Groups, Rings and Modules (example sheet 3)

NIS-B, Lent 2008

1* (i) Let $K = \mathbb{Q}(\alpha)$ where α is the real cube root of 2. What is the minimal polynomial of α over $\mathbb{Q}$?

(ii) Put $\omega = \exp(2\pi i/3)$. Show that $\mathbb{Q}(\omega\alpha)$ is isomorphic to $\mathbb{Q}(\alpha)$.

2* Prove that any finite integral domain is a field.

Suppose that L is an integral domain containing a field K such that L is finite dimensional as a vector space over K. Prove that L is a field. [Hint: Show that multiplication by any nonzero element is an isomorphism of vector spaces.]

3* Which of the following are fields? Which are integral domains?

(i) $\mathbb{Z}[x]/(x^3 - 2)$.

(ii) $\mathbb{Z}[x]/(2, x^3 + x + 1)$.

(iii) $\mathbb{Q}[x]/(x^4 + x^2 + 1)$.

4* Suppose that $K \hookrightarrow L$ is a field extension such that $[L : K] = 2$ (such an extension is called *quadratic*) and the characteristic of K is not 2. Show that there is an element $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^2 \in K$.

5* Find all irreducible polynomials over $\mathbb{F}_2$ of degree at most 4. (One method is to use the "sieve of Eratosthenes": write out all nonconstant polynomials in order of their degree, then repeatly add the first new uncrossed out polynomial to your list of irreducible polynomials and cross out all polynomials of larger degree divisible by it.)

6* Let α be the complex number $e^{2\pi i/5}$. Show that $\mathbb{Q}[\alpha]$ is a field of degree 4 over $\mathbb{Q}$. Show that it contains the field $\mathbb{Q}(\sqrt{5})$.

7 Show that $\binom{p}{n}$ is divisible by p whenever p is prime and $0 < n < p$. If K is a field of characteristic p (this means that $p = 0$ in K, for example Z_p) show that $(x + y)^p = x^p + y^p$. Define $F : K \to K$ by $F(x) = x^p$.

(i) Show that F is an isomorphism from the field K to a subfield of K. (It is called the Frobenius endomorphism.)

(ii) Show that $F(x) = x$ if and only if $x \in \mathbb{F}_p$, the field of p elements.

8* Find the highest common factors of the polynomials $x^3 - 3$ and $x^2 - 4$ in $\mathbb{Q}[x]$ and in $\mathbb{F}_5[x]$. In each case write the highest common factor in the form $(x^3 - 3)a(x) + (x^2 - 4)b(x)$ for polynomials $a(x)$ and $b(x)$.

10 Suppose the roots of $x^3 - e_1x^2 + e_2x - e_3$ are α, β, and γ. Write $1/\alpha + 1/\beta + 1/\gamma$, $\alpha^2 + \beta^2 + \gamma^2$, and $\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2$ in terms of e_1, e_2, and e_3. Find a polynomial whose roots are α^2, β^2 and γ^2.

(11) This exercise extends the construction of the fraction field of an integral domain. Parts (i)-(vii) are entirely routine, while parts (viii) and (ix) (especially (ix)) really contain the point of the construction. Part (x) is a really useful application.

A subset S of a ring A is *multiplicative* if $1 \in S$ and $s, t \in S$ whenever $s, t \in S$.

(i) Show that for any prime ideal P, the subset $A \setminus P$ is multiplicative.

(ii) Show that if $f \in A$, then the set $\{1, f, f^2, ...\}$ is multiplicative.

(iii) Define a relation $\sim$ on $S \times A$ by $(s, a) \sim (s', a')$ if there exists $s'' \in S$ with $s''(a's - as') = 0$. Show that $\sim$ is an equivalence relation. Define $S^{-1}A$ to be the quotient of $S \times A$ by this equivalence relation, and write a/s or $s^{-1}a$ for the equivalence class of (s, a). Also denote $a/1$ by a.

If $S = A \setminus P$, write A_P instead of $S^{-1}A$, and if $S = \{1, f, f^2, ...\}$ write A_f instead of $S^{-1}A$.

