Groups, Rings and Modules (example sheet 2)

NIS-B, Lent 2008

As usual, avoid using the hints as far as possible. If you can do all the starred questions then you will be in good shape for the exam.

(1) Given a ring A and an indeterminate X, denote the ring of formal power series in X with coefficients in A by $A[[X]]$. So a typical element is an infinite sum $\sum_0^\infty a_n X^n$ with $a_n \in A$. These are added, subtracted and multiplied in a purely algebraic way; there is no question of convergence. (This means that we cannot evaluate $\sum_0^\infty a_n X^n$ at a value of X, except at $X = 0$.)

(i*) Show that $\sum_0^\infty a_n X^n$ is a unit if and only if a_0 is a unit in A.

Suppose that A is Noetherian.

(ii*) Show that $\sum_0^\infty a_n X^n$ is nilpotent if and only if every a_n is nilpotent.

(iii) Show that $A[[X]]$ is Noetherian.

[Hint: Suppose that J is an ideal in $A[[X]]$. Mimic the proof of the Hilbert Basis Theorem, but use terms of lowest degree instead of highest. So define I_0 to be the subset of A consisting of constant coefficients of elements of J, I_1 the subset of A consisting of the linear coefficients when the constant term is zero, and so on. Check that the I_n's are ideals of A and form an ascending chain. So $I_m = I_{m+1} = ...$ for some m. Pick finitely many generators $a_{0,i}$ of I_0 and corresponding power series $p_{0,i}$, and do the same for each of $I_1, ..., I_m$. Show that the finite set $p_{j,i}$, where $j = 0, ..., m$, generates J.]

(2) Suppose that p is prime.

(i*) Show that $\mathbb{Z}[X]/(X - p) \cong \mathbb{Z}$.

(ii) If you know about the p-adic integers $\mathbb{Z}_p$, show that $\mathbb{Z}[[X]]/(X - p) \cong \mathbb{Z}_p$.

(3*) (i) State a structure theorem for finitely generated modules over a Euclidean domain A and explain how to derive it from a theorem about matrices over A. Explain how to prove this theorem.

(ii) In terms of your structure theorem from (i), describe the abelian group with generators $e_1, ..., e_4$ and relations $2e_1+3e_2+4e_3 = 5e_2+6e_3+7e_4 = 0$.

(iii) State and solve many more problems like (ii). I suggest problems with 4 or 5 generators and 3 or 4 relations, where the coefficients are single-digit integers.

(iv) A module M over a ring A is *torsion-free* if an equation $am = 0$ implies either $a = 0$ or $m = 0$. Show that a finitely generated torsion-free $\mathbb{Z}$-module M is free. Is this true for all torsion-free $\mathbb{Z}$-modules, or for all finitely generated modules over arbitrary Noetherian rings?

(4) The definition in lectures of "Euclidean domain" involves a function $\phi : A-\{0\} \to \mathbb{N}$ such that whenever $a, b \in A$ with $b \neq 0$, we can write $a = bq+r$ with either $r = 0$ or $\phi(r) < \phi(b)$. Some authors demand also that $\phi(xy) \geq \phi(x)$; show that the two definitions are essentially equivalent. [This is made precise, and a careful argument given, in the Wikipedia article on Euclidean domains. Look it up and read it.]

(5*) (i) Suppose that $\alpha \in \mathbb{C}$ is algebraic; that is, α is a zero of a non-trivial polynomial over $\mathbb{Q}$. Suppose that $f \in \mathbb{Z}[X]$ is its primitive minimal polynomial. Prove that the kernel of the homomorphism $\pi : \mathbb{Z}[X] \to \mathbb{Z}[\alpha]$ defined by $\pi(X) = \alpha$ has kernel equal to the principal ideal (f) and deduce that $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$.

(ii) Generalize this by replacing $\mathbb{Z}$ by any Noetherian UFD and α by any element of a field L that contains the field K of fractions of A, such that α is algebraic over K.

(6) Suppose that A is a Noetherian ring.

(i*) The *nilradical* of A, denoted $r(A)$, is the set of $x \in A$ such that $x^n = 0$ for some n. Prove that $r(A)$ is the intersection of the prime ideals of A. [Hint: Suppose $x \notin r(A)$. Consider the set S of ideals that contain no power of x and show that every maximal element of S is prime.]

(ii*) Suppose that P is a maximal ideal of A and that I is an ideal with $\sqrt{I} = P$. Show that I is primary. [Hint: P/I is the nilradical of A/I, so, by (i), is the unique prime ideal of A/I. So every element of A/I is either a unit or nilpotent, so that every zero-divisor in A/I is nilpotent.]

