Algebra Qualifying Exam Solutions

Fall 2016 - Spring 2019

Yizhou Chen

Preface:

This is a little solution manual of the 6 most recent past algebra quals I have written up. If you want to see the problems, you can find them on the our math department website. If you are interested in older problems and their solutions, two other graduate students Ian Coley and Yacoub Kureh have put their solutions on the internet. These solutions are made possible by the help and support of my dear friends and colleagues Liao Wang, Weiyi Liu, Yudong Qiu, and other algebra enthusiasts on Stackexchange. I have attached some links as references. If you find them incomplete or want to add some other resources, please let me know. Sometime I tend to explain things in a fast and confusing manner. So please don't hesitate to contact me when you find some ideas baffling or questionable. Good luck to all who reasons in an algebraic way!

Useful Links:

Past Exams:
`https://secure.math.ucla.edu/gradquals/hbquals.php`
Ian's Solutions:
`https://www.math.ucla.edu/~iacoley/hw/algqual.pdf`
Yacoub's Solutions:
`https://www.math.ucla.edu/~ykureh/Algebra_Qualifying__Quals__Exams_Solutions.pdf`

Department of Mathematics
University of California, Los Angeles
U.S

Fall 2016:

Solution 1. That's just free product of two copies of $\mathbb{Z}/2$

■

Solution 2. I will just calculate the normalizers by brute force.
So let $\{1, x\}$ be a basis of K over $\mathbb{Q}$. We have a relation $x^2 + ax + b = 0, a, b \in \mathbb{Q}$. Let M be an element of the normalizer. Suppose

$$M : 1 \mapsto u_1 + u_2 x$$

$$x \mapsto u_3 + u_4 x$$

It must commute with the operation of multiplying with x. Thus the following two maps must have the same result:

$$1 \overset{M}{\mapsto} u_1 + u_2 x \overset{\cdot x}{\mapsto} u_1 x - a u_2 x - u_2 b$$

$$1 \overset{\cdot x}{\mapsto} x \overset{M}{\mapsto} u_3 + u_4 x$$

Thus we must have $u_3 + u_4 x = (u_1 - a u_2)x - b u_2 \Rightarrow u_3 = u_1 - a u_2, u_4 = -b u_2$. But then M acting on x would be exactly multiplying x with $u_1 + u_2 x$. Thus $M \in \rho(K^\times) \Rightarrow$ the index is 1.

■

Solution 3. This solution may be an overkill.
Lemma: Let M be A module. Then M is projective if and only if $\exists \{m_i\}_i \subset M$ and $f_i : M \to A$ homomorphism of A-module such that $\Sigma_i f_i(m) m_i$ makes sense and $\Sigma_i f_i(m) m_i = m, \forall m \in M$.
Proof: First we can take $\{m_i\}$ a set of generators of M. Then there is map $g : F \to M$ such that $e_i \mapsto m_i$ where F is a free module and $\{e_i\}$ is a set of basis of F. Then M is projective if and only if $\exists f : M \to F$ such that $gf = id$. Notice the data of this f is exactly $f_j : M \to A$ given by $m_i \mapsto a_{ij}$ where $f(m_i) = \Sigma_j a_{ij} e_j$. Thus the existence of f and the existence of the described $\{f_j\}$ are equivalent.
$\Leftarrow$: Now we know $\mathfrak{a}\mathfrak{b} = A \Rightarrow \exists a_1, ...a_n \in \mathfrak{a}, b_1, ...b_n \in \mathfrak{b}$ such that $\Sigma a_i b_i = 1$. We know that $\forall a \in \mathfrak{a}, b \in \mathfrak{b}, a\mathfrak{b} \subset \mathfrak{a}\mathfrak{b} = A \Rightarrow ab \in A$. Thus $\forall x \in \mathfrak{a}, x = x(\Sigma a_i b_i) = \Sigma(b_i x) a_i \Rightarrow \mathfrak{a} = (a_1, ...a_n)$ as A-module hence finitely generated. For the projectiveness we use the lemma and define $f_j : \mathfrak{a} \to A$ given by $a \mapsto a_j b_j a$ which makes sense since $a_i b_i \in A$.
$\Rightarrow$: Let $\mathfrak{a}$ be generated by $a_1, ...a_n$. By the lemma we have $f_j : \mathfrak{a} \to A$ such that $\Sigma_j f_j(a_i) = a_i$. Let $f_j(a_i) = a_{i,j}$. Define $\mathfrak{b}$ be the submodule of K generated by $\{\frac{a_{i,j}}{a_i a_j}\}_j$. Then we are done.

■

Reference: http://www.math.uchicago.edu/$\sim$ may/MISC/Dedekind.pdf

Solution 4 (Stackexchange). Let the group be $\langle r, s, r^p = s^2 = 1, srs = r^{-1}\rangle$. There 2 kinds of 1 dim complex representations as below:

$$r \mapsto 1, s \mapsto \pm 1$$

There are $\frac{2p-2}{4}$ different kinds of 2 dimensional representations as shown below:

$$r \mapsto \begin{pmatrix} cos\frac{2\pi k}{p} & -sin\frac{2\pi k}{p} \\ sin\frac{2\pi k}{p} & cos\frac{2\pi k}{p} \end{pmatrix}, s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $k \in \mathbb{Z}$, $\frac{2p-2}{4} \geq k \geq 1$. You can check to see if the dimension is right.

■

Solution 5. By the fundamental theorem of Galois theory, it suffices to find a subgroup of $Gal(K/F)$ of order p. This is guaranteed by the generalized first Sylow theorem, since $p|[K : F]$

■

Solution 6. $\forall y \in \mathbb{F}_p, (x + y)^p - a = x^p - a \Rightarrow$ If x_0 is a root of the given polynomial, then $x_0 + y$ is also a root.

■

Solution 7. Suppose for contradiction that $\exists\zeta$ primitive nth root of unity such that $2^{\frac{1}{4}} \in \mathbb{Q}(\zeta)$. Then we consider $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(2^{\frac{1}{4}})) \subset Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, the latter of which is cyclic. So the first group is normal subgroup of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. By the fundamental theorem of Galois theory, $\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}$ is Galois extension. Now we have contradiction because $x^4 - 2$ have root over $\mathbb{Q}(2^{\frac{1}{4}})$ but does not split.

