Algebra Qualifying exams

Daniel Montealegre

November 7, 2013

Spring 13. 1(a) Let $n \geq 1$. Give an example of a field extension L/K with $Gal(L/K) = \mathbb{Z}_n$

Proof. We claim that $L = \mathbb{F}_{p^n}$ and $K = \mathbb{F}_p$ will work. First we show that the extension L/K is of degree n. First of all note that any element in L is a solution of $x^{p^n} - x$ (by Lagrange's theorem) and moreover, note that we have a complete set of solutions. Hence, L is a splitting field of a polynomial over K of degree n, so $[L : K] = n$. Hence, we have that $|Gal(L/K)| = n$. Now we will show that it is cyclic. Define φ to be the map $a \mapsto a^p$. Over a field of characteristic p, we have that this function is a homomorphism $(a + b)^p = a^p + b^p$ (as all the middle terms will vanish in the binomial expansion), and since field homomorphisms are injective, we have an injection of a finite set into itself, so it has to be an automorphism, i.e., $\varphi \in G(L/K)$. It suffices to show that φ has order n. Assume for sake of contradiction that there is a $m < n$ such that $\varphi^m = id$. Then let α be a primitive root of L, we have $\varphi^m(\alpha) = \alpha^{p^m} = id(\alpha) = \alpha$, but this is a contradiction with the fact that α is a primitive element of L, hence, $m \geq n$, and we get our desired result. □

Spring 13.1(b) Give an example of a field extension L/K with galois group A_n.

Proof. □

Spring 13.2 Let $A = \mathbb{C}[x, y]$ be the polynomial ring in two variables. Consider three ideals in A : $(x), (x, y^2), (xy)$. Which of these are prime? Why?

Proof. (x) is prime since $A/(x) = \mathbb{C}[y]$ which is a domain. (x, y^2) is not since $A/(x, y^2) = \mathbb{C}[y]/(y^2)$ but here $y \cdot y = 0$, so we don't have a domain. Lastly, (xy) is not a domain since $x \cdot y \in (xy)$, but $x \notin (xy)$ (if we have $x \in (xy)$ then we would have an element $a \in A$ such that $a(xy) = x$, but note that y is an irreducible appearing in the right hand side, but not in the left hand side, as A is a UFD we get a contradiction), similarly $y \notin (xy)$, and we get the result. □

Spring 13. 3 Let A be the quotient of $\mathbb{C}[a, b, c, d]$ by the ideal generated by $(ad - bc)$. Is A a UFD? Why?

Proof. No. We have $ab = cd$ are distinct factorizations into irreducibles of the same element. The reason why a is irreducible in the quotient ring is... □

Spring 13. 4 Give an example of a commutative ring A and two non-zero A-modules M and N such that

$$M \otimes_A N = 0$$

Explain why this is indeed so.

Proof. Let $A = \mathbb{Z}$ and $M = \mathbb{Z}_2$ and $N = \mathbb{Z}_3$. Then we have $a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$. □

Spring 13.5 Give an example of a ring A and a left A-module which is projective but not free. Prove your statements.

Proof. Consider the $\mathbb{Z}_2$ as a $\mathbb{Z}_6$-module. We have that $\mathbb{Z}_2$ is a projective $\mathbb{Z}_6$ module because $\mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$, so indeed $\mathbb{Z}_2$ is the summand of a free $\mathbb{Z}_6$ module. Note however that it cannot be free since any non-zero free module over $\mathbb{Z}_6$ must have at least 6 elements, but $\mathbb{Z}_2$ only has two. □

Winter 11. 1 Which of the following isomorphisms of abelian groups are possible? Justify your answer.

Proof. $\mathbb{Z}/2 \oplus \mathbb{Z}/2 \cong \mathbb{Z}/4$: not possible. Just note that all the elements on the left hand side have order at most 2, and 1 on the right hand side has order 4.

$\mathbb{Z}/2 \oplus \mathbb{Z}/3 \cong \mathbb{Z}/6$: Just note that $(1,1)$ is a generator for the LHS and it is of order 6.

$\mathbb{Z}/2 \oplus \mathbb{Z}/4 \cong \mathbb{Z}/8$: Not possible. Just note that the left hand side has orders bounded by 4 whereas the right hand side has an element of order 8.

