ALGEBRA FINAL

JAMES CUMMINGS (JCUMMING@ANDREW.CMU.EDU)

Attempt *exactly three questions* from each of the sections “Groups”, “Rings and modules” and “Fields”. You may not collaborate but may use any printed or online source (please give a reference or link), This final is due at 23:59:59 on Sun Dec 18.

Groups

G1 Prove that the group of invertible upper triangular 2×2 matrices with real entries is solvable. Is it nilpotent?

G2 Let G be a finite group, let $H \lhd G$ and let P be a Sylow p-subgroup of H. Prove that $G = HN_G(P)$. Hint: given a group element g, what can you say about P^g?

G3 Let G be a finite group, let p be prime and let $H \leq G$ be a *p-subgroup* (that is a subgroup whose order is a power of p).

Prove that

$$[G : H] \equiv [N_G(H) : H] \mod p.$$

G4 Let the finite group G act on the finite set X. Denote the stabiliser of $x \in X$ by G_x, the orbit of x by O_x, and the set $\{x \in X : g \cdot x = x\}$ by $Fix(g)$.

(a) Prove that $\sum_{g \in G} |Fix(g)| = \sum_{x \in X} |G_x|$.

(b) Prove that the number of orbits is

$$\frac{\sum_{g \in G} |Fix(g)|}{|G|}.$$

G5 Show that in a group of order 48, the intersection of two distinct Sylow 2-subgroups has order 8. Classify all the groups of order 75.

G6 Let G be a finite group, p a prime dividing the order of G and P a Sylow p-subgroup of G. Let x and y be elements of $Z(P)$ which are conjugate in G. Show that x and y are conjugate in $N_G(P)$.

Rings and modules

R1 Let k be a field and let R be the PID $k[x]$, so that every R-module may be regarded as a vector space over k; prove that if M is a cyclic R-module then either $dim_k(M)$ is finite or $M \simeq R$ as an R-module.

R2 Let R be a ring and let M be an R-module. Define $M[x]$ to be the set of polynomials with coefficients in M, and make $M[x]$ into an $R[x]$-module in the obvious way. Prove that if M is a Noetherian R-module then $M[x]$ is a Noetherian $R[x]$-module.

R3 Let N be an R-module. A submodule $M \leq N$ is *maximal* iff $M < N$ and there are no strictly intermediate modules.

Fill in the details of the following sketchy proof that if N is a nonzero fg R-module then it has a maximal submodule.

(a) If $I \neq R$ is an ideal of R, then R/I (considered as an R-module) has a maximal submodule.
(b) If N is a nonzero cyclic R-module, then N has a maximal submodule.
(c) If $n_1, \ldots n_k$ is a generating set of minimal size k for the nonzero fg R-module N, and $N' = Rn_2 + \ldots Rn_k$, then $N' < N$ and N/N' is cyclic.
(d) Every fg nonzero R-module has a maximal submodule.

R4 Let R be a ring and let $Spec(R)$ be the set of prime ideals of R. For each ring element a, let $O_a = \{P \in Spec(R) : a \notin P\}$. Say that a set X of prime ideals is *open* if for every $P \in X$ there exists a such that $P \in O_a \subseteq X$.

(a) Prove that $O_a \cap O_b = O_{ab}$, $O_0 = \emptyset$, $O_1 = Spec(R)$.
(b) Prove that the collection of open sets form a topology for $Spec(R)$, and describe it when $R = \mathbb{Z}$.
(c) Prove that for any R this topology is compact.

R5 Let p be prime. Let $R_n = \mathbb{Z}/p^n\mathbb{Z}$, and let $\pi_n : R_{n+1} \mapsto R_n$ be the surjective HM which maps $a + p^{n+1}\mathbb{Z}$ to $a + p^n\mathbb{Z}$. Define a ring $\mathbb{Z}_p$ as follows: the elements are infinite sequences $(r_0, r_1, \ldots)$ such that $r_i \in R_i$ and $\pi_i(r_{i+1}) = r_i$ for all i. Addition are multiplication are defined coordinatewise

Prove that

(a) $\mathbb{Z}_p$ is uncountable.
(b) $\mathbb{Z}_p$ is an ID which contains an isomorphic copy of $\mathbb{Z}$.
(c) The sequence $(2, 2, 2, \ldots)$ has a square root in $\mathbb{Z}_7$.

R6 Let R be a ring. The *formal power series ring* $R[[x]]$ consists of infinite expressions $a_0 + a_1x + a_2x^2 + \ldots$ with the natural operations. Prove that if R is Noetherian then $R[[x]]$ is Noetherian.

Fields

F1 Let F be the unique subfield of $\mathbb{C}$ which is a splitting field for $x^4 - 2$ over $\mathbb{Q}$. Find $[F : \mathbb{Q}]$. Describe the Galois group of F over $\mathbb{Q}$. Find all the fields which are intermediate between $\mathbb{Q}$ and F,and identify the intermediate fields which are Gakois extensions of $\mathbb{Q}$.

F2 Let p be an odd prime and let $\zeta = e^{2\pi i/p}$, $\alpha = \zeta + \zeta^{-1}$. Show that $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$ and find its degree over $\mathbb{Q}$. For $p = 7$ find the minimal polynomial of α over $\mathbb{Q}$.

F3 Let F be a subfield of $\mathbb{C}$ with $[F : \mathbb{Q}]$ finite. Prove that F contains only finitely many roots of unity (recall that a root of unity is a complex number ζ such that $\zeta^n = 1$ for some $n > 0$).

F4 An *ordered field* is a field F together with a set $P \subseteq F$ of elements such that (defining $-P = \{-a : a \in P\}$)

(a) P is closed under $+$ and $\times$
(b) $P \cap -P = \{0\}$.
(c) $P \cup -P = F$.

Intuitively, you can think of P as the set of field elements which have been designated as non-negative.

Prove that

(a) There is a unique set $P \subseteq \mathbb{R}$ such that $(\mathbb{R}, P)$ is an ordered field.
(b) There is no set $P \subseteq \mathbb{C}$ such that $(\mathbb{C}, P)$ is an ordered field.
(c) There are at least two sets $P \subseteq \mathbb{Q}(\sqrt{2})$ such that $(\mathbb{Q}(\sqrt{2}), P)$ is an ordered field.
(d) If (F, P) is an ordered field then F has characteristic zero and -1 is not a sum of squares in F.

F5 Let $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ be such that $[F : \mathbb{Q}] < \infty$ and F is a Galois extension of $\mathbb{Q}$. Prove that either $F = F \cap \mathbb{R}$ or $[F : F \cap \mathbb{R}] = 2$. What if we drop the assumption that F is a Galois extension of $\mathbb{Q}$?

F6 Let $\alpha = \sqrt[3]{2}$ and let $\gamma = i\sqrt{\alpha - 1}$.

(a) Prove that $E = \mathbb{Q}(\gamma)$ is a radical extension of $\mathbb{Q}$.
(b) Find the least subfield F of $\mathbb{C}$ such that F contains E and F is a Galois extension of $\mathbb{Q}$.