■

Solution 8. Let the left adjoint of F be G. Let $\{*\}$ be the set of one object. Then we know for $B \in Ob(\mathcal{C}), FB = Mor_{Sets}(\{*\}, FB) = Mor_{\mathcal{C}}(G\{*\}, B) \Rightarrow F = Mor_{\mathcal{C}}(G\{*\}, \_)$

■

Solution 9. The functor is given by $Mor_{F-commalg}(F[X,Y]/(XY - 1), \_)$

■

Solution 10 (by Qiu). Consider B as a A-mod by left multiplication. Then A simple $\Rightarrow B$ is semisimple as A-mod. We have the following lemma:
Lemma: A has only one isomorphism class of simple module.
Proof: Since A is of finite dimensional hence artinian, we can take I, a minimal left ideal of A. $\forall a \in A, Ia$ is a left ideal of A. By the minimality of I the map $I \to Ia$ given by $x \mapsto xa$ is isomorphism or 0 map. Now by the simpleness of A (no two sided ideals) we have $A = IA = \Sigma_{a\in A} Ia$. Thus A as a A-module must be a sum of copies of I's. Any simple module of A as a quotient of A must be isomorphic to I.
Now back to the problem, let $B = I^k, A = I^n$. We consider B as a A, A bimodule. Then we have $B = B \otimes_A A = B \otimes_A (I^n) = (B \otimes_A I)^n$. Let $B \otimes_A I = I^l$ then $B = (I^n)^l = A^l$ as A-module. Thus $dim_F(A)|dim_F(B)$

■

Spring 2017:

Solution 1. There are three cases:
1. We have multiples of I, the identity matrix.
2. We have matrices which look like $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$.
3. The last case we must have characteristic polynomial and minimal polynomial are the same. So you can write out the rational canonical form (or companion matrix?) which look like $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ such that the polynomial $x^2 + ax + b$ does not have multiple roots.

■

Solution 2. There are five conjugacy classes in this group: $|\langle 1 \rangle| = 1, |\langle y \rangle| = 4, |\langle x \rangle| = |\langle x^2 \rangle| = |\langle x^3 \rangle| = 5$. So we want to fill out the following chart:

G	$\langle 1 \rangle, 1$	$\langle y \rangle, 4$	$\langle x \rangle, 5$	$\langle x^2 \rangle, 5$	$\langle x^3 \rangle, 5$
χ_1	1	1	1	1	1

Let's start by calculating the one dimensional representations. Let ζ, ξ be primitive 4th, 5th root of unity respectively. Suppose ϕ is a one dimensional representation. Then $\phi(y) = \phi(y^2) \Rightarrow \phi(y) = 1$ or 0. But $y^5 v = 1 \Rightarrow \phi(y) = 1$. But we can have $\phi(x) = \zeta^i, i \in \mathbb{Z}$. So we can have some extra rows. Use Schur's orthogonality (mentioned in the second to last solution in this whole set) we know that all other entries for $\langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle$ are 0. By the first Schur's orthogonality we know that there is only one row left starting with 4. So below is our chart:

G	$\langle 1 \rangle, 1$	$\langle y \rangle, 4$	$\langle x \rangle, 5$	$\langle x^2 \rangle, 5$	$\langle x^3 \rangle, 5$
χ_1	1	1	1	1	1
χ_2	1	1	i	-1	$-i$
χ_3	1	1	$-i$	-1	i
χ_4	1	1	-1	1	-1
χ_5	4	-1	0	0	0

■

Solution 3. One way of doing this is that suppose $H \subset F_2$ a subgroup of index 3. Then F_2 acting on the left cosets gives us a map $F_2 \to S_3$. The map is uniquely determined by

the image of u, v. So there are in total 36 possible maps. Notice the map correspond to a previous subgroup if and only if its image is a transitive subgroup. So we have 26 choice left. Notice if you have cosets $H.xH.yH; H, yH, xH$ correspond to the same subgroup H but the second order correspond to a different map. So our answer would be to divide 26 by 2, which gives us 13.
Another way of thinking about this problem is to use algebraic topology. You have to consider possible choices of 3 sheeted coverings of two circles wedged together. Namely, if you have three points and 2 lines connecting each pair of two, what orientation can you put on the lines under certain rules?

$\blacksquare$

Solution 4. I am not so good with Dedekind domains. So feel free to ignore what I will say. One characterisation of Dedekind domain is noetherian integrally closed domain of Krull dimension 1. Noetherianness is easy. Krull dimension 1 is by Krull's Hauptidealsatz. Domain because of the irreducibility of the polynomial. The only thing left is the integrally closedness. A noetherian domain is integrally closed if and only if the ring is intersection of all its localization at prime ideals of height 1 and all the previous localizations are discrete valuation rings. The first condition is easy, because as long as the denominator is nonunit, you can include it in a maximal ideal. The second condition, a DVR is the same as a local PID. height 1 restricts to the number of generator to 1. So we are good.

$\blacksquare$

Solution 5. This is elementary algebraic geometry. You can do it.

$\blacksquare$

Solution 6. Let $\{x_1, ...x_n\}$ be a set of generators of M over R with minimal cardinality. Then we want to reduce its cardinality. Take $u \in M$, since $M = JM$, we have $u = \Sigma_s j_s u_s$ for $u_s \in M, j_s \in J$. Then we can write $u_s = \Sigma_l r_{s,l} x_l$. By the fact that the Jacobson radical is two sided, we have $u = \Sigma_s k_s x_s$ for $k_s \in J$. Now replace u with x_1 we have $(1 - k_1)x_1 = \Sigma_{s>1} j_s x_s$. Now by the characterisation $J = \{r \in R, 1 + xr \in R^\times, \forall x \in R\}$, we have $1 - x_1 \in R^\times \Rightarrow x_1 \in Rx_2 + ...Rx_n \Rightarrow$ contradiction to the minimality of the previous set of generator.

$\blacksquare$

Solution 7. The roots of the polynomial are $\zeta \cdot ^3\sqrt{2} \pm \sqrt{3}$ where ζ is the third root of unity. So $K = \mathbb{Q}(\zeta, ^3\sqrt{2}, \sqrt{3}) = \mathbb{Q}(i, ^3\sqrt{2}, \sqrt{3}) \Rightarrow [K : \mathbb{Q}] = 12$

$\blacksquare$

Solution 8. The functor is representable, it is $Mor_{Rings^{op}}(End_{\mathbb{Z}}(M), \_)$

$\blacksquare$

Solution 9. The maps $f : R^n \to R^m, g : R^m \to R^n$ that are inverses of each other correspond to matrices A, B with entries in R such that $AB = I_m, BA = I_n$. You can construct right module maps with the same matrices. Thus they are isomorphic as right R modules.

■

Solution 10. The automorphism of K^H over F still extends to K, so our answer would be $Gal(K^H/F) = N_H(G)/H$

■

Fall 2017:

Solution 1. So we have $S \subset C_G(X) \Rightarrow gSg^{-1} \subset C_G(gXg^{-1}) = C_G(Y)$. Also we have $S \subset C_G(Y)$. S, gSg^{-1} are Sylow subgroups of $C_G(Y)$. Thus $\exists a \in C_G(Y), aSa^{-1} = gSg^{-1} \Rightarrow a^{-1}g \in N$. Let $n = a^{-1}g$ then $nxn^{-1} = a^{-1}gxg^{-1}a = gxg^{-1}$.

