UCLA Algebra Qual Solutions

Emil Geisler | emilg@math.ucla.edu

These solutions were written with help from many friends including Ian Shors, Harahm Park, Adam Zheleznyak, Tomoki Oda, Rhea Kommerell, Victoria Quijano, and Matthew Hung in no particular order. If you notice any mistakes or have any comments about the solutions, you should contact me!

Contents

Spring 2025

Exercise 1. Let p be an odd prime number and let K be the splitting field of $x^p - 1$ over $\mathbb{Q}$. Show that K contains a unique subfield F such that $[F : \mathbb{Q}] = 2$ and determine, as property of p, whether F is a real or a complex quadratic extension of $\mathbb{Q}$.

Proof. The splitting field of $x^p - 1$ is the pth cyclotomic field which has Galois group $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. I prove this further below if you haven't seen it. Therefore since $K/\mathbb{Q}$ has a cyclic Galois group of order $p-1$, by the Galois correspondence, there is a unique field extension $L_k/\mathbb{Q}$ for every integer $k|(p-1)$. In particular since p is odd, $2|(p-1)$, so there is a unique subfield F of K such that $[F : \mathbb{Q}] = 2$. It is the fixed field of the unique subgroup $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$ of index 2. This unique subgroup consists of the elements which are squares modulo p. In particular if we write $\zeta \in K$ for a non-trivial root of $x^p - 1$, then the element

$$\alpha = \sum_{h \in H} \zeta^h \in F$$

is fixed by H since for $g \in H$,

$$g(\alpha) = \sum_{h \in H} \zeta^{gh} = \sum_{h \in H} \zeta^h = \alpha$$

Also notice that α is not in $\mathbb{Q}$, since if it were, then it would imply that $\zeta, \zeta^2, \dots, \zeta^{p-1}$ satisfy both $\sum_{i=0}^{p-1} \zeta^i = 0$ and $\sum_{h \in H} \zeta^h = 0$, which contradicts that $[K : \mathbb{Q}] = p-1$. Therefore, $F = \mathbb{Q}(\alpha)$. Thus to check whether F is real or not, it suffices to check whether α is preserved by complex conjugation (after a choice of embedding $K \hookrightarrow \mathbb{C}$, for instance by $\zeta \mapsto e^{2\pi i/p}$). Complex conjugation corresponds to the element $\tau \in G$ defined by $\tau(\zeta) = \zeta^{-1}$. In particular,

$$\tau(\alpha) = \sum_{h \in H} \zeta^{-h} \in F$$

Thus, $\tau(\alpha) = \alpha$ if and only if $-1 \in H$, i.e., -1 is a square modulo p, and otherwise $\tau(\alpha) \neq \alpha$, thus F is not real. It is an important fact in elementary number theory that -1 is a square modulo p if and only if p is congruent to 1 modulo 4. Therefore, F is real if and only if $p \equiv 1 \bmod 4$.

Proving that $K/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$.

The polynomial $x^p - 1$ factors as $(x-1)(x^{p-1} + x^{p-2} + \cdots + 1) = (x-1)\Phi_p(x)$. The polynomial $\Phi_p(x)$ is the pth cyclotomic polynomial and is irreducible. One way to see this is using Eisensteins criterion with a clever choice of change of coordinates $x \mapsto x + 1$.

Thus, the splitting field of $x^p - 1$ is the splitting field of $\Phi_p(x)$. Let $K = \mathbb{Q}[x]/\Phi_p(x)$, which is a field since Φ_p is irreducible over $\mathbb{Q}$. Then K has at least one formal root $\zeta := [x] \in K$ of $\Phi_p(x)$. Also, notice that all powers of ζ also satisfy $(\zeta^k)^p - 1$. Since Φ_p is irreducible of degree $p-1$,

$\zeta, \zeta^2, \dots, \zeta^{p-1}$ are $\mathbb{Q}$-linearly independent, and in particular are distinct elements of K. Therefore, $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ are all distinct roots of $x^p - 1$ in K. Therefore by degree considerations,

$$x^p - 1 = (x-1)(x-\zeta)\dots(x-\zeta^{p-1})$$

so $x^p - 1$ splits in $K[x]$. Thus, K is the splitting field of $\mathbb{Q}$.

In particular, this implies that $K/\mathbb{Q}$ is a Galois extension of degree $p-1$. Let $G = \mathrm{Gal}_{\mathbb{Q}}(K)$. Since K is the splitting field of the irreducible polynomial $\Phi_p(x)$, G acts transitively on the roots of $\Phi_p(x)$ in K, which are $\zeta, \zeta^2, \dots, \zeta^{p-1}$. In particular, for each integer $k \in [1, p-1]$, there is an element $\sigma_k \in G$ such that $\sigma_k(\zeta) = \zeta^k$. Furthermore, this integer k fully determines the element σ_k, since $K = \mathbb{Q}(\zeta)$. Therefore, there is a bijection $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to G$ by $k \mapsto \sigma_k$. It is also a group homomorphism since

$$\varphi(a \cdot b)\Big(\zeta\Big) = \sigma_{a \cdot b}(\zeta) = \zeta^{ab} = \zeta^a \zeta^b = \sigma_a(\zeta)\sigma_b(\zeta) = \varphi(a) \circ \varphi(b)\Big(\zeta\Big)$$

and elements of G are determined by their action on ζ. □

Exercise 2. Let R be a UFD. Show that any non-zero prime ideal of $R[x]$ which contains no non-zero elements of R is principal.

Proof. Let $K = \mathrm{Frac}(R)$ the fraction field of R. Let $\mathfrak{p} \subset R[x]$ be a prime ideal such that $\mathfrak{p} \cap R = \{0\}$. Let $f \in \mathfrak{p}$ of minimal degree, which exists with $\deg f > 0$ since $\mathfrak{p}$ is non-zero and has no elements of degree 0. Let $c(f)$ be the *content* of f: the GCD of its coefficients in R (unique up to a choice of unit). Then we have that $f = c(f) \cdot u \cdot f'$ for f' having content $c(f') = 1$, and u a unit in R. Since $\mathfrak{p}$ is prime and $c(f)$ is not in $\mathfrak{p}$, we must have $f' \in \mathfrak{p}$. Thus, without loss of generality assume that f has content 1. Also notice that if f factored non-trivially in $K[x]$ as $f = g \cdot h$, then it would also factor non-trivially in $R[x]$ by Gauss' lemma. By primality of $\mathfrak{p}$, then one of g, h would be in $\mathfrak{p}$, contradicting the minimality of $\deg f$. Therefore, f has content 1 and is irreducible in $K[x]$, and is thus irreducible in $R[x]$.

We claim that $\mathfrak{p} = (f)$. Suppose that there were $g \in \mathfrak{p}$ such that f did not divide g. Then by the division algorithm, in $K[x]$ there would be $p, q \in K[x]$ such that

$$g(x) = p(x)f(x) + q(x)$$

for $\deg q < f$ and q non-zero. After multiplying by an element $\alpha \in R$ such that $\alpha p(x), \alpha q(x) \in R[x]$, we have

$$\alpha g(x) = \alpha p(x) f(x) + \alpha q(x)$$

for $\alpha p(x), \alpha q(x) \in R[x]$. Since $\alpha g(x), \alpha p(x) f(x)$ are all in $\mathfrak{p}$, so is $\alpha q(x)$. But then $\mathfrak{p}$ contains a non-zero element q of degree less than f which is a contradiction. □

Exercise 3. Show that the alternating group A_4 has a unique irreducible representation of degree 3 over $\mathbb{C}$ and compute the character of this representation.

Proof. Clearly it's enough to just compute the whole character table of A_4. Notice that $|A_4| = 4!/2 = 12$. The fact that they told us there is an irreducible representation of degree 3 is a nice hint: we know $\sum_{\chi \text{irr}} \dim \chi^2 = 12$, so this tells us there are 4 irreducible characters with dimension $1, 1, 1, 3$.

First we compute the conjugacy classes of A_4. A computation shows that the following sets consist of elements which are conjugate:

$$C_1 = \{1\}, C_2 = \{(12)(34), (13)(24), (14)(23)\}$$
$$C_3 = \{(123), (134), (142), (243)\}, C_4 = \{(132), (124), (143), (234)\}$$

To show that these are the conjugacy classes, it suffices to show that $(123), (132)$ are not conjugate in A_4. This is a bit of a pain. In general, a conjugacy class in S_n splits in A_n if and only if it's cycle type consists of distinct odd integers.

Notice that $H = C_1 \cup C_2$ is a normal subgroup of A_4. Therefore we have a short exact sequence:

$$1 \to H \to A_4 \to \mathbb{Z}/3\mathbb{Z} \to 1$$

And in particular this shows that the abelianization $A_4/[A_4, A_4]$ of A_4 is $\mathbb{Z}/3\mathbb{Z}$ (this shows that $[A_4, A_4]$ is contained in H, but $[A_4, A_4]$ is a non trivial normal subgroup of A_4 so they are equal). The one dimensional representations of any finite group G are given by the group homomorphisms $G \to \mathbb{C}^\times$ which are given by $G/[G, G]$. Thus, there are three one dimensional representations of A_4, which are each trivial on H and send C_3, C_4 to a 3rd root of unity. Let $\omega = e^{2\pi i/3}$. Then we have the following character table:

C_1	C_2	C_3	C_4
1	1	1	1
1	1	ω	ω^2
1	1	ω^2	ω

Then by dimension considerations, the third row must be a three dimensional representation. By column orthogonality, this determines the final row.

C_1	C_2	C_3	C_4
1	1	1	1
1	1	ω	ω^2
1	1	ω^2	ω
3	-1	0	0

□

Exercise 4. Let R be an integral domain with quotient field F. Show that if F is finitely generated as an R-module, then $F = R$.

Proof. Of all the commutative algebra theorems to learn for the qual, my favorite for is going up and going down.

Since F is finitely generated as an R-module, the inclusion $R \hookrightarrow F$ is an integral extension of commutative rings. Therefore, the Krull dimension of R is equal to the Krull dimension of F. Therefore, every prime ideal of R is maximal. Since R is a domain, (0) is prime and thus maximal, so $R/(0)$ is a field, i.e., R is a field.

A more hands on solution: suppose there exists a non-zero $\alpha \in R$ such that $\alpha^{-1} \in F$ is not in R. Since F is a finitely generated R-module, α^{-1} is integral over R. Therefore, $R[\alpha]/R$ is an integral extension. Thus, there is some n and elements $a_{n-1}, \dots, a_0 \in R$ such that

$$\alpha^{-n} + a_{n-1}\alpha^{-n+1} + \cdots + a_0 = 0$$

Multiplying by α^{n-1}, we have

$$\alpha^{-1} = -a_{n-1} - a_{n-2}\alpha - \cdots - a_0\alpha^{n-1} \in R$$

so $\alpha^{-1} \in R$. Thus, R is a field. □

Exercise 5. Let G be a p-group for p a prime. Let F be a field of characteristic p. Show that the only irreducible representation of G in finite dimensional F vector spaces is the trivial representation.

Proof. We proceed by induction on $|G|$. For $|G| = 1$, a subrepresentation of F is just a subspace of F. The only non-zero vector space without proper subspaces is the trivial one, so the only irreducible G-representation over F is the trivial representation.

For induction, assume that for all p-groups G' with $|G'| < |G|$, the only irreducible representation of G' is the trivial one. Let $V = F^n$ be a representation of G of dimension greater than 1. Since G is a p-group, it has non-trivial center, so take $1 \neq g \in Z(G)$.

V being a G representation is equivalent to there being a group homomorphism $\rho : G \to \mathrm{GL}(V)$. In particular, notice that $\rho(g)$ has minimal polynomial dividing $x^{|G|} - 1$ since $\rho(g^{|G|}) = \rho(g)^{|G|} = \mathrm{Id}$. In particular we see $x^{|G|} - 1 = (x-1)^{|G|}$ since F is characteristic p. Therefore, the only eigenvalue of $\rho(g)$ is 1. In particular, the subspace $W \subset V$ of 1-eigenvalues of $\rho(g)$ is non-zero. If $W = V$, then $\rho(g)$ acts on V trivially. This would imply that ρ factors as a morphism $\rho : G/\langle g \rangle \to \mathrm{GL}(V)$ since g generates a normal subgroup of G. But then V is a $G/\langle g \rangle$-representation and thus has a non-trivial subrepresentation by induction.

Thus, $W \subset V$ is a non-trivial subspace of V. Furthermore for all $h \in G$ and $w \in W$, we have

$$h \cdot w = h \cdot g \cdot w = g \cdot h \cdot w$$

so $g(h \cdot w) = h \cdot w$, so $h \cdot w \in W$. Therefore, W is a non-trivial subrepresentation of V as desired. □

Exercise 6. Let R be a ring and let F be the forgetful functor R-**Mod** $\to \mathbb{Z}$-**Mod**. Determine with full proofs left and right adjoint functors for F.

Proof. Let us show that as functors R-**Mod** $\to \mathbb{Z}$-**Mod**, we have an equivalence of functors $F \cong \mathrm{Hom}_{\mathbb{Z}}(R, -)$ and an equivalence of functors $F \cong (R \otimes -)$, treating R as a $\mathbb{Z}$-R bimodule. Then by the tensor-hom adjunction, $\mathrm{Hom}_{\mathbb{Z}}(R, -) : R$-**Mod** $\to \mathbb{Z}$-**Mod** has a left adjoint $R \otimes - : \mathbb{Z}$-**Mod** $\to$ R-**Mod**, and $R \otimes -$ has a right adjoint $\mathrm{Hom}_{\mathbb{Z}}(R, -) : \mathbb{Z}$-**Mod** $\to R$-**Mod**, and so F has these same left and right adjoints. Showing these equivalences is straightforward. This exercise is a specific case of the restriction of scalars functor R-**Mod** $\to S$-**Mod** along a ring homomorphism $f : S \to R$ being dully adjoint, with left adjoint extension of scalars: $R \otimes_S -$, and right adjoint coextension of scalars: $\mathrm{Hom}_S(R, -)$. Here R is an R-S bimodule via the ring homomorphism $f : S \to R$. See Wikipedia's change of rings for details. □

Exercise 7. Prove that the group $S_5 \times S_5$ is generated by two elements.

Proof. Recall that S_5 is generated by $\tau = (12), \sigma = (12345)$. This isn't too hard to confirm, since $\sigma\tau\sigma^{-1} = (23), \sigma^2\tau\sigma^{-2} = (34), \sigma^3\tau\sigma^{-3} = (45), \sigma^4\tau\sigma^{-4} = (51)$, and it's not hard to show that these transpositions generate all the transpositions of S_5 and thus all of S_5.

Also notice that $\sigma = \gamma^2$ where $\gamma = \sigma^3 = (14253)$. I claim that $(\tau, \gamma), (\gamma, \tau)$ generate $S_5 \times S_5$. We have that

$$(\tau, \gamma)^2 = (1, \sigma), (\gamma, \tau)^5 = (1, \tau)$$

which generate the subgroup $\{1\} \times S_5 \subset S_5 \times S_5$. Furthermore,

$$(\tau, \gamma)^5 = (\tau, 1), (\gamma, \tau)^2 = (\sigma, 1)$$

which generates the subgroup $S_5 \times \{S_5\} \subset S_5 \times S_5$. Thus, $(\tau, \gamma), (\gamma, \tau)$ generate all of $S_5 \times S_5$. □

Exercise 8. Prove that the ring of all algebraic integers is not a UFD.

Proof. I will let $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ denote the ring of algebraic integers. I claim that there are no irreducible elements of $\overline{\mathbb{Z}}$ - i.e., *non-unital* elements which cannot be written as a product of non-units. If $\alpha \in \overline{\mathbb{Z}}$ is a non-zero non-unit (and an algebraic integer, i.e., satisfying a monic polynomial $f(x) \in \mathbb{Z}[x]$), then $\sqrt{\alpha}$ is also an algebraic integer, satisfying $f(x^2)$. But $\alpha = \sqrt{\alpha}\sqrt{\alpha}$, and so $\sqrt{\alpha}$ is a unit if and only if α is: so it is not a unit. Therefore any non-zero non-unit α in $\overline{\mathbb{Z}}$ can be expressed as a product of non-units, so there are no irreducible elements of $\overline{\mathbb{Z}}$.

Now notice that $\overline{\mathbb{Z}}$ is not a field. For instance, $2 \in \overline{\mathbb{Z}}$ is not a unit, since its inverse in $\overline{\mathbb{Q}}$ is $\frac{1}{2}$, which is not an algebraic integer - for instance because $\frac{1}{2}$ satisfies the non-monic irreducible polynomial $2x - 1$ in $\mathbb{Z}[x]$. Since $\overline{\mathbb{Z}}$ has non-units but has no irreducibles, it is thus not a UFD. $\square$

Exercise 9. Let $A \in M_{n\times n}(F)$ such that the characteristic polynomial of A is its minimal polynomial. Let $B \in M_{n\times n}(F)$ such that $AB = BA$. Show that $B = f(A)$, where f is a polynomial over F.

Proof. Here is a beautiful solution from stack exchange, using the rational canonical form of A. I didn't figure it out, below is a solution using Jordan normal form.

Assume for now that F is algebraically closed. Putting A in Jordan normal form, we can write $F^n = \bigoplus_{i=1}^k V_i$ for V_i a generalized λ_i-eigenspace of A for distinct eigenvalues $\lambda_i \in F$. Since $B(A-\lambda)^n v = (A-\lambda)^n Bv$ for all $\lambda \in F$ and $m \in \mathbb{N}$, B preserves generalized eigenspaces of A. Therefore, with respect to the block decomposition $F^n = \bigoplus_{i=1}^k V_i$, we have that $B = \bigoplus_{i=1}^k B_{\lambda_i}$ is in block form. For λ, λ' distinct eigenvalues of A, notice that $A_\lambda - \lambda' \cdot I$ is invertible, as it consists of Jordan blocks with $\lambda - \lambda'$ on the diagonal. Also, its inverse $(A_\lambda - \lambda')^{-1}$ can be written as a polynomial $g_{\lambda,\lambda'}(A_\lambda)$ for $g_{\lambda,\lambda'} \in F[x]$ since

$$\Big((A_\lambda - \lambda') + \lambda' - \lambda\Big)^n = 0$$

Therefore, if a polynomial f_i can be found for each i such that $B_{\lambda_i} = f_i(A_\lambda)$, then we can write

$$B = f(A), \qquad \text{for} \qquad f = \sum_{i=1}^n f_i \cdot \prod_{j\neq i} (x-\lambda_j)^n g_{\lambda_i,\lambda_j}(x)^n$$

since the polynomial $(x-\lambda_j)^n$ is zero on the Jordan block A_{λ_j}, but $(A_{\lambda_j} - \lambda_i)^n (g_{\lambda_i,\lambda_j})(A_{\lambda_j})^n = I_n$ by definition of g_{λ_i,λ_j}.

Thus, it suffices to consider A with only a single generalized eigenspace. Also we may assume A is a *single* Jordan block since the minimal and characteristic polynomial of A are equal. After subtracting its main diagonal which does not change whether B commutes with A or not, we may assume $\lambda = 0$, so

$$A = \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{bmatrix}$$

If $AB = BA$, then for e_i the elementary column vector with a 1 in the ith position and 0 elsewhere, $A^i e_i = 0$, so $A^i B e_i = BA^i e_i = 0$ for all i. In particular since $\ker A^i = \langle e_1, \ldots, e_i\rangle$, we have

$Be_i \subset \langle e_1, \ldots, e_i \rangle$, so B is upper triangular. Let B have coefficients $b_{i,j}$, so $b_{i,j} = 0$ for $i > j$. Then notice that

$$(AB)_{i,j} = \begin{cases} b_{i+1,j} & i < n \\ 0 & i = n \end{cases}$$

$$(BA)_{i,j} = \begin{cases} b_{i,j-1} & j > 1 \\ 0 & j = 1 \end{cases}$$

Since $AB = BA$, we have $b_{i+1,j} = b_{i,j-1}$ for $i < n$ and $j > 1$. Or rewriting for $k = j - 1$, this says that $b_{i,k} = b_{i+1,k+1}$ for $i < n$ and $k < n$. Thus, B is symmetric along the non-main diagonal and is upper triangular and is thus a polynomial in A.

The only final detail is to consider when F is not algebraically closed. We can still write B as a polynomial $f(A)$ in A with coefficients in $\overline{F}$. We may assume f is degree at most $n-1$ by dividing by the minimal polynomial of A. But then $1, A, A^2, \ldots, A^{n-1}$ are F-linearly independent and thus $\overline{F}$-linearly independent since $M_n(F)$ is the same $\overline{F}$ dimension. So if any of the coefficients of f are not in F, then neither is $f(A)$. □

Exercise 10. Let F be a field and let A be a simple F-algebra of dimension n^2. Prove that $A \xrightarrow{\sim} M_n(F)$ if and only if A has a left ideal of dimension n over F.

Proof. First notice that $M_n(F)$ has a left ideal of dimension n over F, namely the set of matrices which contain $V \subset F^n$ for $\dim V = n - 1$ in their kernel, or specifically the matrices with entries $a_{ij} = 0$ for $j > 1$. Thus it suffices to prove the if statement.

By Wedderburn's theorem, A is isomorphic to $M_k(D)$ for D a finite dimensional division algebra over F. Suppose that $D \neq F$. We will show that A has no left ideal of F dimension n. By dimension considerations, notice that we have $k^2 \dim_F D = n^2$, so $\dim_F D = \frac{n^2}{k^2}$. Thus, let $I \subset M_k(D)$ be a minimal non trivial left ideal, so I contains B for $B \in M_k(D)$ non-zero. In particular, $I = M_k(D) \cdot B$.

Many statements of linear algebra (theory of modules over a field) apply to linear algebra over a division ring. In particular, we have that $M_k(D)$ is the endomorphism ring of D^k in D-**Mod**, and we can write $D^k \cong \ker B \oplus W$ where B acts on $\ker B$ as zero, and $B : W \to D^k$ is injective. Let $l = \dim_D \ker B$. In particular, we can write:

$$B : \ker B \oplus W \to D^k = \begin{bmatrix} 0 & B_1 \end{bmatrix}$$

where B_1 is an injective (full rank) $k \times l$ matrix. Therefore, B_1 has a left inverse $C : D^k \to W$ which is necessarily D-linear. Therefore,

$$M_k(D) \cdot B \subset M_k(D) \cdot \begin{bmatrix} 0 \\ C \end{bmatrix} \begin{bmatrix} 0 & B_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & \mathrm{Id}_{l \times l} \end{bmatrix}$$

Multiplying on the left, this implies that

$$M_k(D) \cdot B \ni \begin{bmatrix} 0 & C' \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & \mathrm{Id}_{l \times l} \end{bmatrix} = \begin{bmatrix} 0 & C' \end{bmatrix}$$

for any $k \times l$ matrix C'. In particular, I is at least $k \cdot l$ dimension over D. Since B is non-zero, $l > 0$, so I is at least k dimension over D. But then

$$\dim_F(I) = \dim_F(D) \cdot \dim_D(I) = \frac{n^2}{k^2} \dim_D(I) \geq \frac{n^2}{k} > n$$

as desired, since $k < n$. □

Fall 2024

Exercise 1. Let G be a finite group and k a field of characteristic p dividing the order of G. Is there any such k, G with an isomorphism of kG-modules $kG \cong M_1 \oplus M_2$ for M_1 with dimension 1 over k?

Proof. No. Let M_1 be a dimension 1 kG-module, so (up to isomorphism), $M_1 = (k, \varphi)$ for $\varphi : G \to k^\times$ a group homomorphism. Suppose for contradiction that $kG \cong M_1 \oplus M_2$ for some kG-module M_2, so there is a surjective kG-module homomorphism $\pi : kG \to M_1$ with a section $\iota : M_1 \to kG$ such that $\pi \circ \iota = \mathrm{Id}_{M_1}$. The morphism π is non-zero, so $\pi(1) \neq 0$. Thus after applying an isomorphism to M_1, we may assume that $\pi(1) = 1 \in k$ without loss of generality. Write $\iota(1)$ in the usual k basis of kG, so $\iota(1) = \sum_{g \in G} a_g g$ for $a_g \in k$. Let e be the identity of G. Since ι is a kG-module homomorphism, for all $h \in G$, we have:

$$\sum_{g \in G} \varphi(h) a_g g = \iota(\varphi(h)) = \iota(h \cdot 1) = h \cdot \iota(1) = \sum_{g \in G} a_g hg = \sum_{h^{-1}g \in G} a_{h^{-1}g} g$$

Since the set $\{g\}_{g \in G}$ forms a k-basis for kG, the coefficient of g on each side must then be equal, so $\varphi(h) a_g = a_{h^{-1}g}$ for all $g, h \in G$. In particular setting $g = e$, we have $a_1 \varphi(h) = a_{h^{-1}}$ for all h. Thus, we have that $\iota(1) = \sum_{g \in G} \varphi(g^{-1}) a_1 g$. Thus,

$$\pi(\iota(1)) = \pi\Big(\sum_{g \in G} \varphi(g^{-1}) a_1 g\Big) = \sum_{g \in G} \varphi(g^{-1}) a_1 \pi(g) = \sum_{g \in G} \pi(1) a_1 = |G| a_1 = 0$$

which contradicts ι being a section of π. □

Exercise 2. Let p, q be distinct prime numbers and consider the number field $K = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. Describe all subfields of K and inclusions between them.

Proof. Notice that K contains $(\sqrt{p} + \sqrt{q})^2 = p + q + 2\sqrt{pq}$, and thus contains $\sqrt{pq}$. Therefore, K contains $(\sqrt{p} + \sqrt{q})\sqrt{pq} = p\sqrt{q} + q\sqrt{p}$. Since p, q are distinct, subtracting $p(\sqrt{q} + \sqrt{p})$ yields $(q - p)\sqrt{p}$, and thus dividing by $q - p$, K contains $\sqrt{p}$. Therefore, K contains $\sqrt{p}$, $\sqrt{q}$, and $\sqrt{pq}$.

