Select Algebra Qual Problems

Yan Tao

1 Preface

This is a compilation of solutions to many of the past UCLA Algebra Qual problems I have written up while preparing for the exam. The problems tend to be sorted by the year but there's no particular order I stuck to. You can find a problem by Ctrl+F and looking for the exam and problem in the format yyF.# (for Fall exams) and yyS.# (for Spring exams). Not all problems are solved here.

Many thanks to Josh Enwright for helpful discussions while compiling these.

2 Algebra

10F.1 Let **Grp** be the category of groups and **Ab** the category of abelian groups. If $\mathcal{F} : \mathbf{Ab} \to \mathbf{Grp}$ is the inclusion of categories, then find a left adjoint to $\mathcal{F}$ and prove it is a left adjoint.

Solution Define $\mathcal{G} : \mathbf{Grp} \to \mathbf{Ab}$ by $\mathcal{G}(G) := G/[G,G]$ (its abelianization), and for any morphism of groups $\varphi : G \to H$ let $\mathcal{G}(\varphi) : \mathcal{G}(G) \to \mathcal{G}(\varphi)(g[G,G]) = \overline{\varphi}(\overline{g}) = \overline{\varphi(g)} = \varphi(g)[H,H]$. We have that

$$\mathcal{G}(\varphi)[(g_1[G,G])(g_2[G,G])] = \varphi(g_1g_2)[H,H] =$$
$$\varphi(g_1)[H,H] \cdot \varphi(g_2)[H,H] = \mathcal{G}(\varphi)(g_1[G,G])\mathcal{G}(\varphi)(g_2[G,G])$$

so that $\mathcal{G}(\varphi)$ is indeed a morphism of the abelian groups. Now let $G \in \mathbf{Grp}, H \in \mathbf{Ab}$. Then for any morphism of groups $\varphi : G \to \mathcal{F}(H)$,

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi(g_2)\varphi(g_1) = \varphi(g_2g_1) \text{ since } H \text{ is abelian, so that}$$
$$[G,G] \subseteq \ker(\varphi) \Rightarrow \mathcal{G}(\varphi)(g[G,G]) = \varphi(g) \text{ for all } g \in G$$

Thus, the following diagram commutes which gives a natural bijection of $\mathrm{Hom}_{\mathbf{Grp}}(G, \mathcal{F}(H))$ and $\mathrm{Hom}_{\mathbf{Ab}}(\mathcal{G}(G), H)$ so that $\mathcal{G}$ is indeed the left adjoint of $\mathcal{F}$.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & \mathcal{G}(G) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathcal{G}(\varphi)} \\ \mathcal{F}(H) & \xrightarrow{\mathrm{Id}} & H \end{array}$$

10F.3 Prove that there is no simple group of order 120.

Solution Suppose G were a simple group of order 120, and let n_5 be the number of Sylow 5-subgroups of G. If $n_5 = 1$, then the Sylow p-subgroup would be normal in G by Sylow's Theorems, which would be a contradiction, so it is greater than 1. By Sylow's Theorems,

$$n_5 | 24 \text{ and } n_5 \equiv 1 (\mathrm{mod}\ 5) \Rightarrow n_5 = 6$$

Then by Sylow's Theorems, $[G : N_G(P)] = n_5 = 6$ for any Sylow 5-subgroup P, so since G is simple there exists an injective group homomorphism $G \to A_6$. Since G has order 120, by Lagrange its index as a subgroup of A_6 is 3. But A_6 is simple, so there exists an injective group homomorphism $A_6 \to A_3$. But this is a contradiction, so there can be no such simple group G of order 120.

10F.5 Prove that if a finite group G acts transitively on a set S having more than one element then there exists an element of G which fixes no element of S.

Solution X has only one orbit under G, so by Burnside's Lemma

$$|G| = \sum_{g \in G} |X^g|$$

Suppose that each g fixes some element of X. Then $|X^g| \geq 1$ for each g, and furthermore $|X^e| = |X| > 1$ since the identity fixes X, so that

$$|G| = \sum_{g \in G} |X^g| > |G| \text{ which is a contradiction}$$

18F.1 Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group (of order 8).
a) Show that every nontrivial subgroup of Q_8 contains -1.
b) Show that Q_8 does not embed in the symmetric group S_7 (as a subgroup).

Solution a) Suppose G is a subgroup of Q_8 where $-1 \notin G$. Then $\pm i, \pm j, \pm k \notin G$ as $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1 \notin G$, so nothing besides 1 is in G and thus G is trivial.

b) Suppose Q_8 embeds into S_7 and let $\sigma_i, \sigma_j, \sigma_k$ be the images of i, j, k respectively. Then $\sigma_1, \sigma_2, \sigma_3$ all have order 4 and $\sigma_i^2 = \sigma_j^2 = \sigma_k^2 := \sigma_{-1}$ is the image of -1. The only elements of order 4 in S_7 are 4-cycles with a disjoint 2-cycle possibly added as well, and the square of each of these consists of two disjoint 2-cycles. Relabelling if necessary, assume without loss of generality that $\sigma_{-1} = (12)(34)$. Then (1324) and (1432) are the only possible 4-cycles $\sigma_i, \sigma_j, \sigma_k$ can contain, so by Pigeonhole Principle two of them contain the same 4-cycle (and without loss of generality, σ_i and σ_j both contain the same 4-cycle). But then $\sigma_i \sigma_j$ does not contain any 4-cycle, so it cannot be equal to σ_k as it would have to be if Q_8 were embedded in S_7, so we have a contradiction so Q_8 does not embed in S_7.

18F.2 Let G be a finitely generated group having a subgroup of finite index $n > 1$. Show that G has finitely many subgroups of index n and has a proper characteristic subgroup (i.e. preserved by all automorphisms) of finite index.

Solution Let H be a subgroup of G of index n and let $g_1, ..., g_m$ be the finitely many generators of G. Then G acts on the set $\{H, x_1 H, x_2 H, ..., x_{n-1} H\}$ of distinct cosets of H transitively by right-multiplication, giving rise to a group homomorphism $\varphi : G \to S_n$ where $\ker(\varphi) = H$. Since φ is determined by $\varphi(g_1), ..., \varphi(g_m)$ and S_n is a finite group, there can only be finitely many such homomorphisms. But $H = \ker(\varphi)$, so there are only finitely many ways to make H, and hence only finitely many subgroups of index n. Finally, for each $\phi \in \mathrm{Aut}(G)$, $\phi(H)$ is an index n subgroup of G, and since there are only finitely many of these,

$$\bigcap_{\phi \in \mathrm{Aut}(G)} \phi(H)$$

is a proper characteristic subgroup of finite index.

18F.3 Let K/F be a finite extension of fields. Suppose there exist finitely many intermediate fields $K/E/F$. Show that $K = F(x)$ for some $x \in K$.

Solution In the case where F is finite, because K is a finite extension K must then be finite, so that $K^\times$ is cyclic, so let x be a generator. Since the order of x is $|K| - 1$, $|F(x)|$ must be at least as large. But $F(x)$ is an F-vector space, so its cardinality is divisible by $|F|$ and is thus at least $|K|$. But $F(x) \subseteq K$, so $F(x) = K$.

In the case where F is infinite, since there exist finitely many intermediate fields, consider $K = F(a, b)$ for $a, b \in K$, as the general case will follow by induction. Since F is infinite and there are finitely many intermediate fields, there exist $y \neq z \in F$ such that $F(ay + b) = F(az + b)$, and set $x := ay + b$. Then $F(x) \subseteq K$, so it will suffice to show that $a, b \in F(x)$ to show that $F(x) = K$. Since $y \neq z$,

$$a = \frac{a(y-z)}{y-z} = \frac{(ay+b)-(az+b)}{y-z} \in F(x)$$

Then we also have that $b = x - ay \in F(x)$, which concludes the proof.

18F.4 Let K be a subfield of the real numbers and f an irreducible degree 4 polynomial over K. Suppose that f has exactly two real roots. Show that the Galois group of f is either S_4 or of order 8.

Solution Let F be the splitting field of f over K and consider the embedding $\text{Gal}(F/K) \to S_4$ given by how each automorphism in the Galois group permutes the roots of f in F. Because f is irreducible, this gives a transitive subgroup of S_4, which by the Orbit-Stabilizer Theorem has order divisible by 4. $\text{Gal}(F/K)$ contains the transposition corresponding to complex conjugation (which transposes the two non-real roots), so it cannot have order 4 since the only transitive subgroups of S_4 of order 4 are the cyclic ones generated by the 4-cycles, which do not contain transpositions. It also cannot have order 12 as the only subgroup of S_4 of order 12 is A_4, which does not contain transpositions. Thus $|\text{Gal}(F/K)|$ must be either 8 or 24, the only two other values which divide 24 and are divisble by 4.

18F.5 Let R be a commutative ring. Show the following:
a) Let S be a nonempty saturated multiplicative set in R, i.e. $ab \in S$ if and only if $a, b \in S$ for all $a, b \in R$. Show that $R \setminus S$ is a union of prime ideals.
b) If R is a domain, show that R is a UFD if and only if every nonzero prime ideal in R contains a nonzero principal prime ideal.