□

Winter 11. 2 Let k be a field, V a finite dimesional vecotr space over k and $A : V \longrightarrow V$ a linear operator. Which of the above statements are true theorems and which are not? Justify your answers:

Proof. $\dim \ker(A) = \dim \mathrm{Im}(A)$: No. Consider the 0 map.

$\dim \ker(A) = \mathrm{codim}\, \mathrm{Im}(A)$: By the rank nullity theorem we have $\dim(V) = \dim \mathrm{Im}(A) + \dim \ker(A)$, and substracting $\dim \mathrm{Im}(A)$ both sides gives the result.

$\mathrm{codim} \ker(A) = \dim \mathrm{Im}(A)$. Again, this is immediate by the Rank and Nullity Theorem.

For sake of completeness I include a statement and proof of the theorem:

Theorem 1. ***Rank and Nullity*** *Using the assumptions of the problem, we always have:* $\dim V = \dim \ker(A) + \dim Im(A)$.

Proof. Let V be n-dimensional. Let $\ker(A)$ be t-dimensional and have basis $v_1, ..., v_t$. Now let $\mathrm{Im}(A)$ be s-dimensional with basis $a_1, .., a_s$. Since they are in the image of A, there exists b_i such that $b_i \mapsto a_i$. I claim $B = \{v_1, ..., v_t, b_1, ..., b_s\}$ is a basis for V, and hence the result would follow. First of all it is a spanning set: Let $v \in V$. Then consider

$A(v) \in \mathrm{Im}(A)$, so we have that $A(v) = c_1a_1 + ... + c_sa_s$. Then the element $v - c_1b_1 + ... + c_nb_n$ is in the kernel of A, so we have that $v - c_1b_1 ... - c_sb_s = d_1v_1 + ... + d_tv_t$, so indeed v is in the span of B. To see that B is linearly independent, consider $c_1v_1 + ... + c_tv_t + d_1b_1 + .. + d_sb_s = 0$. Apply A, and obtain: $d_1a_1 + .. + d_sa_s = 0$, but by choice, $\{a_i\}$ where a basis for the image, so $d_i = 0$. Hence, $c_1v_1 + ... + c_tv_t = 0$ and by choice $\{v_i\}$ is a basis for $\ker(A)$ so $c_i = 0$, and we get the linear independence, and we get that $t + s = n$, just as we wanted to prove.

□

□

Winter 11. 3 Let k be a field. Give an example of a projective left module over the matrix algebra $\mathrm{Mat}_n(k)$ which is not free. Explain why it is projective and why not free.

Proof. □

Winter 11. 4 Let $\mathbb{F}_q$ be a finite field with q elements. Prove that there exists a non-constant polynomial with no roots in $\mathbb{F}_q$

Proof. Consider $f(x) = x^q - x + 1$. Any element $\alpha \in \mathbb{F}_q$ satisfies $\alpha^{q-1} = 1$ by Lagrange's theorem. Then $\alpha^q = \alpha$, so $f(\alpha) = 1$ for all $\alpha \in \mathbb{F}_q$ and we see that f has no roots in $\mathbb{F}_q$. □

Winter 11. 5 Let p be a prime number. Prove that the group formed by matrices of the form $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, $a \in \mathbb{F}_p$, is a Sylow p-subgroup of the finite group $GL_2(\mathbb{F}_p)$.

Proof. First we determine the order of the group $G = GL_2(\mathbb{F}_p)$. There are $p^2 - 1$ ways of choosing the first row vector to be non-zero. Next there are $p^2 - p$ ways of choosing the next row to be linearly independent of the first one. Hence, there are a total of $(p^2 - 1)(p^2 - p) = (p - 1)^2(p + 1)p$ different elements in G. Hence, we are done since it is clear that the matrices of the form $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, $a \in \mathbb{F}_p$ form a subgroup of order p, which is the highest power of p dividing $|G|$.

□

Winter 11. 6 Can $\mathbb{F}_9$ be embedded into $\mathbb{F}_{27}$? Can $\mathbb{F}_4$ be embedded into $\mathbb{F}_{16}$? Justify your answer in each case.