(iii) Suppose that A is a domain and that every prime ideal is principal. Show that A is a PID. [Hint: Prove first that every non-zero prime ideal is maximal. Then observe that if $P = \sqrt{I}$ is maximal, then P is the unique prime ideal containing I. Prove next that every primary ideal is principal, then, via the existence of primary decompositions, that every irreducible element of A is prime. Conclude by using primary decompositions again.]

(7) Zorn's Lemma (in fact equivalent to the Axiom of Choice, so don't try to prove it, it's really an axiom) states that if $(S, \leq)$ is a non-empty partially ordered set and if every totally orderd subset T of S has an upper bound in S, then S has a maximal element s_0. ["Partially ordered" means the following three things: $x \leq x$; if $x \leq y$ and $y \leq z$, then $x \leq z$; and if $x \leq y$ and $y \leq x$, then $x = y$. "Totally ordered" means that for any two elements x, y of T, either $x \leq y$ or $y \leq x$. "Upper bound in S" means that there exists $s \in S$ such that $t \leq s$ for all $t \in T$. "Maximal" means that if $s_0 \leq s$, then $s_0 = s$.]

Use Zorn's lemma to show that every ring has a maximal ideal.

(8) Show that a ring A in which every prime ideal is finitely generated is Noetherian. [Hint: Suppose A is not Noetherian and take S to be the set of ideals that are not finitely generated. Show, via Zorn, that S has a maximal element and that the maximal elements of S are prime, as follows. Suppose that I is maximal in S and $x, y \notin I$, $xy \in I$. Show that there is a finitely generated ideal $I_0 \subset I$ such that $I + (x) = I_0 + (x)$ and that $I = I_0 + x.(I : x)$, where $(I : x) = \{z \in A | xz \in I\}$. Since $(I : x)$ is strictly bigger than I, it is finitely generated, and therefore so is I.]

(9) Suppose that M is an abelian group, *not* necessarily finitely generated. Suppose that there is a function $h : M \to \mathbb{R}_{\geq 0}$ (called a height function) and an integer $m \geq 2$ such that

(i) for every $Q \in M$ there is a constant C_1, depending on Q, such that $h(P + Q) \leq 2h(P) + C_1$ for all $P \in M$;

(ii) there is a constant C_2 such that $h(mP) \geq m^2 h(P) - C_2$ for all $P \in M$;

(iii) for all $C_3 \in \mathbb{R}$, the set $\{P \in M | h(P) \leq C_3\}$ is finite;

(iv) M/mM is finite.

Prove that M is, in fact, finitely generated.

[Hint: Choose finitely many $Q_i \in M$ representing the finitely many elements of M/mM. Then take $P \in M$, and show that by subtracting a suitable $\mathbb{Z}$-linear combination of the Q_i you can get $P' \in M$ with $h(P')$ less than some constant that is independent of P.]

The ring A of symmetric polynomials in $X_1, ..., X_n$ with coefficients in $\mathbb{Z}$ is, by definition, the set of all $\mathbb{Z}$-polynomials in the X_i that are invariant under all permutations of the X_i. For example, $X_1 + X_2$ is symmetric, but $X_1 + X_2^2$ is not. The next question asks you to prove that A is a polynomial ring $\mathbb{Z}[\sigma_1, \ldots, \sigma_n]$ in the so-called *elementary symmetric functions* $\sigma_i = \sigma_i(X_1, \ldots, X_n)$, defined by the identity

$$\prod_1^n (T - X_i) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} - ... + (-1)^n \sigma_n,$$

where T is a further indeterminate. This result goes back to Newton.

(10) (i) Prove that $\mathbb{Z}[\sigma_1, \ldots, \sigma_n] \subset A$.

(ii) Define the *lexicographic* ordering $\leq_{lex}$ on the set of monomials in the X_i by

$$X_1^{p_1} ... X_n^{p_n} \leq_{lex} X_1^{q_1} ... X_n^{q_n}$$

if and only if for some r we have $p_i = q_i$ for all $i < r$ and $p_r > q_r$. Say $M <_{lex} N$ if $M \leq_{lex} N$ and $M \neq N$. Show that this is a total ordering; that is, given any two monomials M, N, exactly one of $M = N$, $M <_{lex} N$ and $N <_{lex} M$ is true.