Notice that $K \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$ since $\sqrt{p} + \sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$. But the above computation shows the reverse inclusion, so in fact $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Since $[\mathbb{Q}[\sqrt{q}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{p}] : \mathbb{Q}] = 2$ (by Eisenstein on $x^2 - q, x^2 - p$), we thus have $[K : \mathbb{Q}] \leq 4$ and $[K : \mathbb{Q}]$ a multiple of 2, so $[K : \mathbb{Q}] = 2$ or 4. Notice that since p, q are distinct, the discriminants of $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{pq})$ are all distinct, since the discriminant of a quadratic number field $\mathbb{Q}(\sqrt{m})$ for m square free (and not 1) is equal to m if $m \equiv 1 \bmod 4$ and $4m$ otherwise (alternatively, in the field $\mathbb{Q}(\sqrt{p})$, can any element square to be equal to q?). Therefore, K properly contains 3 distinct non-trivial number fields. Therefore, $[K : \mathbb{Q}] = 4$. Furthermore, notice that K is the splitting field of $(x^2 - p)(x^2 - q)$ and is thus Galois. Since K properly contains 3 distinct non-trivial number fields and $K/\mathbb{Q}$ is Galois, $G = \mathrm{Gal}_{\mathbb{Q}}(K)$ has at least 3 non-trivial subgroups by the Galois correspondence and $|G| = 4$. There are only two groups of order 4 and only one of them has at least 3 non-trivial subgroups, so $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In this case, G has *exactly* 3 non-trivial subgroups, so the following describes all subfields of K.

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{p}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{q}) \arrow[d, dash] & \mathbb{Q}(\sqrt{pq}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

□

Exercise 3. Let R be a commutative ring and $S \subset R$ a multiplicatively closed subset. Construct a natural transformation (in either direction) between the functors $\operatorname{Hom} S^{-1}R(S^{-1}M, S^{-1}N)$ and $S^{-1}\operatorname{Hom}_R(M, N)$, considered as functors of R-modules M and N. Prove that your natural transformation is an isomorphism if M is finitely presented.

Proof. See problem 9, Spring 2020. □

Exercise 4. Let K be a field and $f : M_m(K) \to M_n(K)$ a K-linear ring homomorphism. Prove that $m \leq n$.

Proof. Let $m > n$, and let $f : M_m(K) \to M_n(K)$ be a K-linear *rng* homomorphism, i.e., it need not send send I_m to I_n. Let us show that f is the zero morphism so there are no such K-linear ring homomorphisms. Since f is a K-linear rng homomorphism, f is also a K vector space homomorphism. Since $M_m(K) \cong K^{m^2}$ as a K vector space and $M_n(K) \cong K^{n^2}$, f has non-trivial kernel so there exists $A \neq 0 \in M_m(K)$ such that $f(A) = 0$. For $1 \leq i, j \leq m$, define $E_{ij} \in M_m(K)$ to be the matrix with coefficients $e_{ab} = \begin{cases} 1 & \text{if } a = i, b = j \\ 0 & \text{else} \end{cases}$. Since A is non-zero, it has some entry $a_{ij} \neq 0$. Then notice that for $k \in [1, m]$, we have $E_{kj}AE_{ik} = a_{ij}E_{kk}$. Therefore,

$$f(E_{kk}) = \frac{1}{a_{ij}} f(E_{kj}AE_{ik}) = \frac{1}{a_{ij}} f(E_{kj})f(A)f(E_{ik}) = 0$$

Thus, $E_{kk} \in \ker f$ for all k, so $I_m = \sum_{k=1}^m E_{kk}$ is in the kernel of f. Thus, $f = 0$ as desired. □

Exercise 5. Let $A = \mathbb{R}[X,Y]/(Y^2 - X^2(X+1))$.

(a) Prove that A is a domain.

(b) Suppose that $A \subseteq B$ is an integral extension with $B \cong \mathbb{R}[Z_1, \ldots, Z_d]$ a polynomial ring over $\mathbb{R}$. What is d?

Proof. (a) A is a domain if and only if the ideal $(Y^2 - X^2(X+1))$ is prime. Since $\mathbb{R}[X,Y]$ is a UFD by Gauss, it suffices to show that $Y^2 - X^2(X+1)$ is irreducible. Let $B = \mathbb{R}[X]$ so $\mathbb{R}[X,Y] = B[Y]$. Notice that B is a UFD (in particular a PID) and $X+1$ is prime. Then, $Y^2 - X^2(X+1)$ satisfies Eisenstein's criterion with respect to the prime $X+1$ and is thus irreducible. Thus, A is a domain.

(b) Recall that integral extensions preserve Krull dimension. Thus, d must be equal to $\dim A$ since $\dim \mathbb{R}[Z_1, \ldots, Z_d] = d$. Thus it suffices to compute $\dim A$. There is an injective $\mathbb{R}$-algebra homomorphism $\mathbb{R}[X] \to A$ defined by $X \mapsto [X]$ by universal property of $\mathbb{R}[X]$ as a free $\mathbb{R}$-algebra. The kernel of this map is $(Y^2 - X^2(X+1)) \cap \mathbb{R}[X] = (0)$, so it is injective. Thus we have

$$\mathbb{R}[X] \subseteq A$$

I claim this is an integral extension. Since A is generated as an $\mathbb{R}[X]$-algebra by Y, it suffices to show Y is integral over $\mathbb{R}[X]$. But Y satisfies a monic polynomial in $(\mathbb{R}[X])[T]$, so $\dim A = \dim \mathbb{R}[X] = 1$.

We can actually explicitly write $A \subseteq \mathbb{R}[t]$. Since A is a domain, let $K = \mathrm{Frac}(A)$, so $A \subseteq K$. Let $t = Y/X \in K$. Then notice that $t^2 = Y^2/X^2 = X+1$, so $\mathbb{R}[t] \subset K$ contains X, and thus also $Y = (t^2-1)t$. Therefore, $A \subseteq \mathbb{R}[t]$.

□

Exercise 6. Let G be the group of 3×3 complex matrices of the form

$$\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

with nonzero entries on the diagonal. Show that G is solvable.

Proof. (I like upper triangular more:) First notice that the transpose map $\mathrm{GL}_n(\mathbb{C}) \xrightarrow{T} \mathrm{GL}_n(\mathbb{C})$ is an isomorphism between $\mathrm{GL}_n(\mathbb{C})$ and $\mathrm{GL}_n(\mathbb{C})^{\mathrm{op}}$. Since for a group G, both G and G^{op} are isomorphic as groups by $g \mapsto g^{-1}$, it suffices to show that the upper triangular matrices are solvable.

To show that G is solvable, it suffices to show that there is a short exact sequence

$$1 \to N \hookrightarrow G \to G/N \to 0$$

for $N \trianglelefteq G$ such that N is solvable and G/N is solvable. Notice that there are group homomorphisms $G \xrightarrow{\psi_k} \mathbb{C}^\times$ for $1 \leq k \leq 3$ by $\psi_k(A) = a_{kk}$ (such set maps certainly exist, and we verify that $\psi_k(A)\psi_k(B) = \psi_k(AB)$). Let

$$N = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{C} \right\}$$

Notice that N is normal since it is the intersection of the normal subgroups $\ker \psi_1(A), \ker \psi_2(A), \ker \psi_3(A)$. Furthermore, G/N is abelian and thus solvable since it is isomorphic to $\mathbb{C}^\times \times \mathbb{C}^\times \times \mathbb{C}^\times$. Thus, it suffices to show that N is solvable. Consider

$$H = \left\{ \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; d \in \mathbb{C} \right\}$$

Let us show that H is normal in N. Notice that we have group homomorphisms $\varphi_1, \varphi_2 : N \to \mathbb{C}$ by $\varphi_1(A) = a, \varphi_2(A) = c$ with notation as above. The intersection of their kernels is thus a normal subgroup of N, which is exactly H. Thus we have

$$1 \to H \hookrightarrow N \to N/H \to 0$$

Notice that $N/H \cong \mathbb{C} \times \mathbb{C}$ (the additive groups) and is thus Abelian. Thus it finally remains to show that H is solvable. In fact, it is easily seen to be Abelian and isomorphic to $\mathbb{C}$, so G is solvable. □

Exercise 7. Let $F = \mathbb{Q}(\sqrt[3]{5})$. Show that for every field E containing $\mathbb{Q}$, the ring $F \otimes_{\mathbb{Q}} E$ is either a field, a product of two fields, or a product of three fields. Give examples of all three cases.

Proof. Notice that $F \cong \mathbb{Q}[x]/(x^3 - 5)$ via the map $x \mapsto \sqrt[3]{5}$. For E a field containing $\mathbb{Q}$, we thus have

$$F \otimes_{\mathbb{Q}} E \cong \mathbb{Q}[x]/(x^3 - 5) \otimes_{\mathbb{Q}} E \cong E[x]/(x^3 - 5)$$

Let is prove this isomorphism. There is a map $\varphi : \mathbb{Q}[x]/(x^3-5) \times E \to E[x]/(x^3-5)$ by $\varphi(f, e) = f \cdot e$, with respect to the inclusions $\mathbb{Q}[x]/(x^3 - 5) \hookrightarrow E[x]/(x^3 - 5), E \hookrightarrow E[x]/(x^3 - 5)$, the first of which exists by the relevant universal properties of $\mathbb{Q}$-algebras. Furthermore, φ is clearly $\mathbb{Q}$-bilinear and thus factors as a $\mathbb{Q}$-algebra homomorphism $\psi : \mathbb{Q}[x]/(x^3 - 5) \otimes_{\mathbb{Q}} E \to E[x]/(x^3 - 5)$. ψ is clearly surjective so it suffices to show that ψ is injective. Since φ is the composition of multiplication in

$E[x]/(x^3-5)$ with inclusions, it suffices to consider when $f \cdot e \in (x^3-5) \subset E[x]$ is satisfied for $f \in \mathbb{Q}[x] \subset E[x]$ and $e \in E \subset E[x]$. Since e is a unit in $E[x]$, this is equivalent to when $f \in (x^3-5)$. Since $(x^3-5)_{E[x]} \cap \mathbb{Q}[x] = (x^3-5)_{\mathbb{Q}[x]}$, $f \in (x^3-5)_{E[x]}$ if and only if $f \in (x^3-5)_{\mathbb{Q}[x]}$. Thus, the kernel of ψ is trivial.

Suppose that x^3-5 factors into irreducibles in $E[x]$ as $g_1(x) \dots g_r(x)$. Since $\mathbb{Q}$ is characteristic 0, each of the g_i are distinct. Furthermore, $r \leq 3$. Thus by Chinese remainder theorem (and since $E[x]$ is a PID):

$$F \otimes_{\mathbb{Q}} E \cong E[x]/(x^3-5) \cong E[x]/g_1 \times \cdots \times E[x]/g_r$$

Furthermore, each of the $E[x]/g_i$ is a PID. Thus, $F \otimes_{\mathbb{Q}} E$ is a product of one, two, or three fields, and this number is determined by how many primes x^3-5 factors into in $E[x]$. Notice that in $\mathbb{Q}$, x^3-5 is irreducible, so $F \otimes_{\mathbb{Q}} \mathbb{Q}$ is a field (for a non-trivial example, $\mathbb{Q}[\sqrt{2}]$ works also since 5 has no cube root in $\mathbb{Q}[\sqrt{2}]$). In F, x^3-5 partially splits as $(x-\sqrt[3]{5})(x^2+x\sqrt[3]{5}+\sqrt[3]{25})$, and splits no further since the roots of $x^2+x\sqrt[3]{5}+\sqrt[3]{25}$ are strictly complex and $F \subseteq \mathbb{R}$. Therefore, $F \otimes_{\mathbb{Q}} F$ is a product of two fields. Finally, x^3-5 fully splits in $\mathbb{C}$ by FTA, so $F \otimes_{\mathbb{Q}} \mathbb{C}$ is the product of three fields, each isomorphic to $\mathbb{C}$. □

Exercise 8. Let R be a commutative ring and M an R-module. Suppose that the functor $F : R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ defined by $F(X) := \mathrm{Hom}_R(M, X)$ has a right adjoint. Show that M is finitely generated as an R-module.

For the dual question (with tensor products) which has a nicer general answer, see problem 8, Fall 2021. This solution was helped by this math overflow post and this stack exchange post.

Motivation for the solution: If $\mathrm{Hom}_R(M,-)$ has a right adjoint, then $\mathrm{Hom}_R(M,-)$ is exact, so M is projective. Clearly this is not enough, since there are projective modules that are not finitely generated. Another key property of having a right adjoint is preserving colimits, so we need to find a colimit that $\mathrm{Hom}_R(M,-)$ will not preserve unless M is finitely generated. Since arbitrary colimits are "generated" by coequalizers (suffices to preserve cokernels in an abelian category) and coproducts, we consider each separately. Since $\mathrm{Hom}_R(M,-)$ is exact by assumption, $\mathrm{Hom}_R(M,-)$ will preserve coequalizers automatically. Thus, we need a coproduct $\coprod A_i$ of R-modules such that $\mathrm{Hom}_R(M, \coprod A_i) \neq \coprod_i \mathrm{Hom}_R(M, A_i)$. In particular, we have a natural map $\coprod_i \mathrm{Hom}_R(M, A_i) \to \mathrm{Hom}_R(M, \coprod A_i)$ by $(\varphi_i) \mapsto \varphi$, where $\varphi(m) = (\varphi_i(m))_i$. This map is clearly injective, so we show it is not surjective for some choice of $\{A_i\}_i$. This amounts to finding a morphism $\psi : M \to \coprod_i A_i$ such that infinitely many of the compositions $M \to \coprod_i A_i \to A_i$ are non-zero (but since it has image in $\coprod_i A_i$, $\psi(m)_i$ is non-zero for only finitely many i for any $m \in M$)

Proof. We proceed by contradiction, so assume that M is not finitely generated. We show that $\mathrm{Hom}_R(M,-)$ does not preserve coproducts. First we show that since M is not finitely generated, there exists an increasing sequence $N_1 \subseteq N_2 \subseteq \dots$ of proper submodules of M whose union is equal to M.

Let S be the set of submodules $N \subset M$ such that M/N is a finitely generated R-module. S is nonempty since $(0) \in S$. Furthermore, S contains every principal ideal, since if $M/(m)$ were finitely generated, M would be. Thus, S has no maximal element, since any maximal element then must contain every $m \in M$, but M/M is (trivially) finitely generated. Therefore by (the contrapositive of) Zorn's lemma, there exists a chain $L_1 \subset L_2 \subset \dots$ with $L_i \in S$ with no upper bound in S. In particular, $L = \bigcup_{i \in I} L_i$ is a submodule of M not contained in S, so M/L is finitely generated, say by $x_1, \dots, x_n$ for $x_i \in M$. Then letting $K = (x_1, \dots, x_n)$ be the submodule of M generated by $x_1, \dots, x_n$, the chain $L_1 + K \subset L_2 + K \subset \dots$ has union $L + K = M$, but none of the modules $L_i + K$ are equal to M since M/L_i is not finitely generated.

Thus, let $N_1 \subset N_2 \subset \dots$ be a chain of proper submodules of M whose union is equal to M. There is a morphism $\psi' : M \to \prod_i M/N_i$ induced by the quotient maps $M \to M/N_i$. Since $\bigcup_{i=1}^{\infty} N_i = M$, for any $m \in M$, m is contained in infinitely many of the N_i. Therefore, $\psi'(m) \in \prod_i M/N_i$ is non-zero in only finitely many indices i. Thus, treating $\coprod_i M/N_i \subset \prod_i M/N_i$ in the usual way, ψ' restricts to a function $\psi : M \to \prod_i M/N_i$.

By the universal property of coproducts, there is a unique R-module homomorphism

$$\coprod_{i=1}^{\infty} \mathrm{Hom}_R(M, M/N_i) \xrightarrow{\Phi} \mathrm{Hom}_R(M, \coprod_{i=1}^{\infty} M/N_i)$$

defined elementwise by

$$(\varphi_i : M \to M/N_i)_{i=1}^{\infty} \mapsto \Big(m \mapsto (\varphi_i(m))_{i=1}^{\infty})\Big)$$

To show that $\mathrm{Hom}_R(M, -)$ does not preserve coproducts, it suffices to show Φ is not an isomorphism. The image of Φ in $\mathrm{Hom}_R(M, \coprod_{i=1}^{\infty} M/N_i)$ are the maps $M \to \coprod_{i=1}^{\infty} M/N_i$ where all but finitely many of the compositions $M \to M/N_i$ are zero. Notice that ψ does not have this property, since all of the submodules $N_i \subset M$ are proper. Thus, $\psi \notin \mathrm{Im}\Phi$, so Φ is not surjective.

□

Exercise 9. Let F be a field of characteristic $\neq 2$, and let $a, b \in F^{\times}$. Let $A := F\langle i, j\rangle/(i^2 - a, j^2 - b, ij + ji)$. Show that A is a simple algebra with center F. You may use the fact that $\dim_F A = 4$.

Proof. **Solution by Rhea Kommerell.**

Note that $1, i, j, ij$ generate A as an F-vector space, so the assumption that F is 4-dimensional says that these elements are linearly independent over F.

To show that A is simple, assume it has a nonzero two-sided ideal I. We will show that $I = A$. Since I is nonzero, it has some nonzero element $c_1+c_2i+c_3j+c_4ij \in I$. Then $a^{-1}i(c_1+c_2i+c_3j+c_4ij)i \in I$ so $c_1 + c_2i - c_3j - c_4ij \in I$. Adding this to our original element of I, we find $2c_3j + 2c_4ij \in I$. Multiplying on both sides by j, we find $2c_3j - 2c_4ij \in I$. Then $2c_3j+2c_4ij+2c_3j-2c_4ij = 4c_3j \in I$. Since k is not characteristic two by assumption, $c_3j \in I$. Since j is a unit in A, we are done as long as $c_3 \neq 0$. If $c_3 = 0$, then $c_4ij \in I$. Since ij is a unit in A, we are done as long as $c_4 \neq 0$. If $c_4 = 0$, then note that $2c_2i + 2c_4ij = 2c_2i \in I$ by following the same argument as above but multiplying by j on both sides instead. Then since i is a unit in A, we are done as long as $c_2 \neq 0$. But if $c_2 = 0$ then our original element of I is just a constant c_1 which is a unit. This completes the proof that $I = A$.

Now to show that the center is F, suppose an element $c_1 + c_2i + c_3j + c_4ij$ is in the center. Then $i(c_1 + c_2i + c_3j + c_4ij) = (c_1 + c_2i + c_3j + c_4ij)i$ so, cancelling c_1i and c_2a on both sides, we get $c_3ij + c_4aj = -c_3ij - c_4aj$. Since ij and j are linearly independent, it follows that $c_3 = c_4 = 0$. A similar argument with multiplying by j shows that $c_2ij + c_4bi = -c_2ij - c_4bi$, so $c_2 = 0$. It follows that the central element lies in F, as desired.

It turns out that this central simple algebra A over k is either a division algebra (non-split case) or isomorphic to $\mathrm{GL}_2(F)$ (split case). In particular, A is split if and only if there is a solution to $ax^2 + by^2 = 1$ for $x, y \in F$. Read section 4 of these notes by Keith Conrad for proofs and discussion. □

Exercise 10. Let G be the (dihedral) group presented by

$$\langle x, y \mid x^5 = y^2 = xyxy = 1\rangle$$

You may use the fact that $|G| = 10$. Compute the character table of G.

Proof. Since G is presented with two generators x, y, every element of G can be written as a word in x and y. Since G contains a relation of the form $xy = y^ax^b$ (in particular, $xy = yx^{-1}$), every element of G can be written in the form x^ay^b for $a, b \in \mathbb{Z}$. Since x has order 5 and y has order 2, every element of G can be written as x^ay^b for $0 \leq a < 5$ and $0 \leq b < 2$. Since $|G| = 10$, every element of G can be written uniquely in this form. Let us compute the conjugacy classes of G.

First we compute the conjugacy classes of the elements $\{1, x, x^2, x^3, x^4\}$. Notice x commutes with each of these elements. Therefore for C_{x^a} the conjugacy class of x^a, the transitive group action $\psi : G \to \mathrm{Aut}(C_{x^a})$ by conjugation has kernel containing x. Since $G/\langle x\rangle$ is generated by y, $\operatorname{coker}\psi$ is generated by y and thus has order 1 or 2. Therefore, $|C_{x^a}| = 1$ or 2. Clearly the conjugacy class of 1 is 1. Since $yxy = x^4$ and $yx^2y = x^3$, the conjugacy class of x contains $\{x, x^4\}$ and likewise $\{x^2, x^3\}$. Since their conjugacy classes are of size at most two, these must be the conjugacy classes of these elements.

Finally we observe that $x^a y x^{-a} = x^{2a}y$. Therefore since we determined the other conjugacy classes, $\{y, xy, x^2y, x^3y, x^4y\}$ is the final conjugacy class.

Notice that since $\{1\}, \{x, x^4\}, \{x^2, x^3\}$ are conjugacy classes, $\mathbb{Z}/5\mathbb{Z} \cong \langle x \rangle < G$ is a normal subgroup of G, and $G/\langle x \rangle \cong \mathbb{Z}/2\mathbb{Z}$. This yields all of the one dimensional representations of G since $[G, G] = \langle x \rangle$. Thus we have the first two rows of the table. Now consider the following group homomorphism:

$$\varphi : \langle x, y \rangle \to \mathrm{GL}_2(\mathbb{R}) \qquad x \mapsto \begin{bmatrix} \cos(2\pi/5) & -\sin(2\pi/5) \\ \sin(2\pi/5) & \cos(2\pi/5) \end{bmatrix}, y \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Notice that $\varphi(x)^5 = \mathrm{Id}, \varphi(y)^2 = \mathrm{Id}$, and $\varphi(x)\varphi(y)\varphi(x)\varphi(y) = 1$. Therefore, φ factors as $\phi : G \to \mathrm{GL}_2(\mathbb{R})$. We easily compute the character of ϕ as the third row of the following table. We notice that $\langle \phi, \rangle \phi_G = 1$, so ϕ is irreducible. Finally, we deduce the final row of the character table using column orthogonality.

$\{1\}$	$\{x, x^4\}$	$\{x^2, x^3\}$	$\{x^a y\}$
1	1	1	1
1	1	1	-1
2	$2\cos(2\pi/5)$	$2\cos(4\pi/5)$	0
2	$2\cos(4\pi/5)$	$2\cos(2\pi/5)$	0

□

Spring 2024

Exercise 1. Let α be a complex root of $x^6 + 3$ and let $K = \mathbb{Q}(\alpha)$.

(a) Show that $K/\mathbb{Q}$ is normal.

(b) Compute the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Let $\omega = e^{2\pi i/12}$, a primitive 12th root of unity. The roots of $x^6 + 3$ in $\mathbb{C}$ are:

$$\omega\sqrt[6]{3}, \omega^3\sqrt[6]{3}, \omega^5\sqrt[6]{3}, \omega^7\sqrt[6]{3}, \omega^9\sqrt[6]{3}, \omega^{11}\sqrt[6]{3}$$

Let us show that for α any of the above complex roots, that $\mathbb{Q}(\alpha)$ contains all of the roots of x^6+3, so $\mathbb{Q}(\alpha)$ is the splitting field of $x^6 + 3$. It suffices to show that $\omega^2 \in \mathbb{Q}(\alpha)$, since each of the roots above differ by an integral power of ω^2. Also, $\omega^2 = e^{i\pi/3} = 1/2 + i\sqrt{3}/2$, so it suffices to show that $i\sqrt{3} \in \mathbb{Q}(\alpha)$. Notice that since $\alpha^6 = -3$, $\alpha^3 = \pm i\sqrt{3}$, so $i\sqrt{3} \in \mathbb{Q}(\alpha)$ as desired. Therefore, $K = \mathbb{Q}(\alpha)$ is the splitting field of $x^6 + 3$ over $\mathbb{Q}$ and thus $K/\mathbb{Q}$ is normal.

Now let us compute $\mathrm{Gal}(K/\mathbb{Q})$. By Eisenstein, $x^6 + 3$ is an irreducible polynomial, so it is the minimal polynomial of α. Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(x^6 + 3) = 6$, so $[K : \mathbb{Q}] = 6$. Therefore, $G = \mathrm{Gal}(K/\mathbb{Q})$ is an order 6 group and thus isomorphic to either S_3 or $\mathbb{Z}/6$. Notice that $\sqrt[3]{3} \in K$, for instance by $(\omega\sqrt[6]{3}) \cdot (\omega^{11}\sqrt[6]{3})$. Therefore, $\mathbb{Q}(\sqrt[3]{3})$ is a subfield of K and thus corresponds to a subgroup H of G. Furthermore, $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ is *not* normal, since $x^3 - 3$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein, and partially (but not fully) splits in $\mathbb{Q}(\sqrt[3]{3})$ since the other roots are imaginary and thus not contained in $\mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{R}$. Therefore, by the Galois correspondence H is not a normal subgroup of G, so G is nonabelian. Therefore, $G \cong S_3$. □

Exercise 2. Prove the following two statements.
Every maximal ideal of $\mathbb{C}[x, y]$ is of the form $\langle x - \alpha, y - \beta\rangle$ for $\alpha, \beta \in \mathbb{C}$.
Every maximal ideal of $\mathbb{R}[x, y]$ is either of the form:

(1) $\langle x - \alpha, y - \beta\rangle$ for $\alpha, \beta \in \mathbb{R}$, or

(2) $\langle l, q\rangle$ where $l \in \mathbb{R}[x, y]$ is linear and q is an irreducible polynomial of degree 2 on either x or y.

Proof.

(a) By Hilbert's Nullstenschatz, maximal ideals of $\mathbb{C}[x, y]$ correspond (inclusion reversing) to minimal (proper) Zariski closed subsets of $\mathbb{C}^2$. Since every point of $\mathbb{C}^2$ is closed, the only minimal closed subsets of $\mathbb{C}^2$ are points (α, β). The correspondence is by $(\alpha, \beta) \mapsto I(\{(\alpha, \beta)\})$ which is the set of polynomials in $\mathbb{C}[x, y]$ which vanish on (α, β). Clearly both $x - \alpha, y - \beta$ are contained in this ideal, and they generate it by polynomial division first in the variable x and then y.

