UCLA Algebra Qualifying Examination Solutions

Yacoub Kureh

Preface

These solutions were written by me in preparation for UCLA's Algebra Qual Exam. I am very much indebted to my colleagues Bonsoon Lin, Alex Tong Lin and Alexander Wertheim for their help and support. Several of the solutions found here are either standard or were found online, but for the most part all have been written in my own words. These solutions are intentionally verbose as I intended for these solutions to be more expository than slick. Any and all errors are my own. Please email me at ykureh@math.ucla.edu with corrections, questions or comments.

UCLA's past exams can be found here:
`http://papyrus.math.ucla.edu/gradquals/hbquals.php`
Note: A future edition will contain a table of contents as well as topic tags.

1 Spring 2016

1.1 Question 1

(a) Give an example of a unique factorization domain A that is not a PID. You need not show that A is a UFD (assuming it is), but please show that your example is not a PID.

There are several examples of UFDs that are not PIDs, such as $F[X, Y]$, a polynomial ring in two variables over a field, or $\mathbb{Z}[X]$, the ring of integer coefficient polynomials. These are UFDs because F and $\mathbb{Z}$ are UFDs and that property of being UFD is preserved under adjoining indeterminates. To see they are not PIDs, consider a well chosen ideal, (X,Y) will do for $F[X, Y]$. This ideal cannot be generated by a single element $f(X, Y)$ in the ring, as we need $f(X, Y)$ to divide X which means it is aX or a constant in the field F, but if it were the latter than the ideal would be the whole ring which it isn't (the ideal consists of nonconstant polynomials). But aX does not divide Y, and so there's not hope for a principal ideal. For $\mathbb{Z}[X]$ consider the ideal $(2, X)$. This is not principle by a similar argument, if it were there'd be a d such that d divides 2 which means d is ± 1 or ± 2. The former case means the ideal is the whole ring which it isn't (the ideal consists of polynomials with even constant term), but ± 2 does not divide X.

(b) Let R be a UFD. Let $\mathfrak{p}$ be a prime ideal such that $0 \neq \mathfrak{p}$ and there is no prime ideal strictly between 0 and $\mathfrak{p}$. Show that $\mathfrak{p}$ is principal.

Now we are given a UFD with a prime ideal $\mathfrak{p}$ such that it has no nontrivial prime ideals strictly contained in it, we want to show $\mathfrak{p}$ is principal. Take some element in $x \in \mathfrak{p}$ and write its unique factorization into primes (in a UFD primes are equivalent to irreducibles) $x = x_1 x_2 \dots x_n$. As $\mathfrak{p}$ is prime we know that $(x_1 x_2 \dots x_{n-1}) x_n \in \mathfrak{p}$ implies either $x_n \in \mathfrak{p}$ or $(x_1 x_2 \dots x_{n-1}) \in \mathfrak{p}$ repeating this, we eventually find some $x_i \in \mathfrak{p}$, but then $(x_i) \subset \mathfrak{p}$ and (x_i) is a prime ideal because it is generated by a prime. So, it must be equal to $\mathfrak{p}$.

1.2 Question 2

Consider the functor F from commutative rings to abelian groups that takes a commutative ring R to the group $R^\times$ of invertible elements. Does F have a left adjoint? Does F have a right adjoint? Justify your answers.

First, we show that for a functor to be left (resp. right) adjoint, then it must preserve initial (resp. terminal) objects. Suppose functors L, R are a left right adjoint pair ($L : C \to D$, $R : D \to C$). That is, $\mathrm{Hom}_D(LA, B) \cong \mathrm{Hom}_C(A, RB)$ for all $A \in C, B \in D$. Suppose $B \in D$ is a terminal object, then for all $A \in C$ we have $|\mathrm{Hom}(LA, B)| = 1$, because by definition of being a terminal object $|\mathrm{Hom}(-, B)| = 1$. Thus we have that $|\mathrm{Hom}_C(A, RB)| = 1$ for all $A \in C$, which is the definition of RB being a terminal object. That is to say, a terminal object remains terminal under right adjoint (however, non-terminal objects may become terminal). Similarly for an initial object and left adjoints: Suppose $A \in C$ is an initial object, then for all $B \in D$ we have $|\mathrm{Hom}(A, RB)| = 1$, because by definition of being an initial object $|\mathrm{Hom}(A, -)| = 1$. Thus we have that

$|\mathrm{Hom}_C(LA, B)| = 1$ for all $B \in D$, which is the definition of LA being an initial object. That is to say, an initial object remains initial under left adjoint (however, non-initial objects may become initial). Now, we note that in the category of commutative rings, the initial object is $\mathbb{Z}$ (the map from $\mathbb{Z}$ to any other ring is completely determine by the morphism property that 0 maps to 0 and 1 maps to 1 and $\mathbb{Z}$ is generated by 1) and the terminal object is the trivial ring (the unique morphism is the zero homomorphism, it preserves 1 as in the zero ring, $0 = 1$). In the category abelian groups, the initial and terminal object is the trivial group. Examining the functor from **CRing** to **Ab** that takes a ring to its group of units, we see that the initial object $\mathbb{Z}$ is sent to the group $\mathbb{Z}/2\mathbb{Z}$, and thus initial-ness is not preserved, so this functor cannot be a left adjoint (i.e. it cannot have a right adjoint). The terminal object, the zero ring, which has one element which is its own unit, is mapped to the trivial group, so terminal-ness is preserved, so this functor may be a right adjoint, i.e. it may have a left adjoint. The routine choice for a left adjoint functor G is the integral group ring functor that takes a group A to the group ring $\mathbb{Z}[A]$. We want to show that there exists a bijection natural in $A \in \mathbf{Ab}$ and $R \in \mathbf{CRing}$ such that

$$\mathrm{Hom}(\mathbb{Z}[A], R) = \mathrm{Hom}(GA, R) \cong \mathrm{Hom}(A, FR) = \mathrm{Hom}(A, R^\times).$$

The proposed bijection takes $\phi \in \mathrm{Hom}(GA, R)$ and maps it to $\phi \restriction_A \in \mathrm{Hom}(A, FR)$. The inverse would take $\psi \in \mathrm{Hom}(A, FR)$ and extend it linearly to $\overline{\psi} \in \mathrm{Hom}(GA, R)$. To see this is an inverse, compare ϕ to $\overline{\phi \restriction_A}$:

$$\overline{\phi \restriction_A}(\sum_{g\in A} n_g g) = \sum_{g\in A} \overline{\phi \restriction_A}(n_g g) = \sum_{g\in A} \left(\sum^{n_g} \phi \restriction_A (g) \right)$$

$$= \sum_{g\in A} \left(\sum^{n_g} \phi(g) \right) = \sum_{g\in A} \phi(n_g g) = \phi(\sum_{g\in A} n_g g).$$

For naturality in A, consider some $f : B \to A$, so that $Gf : \mathbb{Z}[B] \to \mathbb{Z}[A]$ where $Gf \restriction_B = f$. We see that $\phi \in \mathrm{Hom}(GA, R)$ in one direction maps to $\phi \restriction_A \circ f$ and in the other direction $(\phi \circ Gf) \restriction_B$. To test these are the same, take some $b \in B$, we

$$(\phi \circ Gf) \restriction_B (b) = \phi \circ Gf(b) = \phi \circ f(b) = \phi \restriction_A \circ f(b)$$

as $f(b) \in A$. Naturality in R is proved similarly, take some $f : R \to S$, $Ff : R^\times \to S^\times$, where $Ff = f \restriction_{R^\times}$. We see that $\phi \in \mathrm{Hom}(GA, R)$ in one direction maps to $(f \circ \phi) \restriction_A$ and in the other direction maps to $Ff \circ \phi \restriction_A$. To test these are the same, take some $a \in A$. We see that

$$Ff \circ \phi \restriction_A (a) = Ff \circ \phi(a) = f \circ \phi(a) = (f \circ \phi) \restriction (a)$$

as $a \in A$.

1.3 Question 3

Let R be a ring which is left artinian (that is, artinian with respect to left ideals). Suppose that R is a domain, meaning that $1 \neq 0$ in R and $ab = 0$ implies $a = 0$ or $b = 0$ in R. Show that R is a division ring.

Take some nonzero element in the ring $b \in R$. Consider the descending series of left ideals $Rb \supset Rb^2 \supset Rb^3 \supset \ldots$. As the ring is left artinian, we must have that $Rb^i = Rb^{i+1}$. This means that $b^i \in Rb^i$ is in Rb^{i+1}, i.e. $\exists r \in R$ such that $b^i = rb^{i+1}$. Thus $(1-rb)b^i = 0$, as $b \neq 0$ and R is a domain, we have $b^i \neq 0$ and thus $1 - rb = 0$ and so $rb = 1$. Thus b has r as left inverse. By a similar argument, starting with r we can find a left inverse for it, suppose $cr = 1$. Now $c = c1 = c(rb) = (cr)b = 1b = b$. Thus $br = rb = 1$ and so R is a division ring.

1.4 Question 4

Let A be a commutative ring, S a multiplicatively closed subset of A, $A \to A[S^{-1}]$ the localization.

(a) Which elements of A map to zero in $A[S^{-1}]$?

We have a commutative ring A and a multiplicatively closed subset S. The localization map takes $a \in A$ and sends it to $(a, 1) \in R \times S$. Two elements (r_1, s_1) and (r_2, s_2) in the localization are equal if $\exists t \in S$ such that $t(r_1 s_2 - r_2 s_1) = 0$. Thus $(a, 1) = (0, s)$ iff $\exists t \in S$ such that $t(as) = 0$, that is iff $a(ts) = 0$. In the trivial case, $0 \in S$ which means we could use $t = 0$ which would make this true for all $a \in A$ and the localization would be trivial, as in, everything is sent to 0. If this is not the case, i.e. if $0 \notin S$, then we must have that $st \neq 0$ as S is multiplicatively closed. Thus $a(st) = 0$ iff a has a zero divisor in S.

(b) Let $\mathfrak{p}$ be a prime ideal in A. Show that the ideal generated by the image of $\mathfrak{p}$ in $A[S^{-1}]$ is prime if and only if the intersection of $\mathfrak{p}$ with S is empty.