■

Reference: https://math.stackexchange.com/questions/3327435/stabiliser-of-a-subset-of-center

Solution 2. This problem is called Burnside's basis theorem and our $\Phi(G)$ is called the Frattini subgroup. So first we notice that every maximal proper subgroup of G is of index p. This is because any group of order p^2 is either $\mathbb{Z}/p^2$ or some semidirect product of two $\mathbb{Z}/p$ hence must have a proper subgroup. Then for a maximal proper subgroup N, we have $G/N = \mathbb{Z}/p$. Then the quotient is abelian $\Rightarrow$ all the commutators are inside N. Every element is of order p inside the left coset $\Rightarrow$ all elements of the form g^p for $g \in G$ is also inside N. So now we know $\Phi(G) \subset \cap_{H\text{maximal proper subgroup}} H$. Now for the equal sign, notice that $G/\Phi(G)$ is a characteristic subgroup of G with each element of order p. Thus we can consider it as a $\mathbb{Z}/p$-vector space. And each maximal subgroup correspond to a hyperplane. Since the intersection of all hyperplanes is the origin, we have the desired result.

■

Solution 3. We know that M/JM is a A/J module and A/J is semisimple ring $\Rightarrow M/JM$ is semisimple as A-module. We also know $JM \subset ker(t) \Rightarrow JM = 0 \Rightarrow M$ is semisimple. Also M is left ideal because $\forall x \in J, y \in A, a \in M, t(xya) = 0$ since J is a two sided ideal. Now suppose $\exists N$ semisimple left ideal of A then $JN = 0 \Rightarrow JN \subset ker(t) \Rightarrow t(xb) = 0, \forall x \in J, \forall b \in N \Rightarrow N \subset M$. Thus M is largest sesmisimple left ideal of A.

■

Reference: https://math.stackexchange.com/questions/3324395/characterisation-of-largest-semisimple-left-ideal

Solution 4. The proof is essentially the same as the proof of Artin-Tate Lemma. We let $x_1, ...x_n$ be the generators of A over R. Let $y_1, ...y_k$ be the generators of A over B. Let $x_i = \Sigma_j b_{ij} y_j$. Let $y_i y_j = \Sigma_k b_{ijk} y_k$. Let B_0 be the subalgebra of B generated by b_{ij}, b_{ijk} over R. Since $B \subset Z(A)$, we can show that A is a finitely generated module over B_0. B_0 is a finitely generated commutative algebra over noetherian ring R. By Hilbert's basis theorem B_0 is noetherian. Thus A is noetherian B_0-module. Thus B as a submodule of A is finitely generated B_0-module. Thus B is finitely generated algebra over R

■

Reference: https://math.stackexchange.com/questions/3328253/finitely-generated-algebra-over-commutative-ring

Solution 5. This is the density theorem. You can check page 49 of the reference.

■

Reference: https://lkempf.github.io/AlgebraStroppel/algebraII.pdf

Solution 6. $\Rightarrow$: Suppose M torsion free but $M_{\mathfrak{p}}$ is not $R_{\mathfrak{p}}$-torsion free. $r \in R, s, s' \notin \mathfrak{p}, x \in M, \frac{r}{s'} \cdot \frac{x}{s} = 0 \Rightarrow \exists s'' \notin \mathfrak{p}$ such that $s''rx = 0$ and $s''r \neq 0 \Rightarrow x$ is torsion, contradiction.
$\Leftarrow$: Suppose $x \in M$ is a nontrivial torsion of R then $\exists r \in R, rx = 0$. We know r is not unit because otherwise $x = 0$. Thus take $\mathfrak{m}$ be a maximal ideal containing r. Notice that if $\frac{x}{1}$ is $R_{\mathfrak{m}}$-torsion in $M_{\mathfrak{m}}$ then $\exists s \notin \mathfrak{m}, sx = 0$. Then $\exists a, b$ such that $ar + sb = 1 \Rightarrow x = (ar + sb)x = 0$, contradiction. Thus $\frac{x}{1}$ is $R_{\mathfrak{m}}$-torsion in $M_{\mathfrak{m}}$, contradiction.

■

Solution 7. a. Some nice tricks: Start with the polynomial $x^4 - \alpha^4 \in F[x]$. Let the minimal polynomial of α be f. We know f divides the previous polynomial. Moreover, $x^2 - \alpha^4$ is the minimal polynomial of α^2. So we have $[F(\alpha) : F] = [F(\alpha^2) : F] = 2$. So f is of degree 2. We need to choose the other root of f from the roots of $x^4 - \alpha^4$. Our choices are $\pm\alpha, \pm i\alpha$ ($i = \sqrt{-1}$). We can eliminate the first two because $\alpha \notin F$. So f looks like $x^2 - (i+1)\alpha x + i\alpha^2$ (or you substitute the i's with $-i$, not really affect the result, so let's put up with this). So $(i+1)\alpha \in F, i\alpha^2 \in F, i \notin F$. But that implies $i \in F(\alpha) \Rightarrow F(\alpha) = F(i)$. So the only choice for $F(\alpha)$ is $F(i)$.
b. The Galois group is the dihedral group of order 8.

■

Solution 8. We can define the polynomial $h(x) = \frac{f}{g}(g(x)) - f(x) \in F(\frac{f}{g})[x]$. We have $h(x) = 0$ and $degh = d$. So we need to make sure it is the minimal polynomial. Suppose we have $l(x) \in F(\frac{f}{g})[x]$ such that $degl < d, l(x) = 0$. Each coefficient of $l(x)$ looks like $b_{i,n_i}y^{n_i} + ... + b_{i,-m_i}y^{-m_i}$ where $y = \frac{f}{g}$. Without loss of generality we can assume $degf \leq degg$ (otherwise do the later procedures in an inverted manner, namely, eliminate the positive powers and inver the whole thing).Then multiply l with a power of y such that each $m_i = 0$. Then we can consider l as an element in $F(x)[y]$. So the new l looks like $p(y) := a_m y^m + a_{m-1}y^{m-1} + ... + a_0$ where each $a_i \in F[x]$ and has degree less than d. Now suppose $m \geq d$, multiply $p(\frac{f}{g})$ with g^m. Since $p(\frac{f}{g}) = 0$ and f, g coprime we have $g^m | a_m f^m + a_{m-1} f^{m-1} g + ... + a_1 f g^{m-1}$. Because the degree on the right side is strictly less than the degree of the left side, this is not going to happen unless the right side is 0, which means $a_m = 0$. So $l = 0$, contradiction.