Solution a) If $0 \in S$, then for every $x \in R$, $0 = 0x \in S \Rightarrow x \in S$, so $R = S$ and $R \setminus S$ is an empty union. Otherwise, for each $x \notin S$, let $\mathcal{I}_x$ be the set of all ideals of R containing x which do not intersect S. Since $x \notin S$, every xy for every $y \in R$ is also not in S, so that $(x) \in \mathcal{I}_x$ and in particular it is not empty. Partially order $\mathcal{I}_x$ by inclusion, and note that for every chain $\mathcal{C}$ of ideals in $\mathcal{I}_x$, their union $\bigcup_{J \in \mathcal{C}} J$ is an ideal and $(\bigcup_{J \in \mathcal{C}} J) \cap S = \bigcup_{J \in \mathcal{C}} (J \cap S) = \emptyset$, so that by Zorn's Lemma there exists a maximal element $I \in \mathcal{I}_x$. Suppose I is not a prime ideal. Then there exists $ab \in I$ where $a \notin I$ and $b \notin I$. Since $ab \notin S$, either $a \notin S$ or $b \notin S$. Without loss of generality assume the former. Then $I + (a)$ is a strictly larger ideal containing x which also does not intersect S, which contradicts the maximality of I, so that I is prime. Thus every $x \in R \setminus S$ is contained in a prime ideal, so $R \setminus S$ is a union of prime ideals.

b) Suppose R is a UFD and let $\mathfrak{p}$ be any nonzero prime ideal. Then there exists $0 \neq x \in \mathfrak{p}$, and since R is a UFD we write $x = \prod_{i=1}^{n} p_i$ where each p_i is irreducible. Since $\mathfrak{p}$ is a prime ideal, there exists some i for which $p_i \in \mathfrak{p}$, so $\mathfrak{p}$ contains the principal prime ideal (p_i).

Conversely, suppose that every nonzero prime ideal in R contains a principal prime ideal. Let S be the subset of R containing every (nonempty) product of prime elements. It will suffice to show that every nonzero element of R belongs to S. S is clearly multiplicative, and if $ab \in S$, write $ab = \prod_{i=1}^{n} p_i$ with each p_i a distinct prime. Then each p_i must divide either a or b, so that there exist subsets I, J of $\{1, ..., n\}$ with $I \cup J = \{1, ..., n\}$ such that $a = \prod_{i \in I} p_i$ and $b = \prod_{j \in J} p_j$ so $a, b \in S$, so S is a saturated multiplicative set. If there are exponents on the p_i then we obtain the same result by dividing both sides of each equation by p_i and proceeding inductively. Now suppose $0 \neq x \in R \setminus S$. Then by part a x lies in some prime ideal $\mathfrak{p}$ which does not intersect S. By assumption, $\mathfrak{p}$ contains a principal prime ideal (p), but then p is prime so $p \in S$ which contradicts that $\mathfrak{p}$ does not intersect S. Thus S contains every nonzero element of R, so every nonzero element of R is a product of primes, so R is a UFD.

18F.7, 14S.1 Let $F : \mathcal{C} \to \mathcal{D}$ be a functor with right adjoint G. Show that F is fully faithful if and only if the unit of the adjunction $\eta : \mathrm{Id}_{\mathcal{C}} \to GF$ is an isomorphism.

Solution Since G is a right adjoint of F,

$$\mathrm{Mor}_{\mathcal{D}}(F(X), F(Y)) \simeq \mathrm{Mor}_{\mathcal{C}}(X, GF(Y)) \text{ for all objects } X, Y, \in \mathcal{C}$$

F is fully faithful if and only if this set is isomorphic to $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ for all $X, Y \in \mathcal{C}$, if and only if $\eta : \mathrm{Id}_C \to GF$ is a natural isomorphism.

17S.1 Choose a representative for every conjugacy class in the group $GL(2, \mathbb{R})$. Justify your answer.

Solution Let $A \in GL(2, \mathbb{R})$. There are three cases.

Case 1: A has two distinct real eigenvalues. In this case, A must be diagonalizable (over $\mathbb{R}$) so it belongs to the same conjugacy class as the following representative.

$$[A] \ni \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \text{ for each } \lambda_1, \lambda_2 \in \mathbb{R}, \lambda_1 \neq \lambda_2$$

Case 2: A has one real eigenvalue. In this case, let its real eigenvalue be λ. The characteristic polynomial $P(x)$ of A has real coefficients, so since λ is a root, the root of $P(x)/(x - \lambda)$, which is a real number, must also be a root. Therefore λ must have algebraic multiplicity 2. Since A has all its eigenvalues in $\mathbb{R}$, it must have a Jordan canonical form in one of the two conjugacy classes below.

$$[A] \ni \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \text{ or } [A] \ni \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \text{ for each } \lambda \in \mathbb{R}$$

Case 3: A has no real eigenvalues. In this case, for any $v \in \mathbb{R}^2 \setminus \{0\}$, v and Av are linearly independent, as otherwise v would be an eigenvector for A. Let $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Then

$$\begin{aligned} A^2 v &= \begin{pmatrix} a_{11}^2 + a_{12}a_{21} & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{12}a_{21} + a_{22}^2 \end{pmatrix} v = \begin{pmatrix} a_{11}^2 + a_{12}a_{21} \\ a_{21}(a_{11} + a_{22}) \end{pmatrix} \\ &= (a_{11} + a_{22}) \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} - (a_{11}a_{22} - a_{12}a_{21}) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \mathrm{tr}(A)Av - \det(A)v \end{aligned}$$

so that, after changing basis to $\{v, Av\}$ (remaining in the same conjugacy class), we see that A belongs to the same conjugacy class as $\begin{pmatrix} 0 & -\det(A) \\ 1 & \mathrm{tr}(A) \end{pmatrix}$. This matrix has characteristic polynomial $x^2 - ax + b := x^2 - \mathrm{tr}(A)x + \det(A)$, which must have no real roots, so $a^2 - 4b < 0$.

Since every $A \in GL(2, \mathbb{R})$ falls into one of the three cases, its conjugacy class must therefore be represented by one of the following:

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \lambda_1, \lambda_2 \in \mathbb{R} \text{ or } \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \lambda \in \mathbb{R} \text{ or } \begin{pmatrix} 0 & -b \\ 1 & a \end{pmatrix}, a, b \in \mathbb{R}, a^2 - 4b < 0$$

17S.3 Find the number of subgroups of index 3 in the free group $F_2 = \langle u, v\rangle$ on two generators. Justify your answer.

Solution Let G be a subgroup of F_2 and G, xG, yG be its three left cosets. F_2 acts on $\{G, xG, yG\}$ transitively by right-multiplication, giving rise to a group homomorphism $\varphi : F_2 \to S_3$ with transitive image. Since $G = \ker(\varphi)$, it remains to find all such homomorphisms φ. φ is determined uniquely by $\varphi(u)$ and $\varphi(v)$ by the universal property of free groups, so there are the following cases since φ must have transitive image.

Case 1: $\varphi(u)$ is a 3-cycle. Then $\varphi(v)$ can be any element of S_3. This gives 6 different kernels of φ.

Case 2: $\varphi(v)$ is a 3-cycle. Then $\varphi(u)$ can be any element of S_3. Since the two cases where $\varphi(u)$ is also a 3-cycle are counted in Case 1 above, this gives 4 other different kernels of φ.

Case 3: $\varphi(u), \varphi(v)$ are two different transpositions. There are $\binom{3}{2} = 3$ ways to choose $\varphi(u)$ and $\varphi(v)$ giving 3 different kernels of φ.

Hence there are 13 possible kernels of φ, corresponding to 13 different index 3 subgroups of F_2.

17F.1 Let G be a finite group, p a prime number, and S a Sylow p-subgroup of G. Let $N = \{g \in G \mid gSg^{-1} = S\}$. Let X and Y be two subsets of $Z(S)$ (the center of S) such that there is $g \in G$ with $gXg^{-1} = Y$. Show that there exists $n \in N$ such that $nxn^{-1} = gxg^{-1}$ for all $x \in X$.

Solution Since $Y \subseteq Z(S)$, $S \subseteq C_G(Y)$ (the centralizer of Y in G), so it must be a Sylow p-subgroup of $C_G(Y)$ since it is a Sylow p-subgroup of G. We also have $gSg^{-1} \subseteq C_G(Y)$ since gSg^{-1} centralizes $gXg^{-1} = Y$, and this must also be a Sylow p-subgroup of $C_G(Y)$. Therefore S, gSg^{-1} are conjugate by an element $h \in C_G(Y)$, so that $hSh^{-1} = gSg^{-1} \Rightarrow h^{-1}g \in N$. Let $n := h^{-1}g$. Then for all $x \in X$, because $gxg^{-1} \in Y$ we have that

$$nxn^{-1} = h^{-1}gxg^{-1}h = gxg^{-1} \text{ as desired.}$$

17F.2 Let G be a finite group of order a power of a prime p. Let $\Phi(G)$ denote the subgroup of G generated by elements of the form g^p for $g \in G$ and $ghg^{-1}h^{-1}$ for $g, h \in G$. Show that $\Phi(G)$ is the intersection of maximal proper subgroups of G.

Solution Let H be a maximal subgroup of G. Then G/H is of order p, so in particular it is abelian, and therefore $[G, G] \subseteq H$. Therefore it suffices to assume G is abelian, since otherwise we would only need to show that $\Phi(G)/[G, G]$ is an intersection of maximal proper subgroups of $G/[G, G]$. By the classification of finite abelian groups, G is a product of cyclic groups $C_1, ..., C_n$, so that its maximal proper subgroups are exactly $C_1 \times ... \times C_i^p \times ... \times C_n$, so that $\Phi(G)$ is certainly a subgroup of every maximal proper subgroup.

17F.3 Let k be a field and A a finite-dimensional k-algebra. Denote by $J(A)$ the Jacobson radical of A. Let $t : A \to k$ be a morphism of k-vector spaces such that $t(ab) = t(ba)$ for all $a, b \in A$. Assume $\ker(t)$ contains no nonzero left ideal. Let M be the set of elements in A such that $t(xa) = 0$ for all $x \in J(A)$. Show that M is the largest semisimple left A-submodule of A.

Solution First, note that for any left ideal I, $I/J(A)I$ is the maximal semisimple quotient of I, so that I itself is semisimple if and only if $J(A)I = 0$.

