A$, prove that $\mathfrak{a} + \mathfrak{b} = A$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ have no common prime factor. Then deduce in general that if $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$ and $\mathfrak{b} = \prod \mathfrak{p}_i^{f_i}$ with $e_i, f_i \geq 0$ then $\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}_i^{\min(e_i, f_i)}$. Give an ideal-theoretic reason for why this deserves to be denoted $\gcd(\mathfrak{a}, \mathfrak{b})$.

(*ii*) Use the Chinese Remainder Theorem in A to prove *weak approximation*: for maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $e_1, \ldots, e_n \geq 0$ there exists nonzero $b \in A$ such that the prime factorization of (b) has $\mathfrak{p}_i$ appearing with multiplicity exactly e_i. (Hint: prove that $\mathfrak{p}^e/\mathfrak{p}^{e+1}$ in $A/\mathfrak{p}^{e+1}$ is nonzero and principal for any $e \geq 0$.)

(*iii*) Let $\mathfrak{a}$ be a nonzero ideal of A. Construct $a \in A - \{0\}$ such that $(a) = \mathfrak{a}\mathfrak{c}$ with $\gcd(\mathfrak{c}, \mathfrak{a}) = (1)$. Then construct $a' \in A - \{0\}$ such that $(a') = \mathfrak{a}\mathfrak{c}'$ with $\gcd(\mathfrak{c}', \mathfrak{a}) = (1)$ *and* $\gcd(\mathfrak{c}', \mathfrak{c}) = (1)$. Deduce that $\mathfrak{a} = (a, a')$, so $\mathfrak{a}$ has two generators (so A "just barely" may fail to be a PID)! This is mainly of theoretical interest.