■

Solution 9. Let's start with the short exact sequence

$$0 \to L \to R^k \to A \to 0$$

where L is finitely generated over R. Apply the left exact functor $Hom(\_, B)$ we have

$$0 \to Hom(A, B) \to Hom(R^k, B) \to Hom(L, B)$$

The flatness of C implies that the functor $\_\otimes_R C$ is exact. Thus we have the following exact sequence

$$0 \to Hom(A,B)\otimes C \to Hom(R^k,B)\otimes C \to Hom(L,B)\otimes C$$

We replace the B in the second sequence with $B\otimes C$ then we have

$$0 \to Hom(A,B\otimes C) \to Hom(R^k,B\otimes C) \to Hom(L,B\otimes C)$$

Put the last two sequences together we have the following commutative diagram:

$$\begin{tikzcd}
0 & Hom(A,B)\otimes C \arrow[l] \arrow[r] \arrow[d, "\rho_1"'] & Hom(R^k,B)\otimes C \arrow[r] \arrow[d, "\rho_2"] & Hom(L,B)\otimes C \arrow[d, "\rho_3"] \\
0 & Hom(A,B\otimes C) \arrow[l] \arrow[r] & Hom(R^k,B\otimes C) \arrow[r] & Hom(L,B\otimes C)
\end{tikzcd}$$

where ρ_i is the giving by the following general pattern: namely there is always a map $\phi : Hom(X,Y)\otimes Z \to Hom(X,Y\otimes Z)$ given by $f\otimes z \mapsto (x \mapsto (f(x)\otimes z))$. You can check as an exercise that this map is isomorphism when X is free of finite rank. By some diagram chasing, if we can show ρ_3 is injective then ρ_1 is isomorphism. So we can first show that ρ_1 is injective if ρ_2 is isomorphism. Then by substituting A with L we get ρ_3 is injective,

■

Solution 10. a. So F is given by $(A,B)\mapsto A\times B$ on objects and $(A\vec{f}A', B\vec{g}B') \mapsto h$ where h is the unique arrow in the following commutative diagram:

$$\begin{tikzcd}
A \arrow[d, "f"'] & A\times B \arrow[l] \arrow[r] \arrow[d, dotted, "h"'] & B \arrow[d, "g"] \\
A' & A'\times B' \arrow[l] \arrow[r] & B'
\end{tikzcd}$$

A natural candidate of left adjoint of F is the functor $G : \mathcal{C} \to \mathcal{C}^2$ given by $A \mapsto (A,A)$ on objects and $(A\to B) \mapsto (A\to B, A\to B)$ on the morphism. To show G is the left adjoint, it suffices to show that there is the canonical isomorphism $Mor(GX,Y)\cong Mor(X,FY)$. Let $Y = Y_1, Y_2$. Then the canonical isomorphism is given by the following diagram:

$$\begin{tikzcd}
X \arrow[d] & X\times X \arrow[l] \arrow[r] \arrow[d] & X \arrow[d] \\
Y_1 & Y_1\times Y_2 \arrow[l] \arrow[r] & Y_2
\end{tikzcd}$$

I admit it is not crystal clear explanation. So please tell me when you get confused.
b. The category of abelian groups is abelian category. So the idea of product and coproduct are the same. So the previous G functor becomes right adjoint of F by inverting all the arrows in the last diagram (and change product to coproduct).

■

Spring 2018:

Solution 1. Suppose $x = [\mathbb{Q}(\alpha) : \mathbb{Q}], y = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)], z = [\mathbb{Q}(\alpha^n) : \mathbb{Q}]$. By the given condition we know: $x = yz, x = \prod_{i=1}^{k} p_i^{n_i}$ where each p_i is prime then $p_i > n, \forall i$. But we also know $y \leq n \Rightarrow y = 1 \Rightarrow z = x \Rightarrow \mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$.

■

Solution 2. a. Suppose $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$. By Galois theory, $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{Q}(\zeta)$ correspond to a subgroup of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathbb{Z}/6$ of order 2, which is apparently a copy of $\mathbb{Z}/2$ generated by the conjugation map. Now we have a problem: $\mathbb{Z}/2 \subset \mathbb{Z}/6$ is normal since the latter group is abelian, thus $\mathbb{Z}/2$ should correspond to a normal extension. We have a contradiction because $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ is not a splitting field of polynomial. (third root of unity not included).
b. Suppose α has a sube root in $\mathbb{Q}(\zeta, \alpha)$, then the polynomial $X^9 - 3$ would split over $\mathbb{Q}(\alpha, \zeta)$ (we can write it as $\prod_{i=1}^{9}(X - \sqrt[3]{\alpha}\zeta^i)$). But $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 18$ and $[K : \mathbb{Q}] > 18$ where K is splitting field of $X^9 - 3$, since $X^6 + X^3 + 1$ does not split over $\mathbb{Q}(\sqrt[9]{3})$

■

Solution 3. This is a good problem for lunch or dinner, if you find it too boring sitting alone. So the answer is that the quotient is given by gcd of all entries.
Here is the solution if you want to give up the fun: Let e_i be the usual vector with 1 at the ith entry and 0 otherwise. Suppose we start with a matrix M, put E_i (1 on the i, i th entry and 0 otherwise) on the left and e_j on the right you get $M_{i,j}e_j$. Now you can shift the second j around by placing the shifting matrices on the further left. So you get $M_{i,j}e_k, \forall k$. Now with $mI, m \in \mathbb{Z}, I$ the identity matrix, you can put coefficients before $M_{i,j}e_k$ and add them up together. So what you end up with is $(\alpha\mathbb{Z})^n$ where α is the gcd of $\{M_{i,j} \exists M \in I$ such that $M_{i,j}$ is an entry of it$\}$. So the quotient would be a finite abelian group.

■

Solution 4. (Qiu) $D \otimes_k K$ is central simple over K. So it must be in the form $M_{a \times a}(L)$ where L is division algebra over K. By degree reasons if $a > 1$, they must be p. Thus it suffices to show that $D \otimes_k K$ is not division algebra. We can see this by showing that $K \otimes_k K$ is not division algebra. Notice that $K = k[x]/(f)$ where f is the minimal polynomial of a. So $K \otimes_k K = K[x]/(f)$, but in this case f is not irreducible over $K \Rightarrow K[x]/(f)$ is not a domain hence not a division algebra.

■

Solution 5. a. $\Rightarrow$: Suppose f is not surjective but epimorphism. We know $f(M) \neq N$. Then consider $N/f(M)$. We can define two maps $g, h : N \to \mathbb{Z}$ given by the following: $g = 0, h$ is 0 on $f(M)$ by maps some $a \in N/f(M) - \{0\}$ to $1 \in \mathbb{Z}$ (this is a bit abuse of notation, you should think a as one of its preimage in N). Then we have $g \neq h, g \circ f = h \circ f$,

contradiction.
$\Leftarrow$: Suppose $\exists g, h$ such that $g \circ f = h \circ f \Rightarrow \forall a \in N, \exists m \in M$ such that $f(m) = a \Rightarrow g(a) = (g \circ f)(m) = (h \circ f)(m) = h(a) \Rightarrow g = h \Rightarrow f$ is epimorphism.
b. A nice example is the natural injection $\mathbb{Z} \overset{i}{\hookrightarrow} \mathbb{Q}$. If we have $g, h : \mathbb{Q} \to A$ such that $gi = hi$, we have that $g(\frac{p}{q}) = \frac{g(p)}{g(q)} = \frac{h(p)}{h(q)} = h(\frac{p}{q})$. This is an epimorphism which is not surjection.