M is a left ideal of A since for any $a \in A, x \in J(A), m \in M$, since $J(A)$ is a two-sided ideal of A, $ax \in J(A)$ so that

$$t((am)x) = t(m(ax)) = 0$$

since $t(ab) = t(ba)$. Therefore $J(A)M$ is a left ideal of A. By definition, $J(A)M \subseteq \ker(t)$, so since $\ker(t)$ contains no nonzero left ideals, $J(A)M = 0$ and so M is a semisimple left A-submodule of A.

Now let I be any semisimple left A-submodule of A. Then I is a left ideal of A so that $J(A)I = 0$. But then for every $a \in I$, $t(xa) = t(0) = 0$ for every $x \in J(A)$ so that $a \in M$. Thus M is the maximal semisimple left A-submodule of A.

17F.6 Let R be an integral domain and let M be an R-module. Prove that M is R-torsion-free if and only if the localization $M_\mathfrak{p}$ is $R_\mathfrak{p}$-torsion-free for all prime ideals $\mathfrak{p}$ of R.

Solution Suppose M is torsion-free. If $M_\mathfrak{p}$ is not $R_\mathfrak{p}$-torsion-free for some prime ideal $\mathfrak{p}$, then there exist $r \in R \setminus \{0\}, s \in R \setminus \mathfrak{p}$, and $x \in M \setminus \{0\}, t \in R \setminus \mathfrak{p}$ such that

$$\frac{r}{s} \cdot \frac{x}{t} = 0$$

Then there exists $u \in R \setminus \mathfrak{p}$ such that $urx = 0$. But $u \neq 0$ (else it would be in $\mathfrak{p}$) and $r \neq 0$, so since R is an integral domain, $ur \neq 0$. But then $x \in M \setminus \{0\}$ is R-torsion, which is a contradiction. Thus $M_\mathfrak{p}$ is $R_\mathfrak{p}$-torsion-free for every prime ideal $\mathfrak{p}$.

Conversely, suppose that $M_\mathfrak{p}$ is $R_\mathfrak{p}$-torsion-free for every prime ideal $\mathfrak{p}$. Suppose M is not R-torsion-free. Then there exist $r \in R \setminus \{0\}, x \in M \setminus \{0\}$ such that $rx = 0$. r is certainly not a unit, so it is contained in some maximal (hence prime) ideal $\mathfrak{m}$. Then

$$\frac{r}{1} \cdot \frac{x}{1} = 0$$

so that $M_\mathfrak{m}$ is not $R_\mathfrak{m}$-torsion-free, which is a contradiction. Thus M is R-torsion-free.

17F.7 a) Show that there is at most one extension $F(\alpha)$ of a field F such that $\alpha^4 \in F, \alpha^2 \notin F$, and $F(\alpha) = F(\alpha^2)$.
b) Find the isomorphism class of the Galois group of the splitting field of $x^4 - a$ for $a \in \mathbb{Q}$ with $a \notin \pm\mathbb{Q}^2$.

Solution a) Since $\alpha^4 \in F$, $x^4 - \alpha^4 \in F[x]$ and the minimal polynomial f of α must divide this. Moreover, since $\alpha^2 \notin F$, $x^2 - \alpha^4$ is the minimal polynomial of α^2 so that $[F(\alpha) : F] = [F(\alpha^2) : F] = 2$, so $\deg(f) = 2$. f must then have α as a root and one other root, which cannot be $\pm\alpha$ since $\alpha^2 \notin F$. Thus it must be one of the other roots of $x^4 - \alpha^4$, namely $\pm\alpha\sqrt{-1}$. If $\sqrt{-1} \in F$ then we have a contradiction here, so in this case there is no such extension $F(\alpha)$, so for the remainder of this part assume that $\sqrt{-1} \notin F$. Then the constant term of f is $\pm\alpha^2\sqrt{-1} \in F$ (depending on which is the root of f), so that $\sqrt{-1} \in F(\alpha^2) = F(\alpha)$. But then $F(\alpha) = F(\sqrt{-1})$, so in this case there is only one such extension $F(\alpha)$. (part b on next page)

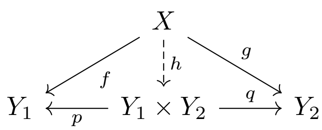
b) The roots of $x^4 - a$ in the algebraic closure of $\mathbb{Q}$ are $\sqrt{-1}^n \sqrt[4]{a}$ for $n = 0, 1, 2, 3$, so its splitting field must contain $\sqrt{-1}$ and $\sqrt[4]{a}$. The field $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{a})$ does contain all of these roots so it is the splitting field of $x^4 - a$. Moreover, since $a \notin \pm\mathbb{Q}^2$, $(\sqrt[4]{a})^2 \notin \mathbb{Q}$ so that $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}] = 4$. Since $\sqrt{-1} \notin \mathbb{Q}(\sqrt[4]{a})$, we must have that $[\mathbb{Q}(\sqrt{-1}, \sqrt[4]{a}) : \mathbb{Q}] = 8$. Thus the Galois group of $x^4 - a$ is isomorphic to a subgroup of S_4 of order 8. But then it is a Sylow 2-subgroup of S_4, so by Sylow's theorems it is isomorphic to D_8.

17F.10 Let $\mathcal{C}$ be a category with finite products, and let $\mathcal{C}^2$ be the category of pairs of objects of $\mathcal{C}$ together with morphisms $(A, B) \to (A, B')$ of pairs consisting of pairs $(A \to A', B \to B')$ of morphisms in $\mathcal{C}$. Let $F : \mathcal{C}^2 \to \mathcal{C}$ be the direct product functor.

a) Find a left adjoint to F.

b) For $\mathcal{C}$ the category of abelian groups, determine whether or not F has a right adjoint.

Solution a) Define $G : \mathcal{C} \to \mathcal{C}^2$ by $G(A) = (A, A)$ and $G(A \to B) = (A \to B, A \to B)$. Now for any $X \in \mathcal{C}, Y = (Y_1, Y_2) \in \mathcal{C}^2$, write any morphism in $\mathrm{Mor}_{\mathcal{C}^2}(GX, Y)$ as (f, g). This gives two morphisms in $\mathcal{C}$: $f : X \to Y_1$ and $g : X \to Y_2$. Then by the universal property of direct products there is a unique h which makes the following diagram commute



This gives a natural injective correspondence $\mathrm{Mor}_{\mathcal{C}^2}(GX, Y) \to \mathrm{Mor}_{\mathcal{C}}(X, FY)$ by $(f, g) \mapsto h$. Finally, for every $h \in \mathrm{Mor}_{\mathcal{C}}(X, GY)$, there is $f = p \circ h, g = q \circ h$ such that $(f, g) \mapsto h$ so that this is surjective as well, so that $\mathrm{Mor}_{\mathcal{C}^2}(GX, Y)$ and $\mathrm{Mor}_{\mathcal{C}}(X, FY)$ are naturally isomorphic and hence G is a left adjoint to F.

b) The category of abelian groups is abelian, so products are equivalent to coproducts and therefore reversing every arrow in part (a) gives a right adjoint to F.

14S.3 Given $\phi : A \to B$ a surjective morphism of rings, show that the image in ϕ of the Jacobson radical of A is contained in the Jacobson radical of B.

Solution Let $J(A), J(B)$ denote the Jacobson radicals of A, B respectively, and let $x \in J(A)$. Then for all $y \in R$, $xy - 1_A$ is a unit in A, so let $u(xy - 1_A) = 1_A$. For all $y' \in B$, since ϕ is surjective there exists a $y \in A$ such that $\phi(y) = y'$. But then

$$\phi(u)(\phi(x)\phi(y) - 1_B) = \phi(u(xy - 1_A)) = \phi(1_A) = 1_B$$

so that $\phi(x)y' - 1_B$ is a unit in B for all $y' \in B$. Therefore $\phi(x) \in J(B)$, so that $\phi(J(A)) \subseteq J(B)$.

14S.6 Let A be a ring and M a Noetherian A-module. Show that any surjective morphism of A-modules $M \to M$ is an isomorphism.

Solution Let $f : M \to M$ be a surjective morphism of A-modules. Consider the ascending chain of submodules given by

$$\ker(f) \subseteq \ker(f^2) \subseteq \ker(f^3) \subseteq \ldots$$

Since M is Noetherian, there exists $n \in \mathbb{N}$ such that for all $N \geq n$, $\ker(f^n) = \ker(f^N)$. Now let $x \in \ker(f^n) \cap \mathrm{Im}(f^n)$. Then there exists $y \in M$ such that $f^n(y) = x$. But then $f^{2n}(y) = f^n(x) = 0$ so $y \in \ker(f^{2n})$. But $\ker(f^{2n}) = \ker(f^n)$, so that $x = f^n(y) = 0$. Thus $\ker(f^n) \cap \mathrm{Im}(f^n) = \{0\}$. But f is surjective, so $\mathrm{Im}(f^n) = M$, so that we must have $\ker(f^n) = \{0\}$. Then $\ker(f) \subseteq \ker(f^n) = \{0\}$, so that f must be injective and so f is an isomorphism.

14S.7 Let G be a finite group and let s, t be two distinct elements of order 2. Show that the subgroup of G generated by s and t is a dihedral group. (The dihedral groups are $D_{2m} = \langle g, h \mid g^2, h^2, (gh)^m \rangle$ for some $m \geq 2$).