(b) Since $\mathbb{C}[x, y]$ is an integral extension of $\mathbb{R}[x, y]$, the morphism $\varphi : \operatorname{Spec}(\mathbb{C}[x, y]) \to \operatorname{Spec}(\mathbb{R}[x, y])$ defined by $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathbb{R}[x, y]$ induced by the inclusion $\mathbb{R}[x, y] \hookrightarrow \mathbb{C}[x, y]$ is surjective. Furthermore, $\mathfrak{p} \in \operatorname{Spec}(\mathbb{C}[x, y])$ is maximal if and only if $\mathfrak{p} \cap \mathbb{R}[x, y]$ is maximal in $\mathbb{R}[x, y]$. Therefore, all of the maximal ideals of $\mathbb{R}[x, y]$ are of the form $\mathfrak{p} \cap \mathbb{R}[x, y]$ for $\mathfrak{m} = \langle x - \alpha, y - \beta\rangle$ with $\alpha, \beta \in \mathbb{C}$. Consider the sequence

$$\mathbb{R}[x, y] \xrightarrow{\iota} \mathbb{C}[x, y] \xrightarrow{\pi} \mathbb{C}$$

Where ι is the usual inclusion and π is defined (by universal property) by $x \mapsto \alpha, y \mapsto \beta$. Notice that $\ker \iota \circ \pi = \mathfrak{p} \cap \mathbb{R}[x, y]$. Thus, $\mathfrak{p} \cap \mathbb{R}[x, y]$ consists of the polynomials which are zero when evaluated in $\mathbb{C}$ with $x = \alpha$ and $y = \beta$. If both $\alpha, \beta \in \mathbb{R}$, it is clear by polynomial division that $\langle x - \alpha, y - \beta\rangle_{\mathbb{R}[x,y]}$ generates $\ker \iota \circ \pi$. Thus, without loss of generality assume that $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Since $[\mathbb{C} : \mathbb{R}] = 2$, let q be the minimal polynomial of α in $\mathbb{R}[x]$. Clearly $q \in \ker \iota \circ \pi$. Since $\alpha \in \mathbb{C} \setminus \mathbb{R}$, there exists some real numbers $r_0, r_1 \in \mathbb{R}$ such that $r_0\alpha + r_1 = \beta$. In particular, $l(x, y) = y - r_0x - r_1 \in \ker \iota \circ \pi$. Let us show that l, q generate $\ker \iota \circ \pi$, which shows that every maximal ideal of $\mathbb{R}[x, y]$ is one of the two described forms. Thus, suppose $p(x, y) \in \ker \iota \circ \pi$, so $p(\alpha, \beta) = 0$ when evaluated in $\mathbb{C}$. Since l is monic of degree one in y, there exists a real polynomial $f \in \mathbb{R}[x, y]$ such that $p - lf$ is a polynomial solely in x. Thus, $p - lf \in \mathbb{R}[x]$ and $(p - lf)$ evaluated at α is 0. Therefore, since q is the minimal polynomial of α in $\mathbb{R}[x]$, q divides $p - lf$, so $p - lf \in \langle l, q\rangle$. Therefore, $p \in \langle l, q\rangle$ as desired.

Exercise 3. Find all positive integers n such that $\cos(2\pi/n)$ is a rational number.

Proof. Let $n \in \mathbb{Z}^+$, and let $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n)$. Assume $\cos(2\pi/n)$ is a rational number. Then $\mathbb{Q}(\zeta) = \mathbb{Q}(i \sin(2\pi/n))$. Furthermore, $\omega = i \sin(2\pi/n)$ is a root of the rational polynomial $x^2 - \cos(2\pi/n)^2 + 1 = 0$. Therefore, $[\mathbb{Q}(i \sin(2\pi/n)) : \mathbb{Q}] \leq 2$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq 2$. Recall that $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is equal to the degree of the nth cyclotomic polynomial Φ_n, which is equal to $\varphi(n)$ for $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ the Euler totient function. Suppose $n = p_1^{r_1} \dots p_k^{r_k}$ for primes $p_1, \dots, p_k$. Recall that $\varphi(n) = \varphi(p_1^{r_1}) \dots \varphi(p_k^{r_k})$ and $\varphi(p^r) > 2$ for all p, r except for $p \in \{2, 3\}$ and $r \in \{1, 2\}$. Therefore, the only possible values n for which $\cos(2\pi/n)$ is rational are when $\varphi(n) \leq 2$, which is only satisfied by the previous note for $n = 1, 2, 3, 4, 6$. We check by hand that each of these has a rational value for $\cos(2\pi/n)$. □

□

Exercise 4. Let R be a Noetherian ring. Let I and J be two ideals of R. Show that

$$\operatorname{Tor}_1^R(R/I, R/J) \simeq (I \cap J)/IJ.$$

Proof. □

Exercise 5. Prove that a finitely generated projective module M over a local ring $(R, \mathfrak{m})$ is free.

Proof. Let P be a finitely generated projective R-module. Let $\mathfrak{m}$ be the unique maximal ideal of R, and let $k = R/\mathfrak{m}$ be the residue division ring. Since P is finitely generated, $k \otimes_R P \cong P/\mathfrak{m}P$ is a finitely generated k module and is thus free, so there is an isomorphism for some n:

$$k^n \xrightarrow{\hat{\psi}} P/\mathfrak{m}P$$

defined by $\hat{\psi} = \begin{pmatrix}[x_1] & \dots & [x_n]\end{pmatrix}$ for $[x_i] \in P/\mathfrak{m}P$. Let $x_1, \dots, x_n \in P$ be representatives of these equivalence classes, and define $\psi : k^n \to P$ by $\psi = \begin{pmatrix}x_1 & \dots & x_n\end{pmatrix}$. Let us first show that ψ is surjective. We have an exact sequence:

$$R^n \xrightarrow{\psi} P \longrightarrow \operatorname{coker}\psi \longrightarrow 0$$

Applying the functor $k \otimes_R -$, which is right exact, we have the following exact sequence:

$$k^n \xrightarrow{\hat{\psi}} k \otimes_R P \longrightarrow k \otimes_R \operatorname{coker}\psi \longrightarrow 0$$

Since $\hat{\psi}$ is an isomorphism, by exactness $k \otimes_R \operatorname{coker}\psi = \operatorname{coker}\psi/\mathfrak{m}\operatorname{coker}\psi = 0$. In particular, $\mathfrak{m}\operatorname{coker}\psi = \operatorname{coker}\psi$, and $\operatorname{coker}\psi$ is the quotient of a finitely generated module and is thus finitely generated. Therefore by non-commutative Nakayama's lemma, since $\mathfrak{m} = J(R)$, $\operatorname{coker}\psi = 0$. Therefore, ψ is surjective. Thus we have an exact sequence:

$$0 \longrightarrow \ker\psi \hookrightarrow R^n \xrightarrow{\psi} P \longrightarrow 0$$

Since P is projective, this sequence splits. Since tensoring is additive, it preserves split exact sequence, so $k \otimes_R -$ applied to this *split* exact sequence is again split exact, and in particular exact:

$$0 \longrightarrow k \otimes_R \ker\psi \longrightarrow k^n \xrightarrow{\hat{\psi}} P \longrightarrow 0$$

Since $\hat{\psi}$ is an isomorphism, $k \otimes_R \ker\psi = \ker\psi/\mathfrak{m}\ker\psi = 0$. Furthermore since the above sequence splits, $\ker\psi$ is a quotient of R^n and is thus finitely generated, so by non-commutative Nakayama's lemma again, $\ker\psi = 0$. □

Exercise 6. Let G be a finite group of order 300. Show that G is not simple by considering its action on its Sylow 5-subgroups.

Proof. Let n_5 be the number of 5-Sylow subgroups of G, i.e., subgroups of order 25. By the Sylow theorems, $n_5|300$ and $n_5 \cong 1 \bmod 5$. Therefore, $n_5 \in \{1, 6\}$ by simple casework. If $n_5 = 1$, then the 5-Sylow of G is unique and thus normal, so G contains a non-trivial normal subgroup. Thus, assume that $n_5 = 6$, and let S be the set of 5-Sylow subgroups. G acts transitively on S by conjugation, which induces a group homomorphism $\psi : G \to S_6$. Since the action is transitive, ψ is non-trivial so $0 \leq \ker\psi \trianglelefteq G$ is a non-zero normal subgroup. Also, $\operatorname{im}\psi$ is a subgroup of S_6. If ψ were injective ab absurdo, then $|\operatorname{im}\psi| = 300$, which does not divide $|S_6| = 720$ and thus ψ could not have been injective at all. Therefore, $\ker\psi \lneq G$ so $\ker\psi \trianglelefteq G$ is a proper normal subgroup of G. □

Exercise 7. Let G be a group and H a subgroup of G.

(a) If G is nilpotent, is H nilpotent?

(b) If H is normal in G and G is nilpotent, is G/H nilpotent?

(c) If H is normal in G and both H and G/H are nilpotent, is G nilpotent?

Proof. (a) Yes. Recall that G is nilpotent if and only if the descending central series $G_0 = G, G_1 = [G, G], \ldots, G_i = [G, G_{i-1}], \ldots$ eventually reaches 0. Let us show that $H_i \subseteq H \cap G_i$ for all $i \in \mathbb{N}$ by induction, which will show that H is nilpotent. This clearly holds for $i = 0$. Then we have that

$$H_{i+1} = [H, H_i] = \{xyx^{-1}y^{-1} \mid x \in H, y \in H_i\} \subseteq \{xyx^{-1}y^{-1} \mid x \in G, y \in G_i\} = [G, G_i] = G_{i+1}$$

by induction, as desired.

(b) Yes. Let $N_0 = G/H, N_1 = [G/H, G/H], \ldots, N_i = [G/H, N_{i-1}]$ be the descending central series of G/H. Let us show by induction that $N_i \subseteq (H \cdot G_i)/H$, which clearly holds for $i = 0$. Let $\pi : G \to G/H$ be the canonical projection. Thus, for $i \geq 0$,

$$N_{i+1} = [G/H, N_i] = \{[x][y][x]^{-1}[y]^{-1} \mid [x] \in G/H, [y] \in N_i\}$$

since $N_i \subseteq (H \cdot G_i)/H$, for every $[y] \in N_i$, there is a representative $y \in G_i$ such that $\pi(y) = [y]$. Therefore,

$$\subseteq \{\pi(xyx^{-1}y^{-1}) \mid x \in G, y \in G_i\} = \pi([G, G_i]) = \pi(G_{i+1}) = (H \cdot G_{i+1})/H$$

as desired. Therefore by induction, there is some n such that $N_n \subseteq (H \cdot (1))/H = (1)$, so G/H is nilpotent.

(c) No. Consider $\mathbb{Z}/3 \trianglelefteq S_3$.

□

Exercise 8.

(a) Let A be a finite abelian group and χ a complex character of A. Show that

$$\sum_{a\in A} |\chi(a)|^2 \le |A| \cdot \chi(1)$$

(b) Let G be a finite group and A an abelian subgroup of G of index n. Let ψ be an irreducible complex character of G. Show that $\psi(1) \le n$ (apply part (a) to the restriction of ψ to A).

Proof. (a) Since A is abelian, all of the irreducible characters of A are one dimensional, and are orthonormal with respect to the inner product on complex class functions of A by

$$\langle \chi_1, \chi_2 \rangle_A = \frac{1}{A} \sum_{a\in A} \overline{\chi_1(a)}\chi_2(a)$$

χ can be written as a finite sum of irreducible characters, so it is equal to

$$\chi = n_1\chi_1 + \cdots + n_k\chi_k$$

for $\chi_1, \ldots, \chi_k$ irreducible characters of A and $n_1, \ldots, n_k$ positive integers. Then we have:

$$\sum_{a\in A} |\chi(a)|^2 = |A|\langle \chi, \chi \rangle_A = |A| \left\langle \sum_{i=1}^{k} n_i\chi_i, \sum_{j=1}^{k} n_j\chi_j \right\rangle_A$$

by bilinearity of $\langle\ ,\ \rangle_A$, we have:

$$= |A| \sum_{i,j=1}^{k} n_i n_j \langle \chi_i, \chi_j \rangle_A$$

since the $\chi_1, \ldots, \chi_k$ are orthornormal, we have:

$$= |A| \sum_{i=1}^{k} n_i^2 \langle \chi_i, \chi_i \rangle_A = |A| \sum_{i=1}^{k} n_i^2 \le |A| \sum_{i=1}^{k} n_i$$

The last inequality is clear since the $n_1, \ldots, n_k$ are positive integers. Furthermore, $\chi(1) = n_1\chi(1) + \cdots + n_k\chi(k) = n_1 + \ldots n_k$ since each of the χ_i are one dimensional, so we have

$$\sum_{a\in A} |\chi(a)|^2 \le |A|\chi(1)$$

as desired.

(b) Let ψ be a complex irreducible character of G. By part (a), we have:

$$\psi(1) = \psi|_A(1) \le \frac{1}{|A|} \sum_{a\in A} |\chi(a)|^2 \le \frac{1}{|A|} \sum_{g\in G} |\psi(g)|^2$$

since ψ is irreducible, $1 = \langle \psi, \psi \rangle_G = \frac{1}{|G|} \sum_{g\in G} |\psi(g)|^2$, so

$$= \frac{1}{|A|} \sum_{g\in G} |\psi(g)|^2 = \frac{|G|}{|A|} = [G : A]$$

□

Exercise 9. Let A be a finite-dimensional algebra over an algebraically closed field k. Recall that the Jacobson radical $J(R)$ of a left Artinian ring R is a nilpotent ideal and $R/J(R)$ is semisimple. Show that the following are equivalent:

(a) The simple A-modules are 1-dimensional.

(b) $J(A)$ is the set of nilpotent elements of A.

Proof. Since A is a finite dimensional algebra over k, it is a finite dimensional vector space over A and thus a left Artinian k module. Therefore, A is left Artinian over itself so $J(A)$ is nilpotent. Thus, $J(A)$ is contained in the set of nilpotent elements of A. Also, $A/J(A)$ is semisimple, and thus by Artin-Wedderburn is isomorphic to a product ring for positive integers $n_1, \ldots, n_r$ and division rings $D_1, \ldots, D_r$ which are finite extensions of k:

$$A/J(A) \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

Since k is algebraically closed, the only finite extension division rings of k are k itself, so in fact

$$A/J(A) \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$$

for $n_1, \ldots, n_r$ positive integers. Let us show that both (a) and (b) are equivalent to $n_1 = \cdots = n_r = 1$.

First notice that any simple module M of A is annihilated by $J(A)$: since $J(A) \cdot M$ is a proper submodule of M by Nakayama and is thus 0 since M is simple. Therefore, the simple modules of A correspond to simple modules of $A/J(A)$. Furthermore, since $A/J(A)$ is semisimple, all of its simple modules appear as direct summands as a module over itself (since $A/J(A)$ surjects onto every simple module, and that surjection splits since $A/J(A)$ is semisimple), and specifically the simple modules are the modules $M_{n_1}(k), \ldots, M_{n_r}(k)$ when written in the form above by the Artin-Wedderburn theorem. Therefore, the simple A-modules all being 1-dimensional is equivalent to $n_1 = \cdots = n_r = 1$.

Let $x \in A$, so x can be written uniquely as $(a + (b_1, \ldots, b_r))$ for $a \in J(A)$ and $(b_1, \ldots, b_r) \in M_{n_1}(k) \times \cdots \times M_{n_r}(k)$. Since $J(A)$ is nilpotent, a is nilpotent, so x is nilpotent if and only if $(b_1, \ldots, b_r)$ is nilpotent. Thus, $J(A)$ containing all the nilpotent elements of A is equivalent to all of the rings $M_{n_1}(k), \ldots, M_{n_r}(k)$ having no nilpotent elements. This is clearly true if and only if $n_1 = \cdots = n_r = 1$, as desired. Thus, (a) $\Leftrightarrow n_1 = \cdots = n_r = 1 \Leftrightarrow$ (b) □

Exercise 10. Let F be a functor from a small category I to the category **Ab** of abelian groups. Show that F admits a colimit by constructing it as a quotient of $\bigoplus_i F(i)$ where i is indexed over the objects of I.

Proof. Let $f_i : F(i) \hookrightarrow \bigoplus_i F(i)$ be the canonical inclusions. Let S be the set of morphisms $\{\theta_\alpha^{ij}\}_{\alpha \in J}$ in $F(I)$, i.e., $\theta_\alpha^{ij} : F(i) \to F(j)$ is the image of a morphism in I by F. Then, define the abelian group A by

$$A = \bigoplus_i F(i) \Big/ \Big(f_j(\theta_\alpha^{ij}(x)) = f_i(x) \;\Big|\; \forall \theta_\alpha^{ij} \in S, \forall x \in F(i) \Big)$$

There are canonical inclusions $g_i : F(i) \to A$ by composing f_i with $\pi : \bigoplus_i F(i) \to A$ the projection map. Then $(A, \{g_i\})$ is a cocone of I. It is straightforward (although tedious) to show that it is initial in the category of I-cocones in **Ab** using the universal property of $\bigoplus_i F(i)$ and the first isomorphism theorem. □

Fall 2023

Exercise 1. Let G be a group, let $H \subset G$ be a subgroup of finite index $n \geq 2$, and let $x \in G$. Prove that $[H : H \cap xHx^{-1}] \leq n-1$.

Proof. Proof 1: inspired by stack exchange. Consider the action of G on the set $G/H \times G/xHx^{-1}$ of left cosets of H and xHx^{-1}. The stabilizer of (H, xHx^{-1}) is $H \cap xHx^{-1}$. Also notice that the orbit of $(H, x^{-1}(xHx^{-1}))$ is of size n, corresponding to the left cosets of H. Thus, either the orbit of (H, xHx^{-1}) is the same (of size n), or is disjoint and thus of size at most $n^2 - n = n(n-1)$. Either way, $[G : H \cap xHx^{-1}] \leq n^2 - n$ which implies $[H : H \cap xHx^{-1}] \leq n-1$ as desired.

Proof 2: Let G act by translation on G/xHx^{-1} by $\psi : G \to \mathrm{Aut}_{\mathbf{Set}}(G/xHx^{-1})$. Then ψ restricts to an action of H on G/xHx^{-1}, which has stabilizer on xHx^{-1} equal to $H \cap xHx^{-1}$. But also, H fixes the left coset $x^{-1}(xHx^{-1})$, so the orbit of xHx^{-1} is either in this orbit and thus size 1 or is disjoint and thus at most size $n-1$. Thus, $[H : H \cap xHx^{-1}] = |\mathrm{Orbit}_{\psi_H}(xHx^{-1})| \leq n-1$. □

Exercise 2. Let A be a commutative Noetherian ring. Prove that every nonzero ideal I of A contains a finite product of nonzero prime ideals.

Proof. Let S be the set of nonzero ideals of A which do not contain a finite product of nonzero prime ideals. Assume for the sake of contradiction that S is nonempty. Since A is Noetherian, S contains a maximal element (by inclusion) I. Since I does not contain a finite product of nonzero prime ideals, I is itself not prime, so there exist $a, b \in A \setminus I$ such that $a \cdot b \in I$. By maximality of I, $I + (a)$ contains a product of nonzero prime ideals $\mathfrak{p}_1 \dots \mathfrak{p}_r$, and $I + (b)$ contains a product $\mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_s$. Notice that $(I + (a))(I + (b)) = I^2 + (a)I + (b)I + (ab) \subset I$. Therefore, $\mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subset I$, a contradiction. Thus, S is empty as desired. □

Exercise 3. Show that there is an isomorphism of $\mathbb{Q}$-algebras $\mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t] \cong \mathbb{Q}[x,y]/(x^2 - y^2)$.

Proof. By universal property of $\mathbb{Q}[t]$ being the free $\mathbb{Q}$ algebra with one variable, there are $\mathbb{Q}$-algebra homomorphisms $\varphi_1, \varphi_2 : \mathbb{Q}[t] \to \mathbb{Q}[x,y]/(x^2 - y^2)$ defined by $t \mapsto x, t \mapsto y$. This induces a map $\psi : \mathbb{Q}[t] \times \mathbb{Q}[t] \to \mathbb{Q}[x,y]/(x^2 - y^2)$ defined by $\psi(p, q) = \varphi_1(p)\varphi_2(q)$. Since φ_1, φ_2 are $\mathbb{Q}$-algebra homomorphisms, ψ is $\mathbb{Q}$ bilinear. Also, ψ is $\mathbb{Q}[t^2]$ balanced since $\varphi_1(t^2) = x^2 \sim y^2 = \varphi_2(t^2)$. Thus ψ induces a $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t] \to \mathbb{Q}[x,y]/(x^2 - y^2)$ by $\varphi(p \otimes q) = \varphi_1(p)\varphi_2(q)$.

By the universal property of free $\mathbb{Q}$-algebras, there is a unique $\mathbb{Q}$-algebra homomorphism $f : \mathbb{Q}[x,y] \to \mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t]$ defined by $f(x) = t \otimes 1$ and $f(y) = 1 \otimes t$. We have that $f(x^2) = t^2 \otimes 1 \sim 1 \otimes t^2 = f(y^2)$, so f factors as a $\mathbb{Q}$-algebra homomorphism $\rho : \mathbb{Q}[x,y]/(x^2 - y^2) \to \mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t]$. Since x, y generate $\mathbb{Q}[x,y]/(x^2 - y^2)$ and $t \otimes 1, 1 \otimes t$ generate $\mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t]$, it suffices to check that $\varphi \circ \rho$ and $\rho \circ \varphi$ are the identity on these elements (easy check) to show they are inverses to one another.

□

Exercise 4. Let K/F be a (finite) Galois extension of fields, and let $\alpha K \setminus F$. Let E be a subfield of K containing F of largest degree over F such that $\alpha \notin E$. Prove that $E(\alpha)/E$ is a Galois extension of prime degree.

Proof. Let $G = \mathrm{Gal}(K/F)$ and $H = \mathrm{Gal}(E/F) \leq G$. Since E is a maximal subfield of K not containing α, by the Galois correspondence, every proper subgroup $H' \leq H$ of H fixes α. Let $N = \mathrm{Gal}(E(\alpha)/F) \lneq H$, which consists of all the $\sigma \in H$ which fix α, which forms a (proper) subgroup of H. Therefore H has the property that the union of every proper subgroup of H is the proper subgroup $N \lneq H$ of H. If H were not cyclic, then each $h \in H$ would generate proper subgroup $\langle h \rangle \lneq H$ and thus be contained in N, a contradiction. Thus, N is a maximal subgroup of H for H cyclic so $N \trianglelefteq H$ and $[H : N]$ is prime, which by the Galois correspondence means $E(\alpha)/E$ is Galois and $[E(\alpha) : E]$ is prime.

□

Exercise 5. Let F be a field, and let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial of degree $n \geq 1$ with coefficients $a_i \in F$. Show that the splitting field of $f(x^2)$ over F contains a square root of $(-1)^n a_0 a_n^{-1}$.

Proof. Fix an algebraic closure $\overline{F}$ of F, and let $r_1, \ldots, r_n$ be the roots of f in $\overline{F}$ so

$$f(x) = a_n(x - r_1) \ldots (x - r_n)$$

Therefore, $f(x^2)$ factors as

$$f(x^2) = a_n(x^2 - r_1) \ldots (x^2 - r_n)$$

Letting s_i be a root of $x^2 - r_i$ in the algebraic closure, we then have:

$$f(x^2) = a_n(x - s_1)(x + s_1) \ldots (x - s_n)(x + s_n)$$

In particular, $s_1, \dots, s_n \in L$ the splitting field of $f(x^2)$ over F and $s_i^2 = r_i$ for $1 \leq i \leq n$. Therefore,

$$L \ni \alpha = \prod_{i=1}^{n} s_i$$

and

$$\alpha^2 = (\prod_{i=1}^{n} s_i)^2 = \prod_{i=1}^{n} r_i = (-1)^n a_0 a_n^{-1}$$

□

Exercise 6. For a positive integer n let C_n be the category with objects $[1, n] := \{1, 2, \dots, n\}$ and morphisms $\mathrm{Mor}(i, j)$ an empty set if $i > j$ and a singleton otherwise. For positive integers m and n, a nonstrictly increasing function $f : [1, m] \to [1, n]$ can be viewed as a functor $C_n \to C_m$. Prove that this functor f has right adjoint if and only if $f(1) = 1$.

Proof. f having a right adjoint g means there is a natural bijection

$$\gamma_{ij} : \mathrm{Mor}_{C_m}(f(i), j) \to \mathrm{Mor}_{C_n}(i, g(j))$$

for all $i \in C_n, j \in C_m$. Since the morphism sets are singletons or empty, any such γ is natural, and this statement is equivalent to

$$f(i) \leq j \text{ if and only if } i \leq g(j)$$

for all $i \in C_n, j \in C_m$. Thus let us show that such a g exists if and only if $f(1) = 1$. If $f(1) \neq 1$, then $f(1) > 1$ but $1 \leq g(1)$ for any nondecreasing function $g : C_m \to C_n$. Thus f does not have a right adjoint.
Now assume that $f(1) = 1$. Define $g : C_m \to C_n$ by:

$$g(j) = \max\{i \in C_n \mid f(i) \leq j\}$$

Notice that this exists since $f(1) = 1$, so there is always at least one element in the set $\{i \in C_n \mid f(i) \leq j\}$. Let us show that f is left adjoint to g by showing that $f(i) \leq j$ if and only if $i \leq g(j)$. If $f(i) \leq j$, then $g(j)$ is the value i' maximal such that $f(i') \leq j$. Thus, $f(i) \leq f(i')$, so $i \leq i'$. Therefore, $i \leq g(j)$. If $f(i) > j$, then $g(j)$ is a value i' with $f(i') \leq j$ by definition, so $f(i) > f(i')$ so $i > i' = g(j)$ as desired.

□

Exercise 7. Let R be a PID and $n \geq 1$. Let M be a finitely generated R^n -module, where R^n is the product of n copies of R. Show that there exists an exact sequence

$$0 \to P \to Q \to M \to 0$$

with P and Q finitely generated projective R^n -modules.

