Algebra Qualifying Exam, Fall 2001

Assume all rings have identity elements and all modules are unital.

Section 1: State the theorems below, defining relevant terms.

i. Hilbert's Nullstellensatz.
ii. The fundamental theorem of Galois theory.
iii. The Noether-Skolem theorem.

Section 2: True/False. If FALSE, provide a counterexample, if TRUE, give a brief justification.

a. If $|G| = n$, $m|n$ then there is a subgroup H of G of order m.
b. If $f : M \to M'$, $g : N \to N'$ are surjective maps of right and left R-modules respectively, then so is $f \otimes_R g$.
c. Any torsion free module over a PID is free.
d. If $\mathbf{F}$ is a field of characteristic p, $\mathbf{F}$ contains exactly one p^kth root of 1.
e. If R is a P.I.D. then R is Noetherian.
f. If $R \subseteq S$ are commutative rings with identity, and $s_1, s_2 \in S$ are integral over R, so is $s_1 + s_2$.

Section 3: Give complete proofs for 4 problems from the following.

(1) Define *solvable* and show that any group of order p^2q is solvable for p, q distinct primes.
(2) Let M be a left R-module which is the sum of its simple submodules. Show that any quotient or submodule of M has the same property.
(3) (a) If an $n \times n$ matrix A satisifies $A^r = 0$ for some r, then A is similar to a matrix with entries all 0 except for some 1s on the diagonal below the main diagonal.
    (b) If the field is algebraically closed and characteristic 0 and $A^r = 1$ for some r, show that A is diagonalizable. What if the field is of positive characteristic?
(4) Let S be a multiplicatively closed subset of a commutative ring R.
    (a) Define $S^{-1}R$ and describe its ring structure.
    (b) If $\mathfrak{m}$ is a prime ideal of R and $S = R - \mathfrak{m}$ show S is multiplicatively closed and $S^{-1}R$ is a local ring.
(5) Suppose $f : R \to S$ is a unital surjection of rings. Let A, B be right and left S-modules respectively. Describe how to give A, B right and left R-modules structures, and prove

$$A \otimes_R B \cong A \otimes_S B.$$

If f is not a surjection, is $A \otimes_R B \cong A \otimes_S B$?

Algebra Qualifying Exam, Fall 2001 - SOLUTIONS

Assume all rings have identity elements and all modules are unital.

Section 1: State the theorems below, defining relevant terms.

i. Hilbert's Nullstellensatz.

If F is an algebraically closed extension of K, and I is a proper ideal of $K[x_1,\ldots,x_n]$ then

$$\sqrt{I} = I(V(I)).$$

Here if I is an ideal of $R = K[x_1,\ldots,x_n]$, $\sqrt{I} = \{u \in R : u^n \in I \text{ for some} n\}$.

$$V(I) = \{(a_1,\ldots,a_n) \in F^n | f(a_1,\ldots,a_n) = 0 \text{ for each} f \in I\}.$$

And if $S \subseteq F^n$, $I(S) = \{f \in K[x_1,\ldots,x_n] : f|_S = 0\}$.

ii. The fundamental theorem of Galois theory.

If $K \to F$ is a finite dimensional Galois extension then there is a bijection between intermediate fields of the extension, $K \to E \to F$, and the set of all subgroups of $\mathrm{Aut}_K(F)$ such that

(a) If $K \subseteq J \subseteq L \subseteq F$ then $|L/J| = [J' : L']$.

(b) F is Galois over any intermediate field E, but E is only Galois over K if E' is normal in G and in this case $G/E' = \mathrm{Aut}_K^E$.

If $G = \mathrm{Aut}_K^F$ satisfies $F^G = K$ then $K \to F$ is Galois.

$$J' = \{g \in \mathrm{Aut}_K^F | g|_J = 1_J\}.$$

when J is an intermediate field. If N is a subgroup of G,

$$N' = \{x \in F : n(x) = x \text{ for all } n \in N\}$$

iii. The Noether-Skolem theorem.

R a simple left Artin ring with center K. A and B finite dimensional (over K) simple K-subalgebras of R (containing K). If there is a K-isomorphism $\alpha : A \to B$ then there is an element $u \in K$ so that $\alpha(x) = uxu^{-1}$ when $x \in A$. (I.e., α extends to an inner automorphism of R).

R is simple if it has no proper 2-sided ideals. R is left-Artin if it satisfies the descending chain condition with respect to left-ideals. The center of R is all the elements of R that commute with each element of R.