I will let P denote the ideal. Suppose the intersection of P and S is not empty, then let p be an element in the intersection, then $p \in A$ maps to $(p, 1)$ in the localization. Thus the ideal generated by the image of P, call it P' contains $(p, 1)$. However, the localized ring $A[S^{-1}]$ contains $(1, p)$, so the ideal P' must contain the product $(1, p) \times (p, 1)$ which is easily seen to be $(1, 1)$. As we have $(1, 1) \in P'$, this ideal must contain all of $A[S^{-1}]$ and is consequently not prime. Now suppose the intersection is empty. Let $a = (a, s_1), b = (b, s_2) \in A[S^{-1}]$ such that $ab = (ab, s_1 s_2) \in P'$. We want to show that a or b is in P'. An element of P' is (p, s_3) where $p \in P$ and $s_3 \in S$. Now, the elements of $P' = \{(p, s) | p \in P, s \in S\}$, thus we have $(ab, s_1 s_2) = (p, s)$. So we have $\exists t \in S$ such that $t(ps_1 s_2 - abs) = 0$ i.e. $tps_1 s_2 = tabs$. This implies that $abts = tps_1 s_2 \in P$ (recall A is commutative.) which forces one of the factors of $abts \in P$ but we know it cannot be t or s by hypothesis of empty intersection, thus it must be either a or b, but this would imply that (a, s_1) or (b, s_2) is in P'. Thus P' is in fact a prime ideal. To see that $P' = \{(p, s) | p \in P, s \in S\}$, we only need to consider containment in one direction as P'

is clearly contained in the ideal generated by the image of P. Let X be that image, then $(X) = \{\sum_i^n (a_i, s_i)(p_i, 1) | n \in \mathbb{N}\}$, so $x \in (X)$ can be written as $\sum_i^n (a_i, s_i)(p_i, 1)$ and using the rules of addition in the localization, this is

$$\left(\sum_i^n \left(\prod_{j \neq i} s_j \right) a_i p_i, \prod_i s_i \right).$$

But $\prod_i s_i \in S$ as it is multiplicatively closed, so we can represent it by just $s \in S$ and $\prod_{j \neq i} s_j a_i p_i \in P$ as P is an ideal, so we represent it by just $p \in P$, thus $x = (p, s)$ where $p \in P$ and $s \in S$.

1.5 Question 5

Let A be the ring $\mathbb{C}\langle u, v\rangle/(uv - vu - 1)$, the quotient of the free associative algebra on two generators by the given two-sided ideal.

(a) Show that every nonzero A-module M has infinite dimension as a complex vector space.

A is the ring $\mathbb{C}\langle u, v\rangle/(uv - vu - 1)$ which means that $[u, v] = 1$. Consider some nonempty A-module. That is, M is an abelian group under addition and we also have the operation $A \times M \to M$ satisfying all the module properties. Note that $\mathbb{C} \subset A$, and thus we have the operation $\mathbb{C} \times M \to M$. Thus M can be thought of as a $\mathbb{C}$ module, i.e. a complex vector space. From linear algebra we know that a nonempty vector space has a nonempty basis B. For sake of contradiction assume that the basis is finite $|B| = n > 0$. Consider the operation on the vector space by elements $u, v \in A$.By the module properties we can see these act as linear operators, and thus we can represent them with finite matrices $X, Y \in M_n(\mathbb{C})$. However we have that these matrices satisfy $XY - YX = I_n$, and computing the trace (which we must be able to do in finite dimension) of both sides gives $0 = Tr(XY) - Tr(YX) = Tr(XY - YX) = Tr(I_n) = n$, a contradiction. Thus we either have that the module is indeed empty or is infinite dimensional with undefined trace on the operators u, v.

(b) Let M be an A-module with a nonzero element y such that $uy = 0$. Show that the elements $y, vy, v^2y, \ldots$ are $\mathbb{C}$-linearly independent in M.

Let $y \in M$, a nonzero element in the nonempty A-module. We want to show that the elements $y, vy, v^2y, \ldots$ are $\mathbb{C}$-linearly independent. This is equivalent to showing that for all $n > 0$ that $c_0y + c_1vy + c_2v^y + \ldots c_nv^ny = 0$ implies that all $c_i = 0$ where the $c_i \in \mathbb{C}$. To see this we consider operating on the sum by u. First we will want to show that $uv^ky = kv^{k-1}y$ for all $k \in \mathbb{N}$. The base case is simply $uvy = (1 + vu)y = y + vuy = y + 0 = y$. Assume the hypothesis is true up to $n - 1$ i.e. $uv^{n-1}y = (n - 1)v^{n-2}y$. The inductive step is simply $uv^ny = uvv^{n-1}y = (1 + vu)v^{n-1}y = v^{n-1}y + vuv^{n-1}y = v^{n-1}y + v(n - 1)v^{n-2}y = nv^{n-1}y$. Thus we can think of u as the differential operator on the variable v. Repeated application of u on $c_0y + c_1vy + c_2v^y + \ldots c_nv^ny = 0$ gives $n!c_ny = 0$ which implies $c_n = 0$ as neither $n!$

nor y are zero. Following in this way we get that $c_{n-1} = 0, \dots c_1 = 0$. Thus all the $c_i = 0$ and so the set $\{v^k y\}$ is $\mathbb{C}$ linearly independent. (Cf. Problem 10 from Fall 2014)

1.6 Question 6

Let K be a field of characteristic $p > 0$. For an element $a \in K$, show that the polynomial $P(X) = X^p - X + a$ is irreducible over K if and only if it has no root in K. Show also that, if P is irreducible, then any root of it generates a cyclic extension of K of degree p.

If the polynomial $P(X)$ has a root $\alpha \in K$, then by the Euclidean algorithm we can divide $P(X)$ by $(x-\alpha)$ and we would find $P(X)$ reduces to $(x-\alpha)g(x)$ where $g(x) \in K[x]$. Suppose now that the polynomial is reducible, then we would have $P(x) = f(x)g(x)$ where the degrees of f, g are between 1 and $p-1$, inclusive (i.e. neither are units). Let's suppose $f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$ where $1 \leq n \leq p-1$. Notice that for all $j \in F_p$ the prime subfield of K, $P(x+j) = (x+j)^p - (x+j) + a = x^p + j^p - x - j + a = x^p - x + a + (j^p - j) = P(x)$ as $j^p = j$ for all $j \in F_p$ (Fermat's little theorem). So we have that $P(x) = f(x+j)g(x+j)$. But notice, that $f(x) \neq f(x+j)$ as $f(x+j) = (x+j)^n + b_{n_1}(x+j)^{n-1} + \ldots = x^n + (nj + b_{n-1})x^{n-1} + \ldots$ and $nj + b_{n-1} \neq b_{n-1}$ unless $nj = 0$, which in an integral domain forces $j = 0$. So f is not invariant. Thus we have p distinct polynomials, $f(x), f(x+1), \ldots, f(x+(p-1))$ which divide a degree p polynomial, so all of these factors must be linear and $P(x) = \prod f(x+j)$. This means that $P(x)$ not only has one root if it is reducible, but has all of its roots in K. If P is irreducible, then adding any root α of P automatically adds all of its roots, which are $\alpha + j$. Thus the extension $K[x]/(P(x))$ is a Galois extension (it's normal since it's splitting and it's seprable as the roots are all distinct) of degree p so its Galois group must be of order p so it is the cyclic group, and the extension is cyclic of degree p.

1.7 Question 7

Show that for every positive integer n, there exists a cyclic extension of $\mathbb{Q}$ of degree n which is contained in $\mathbb{R}$.

By Dirichlet's theorem (cf. Problem 3 from Fall 2013) we know that in the arithmetic progression $1 + 2n, 1 + (2)2n, 1 + (3)2n, ...$ there exists a prime, choose one to be our p, thus $2n|(p-1)$. Let ξ_p be the primitive pth root of unity. We know that $\mathbb{Q}(\xi_p)$ is a cyclic extension of $\mathbb{Q}$ of order $p-1$. As the Galois group G is cyclic we have a unique, and normal, subgroup of index d for each divisor. Take the subgroup H to be one of index n, i.e. it's order is $\frac{p-1}{n}$ which must be even. Claim: $\mathbb{Q}(\xi_p)^H$ is the field we want. First, this field is fixed by an index n subgroup which means it will have degree n over $\mathbb{Q}$. This field is real because H is of even order: H being of even order means that it contains the involution, σ (i.e. $\sigma^2 = e$ but $\sigma \neq e$). We look to see where σ takes the element ξ_p, we must have $\sigma(\xi_p) = \xi_p^a$ and $\xi_p = e(\xi_p) = \sigma^2(\xi_p) = \xi_p^{a^2}$, thus $a = \pm 1 \mod p$, so $a = -1$, as the automorphism is determined just by where ξ_p is sent. Thus $\xi_p + \xi_p^{-1}$ is fixed by σ,

and in fact $\mathbb{Q}(\xi_p)^{\langle\sigma\rangle} = \mathbb{Q}(\xi_p + \xi_p^{-1})$, observe the polynomial $x^2 - (\xi_p + \xi_p^{-1})x + 1$ proves $[\mathbb{Q}(\xi_p) : \mathbb{Q}(\xi_p + \xi_p^{-1})] \leq 2$, but it can't be equal to one since it's a real field, and we conclude by invoking the fundamental theorem of Galois Theory. Thus, we have $\langle e\rangle < \langle\sigma\rangle < H < G$ and so by reverse inclusion $\mathbb{Q}(\xi_p)^G = \mathbb{Q} \subset \mathbb{Q}(\xi_p)^H \subset \mathbb{Q}(\xi_p)^{\langle\sigma\rangle} = \mathbb{Q}(\xi_p + \xi_p^{-1}) \subset \mathbb{Q}(\xi_p)^{\langle e\rangle} = \mathbb{Q}(\xi_p)$. Thus our field is contained in a real field so it must be real.

1.8 Question 8

Character table for S_4.

1.9 Question 9

Show that if G is a finite group acting transitively on a set X with at least two elements, then there exists $g \in G$ which fixes no point of X.

G is finite, so $|G| = n$. The set X is such that $|X| = m \geq 2$. Consider the stabilizer subgroup for $x \in X$. Since the group's action is transtive, we have the orbit for x is all of X and by orbit-stabilizer we have the the stabilizer subgroup has order n/m. As x was arbitrary this is the size of the stabilizer subgroup for all elements of X. Consider the set union of all of the stabilizer subgroups ranging over all $x \in X$. What is the size of this union. We can give an upper bound by assuming perfect disjointness except that the identity is in each stabilizer subgroup, i.e. $m(n/m) - (m-1) = n - m + 1$ but as $m \geq 2$ we know that this is strictly less than n, the order of the group. Thus there is a group element $g \in G$ which is not in stabilizer subgroup for any x thus it has no fixed points. Two possible extensions: 1) Infinite group and finite set or 2) infinite group and infinite set. Note we cannot have a finite group acting transitively on an infinite set. In the first case, our group has to have a quotient group which is a transitive subgroup of S_X. This quotient group G/N will be finite as S_X and its subgroups are finite. This puts us in the above case, and so we have an element gN in the quotient G/N which fixes no points, and so g in the group G fixes no points. In the second case, we have a counter example using $SO(3)$ acting on the sphere, this group action is transitive, but each group element leaves at least two points (the poles) fixed under rotation.