■

Solution 6. We need to work on the following uncompleted character table:

G	$\langle 1 \rangle, 1$	$\langle y \rangle, 3$	$\langle x \rangle, 4$	$\langle x^2 \rangle, 4$
χ_1	1	1	1	1

where the number near the conjugacy class is its size. Now I want to first figure out all the one dimensional irreducible representations: Let χ be such a representation and ζ the third root of 1. We know that $\chi(y) = \chi(z) = \chi(yz)$ and $\chi(y) \in \{\pm 1\}$ since y is of order 2. Thus we must have $\chi(y) = \chi(z) = 1$. So to make χ nontrivial, we have $\chi(x) \in \{\zeta, \zeta^2\}$. So we have two more rows: $(1\ 1\ \zeta\ \zeta^2), (1\ 1\ \zeta^2\ \zeta)$. Use Schur's orthogonality (see problem 11 of fall 2018), the last row should be $(3\ -1\ 0\ 0)$. So the complete character table is:

G	$\langle 1 \rangle$	$\langle x \rangle$	$\langle x^2 \rangle$	$\langle y \rangle$
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	-1

The group is actually A_4

■

Solution 7. We know that the I is a finitely generated B-module. Hence I^k/I^{k+1} is finitely generated B/I-module, $\forall k \in \mathbb{N}$. Let $x_1, \ldots\ldots x_m$ be the generators of I and a_i such that $x_i^{a_i} = 0 \Rightarrow I^a = 0$ where $a = \Sigma_i a_i + 1$. We consider the filtration $I, I^2, \ldots\ldots I^a = 0$. Each successive quotient is finitely generated B/I-module hence finitely generated A-module. Then by induction and short exact sequences of the form $0 \to I^{k+1} \to I^k \to I^k/I^{k+1} \to 0$ we can conclude that I is finitely generated A-mod. Then by SES $0 \to I \to B \to B/I \to 0$ we conclude B is finitely generated A-mod.

■

Solution 8. In the case that $i \notin F$ then $F \otimes_{\mathbb{R}} \mathbb{C} = F[i]$, which is a field. Otherwise there is an idempotent in $F \otimes_{\mathbb{R}} \mathbb{C}$ given by $\frac{1}{2}(1 \otimes 1 + i \otimes i)$, which shows us that the tensor algebra is a product of two fields.

■

Solution 9. Another classical application of Sylow theorems:
Let n_i be the number of Sylow-i groups. If some $n_i = 1$ then we are done. First notice that $616 = 8 \times 7 \times 11$. So we need to calculate n_2, n_7, n_{11}. By Sylow theorems, if none of the previous numbers is 1, we have: $n_2 = 7$ or 11 or $77, n_7 = 22$ or $8, n_{11} = 56$. So the order of the group must be at least $56 \cdot (11-1) + 8 \cdot (7-1) + (8-1) \cdot 7 = 657 > 616$, contradiction.

■

Solution 10. We know that the localization of a noetherian intergal domain is still a noetherian integral domain. Now it suffices to show that $R[S^{-1}]$ is integrally closed and every prime ideal is maximal.
For integrally closedness, the fraction field of $R[S^{-1}]$ is the same as that of R. Take an element there which is integral over $R[S^{-1}]$, let it be a. Then a would satisfy some polynomial like $X^n + \frac{a_{n-1}}{s_{n-1}} X^{n-1} + ... + \frac{a_0}{s_0} = 0$ where $a_i \in R, s_i \in S$. Then we have $sa^n + b_{n-1}a^{n-1} + ...b_0 = 0$ for $s \in S, b_i \in R$. Then $(sa)^n + c_{n-1}(sa)^{n-1} + ... + c_0 = 0$ for $c_i \in R \Rightarrow sa$ integral over $R \Rightarrow sa \in R \Rightarrow a \in R[S^{-1}] \Rightarrow R[S^{-1}]$ integrally closed.
For the second part, we know $Spec(R[S^{-1}]) \subset Spec(R)$. Any prime ideal in $R[S^{-1}]$ is a maximal ideal in R and thus should be a maximal ideal in $R[S^{-1}]$.

■

Fall 2018:

Solution 1. a. Let G be a nontrivial subgroup of Q_8 which does not contain -1. Then we have $G \cap Q_8 - \{\pm 1\} \neq \emptyset$. Any element in the intersection squared would give us -1.
b. Suppose we have the embedding

$$Q_8 \hookrightarrow S_7$$
$$-1 \mapsto a$$
$$i \mapsto x$$
$$j \mapsto y$$
$$k \mapsto z$$

If we write out x, y, z as product of disjoint cycles, then each of them would contain a 4-cycle, because these three elements should be of order 4. In the product there may or may not be a 2-cycle and that's it (otherwise either the order goes wrong or we run out of objects). Thus we can let $x = x_1x_2, y = y_1y_2, z = z_1z_2$ where x_1, y_1, z_1 are 4-cycles. x_2, y_2, z_2 are 2-cycles or identities. Now if x_1, y_1 are the same 4-cycle then $z = xy$ does not have a 4-cycle (instead, a bunch of 2-cycles). Then $x_1 \neq y_1$. Thus $x_1, y_1, z_1 = x_1y_1$ are three distinct 4-cycles.
Now this is where it goes wrong:
Without loss of generality let $x_1 = (1\ 2\ 3\ 4) \Rightarrow a = x^2$ contains $(1\ 3)(2\ 4)$. In fact $a = (1\ 3)(2\ 4)$ because $x_2^2 = 1$. Then we need to find three different 4-cycles, the square of which are the same. This is impossible: suppose the 4-cycle is $(1\ x\ y\ z)$, in order to have $(1\ 3)$ in the square, we must have $y = 3$. Then we are left with only two choices.

■

Solution 2. Let $H \subset G$ be the subgroup of finite index n.
Let's start with a remark: G acts on the left cosets G/H by left multiplication, which gives us a map $G \to S_n$. Notice that this map uniquely determines H because H is exactly the elements in G the image of which under the previous map fixes the first object. Thus we have an injection $\{\text{subgroup of } G \text{ with index } n\} \hookrightarrow \{\text{maps from } G \text{ to } S_n\}$. Now notice that the latter set is finite in the case G is finite. The reason is that there are only finitely many choices for the images of the generators. Thus G only has finitely many subgroups of index n.
For the second part, notice that for a automorphism ϕ of $G, \phi(H)$ is still a subgroup of G of index n. Since there are only finitely many subgroups of index n, the group $\cap_{\phi \text{an automorphism of } G}\phi(H)$, a proper characteristic subgroup of G, as an intersection of finitely many subgroups of index n, is of finite index.

■

Solution 3. This one is very similar to the proof of the primitive element theorem:
In the case F is finite, $F = \mathbb{F}_{p^n}$ for some prime p. Then the generator of the cyclic group K^* would give us the primitive element.

If F is infinite, assume K is not primitive extension. Pick $w \in K$ such that $[F(w) : F]$ is maximal among all $F(a)$ for $a \in K$. Now suppose $F(w) \neq K$. Pick $b \in K, b \notin F(w)$. Consider the family of extensions $\{F(w + \lambda b)\lambda \in F\}$. This must be a finite set since there are only finitely many intermediate fields and $w + \lambda b \notin F$ (by linear independence of two elements). Now $\exists \lambda_1 \neq \lambda_2$ such that $F(w + \lambda_1 b) = F(w + \lambda_2 b) \Rightarrow b, w \in F(w + \lambda_1 b) \Rightarrow [F(w + \lambda_1 b) : F] > [F(w) : F]$, contradiction.