Solution Let H denote the subgroup in question. There exists a finite n such that $|st| = n$ because G is finite, and moreover $n \geq 2$ because $|s| = 2$ means that $t \neq s = s^{-1}$ so $st \neq e$. This gives a surjection $f : H \to D_{2n}$ by $f(s) = g, f(t) = h$. It now suffices to show that f is injective. First note that $|ts| = n$ as well, since

$$t = t(st)^n = (ts)^n t \Rightarrow (ts)^n = e$$

and if $|ts| < n$ then $|st| < n$ by the same equation with the exponent reduced. Suppose that f is not injective. Then there exists a $0 < k < n$ such that $f((st)^k s) = e$ or $f((st)^k t) = e$ (without loss of generality assume the former). Then

$$f((st)^k) = f(s^{-1}) = f(s) = g \Rightarrow f((st)^{2k}) = e \text{ and}$$
$$f((st)^{k+1}) = f(t^{-1}) = f(t) = h \Rightarrow f((st)^{2k+2}) = e$$

so that $f((st)^2) = e$. If k is even, then $f(s) = f((st)^k s) = e$ which is a contradiction, and if k is odd,

$$f(sts) = f((st)^k s) = e \Rightarrow ghg = e$$

which is not true in any dihedral group, so we again have a contradiction. Therefore f is injective.

16F.1 Let G be a group generated by a and b with the only relation $a^2 = b^2 = 1$ for the group identity 1. Determine the group structure of G.

Solution $G \mapsto (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/2\mathbb{Z})$ by letting a denote the nonzero element of the first copy of $\mathbb{Z}/2\mathbb{Z}$ and b the nonzero element of the second copy. By the universal property of free products, this gives a unique group homomorphism. Since this homomorphism has an inverse which maps the nonzero element of the first $\mathbb{Z}/2\mathbb{Z}$ to a and the nonzero element of the second copy to b, it is an isomorphism.

16F.4 Let D be a dihedral group of order $2p$ with normal cyclic subgroup C of order p for p an odd prime. Find the number of n-dimensional irreducible representations of D (up to isomorphisms) over $\mathbb{C}$ for each n, and justify your answer.

Solution Write $D = \langle r, s \mid r^o, s^2, (sr)^2 \rangle$. Then C is the subgroup generated by r. Conjugating these elements gives

$$\begin{aligned}
&r^j r^i r^{-j} = r^i \\
&(sr^j)r^i(sr^j)^{-1} = s(r^j r^i r^{-j})s = r^{-i} \\
&r^j s r^i r^{-j} = sr^{i-2j} \\
&(sr^j)sr^i(sr^j)^{-1} = r^{-j}r^i r^{-j}s = sr^{2j-i}
\end{aligned}$$

Therefore the conjugacy classes of D are given by pairs of rotation ($\{1\}$, $\{r, r^{-1}\}$, $\{r^2, r^{-2}\}$, ..., $\{r^{(p-1)/2}, r^{(p+1)/2}\}$), of which there are $(p+1)/2$, and every reflection lying in the same conjugacy class, as for any i, j we see that

$$sr^i = r^k(sr^j)r^{-k} \text{ where } k = \begin{cases} \frac{i-j}{2} & i-j \text{ is even} \\ \frac{i-j+p}{2} & i-j \text{ is odd} \end{cases}$$

so that D has $(p+3)/2$ many conjugacy classes, and therefore that many total irreducible representations over $\mathbb{C}$. Now,

$$\begin{aligned}
&[r^i, r^j] = 0 \\
&[sr^i, sr^j] = 0 \\
&[r^i, sr^j] = r^i sr^j r^{-i} r^{-j} s = r^i s^2 r^i = r^{2i}
\end{aligned}$$

so that $[D, D] = C$ since for any j, either j or $p + j$ is even so $r^j = r^{2i}$ for $i = j/2$ or $i = (p + j)/2$. Since C has index 2 in D, there must be exactly 2 1-dimensional irreducible representations of D over $\mathbb{C}$. Now, take the following 2-dimensional representations of D over $\mathbb{C}$:

$$r \mapsto \begin{pmatrix} \cos(\frac{2\pi k}{p}) & -\sin(\frac{2\pi k}{p}) \\ \sin(\frac{2\pi k}{p}) & \cos(\frac{2\pi k}{p}) \end{pmatrix}, \; s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ for each } 1 \leq k \leq \frac{p-1}{2}$$

The matrix for r has two distinct complex eigenvalues $\pm e^{2\pi ik/p}$ for each k, with corresponding eigenvectors $(1, \mp i)$. But neither of these spans an invariant subspace, because the matrix for s interchanges the two. Therefore, for each k this defines a 2-dimensional irreducible representation of D over $\mathbb{C}$, and there are $(p-1)/2$ of these. Adding the two 1-dimensional representations gives a total of $(p+3)/2$, so there must be no more irreducible representations of D over $\mathbb{C}$.

16F.5 Let $f \in F[x]$ be an irreducible separable polynomial of prime degree over a field F and let K/F be a splitting field of F. Prove that there is an element in the Galois group of K/F permuting cyclically all roots of f in K.

Solution Consider $\text{Gal}(K/F) \subseteq S_p$ where $p = \deg(f)$ is prime. Then since $p | [K : F] = |\text{Gal}(K/F)|$, by Cauchy's Theorem $\text{Gal}(K/F)$ contains an element of order p. But the only elements of S_p of order p are the p-cycles, so $\text{Gal}(K/F)$ contains a p-cycle, which permutes cyclically all roots of f in K.

16F.6, 19S.6 Let F be a field of characteristic $p > 0$. Prove that for every $a \in F$, the polynomial $x^p - a$ is either irreducible or split into a product of linear factors.

Solution Let L/F be any field extension of F that contains some root α of $x^p - a$. Then L is also of characteristic p, so that

$$(x-\alpha)^p = x^p - \alpha^p = x^p - a \text{ in } L[x]$$

Suppose $x^p - a$ is reducible in $F[x]$. Then $f = gh$ where $g, h \in F[x]$ are not units (i.e. not constant polynomials). Then in $L[x]$ we have that

$$(x-\alpha)^p = g(x)h(x) \Rightarrow g(x) = (x-\alpha)^r \text{ for some } 1 \le r \le p-1$$

since $L[x]$ is Euclidean, and hence a UFD. Therefore $g(x) = (x-\alpha)^r = x^r - r\alpha x^{r-1} + ... + (-\alpha)^r \in F[x]$. In particular $r\alpha \in F$, but $1 \le r \le p$ so $\alpha = r^{-1}(r\alpha) \in F$, so $x^p - a$ splits in $F[x]$ as $x^p - a = (x-\alpha)^p$.

16F.7 Let $f \in \mathbb{Q}[x]$ and $\zeta \in \mathbb{C}$ a root of unity. Prove that $f(\zeta) \neq 2^{\frac{1}{4}}$.

Solution Suppose there exists a root of unity ζ such that $f(\zeta) = 2^{\frac{1}{4}}$. Then $2^{\frac{1}{4}} \in Q(\zeta)$, so we have that

$$\mathrm{Gal}(Q(\zeta)/Q(2^{\frac{1}{4}})) \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

Since ζ is a root of unity, the latter group is cyclic. But then the former group is a normal subgroup of the latter, so that $Q(2^{\frac{1}{4}})/\mathbb{Q}$ is a normal extension. But $x^4 - 2$ is irreducible over $\mathbb{Q}$, has a root (namely, $2^{\frac{1}{4}}$) in $Q(2^{\frac{1}{4}})$, but does not split in this field (since it does not contain the imaginary roots), which is a contradiction, so there exists no such ζ and f.

16F.8 Prove that if a functor $\mathcal{F} : \mathcal{C} \to \mathit{Sets}$ has a left-adjoint functor, then $\mathcal{F}$ is representable.

Solution Let the left adjoint of $\mathcal{F}$ be $\mathcal{G}$. Let S be a singleton set. Then for each $B \in \mathrm{Ob}(\mathcal{C})$, $FB \simeq \mathrm{Mor}_{Sets}(S, \mathcal{F}B) \simeq \mathrm{Mor}_{\mathcal{C}}(\mathcal{G}S, B)$ by adjunction, so that S represents $\mathcal{F}$.

16F.9 Let F be a field and $a \in F$. Prove that the functor from the category of commutative F-algebras to *Sets* taking an algebra R to the set of invertible elements of the ring $R[x]/(x^2 - a)$ is representable.

Solution $R[x]/(x^2 - a) \simeq R^2$ by $a_1 x + a_0 \mapsto (a_1, a_0)$, with (a_1, a_0) invertible if and only if there exist b_1, b_0 such that $(a_0 b_1 + a_1 b_0, a_0 b_0 + a a_1 b_1 - 1) = (0, 0)$. Therefore the given functor is represented by the commutative F-algebra $F[a_1, a_0, b_1, b_0]/(a_0 b_1 + a_1 b_0, a_0 b_0 + a a_1 b_1 - 1)$. Fix disjoint open neighborhoods U_i of $g_i x$, and let $V_i = \bigcap_{j=1}^n g_i g_j^{-1}$. Then the V_i are still disjoint and have the additional property that (if we label $g_1 = e$) $V_i = g_i V$.

18S.1 Let $\alpha \in \mathbb{C}$ and suppose that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite and coprime to $n!$ for some integer $n > 1$. Show that $\mathbb{Q}(\alpha^n) = \mathbb{Q}^{\alpha})$.

Solution $\mathbb{Q}(\alpha^n)$ is an intermediate field of $\mathbb{Q}(\alpha)/\mathbb{Q}$, so that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)]$ divides both $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and n. But since these two are coprime, we must then have that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^n)$.

18S.2 Let $\zeta^9 = 1$ where $\zeta^3 \neq 1$ for $\zeta \in \mathbb{C}$.
a) Show that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$.
b) If $\alpha^3 = 3$, show that α is not a cube in $\mathbb{Q}(\zeta, \alpha)$.