Proof. Let $A = R^n$. Since M is finitely generated, there is a surjection (for sum $m \in \mathbb{N}$) $\psi : A^m \to M$. Thus we have a short exact sequence

$$0 \to \ker \psi \hookrightarrow A^m \to M \to 0$$

Thus let us show that every submodule of A^m is finitely generated projective. First notice that since R is a PID, it is Noetherian, so R^n is Noetherian. Therefore, $\ker \psi \subset A^m$ is finitely generated. Recall that R^n-**Mod** $\cong R$-**Mod** $\times$ R-**Mod** $\times \cdots \times$ R-**Mod** by $M \mapsto (e_1 M, e_2 M, \ldots, e_n M)$ where $e_1, \ldots, e_n$ are the idempotents $(1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)$ of R^n. Therefore, $\ker \psi \cong (N_1, \ldots, N_n) \in R$-**Mod**$\times \cdots \times$ R-**Mod** for $N_1 \subset R^m, N_2 \subset R^m, \ldots, N_n \subset R^m$ ideals. If each of $N_1, \ldots, N_n$ are projective in R-**Mod**, then $\ker \psi$ is projective in R^n-**Mod** since projectiveness is a categorical property. Furthermore, (by the classification of FG modules over a PID), each of $N_1, \ldots, N_n$ are free and thus projective, so $\ker \psi$ is projective.

□

Exercise 8. Let A be a domain that is normal (i.e., integrally closed in its quotient field), and let $\mathfrak{p}$ be a prime ideal of A.

(a) Show that the localization $A_\mathfrak{p}$ is a normal domain.

(b) Suppose that A is Noetherian and that $\mathfrak{p}$ is a minimal nonzero prime ideal of A. Show that $A_\mathfrak{p}$ is a DVR.

Proof. (a) Let k be the fraction field of A, so $A \subset A_\mathfrak{p} \subset k$. Let us show that if $m \in k$ satisfies a monic polynomial in $A_\mathfrak{p}[x]$, then $m \in A_\mathfrak{p}$. Thus, suppose that there exists $a_i, s_i \in (A \setminus \mathfrak{p})$ such that

$$m^n + m^{n-1}\frac{a_{n-1}}{s_{n-1}} + \cdots + \frac{a_1}{s_1} + \frac{a_0}{s_0} = 0$$

Let $\alpha = s_0 \ldots s_n \in A \setminus \mathfrak{p}$. Then we have that

$$\alpha^n(m^n + m^{n-1}\frac{a_{n-1}}{s_{n-1}} + \cdots + \frac{a_0}{s_0})$$

$$(\alpha m)^n + (\alpha m)^{n-1}\frac{\alpha a_{n-1}}{s_{n-1}} + \cdots + (\alpha m)^1 \frac{\alpha^{n-1} a_1}{s_1} + \frac{\alpha^n a_0}{s_0} = 0$$

Notice that $s_i | \alpha$ for $0 \le i \le n-1$, so the coefficients $\frac{\alpha^{n-k} a_k}{s_k} \in A \subset k$. Therefore, $\alpha m \in k$ satisfies a monic polynomial in $A[x]$, so since A is normal $\alpha m \in A$. Therefore, since $\alpha \in A \setminus \mathfrak{p}$, $\frac{\alpha m}{\alpha} \in A_\mathfrak{p}$, so $A_\mathfrak{p}$ is integrally closed.

(b) A DVR is an integrally closed Noetherian domain with Krull dimension 1. Since the prime ideals of $A_\mathfrak{p}$ are in bijection with the prime ideals of A contained in $\mathfrak{p}$, $A_\mathfrak{p}$ has a unique prime. $A_\mathfrak{p}$ is Noetherian since A is and is integrally closed by part (a).

□

Exercise 9. Find the dimensions and characters of all irreducible $\mathbb{Q}$-representations of the cyclic group of order a prime p.

Proof. $\mathbb{Q}$ representations of $\mathbb{Z}/p$ are equivalent to $\mathbb{Q}\mathbb{Z}/p$ modules. Furthermore, $\mathbb{Q}\mathbb{Z}/p$ is a semisimple ring by Maschke's theorem since $\mathbb{Q}$ is characteristic zero. Therefore, all of the irreducible $\mathbb{Q}$ representations of $\mathbb{Z}/p$ appear as direct summands of the regular representation $\mathbb{Q}\mathbb{Z}/p \cong \mathbb{Q}[x]/(x^p - 1)$. Notice that $x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$ is the factorization of $x^p - 1$ into irreducibles in $\mathbb{Q}$. Therefore, as a $\mathbb{Q}[x]/(x^p - 1)$ module with x acting by multiplication by x,

$$\mathbb{Q}[x]/(x^p - 1) \cong \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x^{p-1} + \cdots + 1)$$

Since $x^{p-1} + \cdots + 1$ is irreducible over $\mathbb{Q}$, $\mathbb{Q}[x]/(x^{p-1} + \cdots + 1)$ is a field, and thus is a minimal non-zero ideal of $\mathbb{Q}[x]/(x^p - 1)$. Therefore, $\mathbb{Q}[x]/(x-1), \mathbb{Q}[x]/(x^{p-1} + \cdots + 1)$ are irreducible $\mathbb{Q}[x]/(x^p - 1)$ modules and are clearly distinct. Thus, these are the only two irreducible $\mathbb{Q}$-representations, of dimension 1 and $p-1$. Let χ_1 be the character of $\mathbb{Q}[x]/(x-1)$ and χ_2 the character of $\mathbb{Q}[x]/(x^{p-1} + \cdots + 1)$. Then $\chi_1 \oplus \chi_2 = \chi_{reg}$ the character of $\mathbb{Q}[x]/(x^p - 1)$, which is $\chi(1) = p$ and $\chi(x^l) = 0$ for $0 < l < p$. Also, χ_1 is the trivial representation $\mathbb{Z}/p \mapsto \mathbb{Q}^\times$ by $1 \mapsto 1$, so $\chi_2 = \chi_{reg} - \chi_1$. Thus, $\chi_2(1) = p - 1$ and $\chi_2(x^l) = -1$ for $1 < l < p$.

□

Exercise 10. Let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional irreducible representation of a finite group G over the field of complex numbers. Prove that for every central element $g \in G$, the operator $\rho(g)$ is multiplication by a scalar.

Proof. Notice that $\rho(g) : V \to V$ is a $\mathbb{C}G$ module homomorphism (a homomorphism of G representations) since $\rho(g) \circ \rho(h) = \rho(g \cdot h) = \rho(h \cdot g) = \rho(h) \circ \rho(g)$ for all $h \in G$. Since $\mathbb{C}$ is algebraically closed and V is finite dimensional, there is a non-zero eigenvector $v \in V$ with eigenvalue $\lambda \in \mathbb{C}$, so $\rho(g)(v) = \lambda v$. Therefore, $\rho(g) - \lambda \,\mathrm{Id}_V : V \to V$ is a $\mathbb{C}G$ module homomorphism with nonzero kernel, so $\ker(\rho - \lambda \,\mathrm{Id}_V)$ is a non-trivial $\mathbb{C}G$ submodule of V. Since V is a simple $\mathbb{C}G$ module, this forces $\ker(\rho - \lambda \,\mathrm{Id}_V) = V$, so ρ is multiplication by λ.

□

Spring 2023

Exercise 1. Let $F, F' : \mathcal{C} \to \mathcal{D}$ and $G, G' : \mathcal{D} \to \mathcal{C}$ be four functors such that F is left adjoint to G and F' is left adjoint to G'. Establish a bijection between the natural transformations $\alpha : F \Rightarrow F'$ and the natural transformations $\beta : G' \Rightarrow G$. [Hint: Use $G\alpha G' : GFG' \to GF'G'$].

Proof. Let $\eta : 1_{\mathcal{C}} \Rightarrow GF, \eta' : 1_{\mathcal{C}} \Rightarrow G'F'$, $\epsilon : FG \Rightarrow 1_{\mathcal{D}}, \epsilon' : F'G' \Rightarrow 1_{\mathcal{D}}$ be the units and counits of the adjunctions. Then define a function ψ from the collection of natural transformations $\alpha : F \Rightarrow F'$ to natural transformations $G' \Rightarrow G$ by:

$$\psi(\alpha) = \ G' \xRightarrow{\eta G'} GFG' \xRightarrow{G\alpha G'} GF'G' \xRightarrow{G\epsilon'} G$$

Similarly, define φ from natural transformations $\beta : G' \Rightarrow G$ to natural transformations $F \Rightarrow F'$ by:

$$\varphi(\beta) = \ F \xRightarrow{F\eta'} FG'F' \xRightarrow{F\beta F'} FGF' \xRightarrow{\epsilon F'} F'$$

Let us show that $\varphi \circ \psi(\alpha) = \alpha$. We have:

$$\varphi \circ \psi(\alpha) = \epsilon F' \circ FG\epsilon' F' \circ FG\alpha G'F' \circ F\eta G'F' \circ F\eta'$$

By naturality of $\epsilon F'$, the following diagram commutes for any object $X \in \mathcal{C}$:

$$\begin{tikzcd}
FGF'G'F'(X) \arrow[r, "\epsilon_{F'G'F'(X)}"] \arrow[d, "FG\epsilon'_{F'(X)}"] & F'G'F'(X) \arrow[d, "\epsilon'_{F'(X)}"] \\
FGF'(X) \arrow[r, "\epsilon_{F'(X)}"] & F'(X)
\end{tikzcd}$$

Therefore, we have:

$$= \epsilon' F' \circ \epsilon F'G'F' \circ FG\alpha G'F' \circ F\eta G'F' \circ F\eta'$$

By naturality of $\epsilon F'$ applied to $FG\alpha$, we have for any object X in $\mathcal{C}$:

$$\begin{tikzcd}
FGF(X) \arrow[r, "\epsilon_{F(X)}"] \arrow[d, "FG\alpha_X"] & F(X) \arrow[d, "\alpha_X"] \\
FGF'(X) \arrow[r, "\epsilon_{F'(X)}"] & F'(X)
\end{tikzcd}$$

Therefore, we have

$$= \epsilon' F' \circ (\epsilon F' \circ FG\alpha \circ F\eta)G'F' \circ F\eta' = \epsilon' F' \circ (\alpha \circ \epsilon F \circ F\eta)G'F' \circ F\eta'$$

And by unit-counit relations, we have

$$= \epsilon' F' \circ \alpha G' F' \circ F \eta'$$

Finally by naturality of $\alpha_{G'F'}$, the following diagram commutes for all objects $X \in \mathcal{C}$:

$$\begin{tikzcd}
FG'F'(X) \arrow[r, "\alpha_{G'F'X}"] & F'G'F'(X) \\
F(X) \arrow[u, "F\eta'_X"] \arrow[r, "\alpha_X"] & F'(X) \arrow[u, "F'\eta'_X"']
\end{tikzcd}$$

Therefore, we have:

$$= \epsilon' F' \circ F' \eta' \circ \alpha = \alpha$$

By the counit relations. By a symmetric argument, $\psi \circ \varphi(\beta) = \beta$ for all natural transformations $\beta : G' \Rightarrow G$, so ψ, φ are inverses on the level of sets so ψ is a bijection as desired. □

Exercise 2. Let p, q be distinct prime numbers and consider the number field $K = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. Describe all subfields of K and inclusions between them.

Proof. Notice that K contains $\sqrt{pq}$ and thus both $\sqrt{p}$ and $\sqrt{q}$, so $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Now we can check that p is not a square in $\mathbb{Q}(\sqrt{q})$ explicitly. Suppose let $x = a + b\sqrt{q} \in \mathbb{Q}(\sqrt{q})$ arbitrary. Then if $x^2 \in \mathbb{Q}$, either $a = 0$ or $b = 0$. There are no solutions to $a^2 = p$ or $b^2 = pq$, so p is not a square in $\mathbb{Q}(\sqrt{q})$. Therefore, $[K : \mathbb{Q}(\sqrt{q})] = 2$, so $[K : \mathbb{Q}] = 4$. Also, notice that K is Galois over $\mathbb{Q}$ since it is the splitting field of $(x^2 - p)(x^2 - q)$. Thus, $G = \mathrm{Gal}(K/\mathbb{Q})$ is order 4. Each element $\sigma \in G$ is determined by its action on $\sqrt{p}, \sqrt{q}$, and must map $\sqrt{p}$ to $\pm\sqrt{p}$ and $\sqrt{q} \to \pm\sqrt{q}$. Since there are only 4 possible such automorphisms and $|G| = 4$, each of these choices yields a $\mathbb{Q}$ automorphism of K. Therefore, $G = \langle \sigma, \tau \rangle$ with $\sigma(\sqrt{p}) = -\sqrt{p}, \sigma(\sqrt{q}) = \sqrt{q}, \tau(\sqrt{p}) = \sqrt{p}, \tau(\sqrt{q}) = -\sqrt{q}$. We easily see that $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ which has 5 subgroups, which by the Galois correspondence gives the following tower of subfields of K (with inclusions shown):

$$\begin{tikzcd}
 & K \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt{p}) \arrow[dr, no head] & \mathbb{Q}(\sqrt{q}) \arrow[d, no head] & \mathbb{Q}(\sqrt{pq}) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

□

Exercise 3. Give an example of an infinite field extension $K \subset L$ such that L has only finitely many field automorphisms fixing K.

Proof. Example 1: Let $L = \mathbb{Q}(2^{1/3}, 2^{1/9}, 2^{1/27}, \dots)$. Then any $\mathbb{Q}$ automorphism of L is determined by its action on $2^{1/3}, 2^{1/9}, \dots$. Furthermore, it must send $2^{1/3^n}$ to another root of $x^{3^n} - 1$ in $\mathbb{Q}$. But since $L \subset \mathbb{R}$, there is a unique solution to $x^{3^n} - 1$, so each of $2^{1/3}, 2^{1/9}, \dots$ must be fixed by any $\mathbb{Q}$ automorphism of L. So $\mathrm{Aut}_K(L) = \{\mathrm{Id}_L\}$.

Example 2: Let $K = \mathbb{F}_p(x_0)$, and let $L = K[x_1, x_2, \dots]/(x_i^p - x_{i-1})$. Equivalently, let $K_1 = K[x_1]/(x_1^p - x_0)$, $K_2 = K_1[x_2]/(x_2^p - x_1), \dots$ and let $L = \bigcup_{i=1}^{\infty} K_i$. It is clear that $[L : K] = \infty$. An element $\sigma \in \mathrm{Aut}_K(L)$ is determined by its action on each x_i. By induction, $\sigma(x_n) = x_n$ since x_n must be mapped to a pth root of x_{n-1}, and there is only one. Thus, $\mathrm{Aut}_K(L) = \{\mathrm{Id}_L\}$. □

Exercise 4. Let $M_n(K)$ be the ring of $n \times n$-matrices with coefficients in a field K, for $n \geq 1$. Describe all possible ring homomorphisms $M_n(K) \to K$.

Proof. When $n = 1$, there are many possible $K \to K$ homomorphisms (i.e., Galois theory!). Let us show that for $n \geq 2$ that there are no ring homomorphisms $M_n(K) \xrightarrow{\psi} K$. Suppose such a ψ existed. Let $e_{ij} \in M_n(K)$ be the matrix with all zero entries but a 1 in the ijth entry. Notice that $e_{ii}e_{ij} - e_{ij}e_{ii} = e_{ij}$, but since K is commutative,

$$\psi(e_{ij}) = \psi(e_{ii})\psi(e_{ij}) - \psi(e_{ij})\psi(e_{ii}) = 0$$

Furthermore, letting $j \neq i$, we have that $e_{ij}e_{ji} = e_{ii}$. Thus, $\psi(e_{ii}) = \psi(e_{ij})\psi(e_{ji})$. But notice that $I_n = \sum_{i=1}^n e_{ii}$, so

$$1_K = \psi(I_n) = \sum_{i=1}^{n} \psi(e_i i) = 0$$

which is a contradiction. Thus, such a ψ cannot exist. □

Exercise 5. Let A be a local commutative noetherian ring and M a finitely generated A-module such that every exact sequence $0 \to M'' \to M' \to M \to 0$ remains exact after tensoring with the residue field k of A. Show that M is free.

Proof. Let $\mathfrak{m} \subset A$ be the unique maximal ideal of A so $A/\mathfrak{m} = k$. Since M is finitely generated, $M/\mathfrak{m}M$ is a finitely generated $A/\mathfrak{m} = k$ module and is thus free. Thus, there is an isomorphism $\tilde{\psi} : k^n \to M/\mathfrak{m}M$ defined by $\tilde{\psi}(l_1, \dots, l_n) = [m_1]l_1 + \cdots + [m_n]l_n$, for representatives $m_1, \dots, m_n \in M$.

Then define $\psi : A^n \to M$ by $\psi(a_1, \dots, a_n) = a_1 m_1 + \cdots + a_n m_n$. Let us first show that ψ is surjective. We have an exact sequence

$$\begin{tikzcd} A^n \arrow[r, "\psi"] & M \arrow[r, two heads] & \operatorname{coker}\psi \arrow[r] & 0 \end{tikzcd}$$

Tensoring with k is right exact, so this yields the exact sequence (using the fact that the functors $\otimes_A k$ and $M \mapsto M/\mathfrak{m}M$ are equivalent)

$$\begin{tikzcd} k^n \arrow[r, "\tilde{\psi}"] & M/\mathfrak{m}M \arrow[r] & \operatorname{coker}\psi/\mathfrak{m}\operatorname{coker}\psi \arrow[r] & 0 \end{tikzcd}$$

Since $\tilde{\psi}$ is an isomorphism and this sequence is exact, $\operatorname{coker}\psi = \mathfrak{m}\operatorname{coker}\psi$. Since $\operatorname{coker}\psi$ is a quotient of M, it is a finitely generated A module, and thus by Nakayama's lemma there exists $m \in \mathfrak{m}$ such that $(1-m)\operatorname{coker}\psi = 0$. But since A is local, $(1-m) \in A^\times$, so $\operatorname{coker}\psi = 0$. Thus, ψ is surjective and we have a short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \ker\psi \arrow[r, hook] & A^n \arrow[r, "\psi"] & M \arrow[r] & 0 \end{tikzcd}$$

By assumption, exactness is preserved when tensoring with k, so we have an exact sequence of k modules;

$$\begin{tikzcd} 0 \arrow[r] & \ker\psi/\mathfrak{m}\ker\psi \arrow[r] & k^n \arrow[r, "\tilde{\psi}"] & M/\mathfrak{m}M \arrow[r] & 0 \end{tikzcd}$$

Since $\tilde{\psi}$ is an isomorphism, $\ker\psi = \mathfrak{m}\ker\psi$. Since A is Noetherian, and $\ker\psi$ is a submodule of A^n, $\ker\psi$ is a finitely generated A module. Thus by the same application of Nakayama, $\ker\psi = 0$ and ψ is an isomorphism. □

Exercise 6. Let A be a commutative ring and let $s \in A$. Let $S = \{1, s, s^2, \dots\}$. Show that the following assertions are equivalent:

(a) The canonical morphism $A \xrightarrow{\eta} S^{-1}A$ is surjective.

(b) There is $N > 0$ such that $s^n A = s^N A$ for all $n \geq N$.

(c) For N large enough, the ideal $s^N A$ is generated by an element e with $e^2 = e$.

Proof.

(c) ⇒ (b) Since $e \in s^N A$, let $k \in A$ such that $e = s^N k$. Let us show that for $n \geq N$ that $s^n A = s^N A$. Clearly $s^n A \subseteq s^N A$. Thus take some $e \cdot a = s^N ka \in s^N A$ an arbitrary element of $s^N A$. Let $m \in \mathbb{N}$ such that $m \cdot N > n$. Then we have:

$$e \cdot a = e^m a = s^{mN} k^m a \in s^n A$$

as desired.

(b) ⇒ (a) Take an arbitrary element $\frac{b}{s^r} \in S^{-1}A$. By assumption, $s^{N+r}A = s^N A$, so there is $a \in A$ such that $s^{N+r}a = s^N b$. Then we have that $\frac{b}{s^r} = \frac{a}{1} = \eta(a)$ since:

$$s^N(b - as^r) = s^N b - as^{N+r} = 0$$

Therefore, η is surjective.

(a) ⇒ (c) Since η is surjective, there is some $k \in A$ such that $\eta(k) \sim \frac{1}{s}$. In particular, this means that there is some N such that

$$s^N(sk - 1) = 0 \qquad s^{N+1}k = s^N$$

Let $e = S^N k^N$. Notice that $e^2 = s^{2N}k^{2N} = s^N k^N = e$. Also, k generates $S^N A$ since for any $s^N a \in s^N A$, we have $es^N a = s^{2N}k^N a = s^N a$.

□

Exercise 7. Let k be a field and let $A = k[X,Y]/(X^2, XY, Y^2)$.

(a) Determine the invertible elements of A.

(b) Determine the ideals of A.

(c) Determine the principal ideals of A.

Proof. Notice that $k[X,Y]$ as a k-vector space has basis the polynomials $X^m Y^n$ for $m,n \in \mathbb{N}$. The ideal (X^2, XY, Y^2) is a k-vector space of $k[X,Y]$ with basis all the polynomials $X^m Y^n$ for $m+n \geq 2$. Therefore since quotients commute with the forgetful functor **Ring** → k-**Mod**, A is a 3 dimensional k-vector space with basis $X, Y, 1$. Thus, any equivalence class in A can be identified uniquely with an element of the form $aX + bY + c$ for $a, b, c \in k$. The multiplication between such elements is obvious.

(a) An element $aX + bY + c$ is invertible if $c \neq 0$, with inverse $c^{-1}(1 - aX/c)(1 - bY/c)$. An element $aX + bY$ is not invertible since $(aX + bY)(a'X + b'Y + c') = (c'aX + c'bY) \neq 1$.

(b) and (c) An ideal of A is also a k subspace of A. Let $V = \langle X, Y\rangle_k \subset A$ be the k span of X, Y. $A \setminus V = A^\times$ by part (a), so any non-unital ideal of A us a k-subspace of V. Let us show that all such subspaces are in fact ideals of A. This is clear for (0). Let $W = \langle aX + bY\rangle_k \subset V$ be a one dimensional k subspace of V. It suffices to show that the generator of W is closed under left multiplication by A:

$$(a'X + b'Y + c')(aX + bY) = c'aX + c'bY \in W$$

Thus, each of the one dimensional subspaces of V are principal ideals of A. (0) and A are clearly principal ideals of A. The only remaining possible ideal is V itself, which is clearly an ideal by the above computation. V is not principal since we showed that for all $v \in V$ non-zero, $(v) \subset A$ is a 1 dimensional subspace W of A (and thus not V).

□

Exercise 8. Let G be a finite group and let p be the smallest prime dividing the order of G. Show that a subgroup $H \leq G$ of index p must be normal.

Proof. Let G act on left cosets of H. Standard proof. □

Exercise 9. Let G be a non-abelian finite group of order pq where p and q are prime numbers with $q > p$. Determine the degrees of the irreducible characters of G, and determine the number of irreducible characters of a given degree.

Proof. Since $q > p$, there is a unique q-Sylow, and thus $G = \mathbb{Z}/q \rtimes_\psi \mathbb{Z}/p$ for ψ a non-trivial homomorphism $\mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/q)$. Such a homomorphism exists if and only if $p|(q-1)$, so $p|(q-1)$. The degree of an irreducible character of G divides $|G|$, and thus the possible degrees of irreducible characters of G are $1, p, q$, and pq. Since the sum of the squares of the degrees of the irreducible characters of G is equal to $|G|$ and $(pq)^2 > q^2 > pq$, the irreducible characters of G are all degree 1 or p. Thus let us count the number of degree 1 irreducible characters of G. Every degree 1 representation of G is automatically irreducible. The degree 1 representations of G are the group homomorphism $G \mapsto C^\times$. Since $C^\times$ is Abelian, each such representation factors through $G/[G,G]$, so it suffices to find all group homomorphisms $G/[G,G] \to C^\times$. Since G is non-abelian, $[G,G]$ is a non-trivial normal subgroup. Also, $[G,G]$ is contained in the q-Sylow $N \cong \mathbb{Z}/q$ by construction of the semidirect product, so $[G,G] = \mathbb{Z}/q$ since the only non-trivial normal subgroup of G contained in N is N itself. Therefore, the degree 1 representations of G are given by all group homomorphisms $G/[G,G] \cong \mathbb{Z}/p \to C^\times$. There are p such representations, by $1 \mapsto e^{2\pi i k/p}$ for $0 \leq k < p$. Therefore, there are p degree 1 irreducible characters of G. Suppose there are k degree p irreducible characters of G. Since the sum of the squares of the degrees of the irreducible characters of G is equal to $|G|$,

$$kp^2 + p = pq = |G|$$

$$\Rightarrow k = \frac{q-1}{p}$$

Therefore, G has p degree 1 irreducible characters and $\frac{q-1}{p}$ degree p irreducible characters. □

Exercise 10. Let A be an artinian ring and let M be an A-module. Let $B = \mathrm{End}_A(M)$. Let

$f \in B$ such that $f(M) \subset \mathrm{Rad}(A) \cdot M$, where $\mathrm{Rad}(A) = J(A)$ is the Jacobson radical. Show that $f \in \mathrm{Rad}(B)$.

Proof. To show that $f \in \mathrm{Rad}(B)$, it suffices to show that $(1 - f \circ b) \in B^\times$ for all $b \in B$. Let $g = f \circ b$. Notice that $g(M) = f \circ b(M) \subset f(M) \subset \mathrm{Rad}(A) \cdot M$. If we show that g is nilpotent (there exists $n \in \mathbb{N}$ such that $g^n = 0$), then $1 - g$ is invertible with inverse $1 + g + \cdots + g^{n-1}$. Thus, let us show that g is nilpotent. Notice that

$$g^2(M) = g \circ g(M) \subset g(\mathrm{Rad(A)} \cdot M) = \mathrm{Rad(A)}g(M)$$

since g is an A module endomorphism. In particular applying the above n times, we have

$$g^n(M) \subset (\mathrm{Rad}(A))^n(M)$$

Thus, it suffices to show that $\mathrm{Rad}(A)$ is nilpotent. This is a standard exercise for artinian rings which we repeat here. Since A is artinian, the descending sequence $\mathrm{Rad}(A) \supseteq \mathrm{Rad}(A)^2 \supseteq \dots$ is eventually constant. Thus, there is some n such that $\mathrm{Rad}(A)^n = \mathrm{Rad}(A)^{n+1}$. Since A is artinian it is also Noetherian by Akizuki-Hopkins-Levitzki, and thus $\mathrm{Rad}(A)^n \subseteq A$ is a finitely generated A module and thus by noncommutative Nakayama $\mathrm{Rad}(A)^n = 0$.