Both results will follow from the following theorem:

Theorem 2. *$\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m}$ if and only if $n \mid m$.*

Proof. We know that $G = G(\mathbb{F}_{p^m}/\mathbb{F}_p)$ is cyclic of order m. Assume that $n \mid m$. Then by the cyclic group theorem, we have a subgroup H of G such that H has order n. By Galois correspondance, there exists a field extension L of $\mathbb{F}_p$, contained in $\mathbb{F}_{p^m}$, such that $[L : \mathbb{F}_p] = n$, but since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ we have by uniqueness of finite fields that $L = \mathbb{F}_{p^n}$.

Conversely, assume that $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m}$ then we have that $[\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p]$ and from here we see that $n \mid m$.

□

Winter 11. 7 Which of the following rings are local and which are not? Justify your answer in each case.

Proof. $\mathbb{Z}$: It is not local since it has more than one maximal ideal, namely any ideal of the form (p) for p a prime.

$\mathbb{Z}[1/5]$: Not local. We claim that (2) and (3) are still maximal ideals. To see this assume that there is an M properly containing (2). Then it has an element of the form $x/5^i$ for some x odd. That means that $(x-1)/5^i$ is in (2) as $x-1$ is even. Thus, M contains their difference $1/5^i$, but this is a unit, so $M = \mathbb{Z}[1/5]$. To show that (3) is maximal, again say M properly contains it. Then there is an element in M of the form $x/5^i$. Here we have two cases x is congruent to 1 or congruent to 2 modulo 3. If the latter case happens, then $x/5^i + x/5^i = 2x/5^i$, so we can assume wlog that x is congruent to 1 modulo 3. Thus, M contains $(x/5^i) - (x-1)/5^i = 1/5^i$, so again we have that M contains a unit.

□

Jan 11. 1 Prove that $\mathbb{Q}$ is an indecomposable $\mathbb{Z}$-module. What can you say about $\mathbb{Q}/\mathbb{Z}$?

Proof. Assume that it is decomposable. Then write $\mathbb{Q} = R \oplus P$ with P, R non zero $\mathbb{Z}$-modules. Then let $a/b \in P$ be non-zero and $c/d \in R$ be non-zero. Then $(cb)(a/b) = (ad)(c/d)$ would be an element in both P and R, which is a contradiction.

□

Jan 11. 2 What is the group of automorphisms of $\mathbb{R}$ over $\mathbb{Q}$?

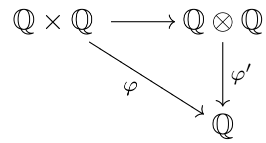
Proof. We claim that the only such automorphism is the identity. Let $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ be an automorphism which fixes $\mathbb{Q}$. First of all we claim that if $x > 0$ then $\varphi(x) > 0$: To see this, if $x > 0$ then $x = \epsilon^2$, so $\varphi(x) = \varphi(\epsilon)^2 \geq 0$, note that $\varphi(\epsilon) \neq 0$ since it is an automorphism and we already have $0 \mapsto 0$. Hence, $\varphi(x) > 0$, just as we wanted. Secondly, we claim that φ is order preserving, i.e., if $a < b$ then $\varphi(a) < \varphi(b)$. To see this, just note that $b - a > 0$ so $\varphi(b-a) > 0$ so $\varphi(b) - \varphi(a) > 0$. Now to finish the problem we want to show that $\varphi(r) = r$ for all $r \in \mathbb{R}$. Consider a sequence $\{q_i\}$ which is increasing whose limit is r and such that $q_i \in \mathbb{Q}$. Then we have that $r = \sup\{q_i\} = \sup\{\varphi(q_i)\}$ and since $\varphi(r) > \varphi(q_i)$, we have that $\varphi(r)$ is an upper bound of $\{\varphi(q_i)\}$ so $\varphi(r) \geq r$. Doing the same with decreasing sequences and infimums we get that $\varphi \leq r$, so we obtain $\varphi(r) = r$. □

Jan 11. 3 Let R be a left Artinian ring and let M be a nonzero left R module. Prove that M has at least one maximal submodule.

Jan 11.4 Let K be an infinite field and let n be a natural number greater than 1. Prove that the set of maximal left ideals of $M_n(K)$ is infinite.