Solution a) Suppose $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$. Then $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt[3]{3})$ is a subgroup of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ which is cyclic since ζ is a root of unity, so that the former is a normal subgroup of the latter. But then $\mathbb{Q}(\sqrt[3]{3})$ must be a normal extension, but it is not since the polynomial $x^3 - 3$ has one root in $\mathbb{Q}(\sqrt[3]{3})$ but not all three. Therefore we have a contradiction, so that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$.

b) Suppose $\alpha = \beta^3$ in $\mathbb{Q}(\zeta, \alpha)$. Then $x^9 - 3$ splits over $\mathbb{Q}(\zeta, \alpha)$ as $x^9 - 3 = \prod_{j=1}^9 (x - \beta\zeta^j)$. Now let K be a splitting field of $x^9 - 3$. Then $\sqrt[9]{3} \in K$, but $x^6 + 3^{1/3}x^3 + 3^{2/3}$ does not split over $\mathbb{Q}(\sqrt[9]{3})$ so that $[K : \mathbb{Q}] \geq 54$. But $[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = 27$, which gives a contradiction, so α is not a cube in $\mathbb{Q}(\zeta, \alpha)$.

18S.3 Let $\mathbb{Z}^n$ ($n > 1$) be made of column vectors with integer coefficients. Prove that for every non-zero left ideal I of $M_n(\mathbb{Z})$, $I\mathbb{Z}^n$ (the subgroup generated by products αv for $\alpha \in M_n(\mathbb{Z})$ and $v \in \mathbb{Z}^n$) has finite index in $\mathbb{Z}^n$.

Solution Let I be a nonzero left ideal and $0 \neq M \in I$. Then the matrix M_i which is M with every row except the i^{th} replaced with zero is in I, because it is M left-multiplied with the matrix which is zero outside of the $(i,i)^{th}$ entry which is 1. Let $e_1, ..., e_n$ be the standard basis vectors in $\mathbb{Z}^n$; then $M_i e_j = M_{ij} e_j$ where M_{ij} is the $(i,j)^{th}$ entry of M. Furthermore, let S_{jk} be a matrix such that $S_{jk} e_j = e_k$, so that we have $(S_{jk} M_i) e_j = M_{ij} e_k$ where the matrix on the left-hand side is certainly in I because M is. Then $I\mathbb{Z}^n$ is generated by

$$G := \{ae_k \mid 1 \leq k \leq n, \exists M \in I : \ a \text{ is the } (i,j)^{th} \text{ entry of M}\}$$

Consider now $\{a \mid ae_k \in G \text{ for some } k\}$. If $ae_k \in G$ for some k, then $ae_k \in G$ for every $1 \leq k \leq n$ by left-multiplying by the correct matrix $S_{k_1 k_2}$. Let the gcd of $\{a \,|\, ae_k \in G \text{ for some } k\}$ (which is always a $\mathbb{Z}$-linear combination of these elements) be α. Then every element of G can be written as a multiple of αe_k for some k, so that $I\mathbb{Z}^n$ is generated by elements of the form $\{\alpha e_k \,|\, 1 \leq k \leq n\}$, so it is a subgroup of $\mathbb{Z}^n$ of index $\alpha^n < \infty$.

18S.4 Let p be a prime number, and let D be a central simple division algebra of dimension p^2 over a field k. Pick $\alpha \in D$ not in the center and write K for the subfield of D generated by α. Prove that $D \otimes_k K \simeq M_p(K)$ (the algebra of $p \times p$ matrices over K).

Solution Because D is central simple over k, $D \otimes_k K$ is central simple over K, so by the Artin-Wedderburn Theorem it is isomorphic to some matrix algebra $M_n(L)$ where L is a division algebra over K. Now, $K = k[x]/(f)$ where f is the minimal polynomial of α, so $K \otimes_k K = K[x]/(f)$, which is not a domain (and hence not a division algebra) because f is not irreducible over K by definition. Therefore $D \otimes_k K$ is not a division algebra either, so $n > 1$. Therefore, since D is p^2-dimensional, we must have that $L = K$ and $n = p$, as desired.

18S.5 Let ALG be the category of $\mathbb{Z}$-algebras and MOD the category of $\mathbb{Z}$-modules.
a) Prove that in MOD, $f : M \to N$ is an epimorphism if and only if it is a surjection.
b) In ALG, does the above equivalence hold? Give a proof or counterexample.

Solution a) Let f be a surjection and $g, h : N \to X$ such that $g \circ f = h \circ f$. Then for every $y \in N$, there exists $x \in f^{-1}(y)$ so that $g(y) = (g \circ f)(x) = (h \circ f)(x) = h(y)$ so that $g = h$. Hence f is an epimorphism. Conversely, suppose f is an epimorphism. Then consider the morphisms $\pi, 0 : N \to N/f(M)$ where $\pi(y)$ is the coset $y + f(M)$ and $0(y) = 0$ for all y. Then $\pi \circ f = 0 \circ f = 0$, so $\pi = 0$. But this is only the case when $f(M) = N$, so f is a surjection.

b) The above equivalence is false. Consider $i : \mathbb{Z} \to \mathbb{Q}$ by $i(n) = n$. Then i is not surjective as, for instance, $1/2$ is not in its image. However, for any $g, h : \mathbb{Q} \to A$ where A is any $\mathbb{Z}$-algebra, we have that if $g \circ i = h \circ i$,

$$g(\frac{p}{q}) = \frac{g(p)}{g(q)} = \frac{g(i(p))}{g(i(q))} = \frac{h(i(p))}{h(i(q))} = \frac{h(p)}{h(q)} = h(\frac{p}{q}) \text{ for all } \frac{p}{q} \in \mathbb{Q}$$

so that $g = h$. Therefore i is a non-surjective epimorphism.

18S.6 Let G be a group with a normal subgroup $N = \langle y, z \rangle$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Suppose that G has a subgroup $Q = \langle x \rangle$ isomorphic to the cyclic group $\mathbb{Z}/2\mathbb{Z}$ such that the composition $Q \subseteq G \to G/N$ is an isomorphism. Finally, suppose that $xyx^{-1} = z$ and $xzx^{-1} = yz$. Compute the character table of G.

Solution The given relations show that all the nontrivial elements of N are conjugate to each other (as $xyzx^{-1} = xyx^{-1}yz = y$), so since N is normal these three elements must form a conjugacy class. Also, since Q is isomorphic to G/N, conjugating x by any element of N does not change which coset of G/N it corresponds to so that x and x^2 define two separate conjugacy classes of cardinality 4. To find the number of irreducible 1-dimensional complex representations of G, note that $Q \simeq G/N$ is abelian of order 3, so there are at least 3 irreducible 1-dimensional complex representations of G. But there cannot be more than 3, since there are only 4 conjugacy classes so there are only 4 irreducible complex representations of G in total, the square of whose dimensions must add up to 12. Therefore there are 3 1-dimensional irreducible representations and 1 3-dimensional irreducible representation. For each 1-dimensional representation χ, we must have that $\chi(y) = \chi(z) = \chi(yz)$, so that $\chi(y) = 1$, so that $\chi(x) \in \{\zeta, \zeta^2\}$ (where ζ is a primitive cube root of unity) if χ is nontrivial. Finally, by Schur's orthogonality the last row must be $(3, -1, 0, 0)$, giving the following character table

G	1	y	x	x^2
1	1	1	1	1
χ_1	1	1	ζ	ζ^2
χ_2	1	1	ζ^2	ζ
χ_3	3	-1	0	0

Remark: This group is just A_4.

18S.7 Let B be a commutative Noetherian ring, and let A be a commutative Noetherian subring of B. Let I be the nilradical of B. If B/I is finitely generated as an A-module, show that B is finitely generated as an A-module.

Solution Since B is Noetherian, I is a finitely-generated B-module, so that each I^k/I^{k+1} is a finitely-generated B/I-module (hence a finitely generated A-module). Let $x_1, ..., x_n$ be the generators of I as a B-module and $e_1, ..., e_n$ exponents such that $x_i^{e_i} = 0$. Then if $e = 1 + \sum_{i=1}^n e_i$, $I^e = 0$. But then $I^{e-1}/I^e = I^{e-1}$ is a finitely generated A-module, and for each $1 \leq k < e-1$ we have the short exact sequences

$$0 \to I^{k+1} \to I^k \to I^k/I^{k+1} \to 0$$

so that by induction we get that I is a finitely-generated A-module. Then the short exact sequence

$$0 \to I \to B \to B/I \to 0$$

gives that B is a finitely-generated A-module, as desired.

18S.9 Show that there is no simple group of order 616.

Solution Suppose that there is a group G of order $616 = 2^3 \cdot 7 \cdot 11$. Let n_p be the number of Sylow p-subgroups of G. Then since G is simple, $n_2, n_7, n_11 \neq 1$ as otherwise that one subgroup would be normal by Sylow's theorems. Therefore

$$n_7|88 \text{ and } n_7 \equiv 1(\text{mod } 7) \Rightarrow n_7 = 8 \text{ or } 22$$
$$n_{11}|56 \text{ and } n_{11} \equiv 1(\text{mod } 11) \Rightarrow n_{11} = 56$$

Since all Sylow 7 and 11-subgroups have prime order, they are all cyclic so that distinct Sylow 7 and 11-subgroups share no elements of order 7 and 11 respectively. Therefore G must contain $56 \cdot 10 = 560$ distinct elements of order 11 from all 56 of its Sylow 11-subgroups. If $n_7 = 22$ it would also contain $22 \cdot 6$ distinct elements of order 7, giving it at least $560 + 132 = 692$ elements which contradicts that it has order 616, so $n_7 = 8$. Then G contains $8 \cdot 6 = 48$ distinct elements of order 7, so it has a total of $560 + 48 = 608$ distinct elements of order 7 or 11. But then the remaining 8 elements can only form one Sylow 2-subgroup (since Sylow 2-subgroups have order 8), which is then normal in G, which is a contradiction. Therefore no such group G can exist.

19F.1 Show that every group of order 315 is the direct product of a group of order 5 with a semidirect product of a normal subgroup of order 7 and a subgroup of order 9. How many such isomorphism classes are there?

