Groups, Rings and Modules (example sheet 4)

NIS-B, Lent 2008

(1) Suppose that A is a subring of B. Assume that B is integral over A; that is, every element x of B is is a zero of a monic polynomial in $A[X]$.
(i*) Suppose that A, B are domains and that B is integral over A. Show that B is a field if and only if A is a field.
(ii*) Deduce that if Q is a prime ideal of B, then Q is maximal in B if and only if $Q \cap A$ is maximal in A.
(iii) State and prove the Noether Normalization Lemma.
(iv) Suppose that field K is finitely generated as a ring over $\mathbb{Z}$. That is, $K = \mathbb{Z}[x_1, ..., x_n]$ for some $x_i \in K$. Show that K is finite (i.e., that K is a finite set). Deduce that if A is any ring that is finitely generated as a ring over $\mathbb{Z}$ and I is a maximal ideal of A, then A/I is finite.
(v) Suppose that G is a finitely generated subgroup of $GL_n(\mathbb{C})$, the group of invertible $n \times n$ matrices over $\mathbb{C}$. ("Finitely generated" for a group means that there exist $x_1, ..., x_n \in G$ such that every element g of G can be written as a product of positive and negative powers of the x_i.) Show that for every $g \in G$ with $g \neq 1$, there is a finite group H and a homomorphism $\phi : G \to H$ with $\phi(g) \neq 1$.

(2) Suppose that D is a regular dodecahedron.
(i*) Show that the group $Rot(D)$ of rotations of D is simple and of order 60.
(ii*) Show that $Rot(D)$ is isomorphic to the alternating group A_5 on 5 letters.

The rest of this question asks you to prove, by induction on n, that A_n is simple for all $n \geq 5$.

Suppose that H is normal in $G := A_n$, that $H \neq 1$ and that $n > 5$. Assume, as the induction hypothesis, that A_{n-1} is simple.
(iii) Put $G_i =$ the stabilizer of i in G. Show that $G_i \cong A_{n-1}$ and deduce that, for all i, $H \cap G_i = 1$ or G_i.
(iv) Show that, if $G_i \subset H$ for one value of i, then $G_i \subset H$ for all i.
(v) Assume that $G_i \subset H$ for some i. Show that H is transitive and deduce that $H = G$.

(vi) Assume that $H \cap G_i = 1$ for all i. Pick $h \in H$, $h \neq 1$, of minimal order. Write h as a product of disjoint cycles, say $h = \sigma_1 . \dots . \sigma_r$, with σ_i of length ℓ_i, say, with $\ell_1 \leq \ldots \leq \ell_r$. Show that the ℓ_i are equal, say to ℓ, that ℓ is prime and that $n = r\ell$. Derive a contradiction by considering separately the following cases: n is prime; $\ell \geq 5$ and $\ell \neq n$; $\ell = 3$; $\ell = 2$.

(3*) Suppose that p is a prime number. A p-group is a finite group whose order is a power of p. The *centre* $Z(G)$ of a group G is the set of elements $z \in G$ such that $zg = gz$ for all $g \in G$.
(i) Prove that if G is a p-group, then $Z(G) \neq 1$.
(ii) Illustrate your answer to (i) when G is the group of matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

and $a, b, c \in \mathbb{Z}/(p)$.
(iii) Suppose that G is a finite group in which $g^2 = 1$ for all $g \in G$. Prove that G is commutative. What happens if instead p is an odd prime and $g^p = 1$ for all $g \in G$?

(4) The $n \times n$ *Vandermonde matrix* is (x_i^{j-1}), where i, j run from 1 to n. Prove that its determinant is $\prod_{i>j}(x_i - x_j)$.

(5*)(i) Show that the symmetric group S_n is generated by the transpositions $(12), (23), \ldots, (n-1, n)$.
(ii) Suppose that H is a transitive subgroup of S_n that contains a transposition and that n is prime. Show that $H = S_n$. Is this true if n is not prime?

(6*) Is $x^3 + x^2 - x + 2$ irreducible in $\mathbb{Q}[x]$?

(7) Suppose that A is a Noetherian subring of B. Show that the set C of elements $x \in B$ that are integral over A is a subring of B. (It is called *the integral closure* of A in B.)

(8) A field K is algebraically closed if every polynomial $f \in K[x]$ has a zero in K (so all its zeros in K). This exercise shows that every countable field k has an algebraic closure, that is, an algebraic extension $k \subset K$ such that K is algebraically closed.
(i) Suppose that $f \in k[x]$ and that g is an irreducible factor of f. Show that $k[x]/(g)$ is an extension of k in which f has a zero. Deduce that there is a finite extension of k in which f factors into linear terms ("f splits completely").

(ii) Show that if Ω is an algebraic extension of k and every $f \in k[x]$ has a zero in Ω, then Ω is algebraically closed.
(iii) Show that $k[x]$ is countable.
(iv) Suppose that $f_1, f_2, ...$ are the elements of $k[x]$. Define fields $E_0 \subset E_1 \subset ...$ inductively as follows: $E_0 = k$ and E_{i+1} is a finite extension of E_i in which f_i splits completely. Show that $\bigcup_i E_i$ is an algebraic closure of k.

There are uncountable fields in real life, e.g., $\mathbb{R}$, the field $\mathbb{Q}_p$ of p-adic numbers (the fraction field of the ring $\mathbb{Z}_p$ of p-adic integers), the field $k_0((t))$ of formal Laurent series in a variable t over a field k_0 (the fraction field of the ring $k_0[[t]]$ of formal power series in a variable t over k_0), which motivates the next exercise.