1.10 Question 10

(a) Determine the Galois group of the polynomial $X^4 - 2$ over $\mathbb{Q}$, as a subgroup of a permutation group. Also, give generators and relations for this group.

The polynomial is irreducible by Eisenstein at $p = 2$. In closure, the polynomial splits as $(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$ and so $i^k \sqrt[4]{2}$ are the four distinct roots and $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field. We can define automorphisms over $\mathbb{Q}$ on the generators $\sqrt[4]{2}$ and i. The automorphisms must permute the roots amongs the roots of their minimal polynomials, which are $X^4 - 2$ and $X^2 + 1$ respectively (these are irreducible, use rational root test on latter). Thus we can have an automorphism τ sending $\sqrt[4]{2}$ to $i\sqrt[4]{2}$ which fixes i and an

automorphism σ which fixes $\sqrt[4]{2}$ and permutes $\pm i$. We can check that these two generate automorphisms generate a group of automorphisms of order 8 which is the degree of the extension by checking $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [Q(\sqrt[4]{2}, i), \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}] = 2 \times 4$. We can check by composing the automorphism that we have $\tau^4 = \sigma^2 = Id$ and that $\sigma\tau = \tau^{-1}\sigma$ and so this group is D_4.

(b) Determine the Galois group of the polynomial $X^3 - 3X - 1$ *over* $\mathbb{Q}$.

The polynomial is irreducible by the rational root test. Thus the Galois group has to be a transitive subgroup of S_3 of which there are only A_3 and S_3. The determinant for the polynomial $x^3 - 3x - 1$ is $-4(-3)^3 - 27(-1)^2 = 81 = 9^2$. Since the discriminant is a square, that implies the quantity $\prod_{i<j}(\alpha_i - \alpha_j) \in Q$. This implies that there are only even permutations, and thus the Galois group lies in A_3, and thus must be A_3.

2 Fall 2015

2.1 Question 1

Show that the inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism in the category of rings with the multiplicative identity.

In categories, an epimorphism is a right-cancellative morphism. To see that the inclusion map $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism, consider two morphism $f, g : \mathbb{Q} \to R$. Consider the compositions $\mathbb{Z} \xrightarrow{f \circ \iota} R$ and $\mathbb{Z} \xrightarrow{g \circ \iota} R$ where $f \circ \iota = g \circ \iota$. We want to show that $f = g$, that is $\forall q \in \mathbb{Q}$, we have $f(q) = g(q)$. For each q, write it as a/b, where $a, b \in \mathbb{Z}$, and $b \neq 0$. We know that $f(a) = f \circ \iota(a) = g \circ \iota(a) = g(a)$ and similarly we have $f(b) = g(b)$. That is, f, g agree on all of $\mathbb{Z}$. However since these are ring homomorphisms, we get

$$f(q) = f(a/b) = f(ab^{-1}) = f(a)f(b)^{-1} = g(a)g(b)^{-1} = g(ab^{-1}) = g(a/b) = g(q).$$

2.2 Question 2

Let R be a principal ideal domain with field of fractions K.

(a) Let S be a non-empty multiplicatively closed subset of $R \setminus \{0\}$. Show that $R[S^{-1}]$ is a principal ideal domain.

Recall that the pullback of a homomorphism between rings takes ideals to ideals. To prove $R[S^{-1}]$ is a PID, consider an ideal in it, J. The pullback of the localization homomorphism $\phi : R \to R[S^{-1}]$ of J is then an ideal in R which must be principal, say (r). Claim: J is generated by image of r under localization, i.e. $J = (r/1)$. In one direction, we have that $r \in (r) = \phi^{-1}(J)$ and so $\phi(r) = r/1 \in J$. Since J is an ideal, it must contain the ideals generated by each of its elements, so $(r/1) \subset J$. In the other direction, consider an element $p/q \in J \subset R[S^{-1}]$, where $p \in R$ and $q \in S$ (remember we can think of p/q as $(p, q) \in R \times S$). As $S \subset R$ we have that $q \in R$ and so $q/1$ is in $R[S^{-1}]$ which means $p/q \times q/1 = p/1 \in J$. We know one preimage of $p/1$, namely p, so $p \in \phi^{-1}(J) = (r)$ and so $p = rs$ and thus we have that $p/q = p/1 \times 1/q = rs/1 \times 1/q = r/1 \times s/q \in (r/1)$. Thus proving the claim.

(b) Show that any subring of K containing R is of the form $R[S^{-1}]$ for some multiplicatively closed subset S of $R \setminus \{0\}$.

Let Q be the subring between R and its field of fractions F. Let $T = \{r \in R | 1/r \in Q\}$. Claim, $Q = R[T^{-1}]$. In one direction, let $r/t = r/1 \times 1/t = r \times 1/t \in R[T^{-1}]$, then as $r \in R \subset Q$ and $1/t \in T^{-1}$ so $t \in T$ so $1/t \in Q$ we have that $r/t \in Q$, giving $R[T^{-1}] \in Q$. In the other direction, let $p/q \in Q$. As R is a PID, we can write p/q in reduced form where $p, q \in R$ are coprime in R meaning $\exists x, y \in R$ such that $xp + yq = 1$. In the field of fractions K we can divide by q to get $x \times p/q + y = 1/q$. All of $x, p/q, y$ are in Q and thus we have that so is $1/q$, as $q \in T$ and so $1/q \in R[T^{-1}]$ thus we have that $p/q \in R[T^{-1}]$ and $Q = R[T^{-1}]$.

2.3 Question 3

Let k be a field and define $A = k[X,Y]/(X^2, XY, Y^2)$.

(a) What are the principal ideals of A?

The quotient ring $A = k[X,Y]/(X^2, XY, Y^2)$ consists of polynomials $aX + bY + c$. Notice that its inverse is $(aX+bY+c)(a'X+b'Y+c') = (ac'+a'c)X+(bc'+b'c)Y+(cc') = 1$ where $c' = 1/c, a' = -a/c^2, b' = -b/c^2$. Thus to be a unit, an element must have a nonzero constant term. The obvious principal ideals are (0) and (1). The latter is equivalent to an ideal generated by a unit, so we should consider ideals of the form $(aX + bY)$. Notice when we multiply this by an element in the ring we get, $(aX + bY)(a'X + b'Y + c') = (ac')X + (bc')Y = c'(aX + bY)$. Thus, for fixed $a, b \in k$, the ideal $(aX + bY)$ cosnsist of k multiples of itself. Thus the nontrivial proper principal ideals are $(X + bY)$ where $b \in K$ and (Y).

(b) What are the ideals of A?

Now broadening the scope to consider all ideals, we try to generate an ideal with any two non-units. If these non-units are k-multiples of each other, we get a principal ideal again. If not, we have $I = (X+bY, X+dY)$ where $d \neq b$ or $J = (X+bY, Y)$. In the former case we can subtract to get that $X + bY - (X + dY) = (b - d)Y \in I$ which means $Y \in I$ and we can use that to get $X \in I$, and so $(X, Y) \subset I$, but $I = (X + bY, X + dY) \subset (X, Y)$. Notice that $A/I = k$ and so the ideal is maximal. We can play as similar game with J and find $J = I$. And so with any two non-units we either generate a principal ideal or the unique maximal ideal (X, Y).

2.4 Question 4

Let K be a field and let L be the field $K(X)$ of rational functions over K.

(a) Show that there are two unique K-automorphism f and g of the field $L = K(X)$ such that $f(X) = X^{-1}$ and $g(X) = 1 - X$. Let G be the subgroup of the group of K-automorphisms of L generated by f and g. Show that $|G| > 3$.

Take an arbitrary element $p(x)/q(x) \in L$, where $p, q \in K[x]$, i.e.

$$p = \sum_i^n p_i x^i, \; q = \sum_j^m q_j x^j$$

where $p_i, q_j \in K$ and $q_j \neq 0$ for at least one i. As f is an automorphism of L we have that

$$f(p(x)/q(x)) = f(p(x)q(x)^{-1}) = f(p(x))f(q(x))^{-1}.$$

As f is a K-automorphism, we have that

$$f(p(x)) = f(\sum_i^n p_i x^i) = \sum_i^n p_i f(x^i) = \sum_i^n p_i f(x)^i = \sum_i^n p_i x^{-i}$$

and similarly for q, which forces $f(p(x)/q(x)) = p(x^{-1})/q(x^{-1})$. Every step follows from the fact that f is an K-autmorphism over L making it the unique such automorphism. Similarly for $g(p(x)/q(x)) = p(1-x)/q(1-x)$, we have that it is the unique such automorphsim. Both of these automorphisms is an involution, however, we find that $f \circ g(x) = f(g(x)) = f(1-x) = 1 - x^{-1}$ and this is different from $f(x)$ and $g(x)$, so this is a different K-automorphsim (composition of K-automorphisms is a K-automorphism). Thus the group of K-automorphisms generated by f and g has more than three elements.

(b) Let $E = L^G$. Show that $P = \dfrac{(X^2 - X + 1)^3}{X^2(X-1)^2} \in E$.

To see that the given $P = \dfrac{(x^2 - x + 1)^3}{x^2(x-1)^2}$ is fixed by the group of automorphisms G it is sufficient to check it is fixed by the generators f and g. Simple checking shows

$$f(P) = \frac{(x^{-2} - x^{-1} + 1)^3}{x^{-2}(x^{-1}-1)^2} = \frac{x^6}{x^6}\frac{(x^{-2} - x^{-1} + 1)^3}{x^{-2}(x^{-1}-1)^2} = P(x)$$

and similarly with

$$g(P) = \frac{((1-x)^2 - (1-x) + 1)^3}{(1-x)^2((1-x)-1)^2} = \frac{(1 - 2x + x^2 - 1 + x + 1)^3}{(1-x)^2(-x)^2} = P(x).$$

(c) Show that $L/K(P)$ is a finite extension of degree 6.