Solution Let H_3 be a Sylow 3-subgroup of G. H_3 is of order 9, so it must be abelian, and its automorphism group has order 6. Let H_5 be any Sylow 5-subgroup of G. Then H_5 has order 5 so that every homomorphism $H_5 \to \mathrm{Aut}(H_3)$ is trivial, so that H_5 centralizes H_3 and therefore $H_3 \subseteq N_G(H_5)$, and this latter group has index at most 7 since it must contain H_3 and H_5. Suppose H_5 is not normal in G. Then by Sylow's Theorems we have that the number of Sylow 5-subgroups $n_5 = [G : N_G(H_5)] = 7 \neq 1 (\mathrm{mod}\ 5)$ which is a contradiction, so that H_5 is normal in G, and so it is the only Sylow 5-subgroup of G. We can similarly deduce (since 7 is coprime to 6, and also $5 \neq 1 (\mathrm{mod}\ 7)$) that the Sylow 7-subgroup H_7 of G is also normal in G. Now H_3, H_5, H_7 intersect each other only trivially (since their nontrivial elements must have order 3 or 9, 5, and 7, respectively), so $G = H_3H_7H_5$ since the latter is a subgroup of order 315. Now, H_3H_7 has order 63, but H_5 must be cyclic so its automorphism group has order 4, so there is no nontrivial homomorphism $H_3H_7 \to \mathrm{Aut}(H_5)$, so that $G = H_3H_7 \times H_5 =: H \times H_5$. H_7 is normal in H because it is normal in G, so that H is the semidirect product of H_3 of order 9 and H_7 of order 7. To form this semidirect product, note that H_3 is isomorphic to either $\mathbb{Z}/9\mathbb{Z}$ or $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ while $\mathrm{Aut}(H_7)$ has order 6, so that there are two homomorphisms from each of the former into the latter (the trivial one, and the one mapping an element of order 3 to an element of order 3), so there are four different ways to form this semidirect product, and hence 4 different groups G of order 315.

19F.6 Classify all finite subgroups of $GL(2, \mathbb{R})$ up to conjugacy.

Solution (*Fairly nonstandard - don't do something like this on the actual algebra qual!*) Let $\langle \cdot, \cdot \rangle_1, \langle \cdot, \cdot \rangle_2$ be inner products on $\mathbb{R}^2$ and let A, B be their matrices respectively. Let $\mathcal{B}_1, \mathcal{B}_2$ be bases for $\mathbb{R}^2$ such that A and B are the identity matrix with coordinates in each basis (these exist by the Spectral Theorem since A, B are symmetric real matrices) and let S be the change of basis matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$. Then $B = SAS^{-1}$, so that the two inner products are conjugate, and therefore their corresponding orthogonal groups $O_i(2) := \{M \in GL(2, \mathbb{R}) \mid \langle Mx, My \rangle_i = \langle x, y \rangle_i \ \forall x, y \in \mathbb{R}^2\}$ are conjugate. In particular, the orthogonal group of every inner product on $\mathbb{R}^2$ is conjugate to the standard orthogonal group $O(2)$. Now let $G \subseteq GL(2, \mathbb{R})$ be a finite subgroup. Then G is a compact group so let μ be the Haar measure on it such that $\mu(G) = 1$. Then let

$$\langle x, y \rangle_G := \int_G \langle gx, gy \rangle d\mu(g)$$

where $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{R}^2$. Then $\langle \cdot, \cdot \rangle_G$ is an inner product for which every element of G is orthogonal, so some conjugate of G is a subgroup of the standard orthogonal group $O(2)$. Let $H := G \cap SO(2)$. Then H is a finite subgroup, so it is cyclic as it can only contain rotations by integer fractions of 2π, so if $H = G$ then G is cyclic. If $H \geq G$ then there exists $g \in G$ such that $\det(g) = -1$. Since $[O(2) : SO(2)] = 2$, g together with H must generate G, so G is isomorphic to a dihedral group where elements of H are the rotations and g is the reflection. Therefore, up to conjugacy, every finite subgroup of $GL(2, \mathbb{R})$ is either cyclic or a dihedral group.

19F.7 Let G be the group of order 12 with presentation

$$G = \langle g, h | g^4 = 1, h^3 = 1, ghg^{-1} = h^2 \rangle$$

Find the conjugacy classes of G and the values of the characters of the irreducible complex representations of G of dimension greater than 1 on representatives of these classes.

Solution From $ghg^{-1} = h^2$ we have $h^2g = gh$, so that for any $h^ig \in G$ we can rewrite it in the form gh^j where $2i \equiv j (\text{mod } 3)$, so it suffices to conjugate h by powers of g to compute its conjugacy class. We have that

$$g^2hg^{-2} = g^2hg^2 = g^2h^4g^2 = g^2gh^2g = g^4h = h \text{ and } g^3hg^{-3} = g^3hg = g^3h^4g = g^3gh^2 = h^2$$

and similarly conjugating h^2 by any power of g gives only h and h^2, so that $\{h, h^2\}$ is a conjugacy class in G. Similarly to the h case, to compute the conjugacy class of G it suffices to conjugate by powers of h since we can write any $gh^j = h^j i$, so we have that

$$hgh^{-1} = hgh^2 = h^4gh^2 = gh^4 = gh \text{ and } h^2gh^{-2} = h^2gh = ghh = gh^2$$
$$h(gh)h^{-1} = hghh^2 = h^4g = gh^2 \text{ and } h^2(gh)h^{-2} = h^2ghh = ghh^2 = g$$
$$h(gh^2)h^{-1} = hgh^2h^2 = h^4gh = gh^3 = g \text{ and } h^2(gh^2)h^{-2} = h^2gh^2h = gh$$

so that $\{g, gh, gh^2\}$ is a conjugacy class. Similarly, we have the conjugacy class $\{g^3, g^3h, g^3h^3\}$ by conjugating $g^3 = g^{-1}$. By the above we see that g^2 commutes with h, so it lies in its own conjugacy class, and conjugating g^2h gives the last conjugacy class $\{g^2h, g^2h^2\}$ since $g(g^2h)g^{-1} = g^3h^4g^3 = g^3gh^2g^2 = g^2h^2$, so these along with the aforementioned $\{h, h^2\}$ and the trivial $\{1\}$ make up all conjugacy classes of G. Because there are six conjugacy classes, there are six irreducible representations of G over $\mathbb{C}$. We see that $\langle h \rangle$ is normal in G because it is the union of conjugacy classes, so $G/\langle h \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ is abelian and therefore there are at least 4 1-dimensional irreducible representations. There cannot be more than 4, since the only larger quotient of G is G itself and G is not abelian. For these representations, we must have that $\chi(h) = \chi(h^2) = \chi(h)^2 \Rightarrow \chi(h) = 1$ (since it is not zero), and $\chi(g^2)^2 = 1 \Rightarrow \chi(g^2) = \pm 1$, and therefore $\chi(g) = \pm\sqrt{\pm 1}$, which gives all four 1-dimensional representations:

G	1	g^2	h	g	g^3	g^2h
1	1	1	1	1	1	1
χ_1	1	1	1	-1	-1	1
χ_2	1	-1	1	i	-i	-1
χ_3	1	-1	1	-i	i	-1
χ_4						
χ_5						

The final representations must be 2-dimensional since their dimensions squared must add to 8. By Schur's orthogonality, $\chi(g) = \chi(g^3) = 0$ as there is no other way to be orthogonal to all of $\pm 1, \pm i$, so we can complete the character table:

G	1	g^2	h	g	g^3	g^2h
1	1	1	1	1	1	1
χ_1	1	1	1	-1	-1	1
χ_2	1	-1	1	i	-i	-1
χ_3	1	-1	1	-i	i	-1
χ_4	2	2	-1	0	0	-1
χ_5	2	-2	-1	0	0	1

19S.1 Let G be a finite solvable group and $1 \neq N \subseteq G$ a minimal normal subgroup. Prove that there exists a prime p such that either N is cyclic of order p or a direct product of such groups.

Solution Since N is normal in G, it must also be solvable, so $N \neq [N,N]$. But $[N,N]$ is characteristic in H and therefore normal in G, so by minimality $[N,N] = 1$ so that N is abelian. Now suppose $p||N|$. Then since N is abelian, it has a characteristic Sylow p-subgroup, so again by minimality that Sylow p-subgroup must be N itself so $|N|$ is a power of p. Finally, pN is a characteristic subgroup of H so we must have that $pN = 1$, so that N has no elements of order greater than p, which implies that N is a product of cyclic groups of order p.

19S.2 An additive group (abelian group written additively) Q is called divisible if any equation $nx = y$ for $0 \neq n \in \mathbb{Z}, y \in Q$ has a solution $x \in Q$. Let Q be a divisible group and A a subgroup of an abelian group B. Give a complete proof of the following: every group homomorphism $A \to Q$ can be extended to a group homomorphism $B \to Q$.

Solution Fix a group homomorphism $\varphi : A \to Q$. Let S be the set (partially ordered under inclusion) of ordered pairs (H, ψ_H) of subgroups H of B containing A and group homomorphisms $\psi : H \to Q$ which extend φ. Let $\mathcal{C}$ be a chain in S; then $H^* := \bigcup_{(H,\psi_H)\in\mathcal{C}} H$ is a subgroup of B which contains A, and defining ψ_{H^*} on this union by $\psi_{H^*}(x) = \psi_H(x)$ whenever $x \in H$ gives a group homomorphism $\psi_{H^*} : H^* \to Q$ which extends φ. Therefore H^* is an upper bound for the chain $\mathcal{C}$, so by Zorn's Lemma we take a maximal element (M, ψ_M) of S. Now let $x \in B \backslash M$. If $x^n \notin B$ for all $n \in \mathbb{Z}$, then define $\psi : \langle M, x\rangle \to Q$ by $\psi(m) = \psi_M(m)$ for each $m \in M$ and $\psi(x) = 1$, which defines a group homomorphism which extends ψ_M over a larger subgroup of B, which contradicts the maximality of M. If $x^n \in M$ for some $n \in \mathbb{Z}$, then define $\psi : \langle M, x\rangle \to Q$ by $\psi(m) = \psi_M(m)$ for each $m \in M$ and $\psi(x) = y$ where $ny = \psi(x^n)$, which gives a well-defined group homomorphism which similarly contradicts the maximality of M. Therefore such an x cannot exist so that $M = B$ which proves the desired extension.