■

Solution 4. Let K' be the splitting field of f. Since everything is separable, it suffices to calculate $[K' : K]$. We can write $f(x) = (x - a)(x - b)(x - c)(x - \bar{c})$ where a, b real, c not. In the case $b \notin K(a), [K' : K] = 24$ and the only choice of Galois group is S_4. In the case $b \in K(a), (x - c)(x - \bar{c})$ does not split over $K(a)$ since $K(a) \subset \mathbb{R}$. Thus $[K' : K] = [K(a) : K] \cdot 2 = 8$.

■

Solution 5. a. First we have $0 \notin S$, otherwise $R = S$ and we have nothing to do here. Then it suffices for $x \notin S$, we find a prime ideal $\mathfrak{p}_x$ such that $\mathfrak{p}_x \cap S = \emptyset$ and $x \in \mathfrak{p}_x$. We do this by first pick I an maximal element of the set $W := \{\text{ideals in } R\{whichcontain\}x \text{ and does not intersect } S\}$. Notice that W is nonempty because $xR \in W$ and such a maximal element exists, because if $\mathcal{C}$ is an ascending chain of ideals in W, then $\cup_{J \in \mathcal{C}} J$ is still an element in W. Suppose I is not prime then $\exists c, d \in R$ such that $cd \in I, c \notin I, d \notin I \Rightarrow cd \notin S$. Without loss of generality assume $c \notin S \Rightarrow I + cR \in W$ and strictly larger than I. Hence contradiction.
b. $\Rightarrow$: Let $\mathfrak{p}$ be a prime ideal. Pick $x \in \mathfrak{p}, x \neq 0$ and of course, x is not a unit, Then let $x = \prod_{i=1}^{k} p_i$ where each p_i is irreducible $\Rightarrow \exists j, p_j \in \mathfrak{p} \Rightarrow (p_j) \subset \mathfrak{p}$ and (p_j) is out pricnipal prime ideal.
$\Leftarrow$: First note that there are irreducible elements in R as generators of principal prime ideals, because there exists prime ideals in R (such as maximal ideals). Then let $S = \{\text{product of irreducible elements with units}\}$. It is easy to see that S is a multiplicative set. For saturatedness, suppose $xy = \prod_{i=1}^{n} a_i, a_i$ distinct irreducibles. Then we have $I, J, I \cup J = \{1, 2, ...n\}$ such that $\prod_{i \in I} a_i \cdot u = x, \prod_{i \in J} a_i \cdot v = y$ where u, v are units. Thus $x, y \in S$. If there are powers on a_i, we can do an easy induction on the power by dividing both sides of the equation (on appropriates letters of course) by a_i.
Now we use result from part a to see that there can't be any nonzero element outside of $S \Rightarrow R - S = \{0\} \Rightarrow R$ is a UFD by definition.

■

Solution 6. a. We can start by showing that trace is nonzero: take $x \in K, x \notin F$, by the transitivity of trace we may assume that $K = F(x)$. Let the solutions of the minimal polynomial of x to be $x_1, ...x_n$. Then trace of x^k is $\Sigma_{i=1}^{n} x_i^k$. Then by a corollary of Artin's theorem on linear independence of characters the previous sum cannot vanish all the time.
Now we can define a pairing $Tr : K \times K \to F$ given by $(x, y) \mapsto Tr(xy)$. Notice that pairing is nondegenerate: if $\exists x \neq 0, Tr(xy) = 0 \forall y \Rightarrow Tr = 0$ contradiction. Then the map $x \mapsto Tr(x \cdot \_)$ gives us an isomorphism of F-vector spaces $K \cong K^V$ where K^V is the dual

of K, because the map is an injective homomorphism between two finite dimensional vector spaces of equal dimensions. Now for the given basis $\{x_i\}$, we pick the dual basis in K^V and then take their inverse image in K under the previous map and obtain the desired $\{y_j\}$.
b. We can start by choosing a basis of K over F which is inside B: Let $\{x_i\}$ be a basis of K over F. Then x_i is algebraic over F. Multiply the coefficients with common denominators in minimal polynomial of x_i over F we know that x_i is algebraic over A. Let the polynomial of x_i over A be $a_nX^n + ... + a_0 = 0$. Then $a_n^nX^n + a_n^{n-1}a_{n-1}X^{n-1} + ... + a_0a_n^{n-1} = 0 \Rightarrow a_nx_i \in B$ then we can substitute x_i with a_nx_i. After the substitution $\{x_i\}$ is still a basis of K over F because they are only under scaling from elements in F.
Now define $B^V := \{x \in K, Tr(xb) \in A, \forall b \in B\}$. Apparently $\forall b \in B, Tr(b)$ as a coefficients in the minimal polynomial of b is inside $A \Rightarrow B \subset B^V$. Now choose basis of K over $F, \{x_i\} \subset B$ and its dual $\{y_j\}$ as described in part a. Now we know that $B^V \subset \Sigma Ay_j$ because for $x = \Sigma a_jy_j \in B^V, a_j \in F, Tr(xx_i) = a_i \in A$. Now A noetherian $\Rightarrow \Sigma Ay_j$ noetherian $\Rightarrow B \subset \Sigma Ay_j$ finitely generated as A-module.

■

Solution 7. This problem is mostly about to find a way out of the maze in definitions of category theory.
For teminologies, let $\eta : id_{\mathcal{C}} \to GF, \epsilon : FG \to id_{\mathcal{D}}$ be the unit and counit respectively.
$\Rightarrow$:
We have the isomorphism $Mor(X,X) \cong Mor(FX,FX) \cong Mor(X,GFX)$ where η_X lives in the last morphism set. If we pull it back in $Mor(FX,FX)$ and show that it's an isomorphism then we are done. This is exactly what we will do:
The last isomorpohism is given by

$$Mor(X,GFX) \cong Mor(FX,FX)$$

$$g \mapsto \epsilon_{FX} \circ F(g)$$

Under this isomorphism we have $\eta_X \mapsto \epsilon_{FX} \circ F(\eta_X) = id_{FX} \Rightarrow \eta_X$ is isomorphism.
$\Leftarrow$:
Basically we want to make the following equation work:

$$Mor(FX,FY) \overset{f \mapsto G(f)\circ\eta_X}{\cong} Mor(X,GFY) \overset{h \mapsto \eta_Y^{-1}\circ h}{\cong} Mor(X,Y)$$

The first one works by adjunction and second by the fact η is natural isomorphism.
Let the previous composition of maps be $\phi : Mor(FX,FY) \to Mor(X,Y)$. Then $\phi(Ff) = \eta_Y^{-1} \circ GFf \circ \eta_X = f$ by the fact that η is natural transformation.
Now the only thing left to show is $F(\eta_Y^{-1} \circ Gf \circ \eta_X) = f$. This need a bit more work. Consider the following diagram:

$$\begin{tikzcd}
FX \arrow[r, "F(\eta_X)"] \arrow[d, "f"] & FGFX \arrow[r, "\epsilon_{FX}"] \arrow[d, "FGf"] & FX \arrow[d, "f"] \\
FY \arrow[r, "F(\eta_Y)"] & FGFY \arrow[r, "\epsilon_{FY}"] & FY
\end{tikzcd}$$

The goal is to show that the left square commute. We already know that the right square commutes and the whole big square commutes. Thus the two paths on the left composing ϵ_{FY} on the left would be the same. We know ϵ_{FY} is isomorphism because it is one side inverse of an isomorphism $F(\eta_Y)$. Thus we can throw ϵ_{FY} away.