Note: usually (or at least in the course this year) we use that $J(A)$ is nilpotent to prove Akizuki-Hopkins-Levitzki, so this argument would be circular. That being said, on the qual you should assume major theorems if it makes things easier. But we don't need Akizuki-Hoplins-Levitzki:

Let $I = \mathrm{Rad}(A)^n$ so $I^2 = I$. For contradiction assume that $I \neq 0$, there is a left ideal K such that $I \cdot K \neq 0$. Take a minimal such K, so $K = (x)$ for some $x \in A$. Then $I^2 \cdot (x) = I(I \cdot (x)) = I \cdot (x)$, so by minimality $I \cdot (x) = (x)$. By noncommutative Nakayama and $I \subset \mathrm{Rad}(A)$, $(x) = 0$. □

Fall 2022

Exercise 1. Find all subfields of the field $F = \mathbb{Q}(2^{1/3}, 3^{1/3})$.

Proof. First notice that $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \omega)$ is the splitting field of $x^3 - 2, x^3 - 3$ for $\omega = e^{2\pi i/3}$. Let us show that $[\mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{3})] = 3$, which will imply that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \omega)/\mathbb{Q})$ is a group of order 18 since $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ by Eisenstein and $[\mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{2}, \omega) : F] = 2$ since F is purely real and ω has an imaginary component.

We will explicitly show that $x^3 - 2$ has no roots in $x^3 - 3$. There are better ways to do this - ramification theory is the best (I don't know it yet). Let $a + b\sqrt{3} + c\sqrt{9} = x \in \mathbb{Q}(\sqrt[3]{3})$ be an arbitrary element with $x^3 = 2$. After multiplying by the common denominators of a, b, c and dividing by any common divisor, assume that a, b, c are coprime integers such that $x^3 = 2k^3$ for some $k \in \mathbb{Z}^+$. Considering the coefficient of 1 and $\sqrt[3]{3}$ in their product, we have $a^3 + 3b^3 + 9c^3 + 18abc \equiv 0 \bmod 2$ and $a^2b + 3ac^2 + 3b^2c \equiv 0 \bmod 2$. In particular,

$$a^3 + b^3 + c^3 \equiv 0 \bmod 2$$

$$a^2b + ac^2 + b^2c \equiv 0 \bmod 2$$

The only solutions to $a^2b + ac^2 + b^2c \equiv 0 \bmod 2$ are if all of a, b, c are even or if exactly two are. But a, b, c are coprime by assumption, so exactly two of them are even. But then $a^3 + b^3 + c^3 \equiv 1 \bmod 2$, a contradiction. So $x^3 - 2$ has no roots in $\mathbb{Q}(\sqrt[3]{3})$ and is thus irreducible.

Thus, $G = \mathrm{Gal}(F(\omega)/\mathbb{Q})$ is order 18. Also, every element of G must send $\sqrt[3]{3}$ to another root of $x^3 - 3$ and likewise for ω with $x^2 + x + 1$ and $\sqrt[3]{2}$ with $x^3 - 2$. There are thus 18 total choices for any element of G on these three elements. Furthermore, any element of G is determined by its action on $\sqrt[3]{3}$, $\sqrt[3]{2}$, and ω, so every choice of permutation of the roots of these polynomials yields an element of G. Thus we can explicitly write a generating set of G:

$$\alpha : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \sqrt[3]{3} \mapsto \omega\sqrt[3]{3}, \omega \mapsto \omega \qquad \beta : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, \sqrt[3]{3} \mapsto \sqrt[3]{3}, \omega \mapsto \omega$$

$$\gamma : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \sqrt[3]{3} \mapsto \sqrt[3]{3}, \omega \mapsto \omega^2$$

It is then easy to compute that $\alpha^3 = \beta^3 = \gamma^2 = \mathrm{id}$, $\alpha\beta\alpha^{-1} = \beta$, $\gamma\alpha\gamma = \alpha^{-1}$, $\gamma\beta\gamma = \beta^{-1}$. By order considerations, this describes G completely as $(\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes_\psi \mathbb{Z}/2$ with $\psi : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/3 \times \mathbb{Z}/3)$ by $\psi(1)(a, b) = (-a, -b)$. The subfields of F correspond to the subgroups of G containing ω. There are the subgroups $G, \langle\gamma\rangle$, and 4 subgroups of order 6: $\langle\alpha, \gamma\rangle, \langle\beta, \gamma\rangle, \langle\alpha\beta, \gamma\rangle, \langle\alpha\beta^2, \gamma\rangle$. The fixed fields G^H of these groups contain $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{3}), \mathbb{Q}(\sqrt[3]{6}), \mathbb{Q}(\sqrt[3]{12})$, and since $x^3 - a$ is irreducible by Eisenstein for $a = 2, 3, 6, 12$, these are exactly the fixed fields by degree considerations. Thus, the subfields of F are these four fields, F itself, and $\mathbb{Q}$. □

Exercise 2. Let $P(x) = x^6 + 3$.

(a) Find the splitting field of P.

(b) Determine the isomorphism type of the Galois group of P over $\mathbb{Q}$.

Proof. (a) $x^6 + 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, or since -3 is not a square in $\mathbb{Q}$. The roots of $x^6 + 3$ (fixing an embedding $\mathbb{Q} \hookrightarrow \mathbb{C}$) are:

$$\omega\sqrt[6]{3}, \omega^3\sqrt[6]{3}, \omega^5\sqrt[6]{3}, \omega^7\sqrt[6]{3}, \omega^9\sqrt[6]{3}, \omega^{11}\sqrt[6]{3}$$

for $\omega = e^{\pi i/6} = \frac{\sqrt{3}+i}{2}$ a primitive 6th root of unity. Clearly the splitting field P contains $F = \mathbb{Q}(\omega\sqrt[6]{3}) \cong \mathbb{Q}(x)/(P(x))$. Let us show this is the splitting field of P by showing that $\omega^2 \in F$, and thus every root of P. Notice that $\omega^2 = e^{\pi i/3} = \frac{1+i\sqrt{3}}{2}$. Also notice that $(\omega\sqrt[6]{3})^3 = \omega^3\sqrt{3} = i\sqrt{3}$, and thus F contains ω^2 as desired. Thus, F is the splitting field of P.

(b) Since $[F : \mathbb{Q}] = 6$, the Galois group of P over $\mathbb{Q}$ is order 6 and thus is either $\mathbb{Z}/6\mathbb{Z}$ or S_3. Notice that $F \ni (\omega\sqrt[6]{3}) \cdot (\omega^{11}\sqrt[6]{3}) = \sqrt[3]{3}$. Therefore, $F \supset \mathbb{Q}(\sqrt[3]{3})$. Also notice that $\mathbb{Q}(\sqrt[3]{3})$ is not a normal extension of $\mathbb{Q}$ since the polynomial $x^3 - 3$ is irreducible over $\mathbb{Q}$ but does not split over $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$ since the other roots of $x^3 - 3$ are imaginary. Therefore, $\mathrm{Gal}(F/\mathbb{Q})$ is not Abelian, so $\mathrm{Gal}(F/\mathbb{Q}) \cong S_3$.

□

Exercise 3. Let G be a finite group, p a prime number and H a subgroup of G with $[G : H] = p$. Assume that no prime number smaller than p divides the order of G. Show that H is normal in G.

Proof. Let S be the set (of size p) of left cosets of H, and let G act on S by left translation. This induces a homomorphism $\psi : G \to S_p$ with $\ker\psi \subset H$. We have that $|G| = |\ker\psi||\operatorname{im}\psi|$, so $|G|\Big|\,|\ker\psi|p!$. Since $(p-1)!$ is relatively prime to G, $|G|\Big|\,|\ker\psi|p$. In particular, $|G| \leq |\ker\psi|p \leq |H| \cdot [G : H]$. But $|G| = |H| \cdot [G : H]$, so $|\ker\psi| = |H|$ and $\ker\psi = H$, so H is normal in G. □

Exercise 4. Let p be a prime number at least 3. Find a set of representatives up to conjugation for the group $\mathrm{GL}(2, \mathbb{Z}/p)$ of 2×2 invertible matrices.

Proof. By Jordan canonical form, every matrix $A \in \mathrm{GL}(2, \mathbb{Z}/p)$ with characteristic polynomial $(x - \lambda_1)(x - \lambda_2)$ for $\lambda_1, \lambda_2 \in \mathbb{Z}/p$ is conjugate to exactly one of the following:

$$\left\{ \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \middle| (\lambda_1, \lambda_2) \in (\mathbb{F}/p^\times)^2/((\lambda_1, \lambda_2) \sim (\lambda_2, \lambda_1)) \right\}$$

$$\left\{ \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \middle| \lambda \in \mathbb{F}/p^\times \right\}$$

Thus, the remaining matrices have irreducible characteristic polynomial, and are thus conjugate to exactly one of the following by Rational canonical form:

$$\left\{ \begin{bmatrix} 0 & -a \\ 1 & -b \end{bmatrix} \middle| x^2 + bx + a \text{ irreducible in } \mathbb{F}_p[x] \right\}$$

□

Exercise 5. Let G be the group presented by $G = \langle a, b \mid a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1} \rangle$. You may use that G has order 8. Compute the character table of G.

Proof. There is a surjective group homomorphism $G \to H$ for H the quaternions, and is an isomorphism since $|G| = |H| = 8$. Since H has 5 conjugacy classes, there are 5 irreducible representations of H (up to isomorphism), and the sum of the squares of their dimensions is 8. Thus, exactly 4 are one dimensional and one is two dimensional. The one dimensional representations are easy enough to find. Orthogonality gives the two dimensional representation.

{1}	{-1}	{i,-i}	{j, -j}	{k, -k}
1	1	1	1	1
1	1	-1	-1	1
1	1	-1	1	-1
1	1	1	-1	-1
2	-2	0	0	0

□

Exercise 6. Let G be a finite group, let V be a finite-dimensional complex vector space and let $\pi : G \to \mathrm{GL}(V)$ an irreducible representation. Let H be an abelian subgroup of G. Show that $\dim V \leq [G : H]$.

Proof. Let us show that if $\dim V > [G : H]$ is a representation of G it admits a proper subrepresentation. π restricts to H, so V is also an H representation. Since the only irreducible representations of an abelian group are one dimensional, $V \cong V_1 \oplus \cdots \oplus V_r$ as H-representations, with each V_i a one dimensional $\mathbb{C}$ vector space with an H action. Thus let $v \in V_1$ non-zero so $hv \in \langle v \rangle$ for all $h \in H$. Let $g_1H, g_2H, \ldots, g_kH$ be the left cosets of H in G, and define $v_1 = g_1 \cdot v, v_2 = g_2 \cdot v, \ldots, v_k = g_k \cdot v$. Let $W = \langle v_1, \ldots, v_k \rangle$ be the $\mathbb{C}$-span of $v_1, \ldots, v_k$. Notice that W is a proper subspace of V since it is dimension at most $[G : H] < \dim V$ and is non-zero since each v_i is non-zero. Thus let us show it is a subrepresentation of V. It suffices to show that for all $g \in G$ and $1 \leq i \leq k$ that $gv_i \in W$. We can write $g = g_jhg_i^{-1}$ for some $1 \leq j \leq k$ and $h \in H$ by considering the left H coset of gg_i. Then, we have:

$$gv_i = g_jhg_i^{-1}g_iv = g_jhv = \lambda g_jv$$

where $\lambda \in \mathbb{C}$ satisfies $hv = \lambda v$, which exists since H acts on v by scalars. Thus, W is a proper subrepresentation of V so V is not irreducible. □

Exercise 7. Let S be a multiplicatively closed subset of a commutative ring R. Show that for a prime ideal $\mathfrak{p}$ in R disjoint from S, the ideal $\mathfrak{p} \cdot R[S^{-1}]$ in the localization $R[S^{-1}]$ is prime. Show that this gives a one-to-one correspondence between prime ideals in R that are disjoint from S and prime ideals in $R[S^{-1}]$.

Proof. Without loss of generality assume S saturated (in particular, contains 1). Let us define a map $\psi : \operatorname{Spec} R \to \operatorname{Spec} R[S^{-1}]$ (where Spec is the prime ideals of the given ring). We will define

$$\psi(\mathfrak{p}) := \{p/s \mid p \in \mathfrak{p}, s \in S\} = \mathfrak{p} \cdot R[S^{-1}]$$

Notice the second equality holds since $\mathfrak{p}$ is an ideal. In particular, this implies that $\psi(\mathfrak{p})$ is an ideal in $R[S^{-1}]$. Now we show it is prime. Assume that $a/s_1 \cdot b/s_2 = p/s \in \mathfrak{p} \cdot R[S^{-1}]$. Then by definition there exists $t \in S$ such that $t(sab - ps_1s_2) =_R 0$, so $abst = ps_1s_2 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime and s, t are in S which is disjoint from $\mathfrak{p}$, either $a, b \in \mathfrak{p}$, so either a/s_2 or b/s_2 are in $\psi(\mathfrak{p})$. Thus, $\psi(\mathfrak{p})$ is prime.

This shows we have a well defined function ψ from primes in R disjoint from S and primes of $R[S^{-1}]$. Now we show it is injective. If $\mathfrak{p} \neq \mathfrak{q}$ so without loss of generality $\exists q \in \mathfrak{q} \setminus \mathfrak{p}$, let us show that $\frac{q}{1} \notin \mathfrak{p}R[S^{-1}]$. For if it were, we would have

$$\frac{q}{1} = \frac{p}{s} \qquad \Rightarrow \exists t \in S \mid t(qs - p) =_R 0$$

$$tqs \in \mathfrak{p}, \text{ a contradiction}$$

Therefore, ψ is injective. Also, ψ is surjective by pulling back any prime ideal $\mathfrak{p}'$ of $R[S^{-1}]$ by the localization map $\eta : R \to R[S^{-1}]$, which then clearly has image $\mathfrak{p}'$ back in $R[S^{-1}]$ by ψ. □

Exercise 8. Let A be a commutative ring. Show that the following two statements are equivalent:

(a) Every prime ideal of A is equal to an intersection of maximal ideals of A.

(b) Given any ideal I of A, the intersection of the prime ideals of A/I is equal to the intersection of the maximal ideals of A/I.

Proof. (a) ⇒ (b): Since every maximal ideal of A/I is prime, it suffices to show that every prime ideal $\mathfrak{p}$ of A/I is the intersection of maximal ideals in A/I. By the correspondence of prime ideals, there exists $\tilde{\mathfrak{p}} \in A$ a prime ideal in A containing I such that $\tilde{\mathfrak{p}}/I = \mathfrak{p}$. By assumption (a), $\tilde{\mathfrak{p}}/I$ is the intersection of maximal ideals $\{\tilde{\mathfrak{m}}_i\}_{i\in J}$ (for some indexing set J). Since their intersection is $\tilde{\mathfrak{p}}$ which contains I, each of the $\tilde{\mathfrak{m}}_i$ contain I and thus correspond to maximal ideals $\{\mathfrak{m}_i\}_{i\in J}$ of A/I. Furthermore by the correspondence theorem:

$$\mathfrak{p} = \tilde{\mathfrak{p}}/I = \Big(\bigcap_{i\in J} \tilde{\mathfrak{m}}_i\Big)/I = \bigcap_{i\in J} \mathfrak{m}_i$$

(b) ⇒ (a): Take any prime ideal $\mathfrak{p}$ of A, so $A/\mathfrak{p}$ is an integral domain and thus (0) is prime. By assumption, the intersection of the prime ideals of $A/\mathfrak{p}$ is equal to the intersection of the maximal ideals, so there is a set $\{\mathfrak{m}_i\}_{i\in J}$ of maximal ideals of $A/\mathfrak{p}$ such that $\bigcap_{i\in J} \mathfrak{m}_i = (0)$. By the correspondence of ideals, each $\mathfrak{m}_i$ corresponds to a maximal ideal $\tilde{\mathfrak{m}}_i$ containing $\mathfrak{p}$, and furthermore $(0) \supseteq \bigcap \tilde{\mathfrak{m}}_i$ implies $\mathfrak{p} \supseteq \bigcap \mathfrak{m}_i$. Since each $\mathfrak{m}_i$ contains $\mathfrak{p}$, we thus have $\mathfrak{p} = \bigcap_{i\in J} \mathfrak{m}_i$, so $\mathfrak{p}$ is the intersection of maximal ideals of A as desired.

□

Exercise 9. Let $\phi : \mathbf{Ab} \to \mathbf{Gp}$ be the functor that takes an abelian group A to A in the category of groups. Show that ϕ has a left adjoint α. Does ϕ has a right adjoint? Does α have a left adjoint? Justify your answers.

Proof. The left adjoint α is the abelianization functor. First isomorphism theorem gives a natural bijection α between their hom-sets, and there are many checks to show it is natural.

ϕ does not have a right adjoint because it does not preserve coproducts: $\phi(\mathbb{Z}/2) \sqcup_{\mathbf{Gp}} \phi(\mathbb{Z}/2) = \mathbb{Z}/2 * \mathbb{Z}/2$ is an infinite group, while $\phi(\mathbb{Z}/2 \times \mathbb{Z}/2)$ is finite.

α does not have a left adjoint because it does not preserve kernels. Consider $C_5 \hookrightarrow^{\psi} A_5$ by $1 \mapsto (12345)$. Then α applied to this diagram yields $C_5 \hookrightarrow 1$, which has kernel C_5. Thus $\ker \alpha(\psi) = 1$. But $\alpha(\ker \psi) = \alpha(C_5) = C_5$. □

Exercise 10. Compute the Jacobson radical $J(R)$ for the following rings R. Justify your answers.

(a) Let $R = \mathrm{End}_{\mathbb{R}}(V)$, for a real vector space V of countably infinite dimension. Compute $J(R)$.

(b) For any finite extension field F of $\mathbb{Q}$, let R be the integral closure of $\mathbb{Z}$ in F. Compute $J(R)$.

Proof. (a) For U a one dimensional subspace of R, the set $\mathfrak{m}_U$ of matrices $A \in R$ vanishing on U is a left ideal of R (easy exercise). Let us show $\mathfrak{m}_U$ is maximal. Let $U = \langle v \rangle$ and $Av \neq \mathbf{0}$. Let us show that the left ideal generated by $\mathfrak{m}_U + A$ is R. Let B be a linear transformation such that $B(Av) = v$. Then $\mathrm{id}_V - BA \in \mathfrak{m}_U$, so $\mathrm{id}_V \in \langle \mathfrak{m}_U + A \rangle$, so $\langle \mathfrak{m}_U = A \rangle = R$ as desired. We have that $J(R)$ is the intersection of all of the left maximal ideals. Thus any $A \in J(R)$ vanishes on every one dimensional subspace of V, and thus is zero, so $J(R) = \{0\}$.

(b) Since R is the ring of integers of a finite field extension of $\mathbb{Q}$, it is a Dedekind domain. Let us show that $J(R) = 0$. Let $a \in R \setminus \{0\}$ and let $I = \langle a \rangle$. I uniquely factorizes into a product of prime ideals, $I = \prod_{i=1}^{n} \mathfrak{p}_i^{m_i}$. By going up, R has infinitely many primes, so there is some $\mathfrak{q}$ prime in R not contained in the set $\{\mathfrak{p}_i\}$. Also, R is Krull dimension 1, so $\mathfrak{q}$ is maximal in I. We have $a \notin \mathfrak{q}$, since otherwise the prime ideal $\mathfrak{q}$ would contain I and thus be a part of its factorization into prime ideals. Therefore, $a \notin \mathfrak{q} \subset \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = J(R)$, so $J(R) = \{0\}$. □

Spring 2022

Exercise 1. Let F be a field of characteristic not 2 and let the symmetric group S_n act on the polynomial ring $F[X_1, \ldots, X_n]$ by permuting the variables, for $n \geq 2$. Let $A = (F[X_1, \ldots, X_n])^{A_n}$ and $B = (F[X_1, \ldots, X_n])^{S_n}$ be the fixed subrings, where $A_n \trianglelefteq S_n$ is the alternating group.

(a) Show that A is an integral extension of B.

(b) Show that $A = B[\delta]$ for some $\delta \in A$ such that $\Delta := \delta^2$ belongs to B.

(c) For $n = 2$, describe Δ as a polynomial in $e_1 = X_1 + X_2$ and $e_2 = X_1 X_2$.

Proof. Define $\delta = \prod_{i<j}(x_i - x_j) \in F[x_1, \ldots, x_n]$. Notice that $\delta \in A$, since any transposition (ab) results in an odd number of sign changes of δ, so $(ab)(\delta) = -\delta$. Thus for all $\sigma \in A_n$, $\sigma(\delta) = \delta$.
Lemma: For all $P \in A$, there exists $Q_1, Q_2 \in B$ such that

$$P = Q_1 + \delta Q_2$$

Proof. Define $Q_1 = \frac{P+(12)P}{2}, R = \frac{P-(12)P}{2}$ so $P = Q_1 + R$. Notice that $Q_1 \in B$ since for all $\sigma \in S_n$, either **1)** $\sigma \in A_n$ and $\tau = (12)\sigma(12)$ is in A_n:

$$\sigma Q_1 = \frac{\sigma P + (12)\tau(12)(12)P}{2} = \frac{P + (12)\tau P}{2} = \frac{P + (12)P}{2}$$

or **2)** $\sigma = \tau(12) = (12)\tau'$ for some $\tau, \tau' \in A_n$:

$$\sigma Q_1 = \frac{(12)\tau' P + \tau(12)(12)P}{2} = \frac{P + (12)P}{2}$$

Now let us show that for all transpositions (ab), $(ab)R = -R$. Since (ab) is a transposition, $(ab) = (12)\tau$ for $\tau \in A_n$ and $(ab) = \tau'(12)$ for $\tau' \in A_n$. Then we have:

$$(ab)R = \frac{(12)\tau P - \tau'(12)(12)P}{2} = \frac{(12)P - P}{2} = -R$$

Now let us show that for each $1 \leq i \neq j \leq n$, the polynomial $(x_i - x_j)$ divides R. It suffices to show that for the evaluation map $\pi : F[X_1, \ldots, X_n] \to F[X_1, \ldots, \hat{X_i}, \ldots, X_n] = R$ defined by $\pi(X_i) = X_j$ and $\pi(X_k) = X_k$ for $k \neq i$, we have $\pi(R) = 0$. Notice that π is unique and exists by the universal property of free commutative F-algebras. Let us show that $\pi = \pi \circ (ij) : F[X_1, \ldots, X_n] \to R$. By the universal property of free algebras, it suffices to show that the maps agree on each X_k. For $k \notin \{i, j\}$ this is obvious since $(ij)X_k = X_k$. We have $(ij)X_i = X_j$ and $(ij)X_j = X_i$, but since $\pi(X_i) = \pi(X_j) = X_j$, $\pi = \pi \circ (ij)$. Therefore,

$$\pi(R) = \pi((ij)R) = \pi(-R) = -\pi(R)$$

Therefore, $\pi(R) = 0$, so $(X_i - X_j)$ divides R. Therefore since each of the polynomials $X_i - X_j$ divide R and each are relatively prime in $F[X_1, \ldots, X_n]$, their product δ divides R. Therefore, $R = \delta Q_2$ for some $Q_2 \in F[X_1, \ldots, X_n]$. Furthermore, for all transpositions (ij), we have $(ij)R = -R$ and $(ij)\delta = -\delta$, so $(ij)Q_2 = Q_2$. Thus, $Q_2 \in B$ as desired. □

(a) and (b) $A = B[\delta]$ by the above lemma and δ is integral over B since $\Delta := \delta^2$ is in B. Therefore, A is integral over B.

(a) $\Delta^2 = (X_1 - X_2)^2 = X_1^2 + X_2^2 - 2X_1X_2 = e_2^2 - 4e_2$

□

Exercise 2. Let R be a ring, $S_1 = (0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0)$ a short exact sequence of right R-modules and $S_2 = (0 \to L \xrightarrow{h} M \xrightarrow{k} N \to 0)$ a short exact sequence of left R-modules in which M is free. Show that if $Z \otimes_R S_2 = (0 \to Z \otimes_R L \to Z \otimes_R M \to Z \otimes_R N \to 0)$ is exact then the sequence $S_1 \otimes_R N$ is exact as well.

Proof. By right exactness of the tensor product, the fact that M is free (and thus $\otimes M$ is exact), and the assumption that $Z \otimes S_2$ is exact, the following diagram is exact:

$$\begin{tikzcd}
 & 0 & 0 & 0 & \\
 & X \otimes N \arrow[u] \arrow[r, "f\otimes N"] & Y \otimes N \arrow[u] \arrow[r, "g\otimes N"] & Z \otimes N \arrow[u] \arrow[r] & 0 \\
0 \arrow[r] & X \otimes M \arrow[u, "X\otimes k"] \arrow[r, hook, "f\otimes M"] & Y \otimes M \arrow[u, "Y\otimes k"] \arrow[r, "g\otimes M"] & Z \otimes M \arrow[u, "Z\otimes k"] \arrow[r] & 0 \\
 & X \otimes L \arrow[u, "X\otimes h"] \arrow[r, "f\otimes L"] & Y \otimes L \arrow[u, "Y\otimes h"] \arrow[r, "g\otimes L"] & Z \otimes L \arrow[u, hook, "Z\otimes h"] \arrow[r] & 0 \\
 & & & 0 \arrow[u] &
\end{tikzcd}$$

Now we perform a diagram chase to show that the top row is exact. It suffices to show that $f \otimes N$ is injective. Let $\sigma \in X \otimes N$ such that $f \otimes N(\sigma) = 0$. The following picture is a better proof than whatever I could write:

$$\begin{tikzcd}
\sigma \arrow[r, "f\otimes N"] & 0 & \\
\exists x \arrow[u, dashed] \arrow[r, hook, "f\otimes M"'] & \bullet \arrow[u] & 0 \\
\exists \alpha \arrow[u] \arrow[r, dashed] & \exists y \arrow[u, dashed] \arrow[r, "g\otimes L"] & \bullet \arrow[u, hook]
\end{tikzcd}$$

□

Exercise 3. Let G be a finite p-group and let $H < G$ be a proper subgroup. We write as usual $H^g = gHg^{-1}$ for every $g \in G$.