19S.3 Let $d > 2$ be a square-free integer. Show that the integer 2 in $\mathbb{Z}[-d]$ is irreducible but the ideal (2) in $\mathbb{Z}[-d]$ is not a prime ideal.

Solution Let $N : \mathbb{Z}[-d] \to \mathbb{Z}$ be defined by $N(a+b\sqrt{-d}) = a^2 + db^2$. Then N is a group homomorphism because $N(a+b\sqrt{-d}) = (a+b\sqrt{-d})(a-b\sqrt{-d})$, and N is nonnegative, so if $xy = 2$ then $N(x), N(y)|N(2) = 4$. If neither x nor y is a unit, then neither $N(x), N(y)$ can be 1 so that $N(x) = N(y) = 2$. Write $x = a + b\sqrt{-d}$; then $a^2 + db^2 = 2$, but $d > 2$ so we have a contradiction since this equation has no integer solutions. Therefore x or y is a unit, so 2 is irreducible.

On the other hand, depending on the parity of d either $1+d$ or $4+d$ is even, so either $(1+d) \in (2)$ or $(4+d) \in (2)$. But $1+d = (1+\sqrt{-d})(1-\sqrt{-d})$ and $4+d = (2+\sqrt{-d})(2-\sqrt{-d})$, but none of these factors are in the ideal (2), so (2) is not a prime ideal.

19S.4, 12S.3 Let R be a commutative local ring and P a finitely generated projective R-module. Prove that P is R-free.

Solution Proceed by induction on the number r of generators of P. Let M be an R-module such that $P \oplus M$ is R-free, say with basis $\{e_1, ..., e_s\}$. Then in the $r = 1$ case if $ax_1 = 0$, then a is a zero divisor in $P \oplus M$ so $a = 0$. Now suppose that any projective R-module generated by r or fewer elements is R-free, and suppose $x_1, ..., x_{r+1}$ generate P and there exist $a_1, ..., a_{r+1} \in R$ such that $a_1x_1 + ... + a_{r+1}x_{r+1} = 0$. Writing $x_i = \sum_{j=1}^{s} b_{ij}e_j$, we have that

$$0 = a_1x_1 + ... + a_{r+1}x_{r+1} = \sum_{j=1}^{s}\left[\sum_{i=1}^{r+1} b_{ij}a_i\right] e_j = 0 \Rightarrow \sum_{i=1}^{r+1} b_{ij}a_i = 0 \text{ for each } j$$

since $P \oplus M$ is free. Let $\mathfrak{m}$ be the unique maximal ideal of R. By Nakayama's Lemma, one of the x_i does not lie in $\mathfrak{m}P$, so without loss of generality assume it's x_{r+1}. Then $b_{(r+1)j} \notin \mathfrak{m}$ for some j, so $b_{(r+1)j}$ is a unit, so dividing the above equation by it gives

$$a_{r+1} = \sum_{i=1}^{r} c_i a_i \text{ for some } c_1, ..., c_r \in R$$

Multiplying this to x_{r+1} gives that

$$\sum_{i=1}^{r}(x_i + c_i x_{r+1}) = 0$$

but the n elements $x_1 + c_1x_{r+1}, ..., x_r + c_rx_{r+1}$ are linearly independent in the projective module $\mathfrak{m}P$, which is free by the inductive hypothesis so that $a_1 = ... = a_r = 0$. But then we must have $a_{r+1} = 0$ as well, so that P is free which completes the induction.

19S.5 Let Φ_n denote the n^{th} cyclotomic polynomial in $\mathbb{Z}[X]$ and let a be a positive integer and p a prime not dividing n. Prove that if $p|\Phi_n(a)$ in $\mathbb{Z}$, then $p \equiv 1(\text{mod } n)$.

Solution $\Phi_n(a)|a^n - 1$ so that $p|a^n - 1$ as well. Therefore p does not divide a, so $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$. Let k be its order. Then since $p|a^n - 1$, $k|n$, and if $k = n$ then we are done because by Lagrange, $k = n|p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$ so $p \equiv 1(\text{mod } n)$. So suppose $k < n$. Then

$$\prod_{d|k} \Phi_d(a) = a^k - 1 \equiv 0(\text{mod} p)$$

so that $p|\Phi_d(a)$ for some $d|k$ since p is prime. Then $X - a|\Phi_d(X), \Phi_n(X)$ so $(X - a)^2|X^n - 1$. Write $X^n - 1 = (X - a)^2 f(X)$, and substitute $X = Y + a$. Then $(Y + a)^n - 1 = Y^2 f(Y + a)$. The coefficient of Y on the right-hand side is zero, so $na^{n-1} \equiv 0(\text{mod} p)$. But then since p does not divide a, it must divide n, which is a contradiction. Therefore $k = n$ indeed.

19S.7, 12S.4 Let F be a field and R the ring of 3×3 matrices over F with $(3,1)$ and $(3,2)$ entry equal to 0.
a) Determine the Jacobson radical J of R.
b) Is J a minimal left (respectively, right) ideal?

Solution a) Let $(a_{ij})_{i,j=1}^{3} = A \in J$. Then $A \in R$ so that $a_{31} = a_{32} = 0$. Additionally, since $A \in J$ we must have that $I - BA \in R^{\times}$ for all $B \in R$, so that

$$a_{33} \neq 0 \Rightarrow I + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{-1}{a_{33}} \end{pmatrix} A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin R^{\times} \text{ so that } a_{33} = 0$$

$$a_{11} \neq 0 \Rightarrow I + \begin{pmatrix} \frac{-1}{a_{11}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \notin R^{\times} \text{ so that } a_{11} = 0$$

$$a_{22} \neq 0 \Rightarrow I + \begin{pmatrix} 0 & 0 & 0 \\ 0 & \frac{-1}{a_{22}} & 0 \\ 0 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & 0 \\ * & 0 & * \\ 0 & 0 & 1 \end{pmatrix} \notin R^{\times} \text{ so that } a_{22} = 0$$

$$a_{12} \neq 0 \Rightarrow I + \begin{pmatrix} 0 & 0 & 0 \\ \frac{-1}{a_{12}} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & 0 \\ * & 0 & * \\ 0 & 0 & 1 \end{pmatrix} \notin R^{\times} \text{ so that } a_{12} = 0$$

$$a_{21} \neq 0 \Rightarrow I + \begin{pmatrix} 0 & \frac{-1}{a_{21}} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \notin R^{\times} \text{ so that } a_{12} = 0$$

Conversely, suppose $A \in R$ is any matrix where every entry except the $(1,3)$ and $(2,3)$ entries are zero. Then for any $B \in R$, BA is zero outside the $(1,3)$ and $(2,3)$ entries, so that $I - BA$ is upper triangular with all 1's on the diagonal and is therefore invertible. Therefore $A \in J$, so that

$$J = \begin{pmatrix} 0 & 0 & F \\ 0 & 0 & F \\ 0 & 0 & 0 \end{pmatrix}$$

b) Let $0 \neq I \subseteq J$ be a left ideal, and let $A \in I \setminus \{0\}$. Then either a_{13} or a_{23} is not zero while all entries besides those two are zero. Without loss of generality assume that a_{13} is not zero (otherwise, permute the first two rows). Then

$$\begin{pmatrix} \frac{1}{a_{13}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I \text{ so that}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in I$$

But then every element of J lies in I so $I = J$. Therefore J is a minimal left ideal. Similarly, let $0 \neq I \subseteq J$ be a right ideal, and let $A \in I \setminus \{0\}$ where we WLOG take $a_{13} \neq 0$, so that

$$A \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{1}{a_{13}} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I \text{ so that}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in I$$

so that again $J = I$ and so J is also a minimal right ideal.

19S.8 Prove that every finite group of order n is isomorphic to a subgroup of $GL_{n-1}(\mathbb{C})$.

Solution By Cayley's Theorem any group of order n embeds into S_n, so it suffices to embed this in $GL_{n-1}(\mathbb{C})$. S_n embeds into $GL_n(\mathbb{C})$ as the group of permutation matrices, which corresponds S_n acting on $\mathbb{C}^n$ by permuting the coordinates, fixing the subgroup generated by $(1, 1, ..., 1)$. Therefore S_n acts on $\mathbb{C}^n/(1, 1, ..., 1) \simeq \mathbb{C}^{n-1}$ which gives an embedding $S_n \to GL_{n-1}(\mathbb{C})$ as desired.

19S.9 a) Find a domain R and two nonzero elements $a, b \in R$ such that R is equal to the intersection of the localizations $R[1/a]$ and $R[1/b]$ (in the quotient field of R) and $aR + bR \neq R$.
b) Let $\mathcal{C}$ be the category of commutative rings. Prove that the functor $\mathcal{C} \to Sets$ taking a commutative ring to the set of pairs $(a, b) \in R^2$ such that $aR + bR = R$ is not representable.