(iv) Show that the operations $+, -, .$ on $S^{-1}A$ defined by $(a/s) \pm (b/t) = (at \pm bs)/st$ and $(a/s).(b/t) = (ab/st)$ are indeed defined, and that with these operations $S^{-1}A$ is a ring with zero element $0/1$ and unit element $1/1$. It is called the *ring of fractions* of A with respect to S, or the *localization* of A with respect to S. We also call A_P the localization of A at P.

(v) Check that if A is a domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is exactly $Frac(A)$. Moreover, if A is a domain, then every $S^{-1}A$ is naturally a subring of $Frac(A)$.

Example: $A = k[x_1, ..., x_n]$, a polynomial ring, and $P = (x_1, ..., x_n)$. Then A_P is the ring of rational functions on k^n that are defined at (or in a neighbourhood of) the origin.

(vi) Show that the map $\phi : A \to S^{-1}A$ defined by $\phi(a) = a/1$ is a ring homomorphism, and that if $\pi : A \to R$ is any ring homomorphism such that $\pi(s)$ is a unit for all $s \in S$, then there is a unique homomorphism $\rho : S^{-1}A \to R$ such that $\rho \circ \phi = \pi$.

(vii) Suppose that I is an ideal in A, and define $S^{-1}I$ to be the subset of $S^{-1}A$ consisting of elements a/s with $a \in I$. Show that $S^{-1}I$ is an ideal in $S^{-1}A$.

(viii) Suppose that J is any ideal in $S^{-1}A$. Define $I = \{x \in A | \phi(x) \in J\}$. Show that I is an ideal in A and that $S^{-1}I = J$. Deduce that if A is

Noetherian, so is $S^{-1}A$.
(ix) Show that the constructions in (ii) and (viii) give a $1-1$ inclusion preserving correspondence between the *prime* ideals of $S^{-1}A$ and the prime ideals of A that are disjoint from S. In particular, the prime ideals of A_P correspond exactly to the prime ideals of A that are contained in P and the prime ideals of A_f correspond exactly to the prime ideals of A that do not contain f.
(x) We showed in lectures that if A is a subring of B such that B is a finitely generated A-module, then every maximal ideal of A extends to a maximal ideal of B. Prove that in fact every prime ideal P of A extends to a prime ideal of B.

12 Suppose that A is a Noetherian ring and that $f : A \to A$ is a surjective ring homomorphism. Prove that f is an isomorphism.

Generalize this to Noetherian A-modules and deduce that if M is a free A-module of rank n and $m_1, ..., m_n \in M$ generate M, then they form a basis of M.

Is the first part true for non-Noetherian rings?

(13) Consider the homomorphism $g : A := k[x, y, z] \to B := k[t]$ of polynomial rings given by $g(x) = t$, $g(y) = t^2$, $g(z) = t^3$. Show that the kernel of g is the ideal $I = (x^2 - y, xy - z)$.

(14) Suppose that A is a subring of B and B is finite over A. Suppose that P, Q are prime ideals of B with $P \subset Q$ and $P \cap A = Q \cap A$. Show that $P = Q$.

HINTS: (2) Show that multiplication by any nonzero element is an isomorphism of sets.

(6) $\alpha + 1/\alpha$.

(11) Put $S = A \setminus P$ and consider $S^{-1}A$ and $S^{-1}B$.

(12) First part: put I_n = kernel of f^n. We need to prove $I_1 = 0$. The I_n form an ascending chain, so $I_n = I_{2n}$ at some point. It's enough to prove $I_n = 0$, so we can replace f by f^n and assume that $ker(f) = ker(f^2)$. Suppose $x \in ker(f)$; since f is surjective, we have $x = f(y)$ for some y. So $0 = f(x) = f^2(y)$, so $y \in ker(f^2) = ker(f)$, which gives $f(y) = 0$.

Second part: polynomial rings in infinitely many variables.

(13) Certainly $I \subset ker(g)$. So g factors as $A \to A/I \to B$. Show that $A/I \equiv k[x]$ and then apply question 12 to $A/I \to B$.

(14) Replace $A \subset B$ by $A/(A \cap P) \subset B/P$ and then use appropriate rings of fractions to replace $A/(A \cap P)$ by its fraction field.