Jan 11.5 Prove that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

Proof. Consider the following diagram



where above we have that $\varphi(a,b) = ab$. We need to show that φ' is a bijection. Note that any element in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ can be written uniquely in the for $x \otimes 1$ because if we had $(a/b) \otimes (c/d) = (ac/b) \otimes (1/d) = (acd)/(bd) \otimes (1/d) = (ac)/(bd) \otimes 1$. This implies that the map is an injection since if we have two elements in $\mathbb{Q} \otimes \mathbb{Q}$ we can write them as $x \otimes 1$ and $y \otimes 1$. This elements have preimages $(1, x)$ and $(1, y)$ (this are not unique but it doesn't matter) in $\mathbb{Q} \times \mathbb{Q}$. Under φ they map to x and y, and under φ' they should map to the same. So $x \otimes 1$ and $y \otimes 1$ map to x and y, and this gives injectivity. Surjectivity is immediate, so indeed we get our desired isomorphism. □

Jan 11.6 What is the transcendence degree of $\mathbb{C}$ over $\mathbb{Q}$.

Proof. Choose a transcendence basis $X = \{x_i\}_{i \in I}$ for $\mathbb{C}$ over $\mathbb{Q}$. Then $\mathbb{C}$ is an algebraic extension of $\mathbb{Q}(X)$. Now here are two rather straightforward facts:

1: If F is any infinite field and K/F is an algebraic extension, then $\#K = \#F$.

2: For any infinite field F and purely transcendental extension $F(X)$, we have $\#F(X) = \max(\#F, \#X)$.

Putting these together we find

$\mathfrak{c} = \#\mathbb{C} = \#\mathbb{Q}(X) = \max(\aleph_0, \#X)$.

Since $\mathfrak{c} > \aleph_0$, we conclude $\mathfrak{c} = \#X$. □

Jan 11.7 Let K be a field and G be a group. Find the least dimension of a simple KG-module.

Jan 11.8 Let R be a commutative local ring. Describe the group of units of R.

Proof. Let M be the unique maximal ideal. I claim that $R^\times = R \backslash M$. If $x \notin R^\times$ then x is not a unit, so (x) is a proper ideal of R. In particular it is contained in a maximal ideal of R, but there is only one such maximal ideal. Hence, we must have $(x) \subset M$, so that means that if $x \notin M$ then x is a unit (by contrapositive). The other direction is easier. If x is a unit, then $x \notin M$ since otherwise M would not be proper. □

Jan 11.9 Let H be an infinite dimensional Hilbert space. Prove the existence of an unbounded linear operator from H to H.

Proof. Let $\{x_i\}_{i \in I}$ be a basis for our Hilbert space with $|x_i| = 1$. Say $\{y_1, y_2, ...\}$ is a countable-infinite subset of $\{x_i\}$. Define $T : y_i \mapsto iy_i$ and fix all the other basis vectors. Then we have that $|T| = \sup_{|x|=1}\{|Tx|\}$ is unbounded as $|Ty_i| = i$. □

Jan 11.10 Let A be a set and B be a proper subset (non-empty). Prove the existence of a function $f : A \longrightarrow A$ such that $f \circ f = f$ and image of f is B.

Proof. Let $f : A \longrightarrow A$ be defined by $f(b) = b$ if $b \in B$ and pick any $b \in B$ and fix it. Then define $f(a) = b$ for all $a \in A \backslash B$. Then we have that the image of f is obviously B, and $f^2 = f$ since for $b \in B$ this is obvious, and for $a \notin B$ we have $f(a) = b$ and $f(f(a)) = f(b) = b$. □

Spring 00. 1 Let T be a linear transformation of a vector space over a field F. Assume that $T^m = I$ for some positive integer m.
a): Assume that F has 0 characteristic. Show that T is diagonalizable.
b): Assume that $\text{char}(F) = p$. Give an example to show that T needs not be diagonalizable.

Proof. a): Let $f(x) = x^m - 1$. Then we have that T satisfies f, and we also have that f is separable since the gcd of f and f' is 1 (here we use the fact that $f' = mx^{m-1}$ is not zero, which we can only assert in zero-characteristic). Since f is separable we have that the minimal polynomial of T is separable, which is a sufficient condition for T to be diagonalizable.

b): Over $\mathbb{F}_2$, consider the identity matrix plus the matrix that has 1 in the $(1, 2)$ entry and 0 elsewhere. This matrix is in Jordan form, so it is not diagonalizable, and it satisfies the polynomial $x^2 - 1$ □