■

Solution 8. A coproduct of two copies of $k[x]$ would do the trick.

■

Solution 9. This calculation is inspired by analysis:
We have

$$\frac{1}{1-gf} = 1 + gf + (gf)^2 + ...$$

$$\frac{1}{1-fg} = 1 + fg + (fg)^2 + (fg)^3 + ...$$

Let $x = 1 + gf + (gf)^2 + ...$ then we would naturally have $1 + fg + (fg)^2 + (fg)^3 + ... = 1 + fxg$. So our candidate would be $1 + fxg$.
Now formally: let $x = (1-gf)^{-1}, y = 1 + fxg$. We have $(1-fg)(1+fxg) = 1 + fxg - fg - fgfxg$.
Plug in $x - xgf = 1 = x - gfx$ we have: $1 + fxg - fg - fgfxg = 1 + fxg - fg - fxg + fg = 1$.
You can show that it is the left side inverse with the same calculation.

■

Solution 10. a. Let ϕ be the map. The map makes sense. The work is to show that the map is bijective.
Injectiveness:
Suppose $\exists a, b$ such that $a(1+x) - by = ay + b(1+x) = 0$. Combine the two equations we have $a(y^2 + x^2 + 2x + 1) = 0$. But the left side is $a(2+2x) \Rightarrow a = 0 \Rightarrow b = 0$.
Surjectiveness:
I suffices to show $(y, 0) \in Im(\phi)$ and $(0, y) \in Im(y)$. Indeed, $(y, 0) = \phi(\frac{y}{2}, \frac{x-1}{2})$ and $(0, y) = \phi(\frac{1-x}{2}, \frac{y}{2})$.
b. The inverse can be explicitly written out: $m_1 \otimes m_2 \mapsto \frac{m_1 m_2}{2(1+x)}$

■

Solution 11. By the given problem we have the following uncompletetd chart and we want to complete it:

G	$\langle 1\rangle$	$\langle g_1\rangle$	$\langle g_1^2\rangle$	$\langle g_2\rangle$
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	......			

Where χ_3 comes from the symmetry that if we have an irreducible representation, we can do a conjugate version of it and it is still an irreducible representation.
Now here are the two orthogonality relations that we are going to use:

$$\Sigma_{g\in G}\chi_i(g)\overline{\chi_j(g)} = \begin{cases} |G| & i=j \\ 0 & \text{otherwise} \end{cases}$$

$$\Sigma_i \chi_i(g)\cdot\overline{\chi_i(g)} = \frac{|G|}{c}$$

where c is the cardinality of $\langle g\rangle$, Now by the given data, multiplication by g_1 gives an injective map from $\langle g_1\rangle$ into $\langle g_1^2\rangle$. Similarly, multiplication by g_1^2 gives an injective map from $\langle g_1^2\rangle$ into $\langle g_1\rangle$. From the two maps we have $|\langle g_1\rangle| = |\langle g_1^2\rangle|$. Let $a = |\langle g_1\rangle|$. Then multiplication by g_1 gives an injective map from $\langle g_1^2\rangle$ into $\{1\}\cup\langle g_2\rangle$, multiplication by g_1 gives injective map from $\{1\}\cup\langle g_2\rangle$ into $\langle g_1$'$\rangle$. From these two maps we have $|\langle g_2\rangle| = a-1$. Let M be the matrix of entries from the character table and let M_{ij} be the jth entry of χ_i. By second orthogonality we have $M_{i2} = M_{i3} = 0$ for $i > 3$. For $i > 3$, apply the first orthogonality to the first row and ith row we have $M_{i1} + M_{i4} = 0 \Rightarrow M_{i4} \in \mathbb{Z} - \{0\}$. Apply the second orthogonality to the last column we have $3 \le 1+1+1+\Sigma_{i>3}||M_{i4}||^2 = \frac{3a}{a-1}$. $a = 1$ doesn't work. If $a = 2$ then there should be three more rows looking like $1\ 0\ 0\ -1$, there are too few choices. If $a = 3$, $\frac{3a}{a-1}$ is not an integer. If $a > 4$, $\frac{3a}{a-1} < 4$. Thus our only choice is that $a = 4$ and the extra row is $3\ 0\ 0\ -1$. So the completed chart is:

G	$\langle 1\rangle$	$\langle g_1\rangle$	$\langle g_1^2\rangle$	$\langle g_2\rangle$
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	-1

This is the character table of A_4. It has cardinality 12. We have $g_1 = (1\ 2\ 3), g_2 = (1\ 2)(3\ 4)$

■

Solution 12. Notice that K contains all the elements in $\overline{F}$ which are algebraic over F, because any algebraic number over F is inside some $\mathbb{F}_{p^n}$, which can be obtained by adjoining a root of unity to F. Suppose D is a division algebra of finite dimension over K. Take $d \in D$ and choose a basis $\{d_1, ...d_n\}$ of D over K. We can associate a matrix under the previous basis with coefficients in F by letting it acts on D by left multiplication.The matrixt has a Jordan canonical form over $\overline{F}$ and we have a polynomial $\prod_{i=1}^{k}(d - x_k)^{m_k} = 0$ where x_k is algebraic over F and with slight abuse of notation I denote the matrix associated to d by d. We know that every division algebra does not have zero divisors. Hence we have $d = x_k$ for some k. By previous argument we have $x_k \in K \Rightarrow d \in K \Rightarrow D = K$. By Artin Wedderborne theorem all the simple finite dimensional algebras over K are in the form $M_{n\times n}(D)$. Thus all the finite dimensional simple algebras are $M_{n\times n}(K)$

■

Spring 2019:

Solution 1. We can start by showing that N is abelian: for $n_1, n_2 \in N, g \in G, gn_1n_2n_1^{-1}n_2^{-1}g^{-1} = gn_1g^{-1}gn_2g^{-1}gn_1^{-1}g^{-1}gn_2^{-1}g^{-1} \Rightarrow [N,N] \lhd G$. By the minimality of N we have $[N,N] = \{1\}$ or N. The second case is impossible because if so, N would not be solvable. But as a subgroup of a solvable group N is always solvable.
Now we have N is abelian. Suppose p a prime and $p||N|$. Let S be the Sylow p subgroup of N. We know $P \lhd N$. $\forall g \in G$, we know gPg^{-1} is a Sylow p subgroup of the group $gNg^{-1} \Rightarrow gPg^{-1} = P \Rightarrow P \lhd G \Rightarrow P = N$.
Now by the characterisation of all the finite abelian groups, the last step is to show that every element in N is of order p. For $x \in N, g \in G, gx^pg^{-1} = (gxg^{-1})^p \Rightarrow pN \lhd G$. Also $pN \subsetneq N$ because there are nontrivial elements in N of order p. Then by the minimality of $N, pN = 0$.