To show that $L/K(P)$, or more suggestively $K(x)/K(P)$ is a finite extension of degree 6, we want to find an irreducible sixth degree polynomial $h(T)$ in $K(P)[T]$ such that $h(x) = 0$, i.e. so that x is a root. An ultimately-but-not-instantly obvious choice is $h(T) = (T^2 - T - 1)^3 - P(x)T^2(T-1)^2$. It's clear that this is degree six in T and has root x. To check irreducibility, we use the general version of Gauss' lemma for UFDs. First of all, note that $K[P]$ is a UFD since K is a field and P is transcendental over K. Note that $K(P)$ is its field of fractions, and Gauss' lemma states that we check irreducibility in $K(P)[T]$ by checking over $K[P][T]$ (in the other direction we would need to check primitivity). We have that $K[P][T] = K[T][P]$ and we can see that the polynomial is irreducible here as it is linear in P and there is no common factor between $(T^2 - T - 1)^3$ and $T^2(T-1)^2$ as there are no common roots. Thus we found the minimal polynomial for x in the field $K(P)$, and it is degree 6, so the extension is degree 6.

(d) Deduce that $E = K(P)$ and that G is isomorphic to the symmetric group S_3.

We have the tower of extension $K \subset K(P) \subset E \subset L$, where we know that $K(P) \subset E$ as $P \in E$. We know that $L/K(P)$ is degree 6, and we can check that subgroup G consists of 6 elements $\{e, f, g, fg, gf, fgf = gfg\}$. By a theorem of Artin we have that L/E is a Galois extension, and since $[L : E] > 3$ and $[L : K(P)] = 6$. By the multiplicativity

of extension degrees $6 = [L : K(P)] = [L : E][E : K(P)] > 3[E : K(P)]$, we are forced to have $[E : K(P)] = 1$, i.e. $E = K(P)$ and so $[L : E] = 6$ and $G = 6$. As there are only two groups of order 6, $\mathbb{Z}/6\mathbb{Z}$ and S_3 we can conclude G is S_3 because we have f, g are two distinct elements of order 2. In fact $f, g, fgf = gfg$ are the three two cycles and $fg = (gf)^2, gf = (fg)^2$ are the two three cycles.

2.5 Question 5

(a) Let G be a group of order $p^e v$ with v and e positive integers, p prime, $p > v$, and v is not a multiple of p. Show that G has a normal Sylow p-subgroup.

G is a group of order $p^e v$ where $p > v$ and p is a prime. Consider the Sylow p-subgroups. Let n_p be the number of such subgroups. This number must be a divisor of v and must be congruent to 1 modulo p. However, as $v < p$, all the divisors of v are also less than p and so we must have n_p. However, by Sylow theorems, all Sylow p-subgroups are conjuate, but since there is only one, it must be self-conjugate for all g, i.e. $gPg^{-1} = P$ for all $g \in G$, thus this Sylow subgroup is normal.

(b) Show that a nontrivial finite p-group has nontrivial center.

Let $|G| = p^n$. Here we use the conjugacy class equation $|G| = \sum_i [G : C_G(g_i)]$ where we choose one representative g_i from each conjugacy class. But indices must all be divisors of p^n, i.e p^m. Notice that $[G : C_G(g_i)] = 1$ iff g_i is central. We know there is at least one, the identity. $|G| - \sum_{i, g_i \neq e} [G : C_G(g_i)] = 1$. If there were no other central elements, then the left hand side is divisible by p while the right hand side is not. Thus there must be at least p central elements.

2.6 Question 6

Let F be a field of characteristic not 2. Let a and b nonzero elements of F. Let R be the F-algebra $R = F\langle i, j\rangle/(i^2 - a, j^2 - b, ij + ji)$, the quotient of the free associative algebra on 2 generators by the given two sided ideal.

(a) Let $\bar{F}$ be an algebraic closure of F. Show that $R \otimes_F \bar{F}$ is isomorphic as an $\bar{F}$-algebra to the matrix algebra $M_2(\bar{F})$.

This is the construction of the quaternion algebra over an algebraically closed field, $\bar{F}$. First note that regardless of the field we can convert any sequence of powers of i and j to one of c, ci, cj, cij where $c \in F$ and by using the relations given where we reduce powers and anti-commute i and j. Let $\alpha, \beta \in \bar{F}$ such that $\alpha^2 = a$ and $\beta^2 = -b$. Then we can make our $\bar{F}$ isomorphism to $M_2(\bar{F})$ by sending

$$i \mapsto \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix} \text{ and } j \mapsto \begin{pmatrix} & \beta \\ -\beta & \end{pmatrix}.$$

We can check all the homomorphism properties

$$\begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix}^2 = a \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \text{ and } \begin{pmatrix} & \beta \\ -\beta & \end{pmatrix}^2 = -b \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

and that

$$\begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix} \begin{pmatrix} & \beta \\ -\beta & \end{pmatrix} = - \begin{pmatrix} & \beta \\ -\beta & \end{pmatrix} \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix}.$$

Extending linearly over $\bar{F}$, we can now check it is an isomorphism. Now we have that

$$c_0 + c_1 i + c_2 j + c_3 ij \mapsto \begin{pmatrix} c_0 + c_1\alpha & c_3\beta + c_4\alpha\beta \\ -c_3\beta + c_4\alpha\beta & c_0 - c_1\alpha \end{pmatrix}.$$

To check injectivity and surjectivity, we can just check that the four-by-four system is invertible,

$$\begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 0 & \beta & \alpha\beta \\ 0 & 0 & -\beta & \alpha\beta \\ 1 & -\alpha & 0 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix}$$

which it is.

(b) Give a basis for R as an F-vector space, justifying your answer.

Since the set $\{1, i, j, ij\}$ are linearly independent over $\bar{F}$ they must be linearly independent over F, and by the above it spans.

Some comments: This construction always yeilds a central simple algebra and by Wedderburn we can assert immediately that we get a matrix ring ring over a division algebra. In fact the only two possibilities here are getting a division algebra of dimension four over the base field or the two by two matrix ring over the base field. Over algebraically closed fields as we had above we always get the matrix algebra. For other cases, it depends on a and b, in a way that can be determined by quadratic forms over the base field.

2.7 Question 7

Character Table for S_4.

2.8 Question 8

Let F be a field. Show that the group $SL(2, F)$ is generated by the matrices $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$ *for elements e in F.*

Recall that the determinant is multiplicative. To see that $SL(F)$ is generated by elements $A^e = \begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ and $A_e = \begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$ for all $e \in F$ we work backwards and attempt to deconstruct an arbitrary matrix $X^1 = \begin{pmatrix} x^1_{11} & x^1_{12} \\ x^1_{21} & x^1_{22} \end{pmatrix} \in SL(F)$ (where the superscript will denote our steps) back into the identity using only various A^e, A_e. Case 1) $x_{21} \neq 0$, then we consider $X^2 = A^{\frac{1-x_{11}}{x_{22}}} X^1$ which now has has $x^2_{11} = 1$. We then multiply $X^3 = A_{-x^1_{21}} X^2$ which gives us $x^3_{11} = 1$ and $x^3_{21} = 0$. Our last step is simple $X^4 = X^3 A^{-x^3_{12}}$ so we get $x^3_{11} = 1$, $x^3_{12} = 0$, and $x^3_{21} = 0$ and since the determinant is one this forces $x^4_{11} = 1$ and so we get back the identity. Case 2) where $x_{21} = 0$ but $x_{12} \neq 0$ follows very similarly. Case 3) where both are zero, we multiply on the left by A_1 and we are back in case 1.

2.9 Question 9

(a) Let R be a finite-dimensional associative algebra over a field F. Show that every element of the Jacobson radical of R is nilpotent.

R is a finite dimensional algebra over a field F. In particular it is a vector space over F. A left ideal of the algebra must in particular be subspaces of R over F and therefore we can see by counting dimensions that we cannot have an infinite descending chain, and thus R is left artinian. Now consider an arbitrary element x in the Jacobson Radical of R, denoted $J(R)$. We have that the chain of left ideals $Rx \supset Rx^2 \supset Rx^3 \supset \dots$ must stabilize giving $Rx^n = \dots Rx^{2n}$ and so $x^n = rx^{2n}$ for some $r \in R$, which we can rewrite as $x^n - rx^{2n} = (1 - rx^n)x^n = 0$. As $x \in J(R)$ we must have $rx^{2n} \in J(R)$, and therefore $1 - rx^{2n}$ must be a unit, otherwise $1 - rx^{2n}$ is in some maximal ideal, and x is in every maximal ideal, so there is a maximal ideal that has 1 in it, a contradiction. Therefore $(1 - rx^n)$ cannot be a zero divisor, and so $x^n = 0$, and so all elements of the Jacobson radical are nilpotent.

(b) Let R be a ring. Is an element of the Jacobson radical of R always nilpotent? Is a nilpotent element always in the Jacobson radical?

R is now an arbitrary ring. (i) No, a nonzero element $x \in J(R)$ is not necessarily nilpotent. In fact, there exists rings where the Jacobson radical has no nilpotent elements. Let R be the formal power series over a field. Then, R is an integral domain, and thus contains no nontrivial nilpotents. We show that the Jacobson Radical is nontrivial. An element in R is invertible if the constant term is invertible, thus the ideal (x) is maximal. In fact, this is the only maximal ideal as its complement consists entirely of units, i.e. this is a local ring. Thus $J(R) = (x) \neq 0$.
(ii) The Jacobson radical of simple rings is 0, so $M_2(\mathbb{Q})$ has a trivial Jacobson radical. However, the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent.

2.10 Question 10

Let p be a prime number. For each abelian group K of order p^2, how many subgroups H of $\mathbb{Z}^3$ are there with $\mathbb{Z}^3/H$ isomorphic to K?

First, let's note that as Z^3 is abelian, all of its subgroups are normal. Thus finding the number of subgroups H such that $Z^3/H \cong K$ where K is an abelian group of order p^2, it is equivalent to finding all the subgroups of index p^2. There's an interesting formula for computing this number recursively: $a_n(\mathbb{Z}^r) = \sum_{k|n} a_k(\mathbb{Z}^{r-1}(n/k)^{r-1}$. Doing this out for $n = p^2$ and $r = 3$ we get $p^4 + p^3 + 2p^2 + p + 1$. This isn't necessary for the problem, but it'll be a good check at the end.

There are two abelian groups of order p^2, the cyclic one and elementary one. In the cyclic case, in order to get an isomorphism between $\mathbb{Z}^3/H$ and $\mathbb{Z}/p^2\mathbb{Z}$ we must have a surjection from $\mathbb{Z}^3$ onto $\mathbb{Z}/p^2\mathbb{Z}$. As $\mathbb{Z}^3$ is the free abelian group on three generators, homomorphisms from it are fully defined by where the generators go. The image is a subgroup of $\mathbb{Z}/p^2\mathbb{Z}$, of which there is only one nontrivial proper one, which is given by $\{0, p, 2p, \ldots, (p-1)p\}$, any element not in here generates the whole group as it will be relatively prime with p^2. Thus, in order to have a surjection we need to make sure that at least one generator from $\mathbb{Z}^3$ goes to a generator of $\mathbb{Z}/p^2\mathbb{Z}$. There are $(p^2)^3$ possible homomorphisms in total, and $(p)^3$ are the bad non-surjective type. So in total there are $p^6 - p^3$ surjective homomorphism.