(iii) Suppose that $0 \neq f \in A$ and that $M = X_1^{p_1} ... X_n^{p_n}$ is the lexicographically least monomial that appears in f and that λ is the coefficient of M in f. By using the fact that f is invariant under the transposition $(i, i+1)$, show that $p_i \geq p_{i+1}$ for all i.

(iv) Prove, by induction on the degree, that every element f of A lies in $\mathbb{Z}[\sigma_1, \ldots, \sigma_n]$. [Hint: consider $f - \lambda \sigma_1^{p_1 - p_2} \sigma_2^{p_2 - p_3} ... \sigma_{n-1}^{p_{n-1} - p_n} \sigma_n^{p_n}$.]

(v) Prove that the σ_i are algebraically independent. [Hint: Use induction on n. Assume that $h(\sigma_1, ..., \sigma_n) = 0$ is a polynomial relation of minimal non-zero degree. For $i \leq n-1$, put $\tau_i = \sigma_i|_{X_n = 0}$, so that $\mathbb{Z}[\tau_1, ..., \tau_{n-1}]$ is the ring of symmetric polynomials in the $n-1$ variables $X_1, ..., X_{n-1}$. By the induction hypothesis, the τ_i are algebraically independent, so that h is divisible by σ_n. Divide by σ_n to conclude.]

(11) This question asks you to show the power sums $p_i = \sum_{j=1}^n X_j^i$ will do as well as the σ_i, provided that $\mathbb{Z}$ is replaced by $\mathbb{Q}$.

Introduce a further indeterminate x and put

$$f(x) = \sum_{i=0}^{n} \sigma_i (-1)^i x^{n-i},$$

where $\sigma_0 = 1$, by definition.

(i) Factorize f in $\mathbb{Z}[X_1, \ldots, X_n][x]$.

(ii) Regard x as a complex number, and show that if $|x|$ is large enough, then

$$\frac{x f'(x)}{f(x)} = \sum_{1 \leq k \leq n} \frac{1}{1 - X_k/x} = \sum_{j \geq 0} p_j x^{-j}.$$

[Hint: look at the derivative of $\log \prod_i (x - X_i)$.]

(iii) Deduce that $p_1 = \sigma_1, p_2 = p_1 \sigma_1 - 2\sigma_2, \ldots,$

$$p_{n-1} = p_{n-2}\sigma_1 - p_{n-3}\sigma_2 + \ldots - (-1)^n p_1 \sigma_{n-2} + (-1)^n (n-1)\sigma_{n-1}$$

and

$$p_k = p_{k-1}\sigma_1 - p_{k-2}\sigma_2 + \ldots - (-1)^n p_{k-n}\sigma_n \quad (k \geq n).$$

(iv) Use the result $A = \mathbb{Z}[\sigma_1, \ldots, \sigma_n]$ from the previous question to deduce that the ring of symmetric polynomials in $X_1, ..., X_n$ with coefficients in $\mathbb{Q}$ is $\mathbb{Q}[p_1, \ldots, p_n]$.

(12*) Suppose that ϕ is an endomorphism of the finite-dimensional complex vector space V. We say that ϕ is *semi-simple* if it can be diagonalized, and *nilpotent* if $\phi^n = 0$ for some n.

(i) Show that $\phi = \phi_s + \phi_n$ with ϕ_s semi-simple, ϕ_n nilpotent and $\phi_s\phi_n = \phi_n\phi_s$. [Hint: Jordan normal form.]

(ii) Show that there are polynomials $p, q \in \mathbb{C}[T]$, depending on ϕ, with zero constant term, such that $p(\phi)$ is semi-simple, $q(\phi)$ is nilpotent and $\phi = p(\phi) + q(\phi)$.

[Hint: Suppose that the distinct eigenvalues of ϕ are $a_1, ..., a_r$, with multiplicities $m_1, ..., m_r$. So the characteristic polynomial of ϕ is $\prod(T - a_i)^{m_i}$ and $V = \oplus V_i$, where V_i is the kernel of $(\phi - a_i)^{m_i}$. Apply the Chinese Remainder Theorem to the PID $\mathbb{C}[T]$ to deduce the existence of $p(T) \in \mathbb{C}[T]$ satisfying all the congruences $p(T) \equiv a_i$ modulo $(T - a_i)^{m_i}$ and $p(T) \equiv 0$ (mod T). Define $q(T) = T - p(T)$ and define $\phi_s = p(\phi)$, $\phi_n = q(\phi)$. Show that ϕ_s and ϕ_n preserve each V_i and are, respectively, semi-simple and nilpotent on each V_i.]

(iii) Show that the decomposition in (i) is unique.