Section 2: True/False. If FALSE, provide a counterexample, if TRUE, give a brief justification.

a. If $|G| = n$, $m|n$ then there is a subgroup H of G of order m.

FALSE. A subgroup of A_4 of order 6 would have index 2, hence would be normal. But the conjugacy classes of A_4 have order 1, 3 and 8, and you can't make 6 elements out of those.

b. If $f : M \to M'$, $g : N \to N'$ are surjective maps of right and left R-modules respectively, then so is $f \otimes_R g$.

TRUE. Given any generator of $M' \otimes_R N'$, $m' \otimes n'$ $m' = f(m)$ and $n' = g(n)$ so $(f \otimes g)(m \otimes n) = m' \otimes n'$. So $f \otimes g$ hits all generators, and is thus onto.

c. Any torsion free module over a PID is free.

FALSE: Take the PID to be $\mathbf{Z}$, and let the torsion free module be $\mathbf{Q}$. $\mathbf{Q}$ is not free since it isn't free on one generator, and if x, y are two elements of $\mathbf{Q}$, there are non-zero integers n, m so that $nx + my = 0$, hence there are no linearly independent sets with more than one element.

d. If $\mathbf{F}$ is a field of characteristic p, $\mathbf{F}$ contains exactly one p^kth root of 1.

TRUE. $x^{p^k}-1$ factors as $(x-1)^{p^k}$ so by unique factorization in $\mathbf{F}[x]$, 1 must be the only root of $x^{p^k}-1$.

e. If R is a P.I.D. then R is Noetherian.

TRUE. For an ascending chain

$$(c_1) \subseteq (c_2) \subseteq \dots$$

we have $c_{i+1}|c_i$. If the inclusion is proper, then c_i does not divide c_{i+1}. Since a PID is a UFD, we can't have an infinite sequence of *proper* divisions.

f. If $R \subseteq S$ are commutative rings with identity, and $s_1, s_2 \in S$ are integral over R, so is $s_1 + s_2$.

TRUE. Since s_1 is integral, $R[s_1]$ is a finitely generated R-module. Also, $R[s_1, s_2]$ is a finitely generated $R[s_1]$-module since s_2 integral over $R[s_1]$, so it is a finitely generated R-module. This implies $s_1 + s_2$ is in a ring that is finitely generated as an R-module, hence $s_1 + s_2$ is integral.

Section 3: Give complete proofs for 4 problems from the following.

(1) Define *solvable* and show that any group of order p^2q is solvable for p, q distinct primes.

We count p-Sylows and q-Sylows. There must be $kp+1$ of the former, and $kp+1$ must divide p^2q, so $kp+1$ must divide q. If $k=0$, there is a unique p-Sylow, which is thus normal. If $k>0$ then $p<q$.

There are $lq+1$ q-Sylows, and $lq+1$ divides p^2q, so divides p^2. So if $l>0$ then either $lq+1=p$ and $q<p$ (so only one p-Sylow by the argument above) or $lq+1=p^2$. In the second case, the q-Sylow subgroups are all cyclic, and hence are disjoint except for e. So there are $p^2(q-1)+1$ elements which occur in *some* q-Sylow subgroup. This leaves precisely p^2 elements that *aren't* of order q, so these elements must make up the only p-Sylow subgroup. Hence there is only one p-Sylow, or $l=0$ and there is only one q-Sylow.

The conclusion is that at least one of the Sylow subgroups is normal. The quotient is either a group of order q or of order p^2. In either case it must be abelian. This gives a (sub) normal series with abelian factors, so the group is solvable.

(2) Let M be a left R-module which is the sum of its simple submodules. Show that any quotient or submodule of M has the same property.

Let N be a quotient of M so there is a short exact sequence

$$0 \to K \xrightarrow{i} M \xrightarrow{j} N \to 0.$$

If S is a simple submodule in M its image in N must be 0 or S. So N is the sum of all the (images of) the simple submodules of M which are not zero in N, i.e. are submodules of N. Hence N has the relevant property.

The simple modules described above give a set of simple modules whose direct sum intersects N in 0. Use Zorn's Lemma to find a maximal set of simple modules $\{S_\alpha\}$ so that $\sum S_\alpha \cap K = 0$. M is isomorphic to $M' = K + (\sum S_\alpha)$. This is easy by a 5-Lemma argument mapping

$$0 \to K \to M' \to (\sum S_\alpha) \to 0$$

to the exact sequence defining K. The map $K \to K$ is an isomorphism, and the map $(\sum S_\alpha) \to N$ will be onto if we begin our chain for Zorn's lemma using the collection of modules in the first paragraph of the proof, and will be one-one since any element of the kernel must be in K.