However, some surjective homomorphisms have the same kernel and thus we are finding the same subgroup H and overcounting them. That is, we may have two surjective $\phi, \phi' : \mathbb{Z}^3 \to \mathbb{Z}/p^2\mathbb{Z}$ where $H = \ker(\phi) = \ker(\phi') = H'$ but $\phi \neq \phi'$. By the universal property of quotient groups as $\mathbb{Z}/p^2\mathbb{Z}$ is the quotient $\mathbb{Z}^3/H$, if $H \subset \ker(\phi')$ then $\exists! psi'$ such that $\phi' = \psi'\phi$. Swapping, we also have $\exists!\psi$ such that $\phi = \psi\phi'$. Composing we get $\phi' = \psi'\phi = \psi'\psi\phi'$ and similarly $\phi = \psi\psi'\phi'$. Following the same construction but with using the same quotient group twice we would find that there is unique map f such that $f\phi = \phi$ and of course the identity works for f but so does $\psi\psi'$ and thus they must be the same. So we get that ψ and ψ' are isomoprhisms of the quotient groups. That is to say, the surjective homomorphisms ϕ and ϕ' with same kernel differ exactly by an isomorphism between their quotient groups. The reverse direction is simpler, i.e. that an automorphism on the quotient group pre-composed with a surjective homomorphism gives another surjective homomorphism with the same kernel. The number of isomorphisms (automorphisms) between $\mathbb{Z}/p^2\mathbb{Z}$ and itself, of which there are $p^2 - p$ (the map is determined by where a generator goes, and it needs to go to a generator of which there are $p^2 - p$). So in total, the number of subgroups is

$$\frac{p^6 - p^3}{p^2 - p} = p^4 + p^3 + p^2.$$

Now we consider the case when our target quotient is $K = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. We perform a similar computation. The nontrivial proper subgroups of K are more complicated, they are all of the order p again, but there are p of them, each generated by any non-identity

element of K. Thus for our map to surjective we need one generator to go to a non-identity element, and another to go an element not in the subgroup generated by image of the other generator. Counting gives $p^6 - p^4 - p^3 + p$ surjective homomorphism. Again, we need to divide by number of automorphisms on K of which there are $(p^2 - 1)(p^2 - p)$, which gives $p^2 + p + 1$. Summing with the number we had before we see agree with the formula above regarding number of index p^2 subgroups of $\mathbb{Z}^3$.

Another method was suggested by BL for the elementary group case. The idea is to consider reduced row echelon 2×3 matrices that correspond to surjective linear maps between vector spaces. We can see there are three kinds,

$$\begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \end{pmatrix}, \begin{pmatrix} 1 & * & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The first has $p \times p$ choices, the second has p choices, and the last has no choices, giving the same $p^2 + p + 1$ as above.

3 Spring 2015

3.1 Question 1

What are the coproducts in the category of groups?

Coproducts in the category of **Groups** are the free products of groups. That is, given two groups A_1, A_2, their categorical coproduct is $A_1 * A_2$, the free product with the standard injection ι_i. To check it is the coproduct we verify the universal property. Given another group C with homomorphisms $f_i : A_i \to C$, we must show that there exists a unique homomorphism f from $A_1 * A_2$ to C such that $f_i = f\iota_i$. Let's try to define f. As $A_1 * A_2$ is the free product, its (reduced) elements consists of words $a_1 a_2 \dots a_n$ where the a_j alternate coming from A_1 and A_2. As f is is a group homomorphism, it respects the group operation which is concatenation, so $f(a_1 a_2 \dots a_n) = f(a_1)f(a_2)\dots f(a_n)$. However, $f(a_j) = f(\iota_{i_j}(a_i)) = f_{i_j}(a_i)$ and thus f is uniquely determined by homomorphism properties and $f_i = f\iota_i$.

3.2 Question 2

Let C be the category of groups and C' be its full subcategory with objects the abelian groups. Let $F : C' \to C$ be the inclusion functor. Determine the left adjoint of F and show that F has no right adjoint.

We first see that for a functor to have a right adjoint (i.e. be a left adjoint) means that it preserves coproducts. Let $A, B \in \mathbf{Ab}$ and $C \in \mathbf{Groups}$ and L and R are left-right adjoints between the two categories. Then

$$Hom(L(A \amalg B), C) \cong Hom(A \amalg B, R(C)) \cong Hom(A, R(C)) \amalg Hom(B, R(C))$$

$$\cong Hom(L(A), C) \amalg Hom(L(B), C) \cong Hom(L(A) \amalg L(B), C).$$

However, as the coproduct between C_2 and itself in **Ab** is the direct sum, i.e. the finite group $C_2 \times C_2$ while the coproduct of C_2 and itself in **Groups** is an infinite group, we see that the coproduct is not preserved ($L(C_2 \amalg_{\mathbf{Ab}} C_2) = C_2 \times C_2 \neq C_2 * C_2 = L(C_2) \amalg_{\mathbf{Groups}} L(C_2)$. The obvious choice for a functor to take a group to an abelian group is the functor which takes a group G to its abelianization G/G' where G' is the normal subgroup generated by all commutators. Denote the inclusion functor by R and this abelianization functor by L The goal is to show that there is a bijection natural in $A \in \mathbf{Ab}$ and $G \in \mathbf{Groups}$ between $Hom(G/G', A) = Hom(L(G), A) \cong Hom(G, R(A)) = Hom(G, A)$. Take a $\phi \in Hom(G, A)$, this is a group homomorphism from an arbitrary group to an *abelian* group A, thus it must factor through uniquely via the abelianization of G/G', giving a unique homomorphism $\phi' : G/G' \to A$. This will be our bijection. It is surjective as any map $\psi \in Hom(G/G', A)$ can be precomposed with the natural projection $\pi : G \to G/G'$, to give $\psi\pi : G \to A$. As this map factors through ψ, it is the unique map to do so and thus we have surjectivity. This is injective suppose $\phi_1, \phi_2 : G \to A$ both factor through ψ, then

$\phi_1 = \psi\pi = \phi_2$. To check naturality in A we consider $f : A \to B \in \mathbf{Ab}$, and note that $Rf = f$. Start with a $\phi \in Hom(G, A)$, in one direction we postcompose with f to get $f\phi$ and then get $\eta(f\phi)$, while following the other direction we get $\eta(\phi)$ and postcompose with $Rf = f$ to get $f\eta(\phi)$. Let's let $\eta(\phi) = \psi$ i.e. $\phi = \psi\pi$ where π is canonical surjection from G to G/G'. The commutativity depends on $\eta(f\phi) = f\psi$, to see this we check universal property. That is to say, if $f\phi = f\psi\pi$ then $f\psi$ is the unique such map and $\eta(f\phi) = f\psi$. But this is true as $\phi = \psi\pi$ and so $f\phi = f\psi\pi$, which gives naturality in one argument. TO check naturality in the other direction, consider some $g : H \to G$. What is $L(g)$? It is a map $L(g) : L(H) = H/H' \to G/G'$, which we define by considering $\pi g : H \to G/G'$ and noting this must factor as $\chi\rho$ for a unique χ where ρ is canonical projection from H to H/H'. That is $L(g) = \chi$ where χ is the unique map satisfying $\pi g = \chi\rho$. So following the diagram in both directions we have $\eta(\phi g)$ and $\psi L(g) = \psi\chi$. To see these are the same, again consider the universal property, if $\phi g = \psi\chi\rho$ then we are done. This check follows from identities above $\phi g = \psi\pi g = \psi\chi\rho$. Thus we have naturality in both components, completely verifying this inclusion functor has a left adjoint, namely the abelianization functor.

3.3 Question 3

Let R be a ring. Show that R is a division ring if and only if all R-modules are free.

First we show that R being a division ring implies all of its R-modules are free. This proof follows identically as with the case for vector spaces. We consider an R-module M and let Σ be the collection of all linearly independent sets in M. If $M = 0$ then its trivially a free module, otherwise it has a nonzero element s and that element $\{s\}$ for a linearly independent set (if it were linearly dependent that would mean $\exists r \neq 0$ in R such that $rs = 0$, but r has an inverse and this means $s = r^{-1}rs = r^{-1}0 = 0$, a contradiction). Thus Σ is not empty and we proceed by checking the hypotheses of Zorn's lemma on Σ with the partial ordering given by inclusion. We see that for any chain we have that the union serves as an upper bound. To see that the union is linearly independent we show that for any finite subset of the union, the vectors are linearly independent, but there has to be some subset in the chain which contains all of the elements because of finiteness and thus we get they are linearly independent. Thus Zorn's lemma guarentees the existence of a maximally linearly independent set B. We check that B spans M. For an arbitrary nonzero $m \in M$ we cannot have that $B \cup \{m\}$ is linearly independent, otherwise we contradict the maximality of B. Thus there exists a finite subset of $C \subset B$ such $\sum_{b\in C} r_b b + rm = 0$ where $r \neq 0$ as B is linearly independent, and at least one of $r_b \neq 0$ as $m \neq 0$. We can rearrange and divide in the division ring to find $m = -\frac{1}{r}\sum_{b\in C} r_b b$, proving it is in the span of B, making B a basis and M a free module.

In the other direction, R being a division ring is equivalent to R having no nontrivial proper left ideals. The forward direction is clear, as all elements are invertible so any nontrivial ideal necessarily contains all of R. In the other direction, if there are no proper

ideals, for all nonzero elements $r \in R$, $Rr = R$ which means r has a left inverse, r' and that $Rr' = R$ and so r' has a left inverse, r'' but $r'' = r''r'r = r$ and so r is invertible and R a division ring. So let's assume R is not a division ring, and thus it does have a nontrivial proper left ideal, it must therefore have a nontrivial maximal left ideal I. Consider the left module $M = R/I$. It is simple since I is left maximal, but by hypothesis it has a basis $\{m_i\}$. By simplicity, we must have that $Rm_1 = M$ since there cannot be a submodule and $Rm_1 \neq 0$ as it is a free basis element. But $R \cong Rm_1 = M$, so R is a simple left module over itself and therefore has no nontrivial proper left ideals, which means it is a division ring.