(a) Show that the normalizer $N_G(H)$ of H in G is strictly larger than H.

(b) Show that if H is not normal in G then there exists another proper subgroup $H < K < G$ and $g \in G$ such that $K^g = K$ but $H^g \neq H$.

Proof. (a) Let us proceed by induction on $|G|$. The claim is trivial for $|G| = p$. Recall that the center $Z(G)$ of a p-group G is always non-trivial. Let $|G| = p^n$, and let $H < G$ be a proper subgroup. If H does not contain $Z(G)$, then $H \subsetneq Z(G) \cdot H$ normalizes H. Thus, assume $Z(G) \subseteq H < G$. By induction, the normalizer $\overline{N} = N_{G/Z(G)}(H/Z(G))$ strictly contains $H/Z(G)$. Let $N = Z(G)\overline{N}$ be the corresponding subgroup of G containing $\overline{N}$, i.e., $\pi^{-1}(\overline{N})$ for $\pi : G \to G/Z(G)$ the quotient map. Let us show that N normalizes G. Then N properly contains H since the correspondence between subgroups of G containing $Z(G)$ and subgroups of $G/Z(G)$ preserves inclusions and proper inclusions.

Let $n \in N$ and $h \in H$. Since $N/Z(G)$ normalizes $N/(Z(H)$, there exists $a, b, c \in Z(G)$ such that $(an)(bh)(an)^{-1} = ch$. Since $Z(G)$ is the center, we thus have

$$(an)(bh)(an)^{-1} = ch$$

$$nhn^{-1} = (b^{-1}c)h \in H$$

Thus, N normalizes H, as desired.

(b) Since H is not normal in G, then $K = N_G(H)$ is not all of G. Therefore, $K' = N_G(K) = N_G(N_G(H))$ properly contains K. Thus, there exists $g \in K' \setminus K$. We have that $K^g = K$ since $g \in N_G(K)$, but $H^g \neq H$ since $g \notin K$, and K is the normalizer of H.

□

Exercise 4. Let R be a commutative ring and M be an R-module.

(a) Show that $\mathrm{Hom}_R(-, M) : R\text{-}\mathbf{Mod}^{\mathrm{op}} \to R\text{-}\mathbf{Mod}$ admits a left adjoint.

(b) Show that for every R-module X, the module $\mathrm{Hom}_R(X, M)$ is a direct summand of $S := \mathrm{Hom}_R(\mathrm{Hom}_R(\mathrm{Hom}_R(X, M), M), M)$.

Proof. (a) By the tensor-hom adjunction, there exists a bijection γ_{MNL} natural in M, N, L:

$$\gamma_{MNL} : \mathrm{Hom}_R(N \otimes L, M) \cong \mathrm{Hom}_R(L, \mathrm{Hom}_R(N, M))$$

Since R is commutative, $N \otimes L \cong L \otimes N$, so there is also a bijection (natural in all three variables) γ':

$$\gamma'_{MNL} : \mathrm{Hom}_R(N \otimes L, M) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_R(L, M))$$

Composing γ'^{-1} and γ we have a natural (in all three variables!) bijection:

$$\mathrm{Hom}_{R\text{-}\mathbf{Mod}}(N, \mathrm{Hom}_R(L, M)) \cong \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(L, \mathrm{Hom}_R(N, M))$$

Identifying $\mathrm{Hom}_{R\text{-}\mathbf{Mod}}(N, \mathrm{Hom}_R(L, M))$ with $\mathrm{Hom}_{R\text{-}\mathbf{Mod}^{\mathrm{op}}}(\mathrm{Hom}_R(L, M), N)$, we have a natural bijection:

$$\mathrm{Hom}_{R\text{-}\mathbf{Mod}^{\mathrm{op}}}(\mathrm{Hom}_R(L, M), N) \cong \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(L, \mathrm{Hom}_R(N, M))$$

Thus, $\mathrm{Hom}_R(-, M) : R\text{-}\mathbf{Mod}^{\mathrm{op}} \to R\text{-}\mathbf{Mod}$ admits the left adjoint $\mathrm{Hom}_R(-, M) : R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}^{\mathrm{op}}$.

(b) Define $\iota : \mathrm{Hom}_R(X, M) \to S$ by $f \mapsto (\varphi \mapsto \varphi(f))$, so ι sends f to the evaluation map e_f at f. We have $\iota(f + ag) = \iota(f) + a\iota(g)$ for all $a \in R, f, g \in \mathrm{Hom}_R(X, M)$, so ι is an R-module homomorphism. Then define $r : S \to \mathrm{Hom}_R(X, M)$ by $\psi \mapsto (x \mapsto \psi(e_x))$, where $e_x \in \mathrm{Hom}_R(\mathrm{Hom}_R(X, M), M)$ is the evaluation map at x. We have $r(\psi + a\phi) = r(\psi) + ar(\phi)$, so r is also an R-module homomorphism. Let us show that $r \circ \iota = \mathrm{Id}_{\mathrm{Hom}_R(X,M)}$, which implies that ι is injective and r is a retraction of ι, so $\mathrm{Hom}_R(X, M)$ is a direct summand of S with respect to the inclusion ι. Thus, let $f \in \mathrm{Hom}_R(X, M)$ and let $x \in X$.

$$r \circ \iota(f)(x) = r\Big(\varphi \mapsto \varphi(f)\Big)(x)$$

Let $\psi \in S$ be $\iota(f)$ defined on elements by $\varphi \mapsto \varphi(f)$. Then,

$$= r(\psi)(x) = \psi(e_x) = e_x(f) = f(x)$$

as desired.

□

Exercise 5. Let k be a commutative ring and let G be a finite group. Prove that k with trivial G action is a projective kG-module if and only if the order of G is invertible in k.

Proof. If $|G|$ is invertible in k, then kG is a semisimple ring and thus every short exact sequence in kG splits. Thus, k is a projective kG-module. I'm not sure if the qual committee would've liked this short of a proof, so consider a short exact sequence

$$0 \to M \to N \to k \to 0$$

for M, N kG-modules and k with trivial G-action. There is a "forgetful" functor $U : kG\text{-}\mathbf{Mod} \to k\text{-}\mathbf{Mod}$ which is restriction of scalars by the ring homomorphism $k \to kG$ by $a \mapsto a1_G$. Since k is a field, M, N, k are all free as k-modules, so the sequence $M \to N \to k$ splits in k-**Mod**. Pick a section $\psi : k \to N$. Then define $\varphi : k \to N$ on the level of sets by

$$\varphi(r) = \frac{1}{|G|}\sum_{g\in G} g\psi(k)$$

Clearly φ is a k-vector space homomorphism as it is the sum of k-**Mod** homomorphisms. Furthermore for all $g \in G$ and $r \in k$,

$$\varphi(gr) = \varphi(r) = \frac{1}{|G|}\sum_{g'\in G} g'\psi(k) = \frac{g}{|G|}\sum_{g'\in G} g'\psi(k) = g\varphi(r)$$

Thus, φ is a kG-module homomorphism, and is a section of the map $N \to k$ since ψ is.

Now suppose $\mathrm{char}(k)\Big|\,|G|$ so $|G|$ is not invertible in k. Define $\psi : kG \to k$ by $\psi\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} a_g$. This is clearly a surjective kG homomorphism, so it suffices to show that ψ has no section. Since k has trivial action of G, for any $\varphi : k \to kG$ a kG-linear homomorphism, we must have $g\varphi(1) = \varphi(1)$ for all $g \in G$. In particular, $\varphi(1)$ must be stable under multiplication by all elements of G. Thus, $\varphi(1) = \sum_{g\in G} ag$ for some $a \in k$. But then we have that $\psi(\varphi(1)) = \psi\Big(\sum_{g\in G} ag\Big) = k \cdot a = 0$. Thus for all kG homomorphisms $\varphi : k \to kG$, the composition $\psi \circ \varphi$ is zero, and thus there are no sections $k \to kG$. Thus, k is not projective as a kG module. □

Exercise 6. Let G be a group of order 30.

(a) Prove that G contains an element of order 15.

(b) Prove that G is the semidirect product of cyclic subgroups of order 15 and 2.

Proof. Let n_2, n_3, n_5 be the number of $2, 3, 5$ Sylows in G. We have that $n_3 \in \{1, 10\}$ by the Sylow theorems since $n_3|G$ and $n_3 \equiv 1 \bmod 3$, and similarly $n_5 \in \{1, 6\}$. Notice that if $n_5 = 6$, then there are 24 elements of order 5 in G. If $n_3 = 10$, there are 20 elements of order 2 in G. These cannot simultaneously be true, so either $n_3 = 1$ or $n_5 = 1$. Let H_1, H_2 thus be a 3-Sylow and 5-Sylow of G respectively, so at least one of them is normal in G. Therefore, $N = H_1H_2$ is a subgroup of G since one of H_1, H_2 is normal in G and the other is a subgroup. Furthermore, 15 divides $|N|$ since $3, 5$ divide N, and $|N| \leq |H_1||H_2| = 15$ so $|N| = 15$. A group of order 15 must have both the number of 3 and 5 Sylows equal to 1 by the Sylow theorems, so $N \cong \mathbb{Z}/5 \times \mathbb{Z}/3$, and G thus contains an element of order 15. Furthermore, $[G : N] = 2$ so $N \trianglelefteq G$. Let H be any Sylow 2-subgroup of G, so $N \cap H = 1$, $N \cdot H = G$. Then $G \cong N \trianglelefteq_\psi H$ for some $\psi : H \to \mathrm{Aut}_{\mathbf{Grp}}(N)$ by the characterization of semidirect products in **Grp**. □

Exercise 7. Let K/F be a finite separable field extension, and let L/F be any field extension. Show that $K \otimes_F L$ is a product of fields.

Proof. Since K/F is a finite separable field extension, it is simple: i.e., generated by a single element α. Thus, the L-linear map $F[x] \to K$ defined by $x \mapsto \alpha$ is surjective, so $K \cong F[x]/p(x)$ for an irreducible polynomial $p(x) \in F[x]$. Thus, we have:

$$K \otimes_F L \cong \Big(F[x]/p(x)\Big) \otimes_F L \cong L[x]/p(x)$$

Let us explicitly show that the second congruence holds. First define $\tilde{\psi} : L[x] \to \Big(F[x]/p(x)\Big) \otimes_F L$ by the universal property by $x \mapsto (x \otimes_F 1)$ since $\Big(F[x]/p(x)\Big) \otimes_F L$ has a natural L-algebra structure. Notice that $\tilde{\psi}(p(x)) = p(x) \otimes 1 = 0$ by F-linearity of $\tilde{\psi}$. Thus, $\tilde{\psi}$ factors as an L-algebra homomorphism $\psi : L[x]/p(x) \to \Big(F[x]/p(x)\Big) \otimes_F L$ defined on monomials by $lx^n \mapsto (x^n \otimes l)$.

Now define a set function $\tilde{\varphi} : F[x]/p(x) \times L \to L[x]/p(x)$ by $\varphi([f], l) = [f \cdot l]$. This map is well defined (and is F-linear in the first coordinate) since if $g = f + rp$ for $f, r \in F[x]$, then $[g \cdot l] = [lf + rpl] = [lf] + [rpl] = [f \cdot l]$. CLearly φ is F-balanced and F-linear in the second coordinate, so $\tilde{\varphi}$ factors as an F-module homomorphism $\varphi : F[x]/p(x) \otimes_F L \to L[x]/p(x)$. On the level of elements, we clearly have that φ, ψ are two sided inverses to one another. Therefore, φ is actually a F-algebra homomorphism and is the inverse to ψ.

Let $p(x) = q_1(x) \cdot \dots \cdot q_n(x)$ be the prime factorization with $q_1, \dots, q_n \in L[x]$ irreducible. Since p is separable, each of the $q_1, \dots, q_n$ are distinct and thus relatively prime. By Chinese remainder theorem, we have:

$$L[x]/p(x) \cong L[x]/q_1(x) \times \dots \times L[x]/q_n(x)$$

and each $L[x]/q_i(x)$ is a field since the ideals $(q_i) \in L[x]$ are maximal. □

Exercise 8. A nonzero idempotent $e = e^2$ in a commutative ring R is called primitive if it cannot be written as the sum of two nonzero idempotents x and y such that $xy = 0$. Prove that every nonzero Noetherian commutative ring admits a primitive idempotent.

Proof. Let $\mathcal{F} = \Big\{(1-e) \mid e \in R\setminus\{0\}, e^2 = e\Big\}$ be a collection of ideals in R. Since R is Noetherian, $\mathcal{F}$ contains a maximal element $I = (1 - e)$ for some idempotent $e^2 = e$ in R. Let us show that e is primitive. Suppose ab absurdo that $e = x + y$ for non-zero idempotents x, y such that $xy = 0$. Let us show that $(1 - x) \supsetneq (1 - e)$, which contradicts the maximality of $(1 - e)$. Notice that $(1 - e) = (1 - x)(1 - y)$, so $(1 - x) \supseteq (1 - e)$. Since e is an idempotent and R is commutative, R is naturally isomorphic to the product of rings $eR \times (1 - e)R$ with eR having ring structure inherited from R with identity element e, and $(1 - e)R$ having identity element $(1 - e)$. In particular, this isomorphism is defined by $\psi : R \to eR \times (1-e)R$ by $\psi(a) = (ea, (1-e)a)$, with inverse $\varphi(a, b) = a+b$. Therefore, $(1 - e)x = (1 - y)(1 - x)x = (1 - y)(x - x^2) = 0$, and similarly $(1 - e)y = 0$. Therefore, $ex = x \in eR$ and $ey = y \in eR$. In particular, $y \notin (1 - e)R$ since $eR, (1 - e)R$ are disjoint ideals of R. However, $y \in (1 - x)R$ since $y = y(1 - x)$. Therefore, $(1 - x) \neq (1 - e)$, so $(1 - x) \supsetneq (1 - e)$ as desired. □

Exercise 9. Let A be a (unital) algebra of dimension n over a field F. Prove that there is a (unital) F-algebra homomorphism from $A \otimes_F A^{\text{op}}$ to the F-algebra of $n \times n$ matrices, where A^{op} is the opposite algebra.

Exercise 10. Let F be a field of characteristic not 2 and let $K = F(\sqrt{a}, \sqrt{b})$ be a biquadratic field extension of degree 4 of F, for $a, b \in F^\times$ not squares. Suppose that $b = x^2 - ay^2$ for some $x, y \in \mathbb{F}$ (i.e., b is a norm for the quadratic extension $F(\sqrt{a})/F$). Prove that there is a field extension L of K that is Galois over F with Galois group the dihedral group of order 8.

Proof. Motivation for the choice of P: suppose that L is a field extension of K with the desired properties. Then by the Galois correspondence, there exist field extensions $F \subsetneq F(\sqrt{a}) \subsetneq K_1 \subsetneq L$ and $F \subsetneq F(\sqrt{b}) \subsetneq K_2 \subsetneq L$ of degree 4 over F such that K_1, K_2 are not Galois over F. Since we are given information about the norm of $F(\sqrt{a})$, let us consider K_1. Since $[K_1 : F(\sqrt{a})] = 2$ (and F is not characteristic 2), $K_1 = \sqrt{\delta}$ for some $\alpha = m + n\sqrt{a} \in F(\sqrt{a})$. By an educated guess, we let $\alpha = x + y\sqrt{a}$ where $x, y \in F$ satisfy $b = x^2 - ay^2$. We claim that $L = F(\alpha, \beta)$ satisfies the desired conditions.

Define:

$$P(T) = (T^2 - x)^2 - y^2 a$$

Let us show that $P \in F[T]$ is irreducible. After choosing specific roots α of $(T^2 - x) - y\sqrt{a}$ and β of $(T^2 - x) + y\sqrt{a}$ in $F(\sqrt{a})$ in an algebraic closure of F, the roots of P are of the form $\alpha := \sqrt{x + y\sqrt{a}}, -\alpha, \beta := \sqrt{x - y\sqrt{a}}, -\beta$. Notice that $P(T)$ does not have any roots in K since if it did have such a root γ, then $(\gamma^2 - x)/y$ would be a root of a in K. Furthermore if P were to factor into quadratics, there are three possible such factorizations, noticing that $\alpha\beta = \sqrt{b}$:

$$(x - \alpha)(x + \alpha) = x^2 - (x + y\sqrt{a}) \qquad (x - \beta)(x + \beta) = x^2 - (x - y\sqrt{a}) \tag{1}$$

$$(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \sqrt{b} \qquad (x + \alpha)(x + \beta) = x^2 + (\alpha + \beta)x + \sqrt{b} \tag{2}$$

$$(x - \alpha)(x + \beta) = x^2 - (\alpha - \beta)x - \sqrt{b} \qquad (x + \alpha)(x - \beta) = x^2 + (\alpha - \beta)x - \sqrt{b} \tag{3}$$

Each of these possible factorizations contains a $\sqrt{a}$ or $\sqrt{b}$ term in one of the coefficients, and thus cannot have coefficients in K since a, b are not squares by assumption. Therefore, P is irreducible over F, so $K_1 = F(\alpha)$ is degree 4 over F. Furthermore, $F(\sqrt{a}) \subset F(\alpha)$ since $(\alpha^2 - x)/y$ is a square root of a. Now let us show that $K_1 \neq K$. If $K_1 = K$, then it would follow that $[K_1 : F(\sqrt{b})] = 2$. Thus, the polynomial $P(T)$ would factor in $F(\sqrt{b})$. By similar logic as before if there were a root $\gamma \in F(\sqrt{b})$ to P, then $(\gamma^2 + x)/y$ would be a root of a in $F(\sqrt{b})$, which is impossible since $[F(\sqrt{a}, \sqrt{b}) : F(\sqrt{b})] = 2$ by assumption. Thus, P would factor into quadratics in $F(\sqrt{b})$. Once again considering the factorizations above, it is clear that the first doesn't work so we must have $\alpha + \beta \in F(\sqrt{b})$ or $\alpha - \beta \in F(\sqrt{b})$. Notice that $\beta = \frac{\sqrt{b}}{\alpha}$, so this is equivalent to saying that $\alpha(1 \pm \frac{1}{\sqrt{b}}) \in F(\sqrt{b})$. But of course this implies that $\alpha \in F(\sqrt{b})$, which is a contradiction since $F(\sqrt{b})$ has no roots of P. Thus, $K_1 \neq K$.

The roots of P are exactly $\alpha, -\alpha, \frac{\sqrt{b}}{\alpha}, -\frac{\sqrt{b}}{\alpha}$. Since $K_1 \neq K$ by the above argument, $\sqrt{b} \notin K_1$. Therefore, $[K_1(\sqrt{b}) : K_1] = 2$, and thus the splitting field $L = F(\alpha, \sqrt{b})$ of P satisfies $[L : F] = 8$. Since L is a splitting field over F, L/F is Galois. Every F automorphism of L is determined by its action on $\alpha, \sqrt{b}$, of which there are 8 possibilities combined since any such automorphism must send α to another root of P and $\sqrt{b} \mapsto \pm\sqrt{b}$. Thus, every such permutation yields an F automorphism of L since $|\operatorname{Gal}(L/F)| = [L : F] = 8$. In particular, $\operatorname{Gal}(L/F)$ contains the following two elements:

$$r(\alpha) = \frac{\sqrt{b}}{\alpha} \qquad r(\sqrt{b}) = -\sqrt{b}$$

$$s(\alpha) = \alpha \qquad s(\sqrt{b}) = -\sqrt{b}$$

It is not hard to see that $s^2 = \text{Id}$ and $r^2(\alpha) = -\alpha$. Thus, r must be order 4 and $r^2 \neq s$. The group $\operatorname{Gal}(L/F)$ is non abelian (since the subfield K_1 is not Galois over F) and of order 8 and thus is isomorphic to the quaternions or D_4. The quaternions have a unique element of order 2, but since s, r^2 are distinct elements of order 2, $\operatorname{Gal}(L/F) \cong D_4$ as desired. □

Fall 2021

Exercise 1. Let $a \in \mathbb{Q}$ and $b, d \in \mathbb{Q}^\times$ and suppose that d is not a cube in $\mathbb{Q}^\times$. Find the minimal polynomial of $a + b\sqrt[3]{d}$ over $\mathbb{Q}$.

Proof. Since d is not a cube in $\mathbb{Q}$, $x^3 - d$ is irreducible in $\mathbb{Q}$ and thus $[\mathbb{Q}(\sqrt[3]{d}) : \mathbb{Q}] = [\mathbb{Q}(a + b\sqrt[3]{d}) : \mathbb{Q}] = 3$. Thus any monic degree 3 polynomial in $\mathbb{Q}[x]$ with $\alpha = a + b\sqrt[3]{d}$ as a root is the minimal polynomial of α. Thus the following is the minimal polynomial of α:

$$f(x) = \left(\frac{x-a}{b}\right)^3 - d$$

□

Exercise 2. Let K be a field, and consider the ring $R = K[x]/(x^2)$. Show that every free submodule N of an R-module M is a direct summand of M.

Proof. We aim to show that for all free modules N and injections $\iota : N \to M$ that the short exact sequence $0 \to N \hookrightarrow M \to M/N \to 0$ splits. This is equivalent to showing that N is injective, so it suffices to show that N satisfies the following lifting property:

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[d] & Y \arrow[dl, dashed, "\exists"] \\
N &
\end{tikzcd}$$

In fact, by an application of Zorn's lemma, it suffices to show that N satisfies the following lifting for any ideal I of R:

$$\begin{tikzcd}
I \arrow[r, hook] \arrow[d] & R \arrow[dl, dashed, "\exists"] \\
N &
\end{tikzcd}$$

Notice that the ideals of R are in correspondence with the ideals of $K[x]$ containing (x^2), which are only the three ideals $(x^2), (x), (1)$. If $I = (1) = R$ or $I = (0)$ a lift trivially exists, so it suffices to show that the following lifting is satisfied:

$$\begin{tikzcd}
(x) \arrow[r, hook, "\iota"] \arrow[d, "\psi"] & R \arrow[dl, dashed, "\exists"] \\
N &
\end{tikzcd}$$

Since N is free let $N = \coprod_{\alpha \in J} R_\alpha$ for some indexing set J. Recall that elements of a coproduct can be written as finite formal sums of the. Thus let $I \subset J$ be a finite subset such that $\psi(x) = \sum_{\alpha \in I} f_\alpha$ for $f_\alpha \in R_\alpha$. Notice that $\psi(0) = x\psi(x) = \sum_{\alpha \in I} x f_\alpha$ so $xf_\alpha = 0$ for each $\alpha \in I$. Since $R \cong K \oplus xK$ as a K-vector space, $xf_\alpha = 0$ implies that $f_\alpha = ax$ for some $a \in K$. Thus, let $g_\alpha \in R_\alpha$ for each $\alpha \in I$ satisfy $xg_\alpha = f_\alpha$. Then there exists a unique R-module homomorphism $\varphi : R \to N$ defined by $\varphi(1) = \sum_{\alpha \in I} g_\alpha$, and clearly $\varphi(x) = \psi(x)$ so φ extends ψ. Thus, N is injective as desired. □

Exercise 3. Show that there are no simple groups of order $24p$, where p is a prime number greater than 11.

Proof. Let G be a group of order $24p$ for p a prime greater than 11, and assume ab absurdo that G is simple. Let n_p be the number of p-Sylows in G. By the Sylow theorems, $n_p | G$ and $n_p \cong 1 \bmod p$. Since $n_p | G$, we have $n_p \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. Since p is a prime greater than 11, none of $\{2, 3, 4, 6, 8, 12\}$ are congruent to 1 mod p. Thus, $n_p = 1$ or $n_p = 24$. If $n_p = 1$, then the unique p-Sylow of G is a proper normal subgroup, a contradiction. Thus, $n_p = 24$. Thus $24 \cong 1 \bmod p$, so $p|23$ so $p = 23$. Since there are 24 p-Sylows, each congruent to $\mathbb{Z}/23\mathbb{Z}$ and with trivial intersection, there are $24 \cdot 22$ elements of order 23 in G. Thus, there are exactly 24 elements of order not equal to 23 in G.

Let n_3 be the number of 3-Sylows in G, which are each isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Since there are exactly 24 elements of order not equal to 23 in G, there are at most 24 elements of order 3 in G, and thus $n_3 \leq 12$. By the Sylow theorems, $n_3 | G$ and $n_3 \cong 1 \bmod 3$, so along with the fact that $n_3 \leq 12$, either $n_3 = 1$ or $n_3 = 4$. If $n_3 = 1$, then the unique 3-Sylow is a proper normal subgroup of G. Thus, $n_3 = 4$. Let S be the set of 3-Sylows in G. G acts transitively (and thus non-trivially) on S by conjugation, which induces a non-trivial group homomorphism $\psi : G \to S_4$. Since $|G| = 24 \cdot 23$ does not divide $|S_4| = 24$, ψ is not injective, and since ψ is non-trivial, $\ker \psi$ is a proper normal subgroup of G. Thus, G is not simple. □

Exercise 4. Let G be a cyclic group of order 12. For each of the fields $F = \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, write the regular representation $F[G]$ as a direct sum of simple (i.e., irreducible) modules.

