ALGEBRA QUALIFYING EXAM, AUGUST 2018

Draft 08/13

1.

(a) Give an example of a ring R and a short exact sequence of R-modules $0 \to A \to B \to C \to 0$ that is not split exact.
(b) Give an example of a flat $\mathbb{Z}$-module that is not free.
(c) Describe all zero-divisors and all units in $\mathbb{Q}[x]/(x^2-1)$.

2. For a finite group G, denote by $s(G)$ the number of its subgroups.

(a) Show that $s(G)$ is finite.
(b) Show that if H is a nontrivial normal subgroup of G, then $s(G/H) < s(G)$.
(c) Show that $s(G) = 2$ if and only if G is cyclic of prime order.
(d) Show that $s(G) = 3$ if and only if G is a cyclic group whose order is a square of a prime.

3. Denote by $M_n(\mathbb{R})$ the ring of all $n \times n$ matrices over $\mathbb{R}$.

(a) Show that for any $A \in M_n(\mathbb{R})$, there exists $B \in M_n(\mathbb{R})$ such that $AB = 0$ and $\mathrm{rk}(A) + \mathrm{rk}(B) = n$.
(b) Prove or disprove that for any $A \in M_n(\mathbb{R})$, there exists $B \in M_n(\mathbb{R})$ such that $AB = BA = 0$ and $\mathrm{rk}(A) + \mathrm{rk}(B) = n$.

4.

(a) Give an example of a field extension $K/\mathbb{Q}$ whose Galois group is $\mathbb{Z}/4\mathbb{Z}$, and prove that it is such an example.
(b) Let K be the field $\mathbb{F}_q(t)$ and let $L = \mathbb{F}_q(t^{1/p})$. The extension L/K is inseparable, thus not Galois. Explain why there are no nontrivial field automorphisms of L fixing K.

5. Let A be a two-dimensional (unital) algebra over a field F. This means that A is an associative, but not necessarily commutative, ring with a unit that contains F as a subring such that the elements of F commute with all alements of A (that is, F is in the center) and A is two-dimensional as a vector space over F.

(a) Show that A must in fact be commutative.
(b) Show that if F is algebraically closed, then either $A \simeq F \times F$ or $A \simeq F[x]/(x^2)$.
(c) Suppose $F = \mathbb{R}$. List (with a proof) all possibilities for A, up to isomorphism.

Solutions

1. (a) Many different examples: for instance, the sequence $0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ of $\mathbb{Z}$-modules.

(b) $\mathbb{Q}$.

(c) Zero divisors are (nonzero) multiples of $x-1$ or of $x+1$. All other non-zero elements are units.

2. (a) Clearly, $s(G)$ is less than the number of all subsets of G, which is finite.

(b) Recall that there is a bijection between subgroups of G/H and subgroups of G containing H. Since G has at least one subgroup that does not contain H (namely, $\{e\}$) we get the desired inequality.

(c) Clearly, $G \neq \{e\}$ (otherwise $s(G)=1$). Hence, the only subgroups of G are $\{e\}$ and G. Take any $a \in G-\{e\}$. The cyclic subgroup generated by a must coincide with G, therefore, G is cyclic; that is, $G \simeq \mathbb{Z}/n\mathbb{Z}$ for some n. Recall that $\mathbb{Z}/n\mathbb{Z}$ has one subgroup of order m for every divisor m of n, so that $s(\mathbb{Z}/n\mathbb{Z}) = \sigma_0(n)$ (the number of divisors of n). We need $\sigma_0(n)=2$, which is equivalent to n being prime.

(d) Now, G must have one more subgroup $H \subset G$, in addition to G and $\{e\}$. Then any $x \in G-H$ generates G, and we again have $G \simeq \mathbb{Z}/n\mathbb{Z}$. Now $\sigma_0(n)=3$, which is equivalent to n being a square of a prime number.

3. Let us prove (b); obviously, (a) is a special case. Let us view matrices as linear maps from $\mathbb{R}^n$ to itself. Then the condition $AB=BA=0$ is equivalent to requiring that $B|_{\operatorname{im}(A)}=0$ and $\operatorname{im}(B) \subset \ker(A)$. So take B to be any isomorphism $\mathbb{R}^n/\operatorname{im}(A) \simeq \ker(A)$ (or rather the composition of such an isomorphism with the natural projection $\mathbb{R}^n \to \mathbb{R}^n/\operatorname{im}(A)$). Such an isomorphism exists because both spaces have dimension equal to $n-\operatorname{rk}(A)$.

4. (a) Let $\zeta = \exp(\frac{2\pi i}{5})$ be the primitive fifth root of unity. It is the root of the cyclotomic polynomial $\frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$, which is irreducible (as can be seen by applying the Eisenstein Criterion after the variable change $t=x-1$). The other roots of this polynomial are ζ^2, ζ^3, and ζ^4, which all belong to $L := \mathbb{Q}(\zeta)$. Therefore, $L/\mathbb{Q}$ is a Galois extension. Its Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$.

(b) We have $L = K(t^{1/p})$, so it suffices to show that any automorphism that fixes K must fix $\alpha := t^{1/p}$. Indeed, α is a root of the polynomial $x^p - t$ over K. Since over L, we have $(x^p-t) = (x-\alpha)^p$, α is the only root of this polynomial (of multiplicity p). Since an automorphism that fixes K must send α to a root of this polynomial, we get the required statement.

5. (a) Take any $x \in A - F$. Since $\{1, x\}$ are linearly independent, they form an F-basis of A. Therefore, it remains to notice that

$$(a+bx)(c+dx) = ac+bcx+adx+bdx^2 = (c+dx)(a+bx) \qquad \text{for all } a,b,c,d \in F.$$

(b) Let x be as before. Since x^2 is a linear combination of $\{1,x\}$, x must satisfy an equation $x^2+ax+b=0$. The map

$$F[x]/(x^2+ax+b) \to A$$

is surjective; since it is a linear map between vector spaces ofthe same dimension, it must be an isomorphism. Thus, $A \simeq F[x]/(x^2+ax+b)$.

Replacing x with $x+(a/2)$, we may assume that the equation on x is of the form $x^2+b=0$. If $b \neq 0$, we may replace x with $x/\sqrt{-b}$, and reduce to one of the two cases: either $b = 0$, and $A \simeq F[x]/(x^2)$, or $b = -1$ and

$$A \simeq F[x]/(x^2 - 1) \simeq F[x]/(x - 1) \times F[x]/(x + 1) \simeq F \times F.$$

(The last line used the Chinese Remainder Theorem, but of course it is not hard to check directly.)

(c) We can argue as in part (b), but now the case $b \neq 0$ splits into two cases: $b > 0$ and $b < 0$. In either situation, we may replace x with $x/\sqrt{|b|}$, giving three possibilities: $b = 0$, $b = -1$, and $b = 1$. As in part (b), the first two possibilities lead to $\mathbb{R}[x]/(x^2)$ and $\mathbb{R} \times \mathbb{R}$, while the third gives $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$. It is clear that these three algebras are non-isomorphic: $\mathbb{C}$ is a field, $\mathbb{R} \times \mathbb{R}$ has zero divisors, but no non-trivial nilpotents, while $\mathbb{R}[x]/(x^2)$ has nilpotents.