3.4 Question 4

Working under the assumption these are to be treated as $\mathbb{Z}$-modules, i.e. Abelian groups.
(a) *Show that $\mathbb{Z}[\frac{1}{p}]/Z$ is an artinian module but not a noetherian module*

It is not Noetherian by considering the ascending chain $(1/p) \subset (1/p^2) \subset \ldots$. These chain does not stabilize. For Artinian, we note that every subgroup is finite and cyclic of the form $(1/n)$, where n is a positive interger. Thus to have a descending chain we would need $(1/n_1) \supset (1/n_2) \supset \ldots$ where $n_{i+1}|n_i$ thus producing a decreasing sequence which must terminate in finite steps, proving it is Artinian.

(b) *Show $\mathbb{Q}/\mathbb{Z}$ is neither Artinian nor Noetherian.*

It is not Noetherian by using the same example above, in fact, the above is subgroup so $\mathbb{Q}/\mathbb{Z}$ cannot be Noetherian, otherwise its subgroup would be. However, it is not Artinian either, we can construct the descending chain by successively removing all elements when written in reduced fraction form whose denominator is a multiple of p for all primes.

3.5 Question 5

Let K and L be quadratic field extensions of a field k. Prove that $K \otimes_k L$ is an integral domain if and only if the k-algebras K and L are not isomorphic.

For this whole problem I shall assume k is not characteristic 2. We know the quadratic extensions are separable and we can also say that $K = k[\alpha]$ and $L = k[\beta]$ where α is root of irreducible $x^2 - a$ and β is root of irreducible $x^2 - b$, where these polynomials are in k and by irreducible we mean irreducible over k. First we prove that if K and L are isomorphic then $K \otimes_k L$ is not an integral domain. Now if we have the isomorphism $f : K \to L$ as a k-algebra isomorphism then $f(\alpha)^2 = f(\alpha^2) = a$ and so $f(\alpha)$ is root of $x^2 - a$ in L. This means that when we tensor

$$K \otimes_k L = k[x]/(x^2 - a) \otimes_k L = L[x]/(x^2 - a) = L[x]/((x - f(\alpha))(x + f(\alpha)))$$

and thus this is not an integral domain. In the other direction, if we assume it is not an integral domain, then we again know that $K \otimes_k L = L[x]/(x - \gamma)(x + \gamma)$ because ID iff ideal is prime iff ideal is generated by irreducible. That is to say we have that $x^2 - a$ must

factor in $L[x]$. Now we note that γ generates a subfield of L isomorphic as a k-algebra to $k[x]/(x^2 - a)$. Both this and L have degree 2 over k, so L is isomorphic to $k(\gamma)$, the isomorphism is defined on generators by $\gamma \mapsto \alpha$. Since both γ and α square to a, this is a homomorphism, as one can check from the definitions. It is surjective since α generates K. Since it sends $q + r\gamma$ to $q + r\alpha$, and $q + r\alpha = 0$ if and only if $q, r = 0$ (since $1, \alpha$ is a basis for K over k), the kernel is trivial, so it's also injective.

3.6 Question 6

Let $K \subset L$ be subfields of $\mathbb{C}$ and let p be a prime. Assume K contains a non-trivial p-th root of unity. Show that L/K is a degree p Galois extension if and only if there is an element $a \in K$ that does not admit a p-th root, such that $L = K(\sqrt[p]{a})$.

This proof is due to AW. First suppose that L/K is a degree p Galois extension, thus it has Galois group C_p as p is prime. Thus we have that the automorphism group has a generator f. Take an element α in $L \setminus K$, and consider the sum $\beta = \sum \xi_p^k f^k(\alpha)$, where ξ_p is a primitive pth root of unity which is in K. Then we have that $f(\beta) = \xi^{-1}\beta$, and so the minimal polynomial of β over K has all of its conjugates as roots, but the conjugates are all $f^k(\beta) = \xi^{-k}\beta$, and thus the minimal polynomial is the pth degree polynomial $\prod(x - \xi^k\beta) \in K[x]$ and in particular the constant term $a = \prod \xi^k\beta = \beta^p \in K$. Thus we have an element not in K whose kth power is in K. And so $K(\beta)$ is a degree p extension that is contained in L and so it must be L. In the other direction, let $\beta = \sqrt[p]{a}$, then β is a root of the polynomial $x^p - a$ which splits over L as $\prod(x - \xi_p\beta)$, and thus L is a splitting field of a separable polynomial, which is equivalent to L being Galois. Now let m_β be the minimal polynomial for β over K which must be at least degree 2 (and less than or equal to p), and thus another one of its roots must be $\xi_p^k\beta$ $k \in \{1, \ldots, p-1\}$ as $m_\beta | (x^p - a)$. So one of the automorphisms of L over K takes β to $\xi_p^k\beta$. This would give this automorphism order p, and so $p \leq |G(L/K) = [L : K] = [K(\beta) : K] \leq p$ where the first inequality comes from what we just showed, the equalities come from Galois theorey, and the last inequality comes from the fact that the minimal polynomial divides a degree p polynomial. Thus equality holds and so $[L : K] = p$.

3.7 Question 7

Determine the ring endomorphisms of $F_2[t, t^{-1}]$, where t is an indeterminate.

An endomorphism ϕ of $\mathbb{F}_2[t, t^{-1}]$ is entirely determined by where t goes because ring homomorphisms are defined to take 0 to 0 and 1 to 1 and by ring homomorphism property, $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{F}_2[t, t^{-1}]$. However we are restricted to taking t only to invertible elements as t is itself invertible. Thus this question is equivalent to determining the units of $\mathbb{F}_2[t, t^{-1}]$. Lets consider the product of two arbitrary elements $(\alpha_{-n}t^{-n} + \ldots + \alpha_m t^m)(\beta_{-k}t^{-k} + \ldots + \beta_l t^l) = \alpha_{-n}\beta_{-k}t^{-n-k} + \ldots + \alpha_m\beta_l t^{m+l}$ where we've collected terms. Notice that there is a highest degree term and lowest degree

term, and there will always be such terms as long as at least one of the polynomials isn't a monomial. Thus for an element to be a unit in the Laurent ring it must be a monomial ut^k, where u is an invertible element in F_2 of which there is only one (pun noted, not intended). And so there is an endomorphism corresponding to every t^k for $k \in \mathbb{Z}$.

3.8 Question 8

Let G be a finite group of order pq, where p and q are distinct primes. Show that

(a)*G has a normal subgroup distinct from 1 and G.*

By Sylow theoems we have the group G whose order is pq has a normal subgroup. Let $p < q$ then we consider the q-Sylow subgroups of G. Let n_q denote how many there are. We know $n_q|p$ and $n_q = 1 \mod q$, but the divisors of p are 1 and p and $p < q$ so $p \neq 1 \mod q$, thus $n_q = 1$ so there is only one q-Sylow group and it must be normal because it is the unique subgroup of that order, since conjugates of a subgroup must be a subgroup of same order, so all the conjugates are equal, thus it is normal.

(b) *if $p \ncong 1 \pmod q$ and $q \ncong 1 \pmod p$, then G is abelian.*

By a similar proof we can see that the p-Sylow subgroup will also be normal. Call these normal subgroups P and Q. Note they have orders p and q and thus are trivially intersecting cyclic groups generated by x and y. As such $xyx^{-1} \in P$ by normality, and thus $xyx^{-1}y^{-1} \in P$ by closure of the subgroup p, and similarly $xy^{-1}x^{-1} \in Q$ by normality, and thus $xyx^{-1}y^{-1} \in Q$ and so it is in $P \cap Q$ and thus it is the identity and so $xy = yx$ and thus all elements commute, so the group is abelian.

3.9 Question 10

Let E, M and F be finite abelian groups and consider group homomorphisms $E \xrightarrow{f} M \xrightarrow{g} F$. Assume g is injective. Show that $|Coker(g \circ f)| = |Coker(g)| \cdot |Coker(f)|$ where $|X|$ denotes the order of a finite set X.

Recall that in the category of Abelian Groups, that the cokernel of a morphism $\phi : G \to H$ is defined as $\text{Coker}(\phi) = H/\text{Im}(\phi)$. As such, we have that $\text{Coker}(g \circ f) = F/\text{Im}(g \circ f), \text{Coker}(g) = F/\text{Im}(g), \text{Coker}(f) = M/\text{Im}(f)$. As $g : M \to F$ is injective, we have that $|\text{Im}(g)| = |M|$, thus $|\text{Coker}(g)| = |F|/|M|$, thus $|\text{Coker}(f)||\text{Coker}(g)| = |F|/|\text{Im}(f)|$. Again due to g being injective, we have that $|\text{Im}(g \circ f)| = |g(\text{Im}(f))| = |\text{Im}(f)|$. So we get the desired result that $|\text{Coker}(g \circ f)| = |\text{Coker}(g)||\text{Coker}(f)|$.

4 Fall 2014

4.1 Question 1

Let G be a finite group. Let $\mathbb{Z}[G]$ be the group algebra of G with augmentation ideal I. Show that $I/I^2 \cong G/G'$ as abelian groups for the derived group G' of G.

Let G be a finite group and $\mathbb{Z}[G]$ the group ring over the integers. Let I be the augmentation ideal. Prove that I/I^2 is isomorphic (as an additive abelian group) to the abelianization $G/[G,G]$. Recall the definition of the augmentation ideal and that set of elements of the form $g-1$ generate it. Notice though that multiplying any two of the generators kills it in the quotient ideal since I^2 is generated by all elements of the form $(g-1)(h-1)$. Also note that in I/I^2 we have that $(g-1)+(h-1) = gh-1 \mod I^2$ because $g-1+h-1-(gh-1) = -gh+g+h-1 = -(g-1)(h-1) \in I^2$.

Consider the homomorphism $f : G \to I/I^2$ where $f(g) = g-1+I^2$. To see it's a homomorphism of groups check $f(gh) = gh-1+I^2 = (g-1)+(h-1)+I^2 = f(g)+f(h)$, representing the group G's binary operation just as gh but the addition group I/I^2's operation using $+$. We check that $G' = [G,G]$ is in the kernel,

$$\begin{aligned} f(ghg^{-1}h^{-1}) &= ghg^{-1}h^{-1} - 1 + I^2 = (gh)(g^{-1}h^{-1}) - 1 + I^2 \\ &= (gh-1) + ((g^{-1}h^{-1}) - 1) + I^2 \\ &= (g-1) + (h-1) + (g^{-1}-1) + (h^{-1}-1) + I^2 \\ &= (g-1) + (g^{-1}-1) + (h-1) + (h^{-1}-1) + I^2 \\ &= (gg^{-1}-1) + (hh^{-1}-1) + I^2 = (1-1) + (1-1) + I^2 \\ &= 0 + I^2. \end{aligned} \tag{1}$$

We knew this had to be true, because I/I^2 is abelian (since it is the additive group structure we care about) and any homomorphism to an abelian group factors through the abelianization, but it's good to check explicitly. As f factors through the abelianization we get a well defined map $\phi : G/G' \to I/I^2$. This map is surjective as every element in I/I^2 is of the form $\sum_g a_g(g-1)+I^2$ and thus has a pre-image of $\prod_g g^{a_g}G'$ (the order of the product does not matter as we are now in the abelianization) which is verified by $\phi(\prod_g g^{a_g}G') = \sum_g a_g\phi(g) = \sum_g a_g(g-1)+I^2$.