Proof. Recall that F representations of G are equivalent (or defined to be) $R = FG$ modules. With this identification, the regular representation is FG as a module over itself. By the universal property of free F-algebras, there is an F-algebra homomorphism $\psi : F[x] \to FG$ defined by $x \mapsto g$ where g is a generator of G. Furthermore ψ is surjective since FG is generated as an F-algebra by g, and the kernel of ψ is generated by $x^{12} - 1$. Therefore, $R = FG \cong F[x]/(x^{12} - 1)$. Let $p_1, \ldots, p_r \in F[x]$ be irreducible so $x^{12} - 1 = \prod_{i=1}^{r} p_i(x)$ is the prime factorization of $x^{12} - 1$. Notice that $x^{12}-1$ is square free in $\mathbb{C}[x], \mathbb{R}[x]$, and $\mathbb{Q}[x]$, so each of the p_i are distinct. Then by the Chinese remainder theorem (and since $F[x]$ is a PID),

$$R \cong F[x]/(p_1) \times F[x]/(p_2) \times \cdots \times F[x]/(p_r)$$

Since $F[x]$ is a PID and thus has Krull dimension 1, each of $F[x]/(p_i)$ are simple modules over themselves. In particular as a module over itself,

$$R \cong F[x]/(p_1) \oplus \cdots \oplus F[x]/(p_r)$$

and each of $F[x]/(p_i)$ are simple R-modules. Thus, to describe $F[G]$ as a direct sum of simple modules, it suffices to factor $x^{12}-1$ in $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. Let $\zeta = e^{2\pi i/12} \in \mathbb{C}$. Then as $\mathbb{C}G$ modules,there is an isomorphism

$$\mathbb{C}G \cong \mathbb{C}[x]/(x-1) \oplus \mathbb{C}[x]/(x-\zeta) \oplus \cdots \oplus \mathbb{C}[x]/(x-\zeta^{11})$$

In $\mathbb{R}[x]$, $x^{12}-1$ factors completely as $x^{12}-1 = (x-1)(x+1)(x^2-(\zeta+\overline{\zeta})x-1)\dots(x^2-(\zeta^5+\overline{\zeta^5})x-1)$. Thus,

$$\mathbb{R}G \cong \mathbb{R}[x]/(x-1) \oplus \mathbb{R}[x]/(x+1) \oplus \mathbb{R}[x]/(x^2-(\zeta+\overline{\zeta})x+1) \oplus \cdots \oplus \mathbb{R}[x]/(x^2-(\zeta^5+\overline{\zeta^5})x-1)$$

Finally in $\mathbb{Q}[x]$, the cyclotomic polynomials are irreducible, so we have as $\mathbb{Q}G$ modules:

$$\mathbb{Q}G \cong \bigoplus_{d|n} \mathbb{Q}[x]/(\phi_d(x))$$

$$= \frac{\mathbb{Q}[x]}{(x-1)} \oplus \frac{\mathbb{Q}[x]}{(x+1)} \oplus \frac{\mathbb{Q}[x]}{(x^2+x+1)} \oplus \frac{\mathbb{Q}[x]}{(x^2+1)} \oplus \frac{\mathbb{Q}[x]}{(x^2-x+1)} \oplus \frac{\mathbb{Q}[x]}{(x^4+x^2+1)}$$

□

Exercise 5. Consider a sequence of sets S_1 for $i \geq 0$ and maps $\psi_i : S_i \to S_{i-1}$ for $i \geq 1$. Suppose that there exists a positive integer N such that the orders of the images of the maps ψ_i are bounded above by N. Show that $\varprojlim S_i$ is finite.

Proof. Recall that $\varprojlim S_i$ can be explicitly represented (as a set) as sequences

$$S := \varprojlim S_i = \Big\{(s_1, s_2, \dots) \mid s_i = \psi_{i+1}(s_{i+1}) \ \forall i \in \mathbb{Z}^+\Big\} \subset \prod_i S_i$$

Let us show that $|S| \leq N$. It suffices to show that if $T = \{(s_1^j, s_2^j, \dots)\}_{j=1}^{N+1}\}$ is a collection of $N+1$ elements of S that some pair of them must be equal. Notice that for each index $i \in \mathbb{Z}^+$ and each $j \in [1, N+1]$ we have $s_i^j = \psi_{i+1}(s_{i+1}^j)$, so $s_i^j \in \text{Im}\psi_i$. Since $|\text{Im}\psi_i| \leq N$, for each i there is some pair $(a_i, b_i) \in [1, N+1]^2$ such that $s_j^{a_i} = s_j^{b_i}$. By pigeonhole principle, there is thus some $j, k \in [1, N+1]$ such that $(s_1^j, s_2^j, \dots)$ and $(s_1^k, s_2^k, \dots)$ agree at infinitely many indices. In particular for all $i \in \mathbb{Z}^+$, there is some $M > i$ such that $s_M^j = s_M^k$. But then we have

$$s_i^j = \psi_{i+1} \circ \cdots \circ \psi_M(s_M^j) = \psi_{i+1} \circ \cdots \circ \psi_M(s_M^k) = s_i^k$$

Thus, $(s_1^j, s_2^j, \dots)$ and $(s_1^k, s_2^k, \dots)$ agree at *every* index and are thus equal. Thus, $|S| \leq N$. □

Exercise 6. Consider the elements $g = (12)$ and $h = (23)$ in the symmetric group S_3. Consider the action of S_3 on the polynomial ring $\mathbb{C}[x, y]$ determined by $g(x) = y$, $g(y) = x$, $h(x) = x - y$, and $h(y) = -y$. (Here S_3 is acting on $\mathbb{C}[x, y]$ as a $\mathbb{C}$-algebra. You need not check that this action is well-defined). Let V be the complex vector space of homogeneous polynomials of degree 3 in x and y; this is mapped into itself by S_3. Compute the character of V. When V is written as a direct sum of irreducible representations of S_3, find the number of times each irreducible representation of S_3 occurs.

Proof. V has a basis of x^3, x^2y, xy^2, y^3 as a $\mathbb{C}$-vector space. Let $\rho : S_3 \to \mathrm{GL}(V)$ be the representation of V induced from the described action of S_3 on $\mathbb{C}[x, y]$. Let us write the matrices for $\rho(g)$ and $\rho(gh) = \rho((123))$ in terms of the basis x^3, x^2y, xy^2, y^3. We have:

$$\rho(g)(x^3) = y^3 \qquad \rho(g)(x^2y) = xy^2 \qquad \rho(g)(xy^2) = x^2y \qquad \rho(g)(y^3) = x^3$$

Thus with respect to the ordered basis x^3, x^2y, xy^2, y^3, we have

$$\rho(g) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \in \mathrm{GL}(V)$$

Similarly,

$$\rho(gh)(x^3) = (y - x)^3 = y^3 - 3x^2y + 3xy^2 - x^3 \qquad \rho(g)(x^2y) = -x(y - x)^2 = -x^3 + 2x^2y - xy^2$$

$$\rho(g)(xy^2) = x^2(y - x) = -x^3 + x^2y \qquad \rho(g)(y^3) = -x^3$$

Thus,

$$\rho(gh) = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 3 & 2 & 1 & 0 \\ -3 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Therefore with $\chi = \mathrm{Tr} \circ \rho$ the character of V, $\chi(\mathrm{id}) = \dim V = 4$, $\chi(g) = 0$ and $\chi(gh) = -1 + 2 = 1$. Recall that the character table of S_3 is given by the following:

	$\{\mathrm{id}\}$	$\{(12), (13), (23)\}$	$\{(123), (132)\}$
Triv	1	1	1
sgn	1	-1	1
W	2	0	-1

Thus, $\chi = a\mathrm{Triv} + b\,\mathrm{sgn} + cW$ for some $a, b, c \in \mathbb{N}$. Since $\chi(g) = 0$, $a = -b$, and since $\chi(\mathrm{id}) = 4$, $a + b + 2c = 4$. This is a (very small) finite arithmetic problem and we find that the only possibility is $\chi = \mathrm{Triv} + \mathrm{sgn} + W$. □

Exercise 7. Define commutative $\mathbb{Q}$-algebras $A = \mathbb{Q}, B = \mathbb{Q}[x]$, and $C = \mathbb{Q}[x]/(x(x - 1))$. Let $A \to C$ and $B \to C$ be the unique $\mathbb{Q}$-algebra homomorphisms such that x in B maps to x in C.

Describe the pullback (also called "fiber product") $R = A \times_C B$ in the category of commutative $\mathbb{Q}$-algebras as the quotient by an explicit ideal of the polynomial ring over $\mathbb{Q}$ on some set of generators. Is R noetherian?

Proof. **Solution by Rhea Kommerell.**

Let $\pi \colon B \to C$ be the map described. As a set, $R = \{(c, p(x)) \in A \times B : \pi(p) = c\}$. Since the map $A \to C$ is injective, R is isomorphic to the set of polynomials $p(x)$ which equal a constant after modding out by $x^2 - x$. Then p must have the form $q(x)(x^2 - x) + c$ for $q(x) \in \mathbb{Q}[x]$ and $c \in \mathbb{Q}$.

As a $\mathbb{Q}$-algebra, R is generated by the set $\{x^i(x^2 - x) : i \geq 0\}$. In other words, there is a surjection $f \colon \mathbb{Q}[x_0, x_1, \ldots] \to R$ given by $x_i \mapsto x^i(x^2 - x)$. It remains to describe the relations on these generators. Certainly there are relations $f(x_i x_j) = f(x_{i+j+2}) - f(x_{i+j+1})$ for every i, j because $x^i x^j (x^2 - x)^2 = (x^{i+j+2} - x^{i+j+1})(x^2 - x)$.
We claim that these are the only relations. Consider the algebra $R' = \mathbb{Q}[x_0, x_1, \ldots]/(x_i x_j - x_{i+j+2} - x_{i+j+1})$. The relations makes it possible to write any element of R' uniquely as a linear polynomial in the x_is. (Uniquely because the relation is associative, that is, $x_i x_j x_k = x_{i+j+k+4} + 2x_{i+j+k+3} + x_{i+j+k+2}$ no matter whether we expand $x_i x_j$ or $x_j x_k$ first.) Similarly, in R, we can write any element uniquely in the form $q(x)(x^2 - x) + c$. Since a linear term in R' corresponds to a term $c_i x^i(x^2 - x)$ in R, this gives a bijection between R' and R. So we have written R as a quotient of a polynomial ring over $\mathbb{Q}$.

The following argument was inspired by Stacks 15.5.1.

We argue that R is actually finite type over $\mathbb{Q}$, hence Noetherian. We will apply the Artin-Tate Lemma to $R \subset A \times B$, which will immediately say that R is finite type as long as we can check the conditions of the lemma - 1. that $A \times B$ is finite over R, and 2. that $A \times B$ is finite type over $\mathbb{Q}$.

1. $A \times B$ is finitely generated as an R-module by the generators $\{(1, 0), (0, 1), (0, x)\}$. For example, we can write $(0, x^k) = (0, x) + \sum_{i=2}^{k}(x^i - x^{i-1})(0, 1) = (0, x^k - x^{k-1} + x^{k-1} - \cdots + x^2 - x + x)$.
2. $A \times B$ is finite type over $\mathbb{Q}$ because it is generated by $\{(1, 0), (0, 1), (0, x)\}$. In particular, both A, B are finite type over $\mathbb{Q}$.

□

Exercise 8. Let A be a commutative ring and T an A-module. Define a functor from A-modules to A-modules by $F(M) = M \otimes_A T$. What is the right adjoint functor of F? Show that if F has a left adjoint, then T must be a flat A-module, and also a finitely generated A-module.

Proof. By the tensor-hom adjunction, the right adjoint functor of F is $\operatorname{Hom}_A(T, -)$. If F has a left adjoint, then F is left exact, so T is flat by definition. Thus let us show that if F has a left adjoint then T is finitely generated. A much more general statement holds: F has a left adjoint if and only if T is finitely presented and projective. We are interested in the *only if* part of the statement, which we will prove here as a slight extension of the problem.

Lemma: Let M be an A-module. If $M \otimes_A \prod A \cong \prod (M \otimes_A A)$ (with respect to the natural map $M \otimes_A \prod A \to \prod M \otimes_A A)$ for all products of A, then M is finitely generated as an A-module.

Consider $\varphi : M \otimes A^M \to M^M$ the natural map defined by $(m \otimes (a_s)_{s\in M}) \mapsto (a_s m)_{s\in M}$ which is an isomorphism by assumption. In particular, the element $\iota = (s)_{s\in M}$ (which represents the identity function $M \to M$ in the product) is in the image of φ, so there exists $m_1, \dots, m_n \in M$ and $\overline{a}^1, \dots, \overline{a}^n \in A^M$ such that

$$\varphi(\sum_{i=1}^n m_i \otimes \overline{a}^i) = \Big(\sum_{i=1}^n m_i a_s^i\Big)_{s\in M} = \iota$$

In particular, this states that for all $s \in S$, there exists $a_s^1, \dots, a_s^n \in A$ such that $\sum_{i=1}^n m_i a_s^i = s$. Therefore, $m_1, \dots, m_n$ generate M as an A-module so M is finitely generated.

Since T has a left adjoint T preserves limits and thus by the **Lemma** is finitely generated. Thus, we have a short exact sequence

$$0 \to N \to F \to T \to 0$$

with F a finitely generated free module. Thus, let us show that N is a finitely generated module so T is finitely presented. By the **Lemma**, it suffices to show that $\otimes_A N$ preserves products of A. Consider the following commutative diagram from applying the functor $\otimes_A \prod A$ and the naturality of the map $L \otimes_A \prod A \to \prod L \otimes_A A$ for all A-modules L:

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & N \otimes_A \prod A \arrow[r] \arrow[d] & F \otimes_A \prod A \arrow[r] \arrow[d] & T \otimes_A \prod A \arrow[d] \\
0 \arrow[r] & \prod N \otimes_A A \arrow[r] & \prod F \otimes_A A \arrow[r] & \prod T \otimes_A A
\end{tikzcd}$$

Since F is finite free, every vertical map except possibly $N \otimes_A \prod A \to \prod N \otimes_A A$ is an isomorphism. Thus by the 5-lemma (after extending the diagram with zeroes to the left), $N \otimes_A \prod A \to \prod N \otimes_A A$ is an isomorphism as desired. Thus, N is finitely generated so T is finitely presented.

Courtesy of this stack exchange post for a much needed hint. □

Exercise 9. The outer automorphism group of a group H is the quotient of the group of automorphisms of H by the subgroup of inner automorphisms. It is known that the outer automorphism group of every finite simple group is solvable. Using that, show that if G is a finite group with a normal subgroup N such that both N and G/N are nonabelian simple groups, then G is isomorphic to the product group $N \times (G/N)$.

Proof. Note that $N, G/N$ are non-trivial. Let $\psi : G \to \operatorname{Aut}(N)$ be the action of G on N by conjugation. Composing with the quotient map, we have $\tilde{\psi} : G \to \operatorname{Aut}(N)/\operatorname{Inn}(N)$. By definition, $\operatorname{Inn}(N) = \psi(N)$. Therefore, $\tilde{\psi}$ factors through the quotient G/N as $\varphi : G/N \to \operatorname{Aut}(N)/\operatorname{Inn}(N)$. It is known (as stated in the problem) that since N is simple, $\operatorname{Aut}(N)/\operatorname{Inn}(N)$ is solvable. Since G/N is simple, either φ is the trivial map or it is injective. But since G/N is nonabelian and simple, G/N is not solvable, and thus cannot be embedded as a subgroup of a solvable group. Therefore, φ is the trivial map.

Therefore $\ker \varphi \cong G/N$ is non-trivial.
Let us show that $\ker \psi \hookrightarrow G \twoheadrightarrow G/N$ yields an isomorphism $\ker \varphi \cong G/N$.

$$\begin{tikzcd}
\ker \psi \arrow[r] \arrow[d, hook] & 0 \arrow[d] \\
G \arrow[r, "\psi"] \arrow[d] & \operatorname{Aut}(N) \arrow[d] \\
G/N \arrow[r, "0"] & \frac{\operatorname{Aut}(N)}{\operatorname{Inn}(N)}
\end{tikzcd}$$

First take any $[g] \in G/N$. Since $\varphi([g]) = 1$, we have $\psi(g) \in \operatorname{Inn}(N)$, so $g = nh$ for $n \in N$ and $h \in \ker \psi$. In particular, $[g] = [h]$, so $\ker \psi \to G/N$ is surjective. Now take any $h \in \ker \psi$ which is mapped to $[1]$, so $h \in N$. Since N is non-abelian and simple, N has trivial center so $\ker \psi \cap N = Z(N) = 1$. Thus, $h = 1$, so $\ker \psi \to G/N$ is injective. Thus, $\ker \psi \to G/N$ is an isomorphism.

Therefore we have nonabelian simple normal subgroups $N \trianglelefteq G$ and $H \trianglelefteq G$, and since $H = \ker \psi$, H commutes with N. Let us show $NH = G$. Take any $g \in G$. Notice that by the commutivity of the above diagram, $\operatorname{Im}\psi = \operatorname{Inn}(N)$. Therefore, $\psi(g) = \psi(n)$ for some $n \in N$, so $g = nh$ for $h \in \ker \psi$. Thus, $NH = G$, so $G \cong N \times H \cong N \times G/N$.

□

Exercise 10. Let R_1 and R_2 be rings (not necessarily commutative), and let M be an (R_1, R_2)-bimodule. Then the matrices

$$\begin{bmatrix} R_1 & M \\ 0 & R_2 \end{bmatrix}$$

form a ring R, by the usual formulas for matrix addition and multiplication. Compute the Jacobson radical of R in terms of M and the Jacobson radicals of R_1 and R_2.

Proof. The Jacobson radical $J(R)$ of R is the intersection of all maximal left ideals of R. For any left ideal I of R_1, the following set is a left ideal of R:

$$S_I := \begin{bmatrix} I & M \\ 0 & R_2 \end{bmatrix}$$

Furthermore, S_I is maximal if and only if I is maximal, since there is a ring homomorphism $R \to R_1$ by taking the upper left coordinate which gives an order preserving bijection between left ideals of R_1 and left ideals of R of the form S_I. Similarly, for any left ideal J of R_2, the following is a left ideal of R, and similarly is maximal if and only if J is maximal:

$$T_J := \begin{bmatrix} R_1 & M \\ 0 & J \end{bmatrix}$$

Therefore,

$$J(R) = \bigcap_{I \subset R \text{ maximal}} I \supset \bigcap_{I \subset R_1 \text{ maximal}} S_I \cap \bigcap_{J \subset R_2 \text{ maximal}} T_J = \begin{bmatrix} J(R_1) & M \\ 0 & J(R_2) \end{bmatrix} =: K$$

Now let us show that for any maximal left ideal I of R that $I \subset K$. This will imply that $J(R) \subset K$, so $J(R) = K$. If I is of the form S_J or T_J as above, clearly $I \subset K$. Otherwise by maximality, I is not contained in any of the S_J or T_J. Let $I_1 \subset R_1$ be the left ideal of elements in the upper left entry of elements in I and $I_2 \subset R_2$ the left ideal of elements in the lower right entry of elements in I. If I_1 or I_2 are proper than they are contained in some maximal ideal and thus I would be contained in some S_J or T_J. Thus,

$$I \supset \begin{bmatrix} R_1 & 0 \\ 0 & R_2 \end{bmatrix}$$

But this means that I contains

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and thus is the unital ideal R. Therefore, $K \subset I$ for all maximal ideals I so $K \subset J(R)$. Therefore,

$$J(R) = \begin{bmatrix} J(R_1) & M \\ 0 & J(R_2) \end{bmatrix}$$

□

Spring 2021

Exercise 1. Prove that the direct sum $\bigsqcup \mathbb{Z}/p\mathbb{Z}$ over all prime integers p is not a direct summand of the product $\prod \mathbb{Z}/p\mathbb{Z}$.

Proof. Let us first characterize all injective homomorphisms $\iota : \bigsqcup \mathbb{Z}/p\mathbb{Z} \to \prod \mathbb{Z}/p\mathbb{Z}$. First notice that the elements of $\bigsqcup \mathbb{Z}/p, \prod \mathbb{Z}/p$ may be written as sequences of elements $a \in \mathbb{Z}/p$:

$$\bigsqcup \mathbb{Z}/p\mathbb{Z} = \left\{(a_2, a_3, \dots) \mid a_p \in \mathbb{Z}/p, a_i = 0 \text{ for all but finitely many } i\right\}$$

$$\prod \mathbb{Z}/p\mathbb{Z} = \left\{(a_2, a_3, \dots) \mid a_p \in \mathbb{Z}/p\right\}$$

Let $\iota : \bigsqcup \mathbb{Z}/p\mathbb{Z} \to \prod \mathbb{Z}/p\mathbb{Z}$ be injective, and let $e_2 = (1, 0, \dots), e_3 = (0, 1, 0, \dots), \dots$ be a natural $\mathbb{Z}$ generating set of $\bigsqcup \mathbb{Z}/p$. For ι to be injective, it must send e_p to an element of order p for each prime p. But the only elements of order p in $\prod \mathbb{Z}/p\mathbb{Z}$ are those of the form $(0, \dots, 0, a, 0, \dots)$ for $a \neq 0 \in \mathbb{Z}/p$. Furthermore, ι is determined by its action on $e_2, e_3, \dots$ since they generate $\bigsqcup \mathbb{Z}/p$. Thus after composing with an isomorphism of $\prod \mathbb{Z}/p$, the only inclusion ι is the obvious inclusion $\iota : \bigsqcup \mathbb{Z}/p \to \prod \mathbb{Z}/p$ sending e_p to e_p.

Since the only inclusions up to isomorphism are the obvious one by the above work, our notation will assume $\bigsqcup \mathbb{Z}/p \subset \prod \mathbb{Z}/p$ in the obvious way. Suppose ab absurdo that $\bigsqcup \mathbb{Z}/p$ were a direct summand of $\prod \mathbb{Z}/p$, so $\prod \mathbb{Z}/p \cong \bigsqcup \mathbb{Z}/p \oplus Q$ for an abelian group Q. This would imply that $\prod \mathbb{Z}/p / \bigsqcup \mathbb{Z}/p \cong Q \subset \prod \mathbb{Z}/p$. Let us show that Q is divisible, but no nontrivial submodule of $\prod \mathbb{Z}/p$ is divisible, a contradiction. Take an equivalence class $[(a_2, a_3, \dots)] \in Q$ and take $n \in \mathbb{N}$. Without loss of generality, assume that $a_p = 0$ for all $p|n$, since two elements of $\prod \mathbb{Z}/p$ are equivalent in Q if they agree in all but finitely many indices. Then, let $b = [(a_2/n), (a_3/n), \dots]$ which is well defined since $n \in \mathbb{Z}/p^\times$ for all $p \nmid n$. Then clearly $nb = a$, so Q is divisible. To show that no nontrivial submodule of $\prod \mathbb{Z}/p$ is divisible, it suffices to show that for all $0 \neq a = (a_2, a_3, \dots) \in \prod \mathbb{Z}/p$, there exists $n \in \mathbb{N}$ such $a \notin n \prod \mathbb{Z}/p$. For any such non-zero a, there is an index $a_q \neq 0$. Then, notice that $a \notin q \prod \mathbb{Z}/p$, as desired.

□

Exercise 2. Let $P \subset \mathbb{Z}[x]$ be a prime ideal such that $\mathbb{Z} \cap P = 0$. Prove that P is a principal ideal.

Proof. Suppose $P \neq 0$ without loss of generality. Let $g \in P$ be a non-zero element of minimal degree in P, and let $c \neq 0$ be the GCD of its coefficients, so $g/c = f \in \mathbb{Z}[x]$. Then $f \cdot c \in P$, and since P is prime but $c \notin P$ since $\mathbb{Z} \cap P = 0$, we must have $f \in P$. Let us show $P = \langle f \rangle$. Let $h \in P$ a non-zero element. In $\mathbb{Q}[x]$, by polynomial division, there exist elements $p \in \mathbb{Q}[x], q \in \mathbb{Q}[x]$ with $\deg q < f$ such that $h = pf + q$. Multiplying both sides of the equation by D, where $D \in \mathbb{Z}$ is the GCD of the coefficients of p and q,

$$Dh = (Dp)f + Dq \in \mathbb{Z}[x]$$

Therefore, $Dq = Dh - (Dp)f \in P$, but q is of degree less than f, and thus $q = 0$ since $\mathbb{Z} \cap P = 0$. Thus, $h = pf$. By Gauss' Lemma, since f divides h in $\mathbb{Q}[x]$, f divides h in $\mathbb{Z}[x]$ (since the GCD of the coefficients of f is 1), so $P = \langle f \rangle$ as desired.

□

Exercise 3. Prove that every group generated by two involutions (elements of order 2) is solvable.

Proof. Let H be a group generated by two involutions h_1, h_2. Then there is a surjective group homomorphism (by universal property of free group and first isomorphism theorem) $G \xrightarrow{\psi} H$ by $a \mapsto h_1, b \mapsto h_2$ where $G = \langle a, b \mid a^2 = b^2 = 1 \rangle$, and so $H \cong G/\ker\psi$ by first isomorphism theorem. Therefore, since the quotient of a solvable group is solvable, it suffices to show that G is solvable.

Consider the subgroup $N = \langle ab \rangle \leq G$. Notice that

$$b(ab)b^{-1} = ba = (ab)^{-1} = a(ab)a^{-1}$$

Therefore, N is a normal subgroup of G since a, b generate G, ab generates N, and $aNa^{-1} = N, bNb^{-1} = N$. Notice that

$$G/N = \langle a, b \mid a^2 = b^2 = ab = 1 \rangle \cong \mathbb{Z}/2$$

Furthermore, N is cyclic since it is generated by a single element and thus Abelian. Therefore, $1 \trianglelefteq N \trianglelefteq G$ is a subnormal tower of G such that $G/N, N/1$ are abelian, so G is solvable. □

Exercise 4. Prove that the field extension $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2})$ over $\mathbb{Q}$ is Galois and determine its Galois group.