Solution a) Let $R = \mathbb{C}[x, y]$ and $a = x, b = y$. Then $xy \in R \setminus (aR + bR)$ so they are not equal, and we do indeed have $R = R[1/a] \cap R[1/b]$ as the denominators of polynomials in the former and latter rings can only contain x and y respectively.

b) Suppose that the given functor is representable by an object A. Then $\text{Hom}(A, A)$ contains a universal element (x, y), so let R, a, b be as in (a). Then $aR[1/a] = R[1/a] \Rightarrow aR[1/a] + bR[1/a] = R[1/a]$ so that $(a, b) \in \text{Hom}(A, R[1/a])$ and therefore there exists a unique ring homomorphism $f : A \to R[1/a]$ such that $f(x) = a, f(y) = b$. Similarly, there exists a unique ring homomorphism $g : A \to R[1/b]$ such that $g(x) = a, g(y) = b$. Considering both f, g as maps $A \to Frac(R)$ the fraction field of R, we see that f, g restrict to the same ring homomorphism $h : A \to R[1/a] \cap R[1/b]$ by the universality of (x, y), and since $R[1/a] \cap R[1/b] = R$ from part (a), this means that $h(x) = a, h(y) = b$. But then $(a, b) \in \text{Hom}(A, R)$ so that $aR + bR = R$, which we see from part (a) is not the case, so we have a contradiction and so the given functor is not representable.

19S.10 Let $\mathcal{C}$ be an abelian category. Prove that TFAE:
(1) Every object of $\mathcal{C}$ is projective.
(2) Every object of $\mathcal{C}$ is injective.

Solution Every object of $\mathcal{C}$ is projective if and only if every short exact sequence $0 \to X \to Y \to P \to 0$, with P any object, splits, if and only if every short exact sequence in $\mathcal{C}$ splits, if and only if every short exact sequence $0 \to I \to X \to Y \to 0$, with I any object, splits, if and only if every object of $\mathcal{C}$ is injective.

15F.1 Show that the inclusion map $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism in the category of rings with multiplicative identity.

Solution Let $i : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. For any $g, h : \mathbb{Q} \to R$ where R is any ring with identity we have that $g(x)g(x^{-1}) = g(1) = 1$ so that $g(x)$ is a unit with inverse $g(x^{-1})$, and similarly for h. If $g \circ i = h \circ i$,

$$g(\frac{p}{q}) = \frac{g(p)}{g(q)} = \frac{g(i(p))}{g(i(q))} = \frac{h(i(p))}{h(i(q))} = \frac{h(p)}{h(q)} = h(\frac{p}{q}) \text{ for all } \frac{p}{q} \in \mathbb{Q}$$

so that $g = h$. Therefore i is an epimorphism.

15F.2 Let R be a PID with field of fractions K.
a) Let S be a multiplicatively closed subset of $R \setminus \{0\}$. Show that $R[S^{-1}]$ is a PID.
b) Show that any subring of K is of the form $R[S^{-1}]$ for some multiplicatively closed subset S of $R \setminus \{0\}$.

Solution a) Let I be an ideal of $R[S^{-1}]$, and let J be the ideal of R such that $I = JR[S^{-1}]$. Since R is a PID, $J = (x)$ for some $x \in R$. Now $(x) \subseteq I$ and if $y \in I$, then write $y = y_j y_s$ where $y_j \in J$ and $y_s \in R[S^{-1}]$. Then $y_j = nx$ for some $n \in R$, so $y = nxy_s \in (x)$ so that $I = (x)$ and is therefore principal, so since I was arbitrary $R[S^{-1}]$ is a PID.

b) Let A be a subring of K containing R as a subring. Then let $S = R \cap A^\times$, which is a multiplicative subset of R not containing zero. Then the inclusion map $i : R \to A$ certainly sends every element of S to a unit, so by the universal property of $R[S^{-1}]$ i factors as $i = f \circ j$ where $j : R \to R[S^{-1}]$ is the usual inclusion. But then f must be the identity map on R, and therefore on S since it is a subset of R, and therefore on S^{-1} since f is a ring homomorphism. Therefore $f : R[S^{-1}] \to A$ is an isomorphism, so that A takes the form $R[S^{-1}]$ as desired.

15S.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?
b) What are the ideals of A?

Solution a) A contains no degree 2 polynomials and every degree 0 polynomial is a unit because k is a field, so the only principal ideals of A are generated by elements of the form $ax + by$ for $a, b \in k$.

b) The only ideal generated by more than one element is (x, y). To see this, first note that all ideals of $k[X,Y]$ (and hence all ideals of $k[X,Y]/(X^2, XY, Y^2)$) are finitely generated since k is a field. Consider therefore the ideal $I = (a_1x + b_1y, ..., a_nx + b_ny)$. Then at most two of the vectors (a_i, b_i) can be linearly independent in k^2 so that the rest of them must be k-linear combinations, so either I is principal or I takes the form $I = (a_1x + b_1y, a_2x + b_2y)$ where (a_1, b_1) and (a_2, b_2) are linearly independent in k^2. In this case, there is a unique solution to the system of equations $c_1a_1 + c_2a_2 = 1$ and $c_1b_1 + c_2b_2 = 0$ for $c_1, c_2 \in k$, so that $c_1(a_1x + b_1y) + c_2(a_2x + b_2y) = x \in I$. Then either b_1 or b_2 is nonzero (otherwise we wouldn't have linear independence), and WLOG it's b_1, so that $y = b_1^{-1}(-a_1x) \in I$, so that $(x, y) \subseteq I$, and the other containment is clear, so $I = (x, y)$. Therefore (x, y) is the only nonprincipal ideal of A.

15S.5 a) Let G be a group of order $p^e v$ with v, e positive integers, p prime, $p > v$, and v not a multiple of p. Show that G has a normal Sylow p-subgroup.
b) Show that a nontrivial finite p-group has nontrivial center.

Solution a) By Sylow's theorems, we must have that the number n_p of Sylow p-subgroups satisfies

$$n_p | v \text{ and } n_p \equiv 1 (\text{mod } p)$$

But since $p > v \geq n_p$, we must have that $n_p = 1$, so by Sylow's theorems since there is a unique Sylow p-subgroup it is normal.

b) Let G be a nontrivial p-group with trivial center. Then G acts on itself by conjugation, so the size of the conjugacy class containing any element other than the identity is divisible by p, since conjugating it by any other element (which has order divisible by p) must be nontrivial. But now writing G as the disjoint union of its conjugacy classes, we see that $\{e\}$ is its own conjugacy class, so we get that $|G|$ is a sum of numbers divisible by p and 1, so that $|G| \equiv 1 (\text{mod } p)$, which contradicts that G is a nontrivial p-group. Therefore every nontrivial p-group has nontrivial center.

15F.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 $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$.

Solution $GL(2, F)$ is generated by the 2×2 elementary matrices:

$$A_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, B_\lambda = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, C_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, D_\lambda = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}, E = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$SL(2, F)$ contains only the matrices with determinant 1, i.e. $A_1 = B_1 = I$ as well as C_λ and D_λ for each $\lambda \in F$. Therefore the C_λ and D_λ generate $SL(2, F) \subseteq GL(2, F)$.

15F.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 $\mathbb{Z}^3/H \simeq K$?

Solution By the classification of finitely generated abelian groups, $K \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $K \simeq (\mathbb{Z}/p\mathbb{Z})^2$, and $H = n_1\mathbb{Z} \times n_2\mathbb{Z} \times n_3\mathbb{Z}$ so that $Z^3/H = (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times (\mathbb{Z}/n_3\mathbb{Z})$. If $K \simeq \mathbb{Z}/p^2\mathbb{Z}$, then K is cyclic so it is not a nontrivial direct product as those groups would be smaller so they cannot have any elements of order p^2. Therefore we must have that two of n_1, n_2, n_3 are 1 and the other is p^2, so there are $\binom{3}{1} = 3$ ways to choose H in this case. If $K \simeq (\mathbb{Z}/p\mathbb{Z})^2$, then once again each cyclic factor of K is not a nontrivial direct product, so that two of n_1, n_2, n_3 must equal p while the other one is 1, so there are $\binom{3}{2} = 3$ ways to choose H in this case as well.

11F.8 Let Γ be the Galois group of $X^5 - 9X + 3$ over $\mathbb{Q}$. Determine Γ.

Solution By Eisenstein's criterion $p(X) = X^5 - 9X + 3$ is irreducible, so that Γ contains an element of order 5. Considering the embedding $\Gamma \to S_5$, we see that the image of Γ contains a 5-cycle. Now by Descartes' rule of signs, p has exactly one negative real root and either 0 or 2 positive real roots, and since $p(0) = 3 > 0$ and $p(1) = -5 < 0$, by the Intermediate Value Theorem p has at least one positive root so it has two. Therefore two of its roots are not real, so complex conjugation as an element of Γ maps to a transposition. Therefore $\Gamma \to S_5$ is surjective, since the 5-cycle and transposition generate S_5, so that $\Gamma \simeq S_5$.

19F.4 Find all isomorphism classes of simple left-modules over the ring $M_n(\mathbb{Z})$.

Solution By the Morita equivalence of $M_n(\mathbb{Z})$ to $\mathbb{Z}$ we have that if M is a simple left $M_n(\mathbb{Z})$-module then $M = X^n$ where X is a simple left $\mathbb{Z}$-module. Then $X \simeq \mathbb{Z}/p\mathbb{Z}$ for some prime p, so that $M \simeq (\mathbb{Z}/p\mathbb{Z})^n$ for some prime p.

19F.5 Let R be a nonzero commutative ring. Consider the functor t_B from the category of R-modules to itself given by taking the (right) tensor product with an R-module B.
a) Prove that t_B commutes with colimits.
b) Construct an R-module B (for each R) such that t_B does not commute with limits in the category of R-modules.

Solution a) t_B has a right adjoint, namely the functor represented by B, so it commutes with all colimits.

b) Let $B := R[[t]]$ and A a free R-module of infinite rank. But the natural map $A \otimes_R B \to A[[t]]$ is not surjective, since the image contains only power series whose coefficients span a finite rank submodule of A.