■

Solution 2. Here is a sketch of the proof. I am not 100 percent sure if it works (on some set theory level). Define $W := \{C \subset B, \forall x \in C, \mathbb{Z}x \cap A = \emptyset\}$. Let $A' = \{x \in B, \mathbb{Z}x \cap A \neq \emptyset\}$. Then by Zorn's lemma we can pick a maximal element C from W(if $A' \neq B$) and show $B = C \oplus A'$. Then we can define the map to be 0 on the map and the on A' it is $x \mapsto \frac{f(nx)}{n}$ where $nx \in A, n \in \mathbb{Z}, f$ is the given homomorphism.

■

Solution 3. The basic idea is that we can use the idea of module. We define $||||$ in the following way: $||a + b\sqrt{-d}|| := a^2 + b^2d$. Then we can prove $x|y \Rightarrow ||x|||||y||$. Thus $x|2 \Rightarrow ||x|||4 \Rightarrow ||x|| = 1$ or 2 or 4. The first two possibilities implies x is ± 1. The last one says x is ± 2 or $1 \pm \sqrt{-3}$ in case $d = 3$. That does not divide 2 of course. So 2 is irreducible. But (2) is not irreducible. In case $2|d$, we have $(\sqrt{-d})^2 \in (2)$ but $\sqrt{-d} \notin (2)$. Otherwise $(1 + \sqrt{-d})(1 - \sqrt{-d}) \in (2)$ but $1 + \sqrt{-d} \notin (2)$.

■

Solution 4. We can take $P = Rx_1 + ...Rx_k$ for $x_i \in P$ where k is minimal. Then we have $P \oplus Q = R^k$ for some Q. Let $\mathfrak{m}$ be the maximal ideal of R. Then we have $R^k \otimes R/\mathfrak{m} = R/\mathfrak{m} \otimes (P \oplus Q) \Rightarrow (R/\mathfrak{m})^k = P/\mathfrak{m}P \oplus Q/\mathfrak{m}Q$. Then by dimension reasons $Q/\mathfrak{m}Q = 0$. Then by Nakayama's lemma $Q = 0 \Rightarrow P = R^k$ hence free.

■

Solution 5. First suppose a has order k mod p. Then we have $p|\Phi_n(a) \Rightarrow p|a^n - 1 \Rightarrow k|n \Rightarrow k = n$ or $k < n$.
In the case $k = n$, then we know by Fermat's little theorem that $a^{p-1} \equiv 1 mod p \Rightarrow n|p-1 \Rightarrow p \equiv 1 mod n$.
In the case $k < n$, we have $X^n - 1 = \prod_{m|n} \Phi_m(X)$. By the fact $k|n, (X-a)|\Phi_k(X), (X -$

$a)|\Phi_n(X) \Rightarrow (X-a)^2|X^n-1$. Now we let $X^n - 1 = (X-a)^2 f(X)$. Let $X = Y + a$ then we have $(Y+a)^n - 1 = Y^2 f(Y+a)$. By observation on the right side we know that the coefficient of the first degree term on the left side is $0 \Rightarrow na^{n-1} \equiv 0 mod p$. We know that $a \not\equiv 0 mod p$ (otherwise $p \not| \Phi_n(a)$). Thus $p|n$. This case should not be taken into consideration.

■

Solution 6. This problem is the same as #6, Fall 2016

■

Solution 7. a. I use the following characterization of the Jacobson radical: $J(A) = \{a \in A, \forall x \in A, 1 + xa \in A^\times\}$. Let $a = (a_{i,j})$ be an element in J. The last row of a must be zero, otherwise we have $I + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -a_{3,3}^{-1} \end{pmatrix} \cdot a$ has the last row zero hence not invertible. For the same reason the other two diagonals must also be 0. Now a looks like $\begin{pmatrix} 0 & u & v \\ w & 0 & x \\ 0 & 0 & 0 \end{pmatrix}$. If $u \neq 0$. Then $I + \begin{pmatrix} 0 & 0 & 0 \\ 0 & -u^{-1} & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot a$ has a row of zero in the middle hence not invertible. Thus $u = 0$. For the same reasons $v = w = x = 0 \Rightarrow a = 0 \Rightarrow J = 0$.
b. Yes of course because it is 0.

■

Solution 8. We know $S_{n-1} \subset GL_{n-1}(\mathbb{C})$. So the problem is to embed a group of order n into S_{n-1}. By taking the group action of left multiplication on left cosets of a subgroup, this is always possible unless the group does not have nontrivial subgroup. By the Sylow theorems, this happens only if the group is $\mathbb{Z}/p$, you can just embed it into $\mathbb{C}$ by sending the generator to a primitive pth root of unity.

■

Solution 9. a. $R = \mathbb{C}[x, y], a = x, b = y$
b. I asked the question on stackexchange, You can check it out here:
`https://math.stackexchange.com/questions/3324366/showing-a-functor-is-not-representable`
There is also a specific way of doing this problem in this case: Take the R as described in part a. By Yoneda's lemma, assume the functor is representable, Then $\exists (x, y) \in A^2$ with the following universal property: For any ring $B, (z_1, z_2) \in B^2$ then $\exists! f : A \to B$ ring map such that $f(x) = z_1, f(y) = z_2$. In fact, this universal element is given by our isomorphism in $Mor(Hom(A, \_), F)$ under the iso $Mor(Hom(A, \_), F) \cong F(A)$. Now we have morphism $f : A \to R[\frac{1}{a}]$ such that $f : x \mapsto a, y \mapsto b$. Also we have $g : A \to R[\frac{1}{b}]$ such that $g : x \mapsto a, y \mapsto b$. Now we consider f, g as maps from A to $Frac(R)$. Let $h = f - g$. Then $h(x) = h(y) = 0 \Rightarrow h(1) = h(x)h(c_1) + h(y)h(c_2) = 0$ for some $c_1, c_2 \in A \Rightarrow h = 0 \Rightarrow f = g$. Thus f, g must take values in $R[\frac{1}{a}] \cap R[\frac{1}{b}] = R \Rightarrow$ we can take a map $f : A \to R$ sending (x, y) to (a, b), which is inside $Hom(A, R)$. Then we have contradiction because $(a, b) \notin F(R)$

■

Solution 10. An object A is projective $\Leftrightarrow$ every SES $0 \to X \to Y \to A \to 0$ splits. An object B is injective $\Leftrightarrow$ every SES $0 \to X \to X \to Y \to 0$ splits. Thus every object is projective $\Leftrightarrow$ every SES splits $\Leftrightarrow$ every object is injective.

■