Groups, Rings and Modules
(example sheet 1)

NIS-B, Lent 2008

As ever, use the hints provided only as a last resort. (1*) Which of the following are rings, integral domains, fields?

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, the set of C^∞ functions $f : \mathbb{R} \to \mathbb{R}$, the set of holomorphic functions $f : \mathbb{C} \to \mathbb{C}$, $\mathbb{Z}/n$.

(2*) Let R denote the ring of C^∞-functions $\mathbb{R} \to \mathbb{R}$.
(i) Show that the ideal I of functions vanishing at 0 is principal and give a generator.
(ii) Define f by $f(0) = 0$ and $f(x) = e^{-x^{-2}}$ if $x \neq 0$. Show that $f \in R$.
(iii) Show that R is not Noetherian.

[Hint: consider the ideal I_n generated by the 2^nth root of f.]

(iv) Use Taylor series to construct a homomorphism from R to $\mathbb{R}[[x]]$, the ring of formal power series in one variable. Show that f is in the kernel.
(v) Show that $\mathbb{R}[[x]]$ is a PID. Identify its irreducible elements.

[Remark: This function f might appear to be merely some hideous counter-example. In fact, it plays a very positive part in mathematics. For example, it can be used as a device to glue together two C^∞ functions defined on open intervals with disjoint closures to get a C^∞ function on all of $\mathbb{R}$. (Exercise: do this.) It has a similar use in higher dimensions, to construct "partitions of unity", which are a key technical device in the calculus and geometry of manifolds.]

(3) (i*) Suppose that A is Euclidean with Euclidean function ϕ. Is it true that, given $a, b \in A$ with $b \neq 0$, the elements $q, r \in A$ with $a = bq + r$ with either $r = 0$ or $\phi(r) < \phi(b)$, the elements q, r are uniquely determined by a, b?

(ii*) Show that $\mathbb{Z}[i]$ is Euclidean. [This is bookwork.]

(iii) Try to adapt the proof given in lectures that $\mathbb{Z}[i]$ is Euclidean to rings of the form $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ for various square-free positive $d \equiv 3 \pmod 4$. (You will have to replace the square lattice used for $\mathbb{Z}[i]$ by something else.)

Use this to find which prime numbers p can be written as $p = m^2 + 3n^2$, etc.

(4*) (i) Factorize $3 + 4i$ into irreducibles in $\mathbb{Z}[i]$.

(ii) Find the units in the ring $\mathbb{Z}[i]$ and in the polynomial rings $k[X]$ and $\mathbb{Z}[X]$, where k is a field. [A unit is an element u with a multiplicative inverse.]

(5) Which of the following rings are Noetherian?

(i) The ring of rational functions of z having no pole on the unit circle $|z| = 1$.

(ii) The ring of power series in z having a positive radius of convergence.

(iii) The ring of power series in z with an infinite radius of convergence.

(iv*) The ring of polynomials in z whose first n derivatives vanish at the origin (n is a fixed integer).

(v*) The ring of polynomials f in the variables z, w such that $\frac{\partial f}{\partial w}$ vanishes at $z = 0$.

(Throughout, the coefficients are complex numbers.)

(6*) A ring A is *graded* if it is a direct sum $A = \oplus_{n \geq 0} A_n$ such that each A_n is closed under addition and $A_m.A_n \subset A_{m+n}$.

Suppose that A is graded. Show that A is Noetherian if and only if A_0 is Noetherian and A is finitely generated as an A_0-algebra. [Do not just state Hilbert's Basis theorem, but prove it.]

(7) (i) Define the notions of *maximal, prime, primary, irreducible, radical* as applied to ideals.

(ii) Give examples of each in the ring $\mathbb{Z}$. In particular, give an example of a primary ideal that is not prime and a prime ideal that is not maximal.

(iii) Show that the radical of a primary ideal is prime.

(iv) Show that if $P, I_1, ..., I_n$ are ideals with P prime and $\bigcap_1^n I_j \subset P$, then $I_i \subset P$ for some i. Show moreover that if each I_j is primary, then $\sqrt{I_i} \subset P$ for some i, and that if each I_j is prime, then $I_i = P$ for some i.

(v) Give an example of a primary ideal that is not irreducible. [Hint: play around with ideals of $k[x, y]$ generated by monomials in x, y.]

(8*) Suppose that k is a field (algebraically closed if you like) and that $R = k[X, Y, Z]/(XY - Z^2) = k[x, y, z]$, where x is the residue class of X, etc. Show that $P = (x, z)$ is a prime ideal in R, that $\sqrt{P^2} = P$ but that P^2 is not primary.

(9) (i*) Show that the ideal $I = (X^2, XY)$ in $k[X, Y]$ has prime radical, but is not primary.

(ii) Find its primary decomposition.

(10*) A *discrete valuation* of a field K is a map $v : K^* \to \mathbb{Z}$ such that $v(xy) = v(x) + v(y)$ and $v(x + y) \leq \max\{v(x),\ v(y)\}$.

(i) Fix a prime number p and define $v_p : \mathbb{Q}^* \to \mathbb{Z}$ by $v_p(x) = r$ if $x = p^r.\frac{a}{b}$ where a, b are prime to p. Show that v_p is a discrete valuation of $\mathbb{Q}$.

(ii) The *discrete valuation ring* (abbreviated to DVR) O_v of v is $\{x \in K^* | v(x) \geq 0\} \cup \{0\}$. Show that O_v is a subring of K and that $K = Frac(O_v)$.

(iii) Show that O_v is a PID and describe all its ideals.

(iv) Assume that $im(v) = \mathbb{Z}$. Show that O_v has a unique maximal ideal M, and that M is generated by any element x such that $v(x) = 1$.

(v) What happens if $im(v) \neq \mathbb{Z}$?

(vi) Generalize the construction in (i) to find valuations of the field $k(X)$ of rational functions in one variable. Describe the corresponding DVRs.

(vii) Show that DVRs are exactly the integral domains A containing an element x such that every non-zero ideal is generated by a power of x.

(11*) Find a finite set of generators of the ideal I of the polynomial ring $k[x, y]$, where I is generated by the infinite set $\{x^{2n} - y^{3n} | n \in \mathbb{N}\}$.

(12*) Compute the dimension as a k-vector space of the quotient ring $k[x, y]/(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$ in the following two cases:

(i) $f = x^2 - y^3$;

(ii) $f = x^2y - x^2y^2$.

(13*) Suppose that $I_0 \subset I_1 \subset ...$ is an ascending chain of ideals. Show that $\bigcup_{n\geq 1} I_n$ is also an ideal.

(14*) Show that the dimension of the space $P_{n,d}$ of polynomials of degree $\leq d$ in n variables is the binomial coefficient $\frac{(n+d)!}{n!d!}$. Find the dimension of the space of homogeneous polynomials of degree d in $n + 1$ variables.

(15) Suppose that k is algebraically closed. A *line* in $\mathbb{A}^3_k$ is the variety defined by two linearly independent members of $P_{3,1}$ that do not generate the ideal (1) in $k[x, y, z]$. (In other words: a line is what you think it is.)

(i) Show that, given three lines in $\mathbb{A}^3_k$, there is at least one member of $P_{3,2}$ that vanishes along all of them.

(ii) Show that if the lines are skew (i.e., there is no plane containing any two of them), then this member of $P_{3,2}$ is unique up to scalars.

[(i) is just algebra. However, (ii) is more geometric. It is most naturally done as an exercise concerning quadric surfaces and the curves on them.]

(16*) Show that $R[x, y]/(y - f(x)) \cong R[x]$ for any ring R and $f(x) \in R[x]$.