Thus we ϕ induced a group homomorphism from G/G' to I/I^2 which we prove is an isomorphsim by giving an inverse. In the other direction define a homomorphism $g : I \to G/G'$ by taking $g(\sum_g a_g(g-1)) = \prod_g g^{a_g}G'$ which is well defined because the multiplicative ordering in G/G' is arbitrary as the group is abelian. To see that I^2 is in the kernel we check its generators are: $g((h-1)(g-1)) = g(hg-h-g+1) = g((hg-1)-(h-1)-(g-1)) = hgh^{-1}g^{-1}G' = G'$. Thus we get an induced map $\psi : I/I^2 \to G/G'$. We check they are inverses $\psi(\phi(gG')) = \psi(g-1+I^2) = gG'$ and $\phi(\psi(g-1+I^2)) = \phi(gG') = g+I^2$. Thus we have the desired isomorphism.

4.2 Question 2

Let $\mathbb{F}_p$ denote the finite field of p elements. Consider the covariant functor F from the category of commutative $\mathbb{F}_p$-algebras with a multiplicative identity to abelian groups sending a ring R to its p-th roots of unity, that is, $F(R) = \zeta \in R | \zeta^p = 1$. Answer the following questions and justify your answers.[1]

(a) *Give an example of a finite local ring R such that $F(R)$ has p^2 elements.*

In a field of characteristic p, the pth roots of unity are solutions to $x^p - 1$ which has, as this is a field, *at most* p roots. In fact though, $x^p - 1 = x^p - 1^p = (x-1)^p$ and thus this polynomial has repeated roots and 1 is the only pth root of unity in any field of characteristic p, thus fields are clearly the wrong place to look. There are two usual sources for $\mathbb{F}_p$ algebras, matrices and polynomials, in this case we find polynomials over $\mathbb{F}_p$ to be good. As we desire a finite algebra which is not a field, we must have that $\mathbb{F}_p[x]$ be quotiented by an ideal generated by a non-irreducible polynomial. We use x^3 (the reason for which becomes apparent soon), which turns it into $\mathbb{F}_p[x]/(x^3) = \{a_0 + a_1 x + a_2 x^2 | a_i \in \mathbb{F}_p\}$ a finite algebra. Note that (x) is the unique maximal ideal, as its complement are polynomials with nonzero constant term which are invertible

$$(a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 = 1$$

which can be solved for $b_i \in \mathbb{F}_p$ iff $a_0 \neq 0$. Thus this ring is local too. Now we need to check it has p^2 $p^t h$ roots of unity:

$$(a_0 + a_1 x + a_2 x^2)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} = a_0^p = a_0 = 1.$$

Thus the pth roots of unity are all polynomials with constant term 1, as the linear and quadratic term can be chosen arbitrarily. This justifies the use of x^3 and also why we needed $p > 2$ otherwise, we would be left with $(a_0 + a_1 x + a_2 x^2)^p = a_0 + a_1 x^2 = 1$ which forces a_1 to be zero, meaning it only had p roots.

(b) *Let $Aut(F)$ be the set of natural transformations of F into itself inducing a group automorphism of $F(A)$ for all commutative rings A with identity. Prove that F is representable and use the Yoneda Lemma to compute the order of $Aut(F)$.*

As with most questions regarding representable functors of this nature, we want to find an $\mathbb{F}_p$-algebra which has an element that can pick out the elements from other $\mathbb{F}_p$-algebra satisfying our conditions, in this case, they must be pth roots. Thus we are led to $A = \mathbb{F}_p[x]/(x^p - 1)$. An algebra homomorphsim from A any other $\mathbb{F}_p$ algebra is entirely determined by where x goes as everything else is determined by linearity. The restriction though is that x must go to something whose p-th power is 1 as $\phi : A \to R$, in which $\phi(x)^p = \phi(x^p) = \phi(1) = 1$. As the functor is representable, the Yoneda lemma provides a simple characterization of the natural transformation of the functor

[1] Throughout we assume p is meant to be an odd prime.

to itself, by way of homomorphisms from A to itself and natural isomoprhisms corresponding to automorphisms of A. To simplify, we note that as $x^p - 1 = (x-1)^p$ that $A \cong \mathbb{F}[x]/(x^p) = B$. Now we need consider automorphism on B. As before a homomorphism is determined by where x goes and it must go to p-nilpotent elements of B, of which there are $p^(p-1)$. To be an automorphism though, a homomorphism must be invertible. Let $\phi(x) = a_1x + \ldots + a_{p-1}x^{p-1}$ and attempt to construct its inverse $\psi(x) = b_1x + \ldots + b_{p-1}x^{p-1}$, then $x = \psi(\phi(x)) = \psi(a_1x + \ldots + a_{p-1}x^{p-1}) = a_1\psi(x) + \ldots + a_{p-1}\psi(x)^{p-1} = a_1(b_1x + \ldots + b_{p-1}x^{p-1}) + a_2(b_1x + \ldots + b_{p-1}x^{p-1})^2 + \ldots a_{p-1}(b_1x + \ldots + b_{p-1}x^{p-1})^{p-1} = a_1b_1x + O(x^2)$ and so we are required that $a_1 \neq 0$. This is the only restriction and so we have $(p-1)p^{p-2}$ automorphisms of B and thus $(p-1)p^{p-2}$ automorphism of A and thus $(p-1)p^{p-2}$ natural automorphism of the functor F.

4.3 Question 3

Pick a non-zero rational number x. Determine all possibilities for the Galois group G of the normal closure of $\mathbb{Q}[\sqrt[4]{x}]$ over $\mathbb{Q}$, where $\sqrt[4]{x}$ is the root of $X^4 - x$ with maximal degree over $\mathbb{Q}$.

The polynomial $X^4 - x$ factors over $\mathbb{C}$ as $(X-\alpha)(X-i\alpha)(X+\alpha)(X+i\alpha)$. If $x = 0$ which makes $\alpha = 0$, we will have the trivial Galois group. If not, then as $X^4 - x$ cannot factor completely over $\mathbb{Q}$ since we have complex roots, we get a nontrivial Galois group. Another possibility is that it factors partially. One possibility is as $(x-\alpha)(x+\alpha)(x^2+\alpha^2)$ where this is a quadratic extension and the Galois group is C_2. The second possibility is as $(x^2 + ax + a^2/2)(x^2 - ax + a^2/2)$, the product of two quadratics with the same discriminant, meaning the Galois group is C_2. The third possibility is that we factor as $(x^2 - \alpha^2)(x^2 + \alpha^2)$. As the discriminant of the two quadratics differs by a negative sign, we have that the Galois group is the Klein 4 group. These are the only possibilities of the polynomial being reducible, so we now consider the case when $X^4 - x$ is fully irreducible. The resolvent of the quartic is $X^3 + 4xX = X(X^2 + 4x)$. If x is the some negative square, i.e. $x = -c^2$ then the resolvent factors completely as $X(X+2c)(X-2c)$ and so we have the Klein 4-group again. Supposing we are not in this case we will need the discriminant which is $D = -256x^3$. As $X^2 + 4x$ remains irreducible in $\mathbb{Q}(\sqrt{D})$, we have the Galois group is D_8 the dihedral group of order 8. These are all possibilities. See section 14.6 of Dummit and Foote for greater detail about finding Galois groups for quartics and for derivation of the resolvent and discriminant.

4.4 Question 4

Let D be a 9-dimensional central division algebra over $\mathbb{Q}$ and $K \subset D$ be a field extension of $\mathbb{Q}$ of degree > 1. Show that $K \otimes_{\mathbb{Q}} K$ is not a field and deduce that $D \otimes_{\mathbb{Q}} K$ is no longer a division algebra.

We have the K is a proper field extension of $\mathbb{Q}$ of finite degree. Since we are over $\mathbb{Q}$

this must be a simple extension $K \cong Q[x]/(f(x))$ for an irreducible $f(x) \in Q[x]$, where K has a root α of f. However $K \otimes K \cong K \otimes Q[x]/(f(x)) \cong K[x]/(f(x))$. This is not a field because $f(x)$ is reducible in $K[x]$, i.e. $f(x) = (x-\alpha)g(x) \in K[x]$ where $(x-\alpha)$ and $g(x)$ are coprime so $K[x]/(f(x)) \cong K[x]/(x-\alpha) \times K[x]/(g(x))$ by the Chinese Remainder Theorem. So we can check this is not an integral domain as $(1,0)\cdot(0,1) = (0,0)$. Put another way, the ideal $(f(x))$ is not prime $K[X]$ and as such the quotient by it has zero divisors, name $(x-\alpha)g(x) = 0$ in $K[x]/(f(x))$. Thus this tensor product is not a field. The second part follows from $D \otimes K$ contain $K \otimes K$ which isn't a domain, so it cannot be a division algebra (there can be no invertible zero divisors).

4.5 Question 5

Let R be a commutative algebra over $\mathbb{Q}$ of finite dimension n. Let $\rho : R \to M_n(\mathbb{Q})$ be the regular representation, and define Tr: $R \to \mathbb{Q}$ by the matrix trace of ρ. If the pairing $(x,y) = Tr(xy)$ is non-degenerate on R, prove that R is semi-simple.

We proceed by induction on the dimension. The base case $k = 1$ is trivial as R would be simple and thus semi-simple. Assume it is true for all dimensions $k < n$. Let R be an n dimensional commutative algebra over $\mathbb{Q}$. It is Artinian. If R is simple then we are done, if not then there is a nontrivial minimal ideal I (R is commutative so ideals are all two-sided). As I is minimal it is simple. Now we consider its complement with respect to the bilinear form $I' = \{y \in R | \forall x \in I \langle y, x\rangle = 0\}$. We can check this is an ideal: $y, y' \in I'$ then $\forall x \in A$ we have $< y+y', x >= Tr((y+y')x) = Tr(yx) + Tr(y'x) = 0$, similarly $r \in R, y \in I'$ we have $\forall x \in A$ have $< ry, x >= Tr(ryx) = Tr(yxr) = 0$ because $xr \in I$ as I is an ideal. By non-degeneracy, $I' \neq R$. Now we want to show that, $I \cap I' = 0$, in which case we get that the bilinear form restricted to I and I' is non-degenerate and that $R = I \oplus I'$, which proves R is semisimple by the inductive hypothesis as both I, I' are proper and thus have strictly smaller dimension.