(9) Here we show, via an explicit use of Zorn's lemma, that every field k has an algebraic closure.

Take a set x_f of indeterminates, one for each non-constant monic $f \in k[x]$. In the infinite polynomial ring $A = k[\{x_f | f \in k[x]\}]$, consider the ideal I generated by the elements $f(x_f)$.
(i) Show that $I \neq A$.
(ii) Show that there is a maximal ideal M containing I and that $\Omega = A/M$ is an algebraic closure of k.

(10*) (i) Show that the subset V of S_4 defined by

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

is a subgroup of A_4 and that A_4 is not simple.
(ii) Describe V in terms of modules.
(iii) Write the product (123)(12345) as a product of disjoint cycles.

(11*)(i) State the Sylow theorems.
(ii) Suppose that p, q, r are distinct prime numbers. Show that no group of order pqr is simple.

HINTS: (1)(iv) Suppose first that K has characteristic 0. Then $\mathbb{Z} \subset \mathbb{Q} \subset K = \mathbb{Z}[x_1, ..., x_n] = \mathbb{Q}[x_1, ..., x_n]$, so by NNL there is a polynomial subring $\mathbb{Q}[t_1, ..., t_r]$ of K with K f.g. as a module over $\mathbb{Q}[t_1, ..., t_r]$. Then, by (i*), $\mathbb{Q}[t_1, ..., t_r]$ is a field, so $r = 0$. So K is algebraic over $\mathbb{Q}$, so for each i there is a non-zero $a_i \in \mathbb{Z}$ with $a_i x_i$ integral over $\mathbb{Z}$. Then K is finitely generated as a module over $\mathbb{Z}[1/a]$, with $a = \prod a_i$. So $\mathbb{Z}[1/a]$ is a field; derive a contradiction to this.

So K has characteristic $p > 0$, and is then f.g. as a ring over $\mathbb{F}_p$. The same argument shows that K is algebraic over $\mathbb{F}_p$, so finite.

(1)(v) Pick a finite set of generators g_i of G; these are matrices over $\mathbb{C}$. So there is a subring $A = \mathbb{Z}[x_1, ..., x_n]$ generated by the entries of all the g_i. Now $G \subset GL_n(A)$.

Suppose $1 \neq g \in G$. Either g has an off-diagonal entry $f \neq 0$ or it has a diagonal entry $f + 1 \neq 1$. Put $A[1/f] = R$ and regard G as a subgroup of $GL_n(R)$. Take any maximal ideal I of R and take $H = GL_n(R/I)$; note that R/I is finite, by (iv).

(3)(i) Consider the action of G by conjugation on $Z(G)$ and use the orbit-stabilizer theorem.

(ii) $Z(G)$ is the subgroup where $a = c = 0$.

(iii) Consider G as in (ii). Show that if

$$h = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

then

$$h^n = \begin{pmatrix} 1 & na & n(n-1)ac/2 \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}.$$

(4) Regard this as an identity in the polynomial ring $A = \mathbb{Z}[x_1, ..., x_n]$. Consider what happens if two of the variables are set equal to each other and exploit the fact that A is a UFD.

(5)(i) We know that S_n is generated by transpositions, so we need only show that (ij) lies in the subgroup generated by the given elements. Check that if $i \leq j - 2$, then $(i, i+1)(ij)(i, i+1) = (i+1, j)$.

(ii) Transitivity plus the orbit-stabilizer theorem shows that n divides the order of H. Cauchy's theorem, or Sylow's theorem, shows that H has an element σ of order p; it must be an n-cycle. Put $\sigma = (12...n)$ and $\tau = (ij)$, with $i < j$. Then $\sigma^{j-i}\tau\sigma^{i-j} = (jk)$ with $k - j = j - i$, modulo n. So we get a sequence $(ij), (jk), (kl), ...$ that can be used instead of $(12), (23), (34), ...$ to generate S_n.

Take $n = 4$ and consider the dihedral subgroup D_8 of S_4.

(7) Suppose $x, y \in C$. Each of $x \pm y, xy$ lies in $A[x, y]$.

(8)(ii) Let $f = \sum_0^n a_i x^i \in \Omega[x]$. There is a finite extension $\Omega \subset \Omega'$ such that f has a zero $\alpha \in \Omega'$. Consider the extensions

$$k \subset k[a_0, ..., a_n] \subset k[a_0, ..., a_n, \alpha].$$

These are algebraic, so finite. So α lies in a finite extension of k and so is a zero of a polynomial $g \in k[x]$. By assumption, all the zeros of g lie in Ω.

(9)(i) If $1 \in I$, then there are finitely many $f_1, ..., f_n \in k[x]$ and an equation

$$1 = g_1 f_1(x_{f_1}) + ... + g_n f_n(x_{f_n}),$$

with $g_i \in A$.

There is a finite extension K of k in which every f_i has a zero, say a_i. Then there is a ring homomorphism $\pi : A \to K$ with $\pi(x_{f_i}) = a_i$ and $\pi(x_f) = 0$ if $f \neq f_1, ..., f_n$. Then $\pi(f_i(x_{f_i})) = 0$, so that in K we have $1 = 0$. This contradiction shows that $1 \in I$.
(ii) M exists, by Zorn's lemma (see previous examples sheet). Ω contains k and every non-constant polynomial in $k[x]$ has a zro in Ω.