Math 676, Homework 2 (version 2, corrected)

1. Let A be a commutative ring with unit. Verify the equivalence of the three conditions for an A-module M to be Noetherian:

(1) All submodules N of M are finitely generated.

(2) Any strictly increasing chain of submodules $N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_r \subsetneq \cdots \subset M$ of M has finite length.

(3) Every subcollection $\{N_\alpha\}$ of submodules of M has a maximal element.

2. Prove that a principal ideal domain (PID) A is integrally closed in its quotient field $K = Frac(A)$.

3. An *order* in an algebraic number field K is a subring B of the ring of integers O_K such that $1 \in B$ and $K = Frac(B)$.

(a) Prove that B has an integral basis over $\mathbb{Z}$, i.e. it is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

(b) Prove that all finitely generated B-modules in K are free of rank $[K : \mathbb{Q}]$. In particular, conclude that B is a Noetherian ring. (Hint: generalize the proof in class for the ring of integers O_K.)

4. Consider the order $B = \mathbb{Z}[5\sqrt{5}]$ in $\mathbb{Q}[\sqrt{5}]$, i.e. B is the ring generated by $5\sqrt{5}$ over $\mathbb{Z}$.

(a) Prove that B is not a Dedekind domain. For the three defining properties (Noetherian; integrally closed in $Frac(B)$; prime ideals are maximal) determine which hold and which fail in B.

(b) Show that every ideal of B has a finite factorization into irreducible ideals. (Irreducible means no further factorization).

(c) Show that B does not have unique factorization of ideals into prime ideals.

5. Let B be an order in a number field K, and let $B = \mathbb{Z}[\alpha_1, ..., \alpha_n]$ be an integral basis of B (Problem 3). The discriminant of B is $d[\alpha_1, ..., \alpha_n]$, where $n = [K : \mathbb{Q}]$.

(a) Show that the discriminant is independent of the integral basis chosen, so it can be denoted d_B.

(b) Show that if d_B is squarefree, then $B = O_K$ is the ring of integers of K.

(c) Give an example of a quadratic field that shows that the converse of (b) does not hold.

6. Prove that if R is a Dedekind domain, then every ideal I is generated by two elements. More precisely, show that given any $\alpha \in I$ there exists $\beta \in I$ such that $I = (\alpha, \beta)$ (as an R-module), as follows.

(a) Prove the Chinese Remainder Theorem for general commutative rings R. Two ideals I, J in R are relatively prime if $I + J = R$. Show that if $I_1, ..., I_n$ are pairwise relatively prime then the (product of projections) mapping

$$R/(\cap_{j=1}^{n} I_j) \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n).$$

is an isomorphism.

(b) Factor I into prime ideals, then factor (α) into prime ideals. Use the Chinese Remainder Theorem for ideals to find an element $\beta \in I$ whose prime factorization (β) avoids any extra ideal divisors in (α) not occurring in the prime factorization of I. Show β has the required property above.

7. A number field is *totally real* if all embedding of K into $\mathbb{C}$ are real (i.e. a primitive element and all of its conjugates are real.) A field L is a CM field if it is a totally imaginary extension of degree 2 over a totally real field That is, $L = K(\sqrt{\beta})$ where β and all of its conjugates over $\mathbb{Q}$ are negative real numbers. [The name "CM-field" abbreviates "complex multiplication", such fields arise from endomorphisms on certain elliptic curves/ abelian varieties.] Prove that every abelian extension of $\mathbb{Q}$ is either totally real or else a CM-field.

8. Let K be a number field with $[K : \mathbb{Q}] = n$, and consider $K = \mathbb{Q}[\alpha_1, ..., \alpha_n]$ with each $\alpha_1 \in O_K$. Show the discriminant $D = d[\alpha_1, ..., \alpha_n]$ is an integer with $D \equiv 0$ or $1 \pmod 4$. (This is discriminant of the module $B = \mathbb{Z}[\alpha_1, ..., \alpha_n]$. When $B = O_K$ this congruence is called *Stickelberger's criterion.*)

(*Hint.* Express D as the square of the determinant of the conjugates of $\sigma_j(\alpha_i)$. In the expression for determinant as $n!$ terms, let P be sum of terms for even permutations and N sum of odd permutation terms. Then $D = (P - N)^2 = (P + N)^2 - 4PN$. Then prove that $P+N$ and PN are in $\mathbb{Z}$, by showing they are algebraic integers and in $\mathbb{Q}$.)

9. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ be the splitting field for $(x^2-3)(x^2-5) = 0$ over $\mathbb{Q}$.

(a) Prove that $\alpha = \sqrt{3} + \sqrt{5}$ is a primitive element of $K = \mathbb{Q}(\alpha)$.

(b) Compute the discriminant of the order $B = \mathbb{Z}[\alpha]$ in two ways. First compute it as a determinant of the trace bilinear form. Secondly, compute it as $(-1)^{n(n-1)/2} \prod_{\sigma \neq \tau}(\sigma(\alpha) - \tau(\alpha))$, where σ, τ run over all embeddings of K in $\mathbb{C}$ (with $n = [K;\mathbb{Q}] = 4$ here)

10. (*) [S. Ramanujan (Question 1076, J. Indian Math. Soc. XI, p. 199] Show that:

(a) $\left(7\sqrt[3]{20} - 19\right)^{\frac{1}{6}} = \sqrt[3]{\frac{5}{3}} - \sqrt[3]{\frac{2}{3}}$

(b) $\left(4\sqrt[3]{\frac{2}{3}} - 5\sqrt[3]{\frac{1}{3}}\right)^{\frac{1}{8}} = \sqrt[3]{\frac{4}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{1}{9}}$

To Ramanujan's problem, we add the (easier) questions:

(c) Which of the numbers (a) and (b) are algebraic integers? Which are units?

Remarks. (1) Ramanujan's problem was left unsolved; no solution was submitted. This may be because it has a misprint (corrected above).

(2) These identities should be verifiable by computer, using PARI or MAGMA.