By minimality, I^2 is either 0 or I. Suppose it is 0 then all elements in I are nilpotent and nilpotent elements have zero trace. Thus, for any $x \in I$ and for any $r \in R$, we have $rx \in I$ which makes it nilpotent. But this would mean that $\forall r \in R, \langle r, x\rangle = Tr(rx) = 0$, contradicting non-degeneracy and nontriviality of I. So we have $I^2 = I$ Again by minimality $I' \cap I$ is 0 or $I \subset I'$. In the latter case we can take $x \in I$ and $r \in R$ then $\langle r, x\rangle = \langle r'r'', x\rangle = \langle r', r''x\rangle = 0$ as $r''x \in I \subset I'$ again contradicting nondegeneracy. Thus we have $I \cap I' = 0$. Now to see $R = I + I'$ we check dimensions. As R is finite dimension, it has the same dimension as its dual, and because the form is non-degenerate we get that it is an isomorphism $\phi : r \mapsto \langle r, -\rangle$. We have that $\phi(I') = I^0$ (the symbol superscript 0 in this notation indicated the annihilator of a subset of a vector space), this can be checked, $y \in I'$ maps to $\langle y, -\rangle$ which by definition annihilates all of I. As it is an isomorphism, every annihilator has a unique pre-image, so $r \in R$ such that $\langle r, -\rangle$ annihilates I but this is the definition of $r \in I'$. So we have $\dim(I') = \dim(I^0)$ and so $\dim(R) = \dim(I) + \dim(I^0) = \dim(I) + \dim(I')$ showing that $R = I \oplus I'$. Now to see

both I and I' inherit the form in a non-degenerate way: take $x \in I$ and suppose that $\langle x, x' \rangle = 0$ for all $x' \in I$ then $x \in I'$ which shows it is 0 because $I \cap I' = 0$ we have I' is non-degenerate which makes it semisimple. Let $y \in I'$, by nondegeneracy over R, there exists $r \in R$ such that $\langle y, r \rangle \neq 0$ but $r = x' + y'$ where $x' \in I$ and $y' \in I'$ and so we get $0 \neq \langle y, r \rangle = \langle y, x' + y' \rangle = \langle y, x' \rangle + \langle y, y' \rangle = \langle y, y' \rangle$ and so I' is nondegenerate, and thus semisimple. This proves the assertion that R is semisimple.

An alternate proof uses the result from Fall 2015, Question 9a, where it was shown that the elements of the Jacobson radical of a finite dimensional algebra over a field are nilpotent. Thus take $x \in J(R)$ and for any $r \in R$ we have that $xr \in J(R)$ and is consequently nilpotent which means it has trace zero, thus $\langle x, r \rangle = Tr(xr) = 0$ and by non-degeneracy we have $x = 0$. So $J(R) = 0$ which is another characterization of R being semisimple.

4.6 Question 6

Let G be a finite group and let p be the smallest prime number dividing the order of G. Assume G has a normal subgroup H of order p. Show that H is contained in the center of G.

Let G be a group of order n and let p be the smallest prime dividing n. Suppose there exists a normal subgroup $H \trianglelefteq G$ of order p. Let G act on the elements of H by conjugation, $g(h) = ghg^{-1} \in H \ \forall g \in G, h \in H$ since H is normal and $f(g(h)) = f(ghg^{-1}) = fghg^{-1}f^{-1} = fgh(fg)^{-1} = fg(h)$. Now we know that the identity is in its own orbit because $g1g^{-1} = 1$ for all g. Consider the orbit of any non-identity element $x \in H$, it's orbit can be of size 1 to $p - 1$. By Orbit-Stabilizer, we have that $|Orb(x)| = |G/Stab(x)|$ where $Stab(x) = C_G(x)$ the centralizers of x, so the size of the orbit must divide G, but p was the smallest prime dividing $|G|$ so the only smaller integer dividing G is 1, so the orbits of all the elements $x \in H$ are of size one, which means all the elements are central, i.e. $gxg^{-1} = x$ for all $g \in G$, so H is contained in the center of G.

4.7 Question 7

Let G be a finite group and P a Sylow 2-subgroup of G. Assume P is cyclic, generated by an element x. Show that the signature of the permutation of G given by $g \mapsto xg$ is 1. Deduce that G has a non-trivial quotient of order 2. Let $|P| = 2^n$, then $|G| = 2^n m$ where $2 \nmid m$, i.e. m is odd. We also have $P = \langle x \rangle = \{1, x, \ldots, x^{2^n - 1}\}$ where $|x| = 2^n$. We're considering the action of G on itself by left multiplication, specifically looking at the permutation signature of x. Start with some $g \in G$, we know $g, x, \ldots, x^{2^n - 1}g$ are distinct as $x^m g = x^l g$ implies $x^{m-l} = 1$ which is not true for $0 \leq l < m \leq 2^n - 1$ and that acting by x once more would go back to g as $xx^{2^n - 1}g = x^{2^n}g = 1g = g$. This forms a 2^n cycle in the permutation by x. Taking some h not in this cycle above, we see that $h, xh, \ldots, x^{2^n - 1}h$ is disjoint from the cycle above because $x^m h = x^l g$ implies $h = x^{\bar{l-m}}g$ where $l \bar{-} m$ is

least positive integer equivalent to $l - m$ modolu 2^n and this would imply h was in the list above–a contradiction. Continuing this way, we see that x consists of m disjoint 2^n cycles. A 2^n cycle has signature -1 and taking an m products of such cycles, where m is odd, implies that x has signature -1. This means the map from composition homomorphism from G to S_G to $C_2 = \{1, -1\}$ is surjective, and so by the isomorphism theorems, G has a quotient isomorphic to C_2, i.e. a nontrivial quotient of order 2.

4.8 Question 8

Let A be a ring. Assume there is an infinite chain of left ideals $I_0 \subset I_1 \subset \ldots \subset A$ with $I_i \neq I_{i+1}$ for $i \geq 0$. Show that A has a left ideal that is not finitely generated as a left A-module.

This problem is just about the equivalence of definitions for a Noetherian ring. We consider two proofs which are really the same. First, suppose to the contrary that there were no infinitely generated ideals. Then we would have the ideal $J = \bigcup I_i$ (J has the properties of an ideal, any two elements in it will both belong to some I_j and thus can be added, the multiplication property similarly holds) is finitely generated by some $\{x_1, \ldots, x_k\}$, thus $(x_1, \ldots, x_k) = J$, but each must belong to some I_i in the chain, and since it is an ascending chain and there are only k of them, there exists some I_N that contains all of them and so $J = (x_1, \ldots, x_k) \subset I_N \subset J$ and so $I_{N'} = I_N$ for all $N' \geq N$, contradicting the hypothesis that the chain does not stabilize. This proof by contradiction only gives existence, but it inspires the second proof which builds an infinitely generated ideal from the chain. Let $x_1 \in I_1$ and $x_j \in I_j - I_{j-1}$ (which we can do because each inclusion in the hypothesis is strict). Let $I = (x_j)_{j \in \mathbb{N}}$. Claim: I is not finitely generated. Suppose it were, that is $\exists S = \{s_1, \ldots, s_k\}$ such that $I = (S)$. Then $S \subset I$ and so $s_i \sum_j^{n_i} a_j x_j$ (elements of ideals generated by infinite sets are still only finite sums). Let $n = \max(n_i)$, then $S \subset I_n$ and so $I \subset (S) \subset I_n$. But $x_{n+1} \in I$ cannot be in I_n by construction and so we have a contradiction.

4.9 Question 9

Let A be a ring and let $i, j \in A$ such that $i^2 = i$ and $j^2 = j$. Show that the left A-modules Ai and Aj are isomorphic if and only if there are $a, b \in A$ such that $i = ab$ and $j = ba$.

This solution is direct from ATL and BL. In one direction, suppose there exists $a, b \in A$ such that $i = ab$ and $j = ba$, let's try to construct an A-module isomorphism ϕ between Ai and Aj. A good guess leads us to trying $\phi(i) = aj$ and extending linearly. That is $\phi(ri) = r\phi(i) = raj$ for all $r \in A$ and $\phi(ri + r'i) = \phi((r + r')i) = (r + r')aj = raj + r'aj = \phi(ri) + \phi(r'i)$. Now we note that $aj = \phi(i) = \phi(ii) = i\phi(i) = iaj$, which is fine as $iaj = (ab)aj = a(ba)j = ajj = aj$. Is this an injection? Suppose $\phi(ci) = \phi(c'i)$, then we have $caj = c'aj$. Multiplying on the right by b gives us $c'i = c'ii = c'abab = c'ajb = cajb = cabab = cii = ci$, so yes it is injective. Is it surjective? For all $rj \in Aj$, we have

that $\phi(rbi) = rbaj = rjj = rj$, so it is in fact an isomorphism.

In the reverse direction, we have an isomorphism, let's have $\phi : Ai \to Aj$ and ψ is its inverse isomorphism. We have that $\phi(i) = cj$ and $\psi(j) = di$ for some $c, d \in A$. By A-module morphism properties, $\phi(i) = \phi(ii) = icj$ and similarly $\psi(j) = jdi$. Let $a = icj$ and $b = jdi$. We have that$i = \psi(\phi(i)) = \psi(icj) = ic\psi(j) = icjdi = icjjdi = ab$ and similarly $j = \phi(\psi(j)) = \phi(jdi) = jdi\phi(i) = jdicj = jdiicj = ba$.

4.10 Question 10

Let n be a positive integer. Let A_n be the $\mathbb{Q}$-algebra generated by elements $x_1, \ldots, x_n, y_1, ..., y_n$ with relations $x_i x_j = x_j x_i$, $y_i y_j = y_j y_i$ and $y_i x_j - x_j y_i = \delta_{ij}$ for $1 \leq i, j \leq n$. Show that there is a representation of A_n on the vector space $\mathbb{Q}[t_1, \ldots, t_n]$ where x_i acts by multiplication by t_i and y_i acts as $\frac{\partial}{\partial t_i}$.

See Spring 2016 Question 5 for the $n = 1$ version of the question which extends in the natural mutlivariable calculus way.