It follows that K can be written as a quotient of M, and hence is a sum of its simple submodules by the first paragraph.

(3) (a) If an $n \times n$ matrix A satisifies $A^r = 0$ for some r, then A is similar to a matrix with entries all 0 except for some 1s on the diagonal below the main diagonal.
(b) If the field is algebraically closed and characteristic 0 and $A^r = 1$ for some r, show that A is diagonalizable. What if the field is of positive characteristic?

The minimal polynomial of A is x^r for some r. So the invariant factors are x^i for various values of i dividing r.

So the various companion matrices are of the form desired. So the rational canonical form has the desired form, and that matrix is similar to A since it corresponds to a change-of-basis.

In the second case, the minimal polynomial divides $x^r - 1$. So the elementary divisors are powers of prime polynomials (necessarily linear since the field is algebraically closed). Since we have characteristic 0, the roots of $x^r - 1$ (and thus of the minimal polynomial) are distinct. So each elementar divisor is a linear polynomial. So the Jordan canonical form is diagonal.

In characteristic $p > 0$, the $p \times p$ matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

is already in Jordan canonical form, with minimal polynomial $(x-1)^p = x^p - 1$ and one Jordan block.

(4) Let S be a multiplicatively closed subset of a commutative ring R.
(a) Define $S^{-1}R$ and describe its ring structure.
$S^{-1}R$ is the set $R \times S$ modulo the equivalence relation $(r, s) \sim (r', s')$ if $t(rs' - r's) = 0$ for some $t \in S$.
We add by $(r, s)+(r', s') = (rs'+r's, ss')$ and multiply by $(r, s)(r', s') = (rr', ss')$. One needs to check that these operations are well-defined and that associativity and both distributivity axioms hold.
(b) If $\mathfrak{m}$ is a prime ideal of R and $S = R - \mathfrak{m}$ show S is multiplicatively closed and $S^{-1}R$ is a local ring.
First S is multiplicatively closed since ss' not in S implies it is in $\mathfrak{m}$ so one of s or s' must be in $\mathfrak{m}$ (and hence not in S).
We let M be the ideal of $S^{-1}R$ given by $\{(m, s) : m \in \mathfrak{m}\}$. Any other element of $S^{-1}R$ is a unit, so if this is an ideal it is maximal. It is closed under sums because $\mathfrak{m}$ is an ideal so

$$(m, s) + (m', s') = (ms' + m's, ss') \in M$$

and it absorbs multiplication since $(m, s)(r, t) = (mr, st)$ which is in M if (m, s) is.
If P is any ideal not contained in M, P must contain a unit, so M is the unique maximal ideal.

(5) Suppose $f : R \to S$ is a unital surjection of rings. Let A, B be right and left S-modules respectively. Describe how to give A, B right and left R-modules structures, and prove

$$A \otimes_R B \cong A \otimes_S B.$$

If f is not a surjection, is $A \otimes_R B \cong A \otimes_S B$?

We make A into an R-module by defining $ar = af(r)$. The fact that f is a ring map tells us this is associative, and the fact that f is additive tells us tha this is distributive. We do the same for B but on the right.

To establish our isomorphism, we note that the relations defining the two tensor products are the same except we have $(ar, b) = (a, rb)$ for all $r \in R$ on the left, and $(as, b) = (a, sb)$ for all $s \in S$ on the right. But by our definition of the R action, a relation of type $(ar, b) = (a, rb)$ as appears on the right, is really one of the form $(af(r), b) = (a, f(r)b)$ as on the left. Similarly, given $s \in S$, $s = f(r)$ for some $r \in R$. So $(as, b) = (af(r), b) = (ar, b)$ and similarly $(a, sb) = (a, rb)$. So any relation on the right occurs as one on the left.

So the relations defining $A \otimes_R B$ are the same as those defining $A \otimes_S B$.

If f not a surjection, there is no reason to expect an isomorphism. For example, $R = \mathbf{k}, S = \mathbf{k}[x]$, $A = S, B = k$ with x acting as 0 on k. Then $k[x] \otimes_{k[x]} k \cong k$, but $k[x] \otimes_k k \cong k[x]$, which have different sizes as k-vector spaces.