Proof. Let $L = \mathbb{Q}(\sqrt{-3}, \sqrt[6]{2})$. First notice that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ since $x^6 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein. Also, the remaining roots of $x^6 - 2$ are $\omega^j \sqrt[6]{2}$ for $0 < j < 6$ and $\omega = e^{\pi i/3} = \frac{1+\sqrt{-3}}{2}$. Therefore, $x^6 - 2$ splits in L. Also, $x^6 - 2$ does not split in $\mathbb{Q}(\sqrt[6]{2})$ since $\mathbb{Q}(\sqrt[6]{2}) \subset \mathbb{R}$ and $x^6 - 2$ does not split in $\mathbb{R}$. Therefore, the splitting field of $x^6 - 2$ is at least degree 12 over $\mathbb{Q}$ and is contained in L, and thus is equal to L. Furthermore, $\mathrm{Gal}(L/\mathbb{Q}) = G$ is of order 12, and each $g : \mathrm{Gal}(L/\mathbb{Q})$ is determined by its action on $\sqrt[6]{2}, \sqrt{-3}$. Furthermore, $g(\sqrt[6]{2})$ must be a root of $x^6 - 2$ and similarly for $g(\sqrt{-3})$ and $x^2 + 3$. Thus, there are only 12 possibilities for elements of $\mathrm{Gal}(L/\mathbb{Q})$, and since $|G| = 12$, all such possibilities yield a $\mathbb{Q}$ automorphism of L. In particular, we have $\mathbb{Q}$ automorphisms of L σ and τ which are of order 6 and 2 respectively:

$$\sigma(\sqrt[6]{2}) = \omega\sqrt[6]{2} \qquad \sigma(\sqrt{-3}) = \sqrt{-3}$$

$$\tau(\sqrt[6]{2}) = \sqrt[6]{2} \qquad \tau(\sqrt{-3}) = -\sqrt{-3}$$

Furthermore, we check that $\sigma\tau\sigma\tau = \mathrm{id}_L$:

$$\sigma\tau\sigma\tau(\sqrt[6]{2}) = \sigma\tau\sigma(\sqrt[6]{2}) = \sigma\tau(\omega\sqrt[6]{2}) = \sigma(-\omega\sqrt[6]{2}) = \sqrt[6]{2}$$

$$\sigma\tau\sigma\tau(\sqrt{-3}) = \sigma\tau(-\sqrt{-3}) = \sqrt{-3}$$

Therefore, G has relations $\sigma^6 = \tau^2 = \sigma\tau\sigma\tau = 1$, so $D_6 \twoheadrightarrow G$. By order considerations, $D_6 \cong G$. Now let us show that $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2}) = L$. It is clear that $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2}) \subset L$, so by the Galois correspondence there is a subgroup $H \subset G$ such that $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2}) = L^H$. Thus it suffices to show that $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2})$ is not fixed by any non identity element of G so $H = 1$. For $0 < j < 6$, we have $\sigma^j(\sqrt{-3} + \sqrt[6]{2}) = \sqrt{-3} + \omega^j\sqrt[6]{2}$. And for $0 \le j < 6$, we have $\sigma^j\tau(\sqrt{-3} + \sqrt[6]{2}) = -\sqrt{-3} + \omega^j\sqrt[6]{2}$. Thus σ^j and $\sigma^j\tau$ do not fix $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2})$ for any $0 \le j < 6$ (except the identity), so $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2}) = \mathbb{Q}(\sqrt{-3}, \sqrt[6]{2})$ as desired. □

Exercise 5. Let G be a finite group and let $g \in G$. Suppose for every irreducible complex character χ of G we have $|\chi(g)| = |\chi(1)|$. Prove that g is in the center of G.

Proof. Let C be the conjugacy class of g. By column orthogonality,

$$\sum_{i=1}^{r} |\chi_i(g)|^2 = \frac{|G|}{|C|}$$

Where $\chi_1, \dots, \chi_r$ are the irreducible characters of G. Using column orthogonality with the identity (or because it's a well known identity on its own),

$$\sum_{i=1}^{r} |\chi_i(1)|^2 = |G|$$

Therefore, $|C| = 1$, so g is in the center of G. □

Exercise 6. Let A be a commutative ring, let P be a flat A-module and let I be an injective A-module. Show that $\mathrm{Hom}_A(P, I)$ is an injective A-module.

Proof. To show $\mathrm{Hom}_A(P, I)$ is injective, we must show that $\mathrm{Hom}_A(-, \mathrm{Hom}_A(P, I))$ is exact. $\mathrm{Hom}(-, M)$ is always left exact, so it suffices to show that for an injection $M \xrightarrow{f} N$ that the induced morphism f_* is surjective:

$$\mathrm{Hom}_A(N, \mathrm{Hom}_A(P, I)) \xrightarrow{f_*} \mathrm{Hom}_A(M, \mathrm{Hom}_A(P, I))$$

By naturality of the tensor-hom adjunction γ, the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}_A(P \otimes N, I) \arrow[r, "\sim", "\gamma"'] \arrow[d, "(P\otimes f)_*"] & \mathrm{Hom}_A(N, \mathrm{Hom}_A(P, I)) \arrow[d, "f_*"] \\
\mathrm{Hom}_A(P \otimes M, I) \arrow[r, "\sim", "\gamma"'] & \mathrm{Hom}_A(M, \mathrm{Hom}_A(P, I))
\end{tikzcd}$$

Since P is flat, $P \otimes M \xrightarrow{P\otimes f} P \otimes N$ is injective since $P \otimes -$ preserves injections. Therefore, $(P \otimes f)_*$ is surjective in the above diagram since I is injective. In more detail, applying $\mathrm{Hom}(-, I)$ to the short exact sequence

$$0 \to P \otimes N \xrightarrow{P\otimes f} P \otimes N \to \ker P \otimes f \to 0$$

yields a short exact sequence

$$0 \to \mathrm{Hom}(\ker P \otimes f, I) \to \mathrm{Hom}(P \otimes N, I) \xrightarrow{P\otimes f} \mathrm{Hom}(P \otimes M, I) \to 0$$

Therefore since the diagram commutes and γ is a bijection, f_* is surjective. □

Exercise 7. Let p be a prime number, k a field of characteristic p and G be a (finite) p-group. Let M be a finitely generated kG-module that admits a k-basis B such that $G \cdot B \subseteq B \subset -B$ (i.e. $\forall g \in G, \forall b \in B, g \cdot b = \pm b'$ for $b' \in B$). Show that M admits a k-basis B_0 invariant under G (i.e. $G \cdot B_0 \subseteq B_0$ without sign).

Proof. □

Exercise 8. Let A be a (non-zero) ring in which the only right ideals are (0) and A. Show that A is a division ring.

Proof. Notice the assumption implies that A is not the zero ring, i.e., $1 \neq 0$. For all non-zero $a \in A$, $a \cdot A$ is a non-zero right ideal of A, and thus equal to A since $(0), A$ are the only right ideals of A by assumption. Thus, there exists $c \in A$ such that $ac = 1$. c is also non-zero, so there exists $b \in A$ such that $cb = 1$. Furthermore, we have

$$a = a(cb) = (ac)b = b$$

Therefore, $ac = ca = 1$, so A is a division ring. □

Exercise 9. Let R be a commutative ring and A, B be two (not necessarily commutative) R-algebras. Consider the functor $\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A \otimes_R B, -) : R\text{-}\mathbf{Alg} \to \mathbf{Set}$, from R-algebras to sets. Construct two homomorphisms $f : A \to A \otimes_R B$ and $g : B \to A \otimes_R B$ and show that they induce an injection

$$\eta_C : \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A \otimes_R B, C) \to \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A, C) \times \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(B, C)$$

natural in $C \in R$-**Alg**. Identify the image of η_C explicitly.

Exercise 10. Let A be a ring. Let $m, n \geq 1$ and P be a right A-module such that $P^n \cong A^m$. Show that $S \mapsto P \otimes_A S$ defines a bijection between the set of isomorphism classes of simple A-modules and that of simple $\mathrm{End}_A(P)$-modules.

Proof. Let us first show that $P \otimes_A - : A\text{-}\mathbf{Mod} \to \mathrm{End}_A(P)\text{-}\mathbf{Mod}$ is an equivalence of categories. By Morita equivalence, it suffices to show that P is a finitely generated projective generator of A-**Mod**. It is clear that P is finitely generated since P^n is. Since P is a direct summand of A^m which is free, P is projective. Furthermore, it is a projective generator since every A-module is surjected onto by a coproduct of A^m, and thus by a coproduct of P^n. Thus let us show that being simple is a categorical property, so $P \otimes -$ induces a bijection on isomorphism classes of simple A-modules and simple $\mathrm{End}_A(P)$-modules.

A simple A-module M is one which has no proper sub A-modules. In particular, $\mathrm{Hom}_A(N, M)$ consists of endomorphisms and the zero morphism for all $N \in A$-**Mod**. This is a purely categorical statement, so in particular if M is simple, then $P \otimes M$ is simple in $\mathrm{End}_A(P)$-**Mod** since $\mathrm{Hom}_{\mathrm{End}_A(P)}(N, P \otimes M) \cong \mathrm{Hom}_A(N', M)$ for N' the image of N under the inverse equivalence $\mathrm{End}_A(P)\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}$. □

Fall 2020

Exercise 1. Let $p < q < r$ be primes and G a group of order pqr. Prove that G is not simple and, in fact, has a normal Sylow r-group.

Proof. Let n_r be the number of r-Sylows, and similarly for n_p, n_q. Suppose for the sake of contradiction that $n_r \neq 1$. Since $n_r | pqr$ and n_r is relatively prime to r, then $n_r \in \{p, q, pq\}$. Since $n_r \equiv 1 \bmod r$ and $p < q < r$, we must have $n_r = pq$. Therefore, there are $(r-1)pq$ elements of order r in G, since every r-Sylow is congruent to $\mathbb{Z}/r\mathbb{Z}$. Thus, there are pq other elements in G. Since $n_q | pr$, $n_q \in \{1, p, r, pr\}$. Since $q > p$ and $n_q \equiv 1 \bmod q$, $n_q \in \{1, r, pr\}$. Thus if $n_q \neq 1$, then $n_q \geq r$. But this would imply that there are $n_q(q-1) \geq r(q-1) \geq qp$ elements of order q in G, which is impossible given there are $(r-1)pq$ elements of order r. Therefore, $n_q = 1$, so there is a unique q-Sylow $N \trianglelefteq G$. Let H be any of the n_r r-Sylows. Then $N \cdot H$ is a subgroup of G of order $|N \cdot H| = rq$. Therefore, $[G : N \cdot H] = p$, the smallest prime dividing $|G|$, so $N \cdot H$ is normal in G. But since conjugation of G acts on the r-Sylows transitively, this implies that every r Sylow is contained in $N \cdot H$, which is impossible since $|N \cdot H| < (r-1)pq$. Therefore, $r = 1$. □

Exercise 2. Show that groups of order $231 = (3)(7)(11)$ are semi-direct products and show that there are exactly two such groups up to isomorphism.

Proof. Let G be a group of order 231. Let H_3, H_7, H_{11} be $3, 7$, and 11 Sylows of G respectively, so $H_n \cong \mathbb{Z}/n\mathbb{Z}$. Let n_{11} be the number of 11 Sylows in G. Since $n_{11} \in \{1, 3, 7, 21\}$ and $n_{11} \equiv 1 \bmod 11$, we must have $n_{11} = 1$. Therefore, H_{11} is normal, so $N = H_7 \cdot H_{11}$ is a subgroup of G, of order a multiple of both 7 and 11. Thus, $|N| = 77$ and $[G : N] = 3$, so $N \trianglelefteq 3$. Furthermore, we have:

$$H_3 \cap N = e$$

$$H_3 \cdot N = G$$

$$N \trianglelefteq G$$

So $G \cong N \rtimes_\alpha H_3$ for some $\alpha : H_3 \to \mathrm{Aut}(N)$. Therefore, G is a semi direct product as desired. Let us show that there are exactly two homomorphisms $\alpha : H_3 \to \mathrm{Aut}(N)$ up to isomorphism of the semidirect product. Notice that the only group of order 77 is $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, so $N \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Therefore,

$$\mathrm{Aut}(N) \cong (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2)^2 \times (\mathbb{Z}/3) \times (\mathbb{Z}/5)$$

Thus, we aim to characterize homomorphisms $\alpha : H_3 \to (\mathbb{Z}/2)^2 \times (\mathbb{Z}/3) \times (\mathbb{Z}/5)$ up to isomorphism of the domain or codomain. By the universal property of the direct product, this amounts to finding homomorphisms from $\mathbb{Z}/3$ into $\mathbb{Z}/2, \mathbb{Z}/5$ and $\mathbb{Z}/3$. There are no non-trivial homomorphisms $\mathbb{Z}/3 \to \mathbb{Z}/2, \mathbb{Z}/5$. Therefore, we only need to consider homomorphisms $\mathbb{Z}/3 \to \mathbb{Z}/3$. There are three such homomorphisms (given by multiplication), but $1 \mapsto 1$ and $1 \mapsto 2$ are identical after composing with an isomorphism of $\mathbb{Z}/3$, and thus yield the same semidirect product. Thus, letting $\alpha : H_3 \to \mathrm{Aut}(N)$ be the homomorphism defined by $1 \mapsto 1$ on the $\mathbb{Z}/3$ component of $\mathrm{Aut}(N)$, the only groups of order 231 (up to isomorphism) are:

$$H_3 \times N \qquad\qquad H_3 \trianglelefteq_\alpha N$$

□

Exercise 3. A ring R (commutative or non-commutative) is called a domain if $ab = 0$ in R implies $a = 0$ or $b = 0$. Suppose that R is a domain such that $M_n(R)$, the ring of $n \times n$ matrices over R, is a semisimple ring. Prove that R is a division ring.

Proof. There is an equivalence R-**Mod** $\to M_n(R)$-**Mod** by $R^n \otimes -$, with R^n an R-$M_n(R)$ bimodule. Since $M_n(R)$ is semisimple, every short exact sequence in $M_n(R)$-**Mod** splits. Therefore, every short exact sequence in R-**Mod** splits, so R is semisimple (we've argued that a ring A being semisimple is a categorical property of A-**Mod**). By Wedderburn, $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ for (non-zero) division rings $D_1, \ldots, D_r$ and $n_1, \ldots, n_r \in \mathbb{Z}^+$. Notice that $M_m(D)$ is not a domain for $m > 1$, for instance by $\begin{bmatrix} 1 & 0 & \ldots \\ 0 & 0 & \\ \vdots & & \end{bmatrix} \begin{bmatrix} 0 & 0 & \ldots \\ 0 & 1 & \\ \vdots & & \end{bmatrix} = 0$. Furthermore, the product of two non-zero rings A, B is not an integral domain, by $(\mathrm{id}_A, 0) \cdot (0, \mathrm{id}_B) = (0, 0)$, so $r = 1$. Therefore, $R \cong M_1(D)$ for a division ring D, so $R \cong D$ and R is a division ring. □

Exercise 4. Let M be a left R-module. Show that M is a projective R-module if and only if there exist $m_i \in M$ and R-module homomorphisms $f_i : M \to R$ for each $i \in I$ such that the sets $\{m_i\}_{i \in I}, \{f_i\}_{i \in I}$ satisfy:

(a) If $m \in M$, then $f_i(m) = 0$ for all but finitely many $i \in I$.

(b) If $m \in M$, then $m = \sum_{i \in I} f_i(m) m_i$.

Proof. First suppose that such $\{m_i\}_{i \in I}, \{f_i\}_{i \in I}$ exist. Then consider the R-module homomorphism $R^I \xrightarrow{g} M$ by $g(e_i) = m_i$ where e_i is the usual basis vector for the ith coordinate of R^I. Notice that this map is well defined and unique by the universal property R^I. Then define $h : M \to R^I$ by

$$h(m) = \sum_{i \in I} f_i(m) e_i$$

h is an R-module homomorphism since for each $i \in I$ the function $m \mapsto f_i(m)e_i$ is an R-module homomorphism, and is well defined since $f_i(m) = 0$ for all but finitely many $i \in I$. Now notice that

$$g \circ h(m) = g\bigg(\sum_{i \in I} f_i(m)e_i\bigg) = \sum_{i \in I} f_i(m)m_i = m$$

Therefore, g surjects from R^I onto M and h is a section, so M is a direct summand of R^I and thus free.

Now suppose that M is projective. There exists a free module with a surjection g by $R^I \xrightarrow{g} M$ (for instance, by letting I be indexed by M and mapping $e_m \mapsto M$). Since M is projective, the following short exact sequence splits:

$$0 \to \ker g \to R^I \xrightarrow{g} M \to 0$$

In particular, there is a section $h : M \to R^I$. Define $f_i : M \to R$ by h composed with the ith projection $R^I \to R$. Notice that for all $m \in M$, $h(m) \in R^I$ and thus all but finitely many of the coordinates of $h(m)$ (as an I tuple of R) are non-zero. Therefore, all but finitely many of $f_i(m)$ are non-zero. Furthermore, letting $m_i = g(e_i)$ for the usual basis vectors e_i of R^I, we have:

$$\sum_{i \in I} f_i(m)m_i = \sum_{i \in I} f_i(m)g(e_i) = g\bigg(\sum_{i \in I} f_i(m)\bigg) = g \circ h(m) = m$$

□

Exercise 5. Let F be a field and $f(x) = x^6+3 \in F[x]$. Determine a splitting field K of $f(x)$ over F and determine $[K : F]$ and $\mathrm{Gal}(K/F)$ for each of the following three fields: $F = \mathbb{Q}, F = \mathbb{F}_5, F = \mathbb{F}_7$.

Proof. **Case 1:** $F = \mathbb{Q}$
Let $\omega = e^{2\pi i/12}$. Then the roots of f are

$$\omega\sqrt[6]{3}, \omega^3\sqrt[6]{3}, \omega^5\sqrt[6]{3}, \omega^7\sqrt[6]{3}, \omega^9\sqrt[6]{3}, \omega^{11}\sqrt[6]{3}$$

Therefore, the splitting field $K/\mathbb{Q}$ is generated by these 6 elements. Also, notice that $[\mathbb{Q}(\omega\sqrt[6]{3}) : \mathbb{Q}]$ since $x^6 + 3$ is irreducible by Eisenstein. Let us show that $K = \mathbb{Q}(\omega\sqrt[6]{3})$. It suffices to show that $\omega^2 = \frac{1+i\sqrt{3}}{2} \in \mathbb{Q}(\omega\sqrt[6]{3})$, and in particular that $i\sqrt{3} \in \mathbb{Q}(\omega\sqrt[6]{3})$. Notice that $(\omega\sqrt[6]{3})^3 = \omega^3\sqrt{3} = i\sqrt{3}$, so $[K : \mathbb{Q}] = 6$ as desired. Therefore, $|\mathrm{Gal}(K/\mathbb{Q})| = 6$. Notice that $L := \mathbb{Q}(\omega^2\sqrt[3]{3}) \subseteq K$, and $\omega^2\sqrt[3]{3}$ is a root of $x^3 + 3$. However, the splitting field of $x^3 + 3$ (irreducible by Eisenstein) is not degree 3 over $\mathbb{Q}$, since $L \cong L' := \mathbb{Q}(\sqrt[3]{3})$ is a purely real extension of $\mathbb{Q}$ and thus not a splitting field of $x^3 + 3$. Therefore, K contains a subfield which is not Galois over $\mathbb{Q}$, and thus $\mathrm{Gal}(K/\mathbb{Q})$ is not abelian. Therefore since $|\mathrm{Gal}(K/\mathbb{Q})| = 6$, $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

Case 2: $F = \mathbb{F}_5$
Notice that if $\alpha \in \overline{F}$ satisfies $\alpha^2 = 3$, then $\alpha^6 + 3 = 3^3 + 3 = 0 \bmod 5$. Thus, (x^2+3) divides $x^6 + 3$ in F. Let $K = F(\alpha)$ be the splitting field of $x^2 + 3$, so $[K : F] = 2$ ($x^2 + 3$ is irreducible by casework). Also, $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2$ and is generated by the Frobenius automorphism ϕ_5 defined by $x \mapsto x^5$. Let us show that $x^6 + 3$ splits in K. It suffices to show that there are 6 distinct roots of $x^6 + 3$ in K. Suppose $(a + b\alpha)$ were a root of $x^6 + 3$ for $a, b \in \mathbb{Z}/5$. We have

$$(a + b\alpha)^6 = \phi(a + b\alpha)(a + b\alpha) = (a - b\alpha)(a + b\alpha) = a^2 - b^2\alpha^2 = a^2 + 2b^2 = 2$$

By casework, we find that $\pm(\alpha), \pm(2 + 2\alpha), \pm(2 + 3\alpha)$ are roots of $x^6 + 3$. Therefore, $x^6 + 3$ splits over K.

Case 3: $F = \mathbb{F}_7$
In this case, we have

$$x^6 + 3 = (x^3 - 2)(x^3 + 2)$$

and since x^6+3 has no roots in $\mathbb{F}_7$ by Fermat's little theorem, both x^3-2 and x^3+2 are irreducible. Furthermore, recall that the product of all irreducible degree 3 and degree 1 polynomials in $\mathbb{F}_7$ is equal to $x^{7^3} - x$ which splits over $K = \mathbb{F}_{7^3}$. Therefore, if L is the field $F[\alpha]$ for any root α of $x^3 - 2$ in $\overline{\mathbb{F}_7}$, then L is the unique extension of $\mathbb{F}_7$ of degree 3 and both $x^3 - 2, x^3 + 2$ split in L. Therefore, letting $K = L$ be the splitting field of $x^6 + 3$, $[K : \mathbb{F}_7] = 3$ and $\mathrm{Gal}(K/\mathbb{F}_7) \cong \mathbb{Z}/3$. □

Exercise 6. Let $K_1 \subset K_2 \subset K_3$ be fields with K_3/K_2 and K_2/K_1 both Galois. Let L be a minimal Galois extension of K_1 containing K_3. Show if the Galois groups $\mathrm{Gal}(K_3/K_2)$ and $\mathrm{Gal}(K_2/K_1)$ are both p-groups so is the Galois group $\mathrm{Gal}(L/K_1)$.

Proof. By the Galois Correspondence, we have the following, for $G = \mathrm{Gal}(L/K_1), H_2 = \mathrm{Gal}(L/K_2), H_3 = \mathrm{Gal}(L/K_3)$:

$$1 \leq H_3 \trianglelefteq H_2 \trianglelefteq G$$

(But in particular, H_3 may not be normal in G - this would be the statement that K_3/K_1 is Galois). Furthermore, $G/H_2 \cong \mathrm{Gal}(K_2/K_1)$ is a p-group and $H_2/H_3 \cong \mathrm{Gal}(K_3/K_2)$ is a p-group. Also, since L is a minimal Galois extension of K_1 containing K_3, H_3 **contains no (non-trivial) normal subgroups** of G - otherwise, such a normal subgroup would correspond to a subfield of L which contains K_3 and is Galois over K_1. We exclude the case of $H_3 = 1$, since in this case the claim is trivial, so in particular we may assume that H_3 is not normal in G. Consider the derived series $G_1 = [G, G], G_2 = [G_2, G_2], \ldots$ of characteristic subgroups of G. First notice that since G/H_2 is a p-group, it is solvable, so the derived series

$$\overline{G_1} = [G/H_2, G/H_2], \overline{G_2} = [\overline{G_1}, \overline{G_1}], \ldots$$

is eventually zero. Also, letting $\pi : G \to G/H_2$ be the quotient map, we have

$$\pi(G_1) = \pi([G, G]) = [\pi(G), \pi(G)] = [G/H, G/H] = \overline{G_1}$$

Therefore, $\pi(G_1) = \overline{G_1}$. Similarly, $\pi(G_2) = \overline{G_2}$, and by finite induction there is some n such that $\pi(G_n) = \overline{G_n} = 0$ and thus $G_n \subset H_2$. By the same argument (since H_2/H_3 is also a p-group and thus solvable), there is some m such that $G_m \leq H_3$. But since H_3 contains no non-trivial normal subgroups, $G_m = 0$, so G is solvable.

Let N be a normal subgroup of G containing H_3 of minimal order, so N is a minimal (non-trivial) normal subgroup of G containing H_3. By S2019#1, $N \cong \overbrace{C_q \times \cdots \times C_q}^{r}$ for a prime $q \in \mathbb{Z}$ and $r > 0$. We also have that $|N| = [N : H_3] \cdot |H_3|$, $[N : H_3] > 1$, and $[N : H_3]$ divides $[G : H_3] = p^k$. Therefore, p divides $[N : H_3]$ and thus the order of N, so $q = p$. Therefore, H_3 is order a power of p, so

$$|\operatorname{Gal}(L/K_1)| = |G| = [G : H_2][H_2 : H_3] \cdot |H_3|$$

is a power of p. □

Exercise 7. Let R be a Dedekind domain with quotient field K and I a nonzero ideal in R. Show both of the following:

(a) Every ideal in R/I is a principal ideal.

(b) If J is a fractional ideal of R, i.e., $0 \neq J \subset K$ is an R-module such that there exists a $d \in R$ with $dJ \subset R$, then there exists a $0 \neq x$ in K such that $I + xJ = R$.

Proof. □

Exercise 8. Consider $R = \mathbb{C}[X,Y]/(X^2, XY)$. Determine the prime ideals $\mathfrak{p}$ of R. Which of the localizations $R_\mathfrak{p}$ are integral domains?

Proof. The prime ideals of R are in (bijective, inclusion preserving, quotient preserving) correspondence with the prime ideals of $\mathbb{C}[X,Y]$ containing X^2 and XY. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{C}[X,Y]$ containing X^2, XY. Since $\mathfrak{p}$ contains X^2, it contains X by primality. Since the prime ideals of $\mathbb{C}[X,Y]$ containing X are in correspondence with the prime ideals of $\mathbb{C}[X,Y]/(X) \cong \mathbb{C}[Y]$, we restrict our search to the prime ideals of $\mathbb{C}[Y]$. The prime ideals of $\mathbb{C}[Y]$ are the prinicipal ideals generated by prime elements (and the (0) ideal) since $\mathbb{C}[Y]$ is a PID. Furthermore since $\mathbb{C}$ is algebraically closed, the only prime ideals of $\mathbb{C}[Y]$ are those of the form $(Y - \alpha)$ for $\alpha \in \mathbb{C}$. Tracing back through the correspondence, the prime ideals of R are thus the following, where $x = [X], y = [Y]$ are the equivalence classes of X, Y in R:

$$(x) \qquad \Big\{(x, y - \alpha) \mid \alpha \in \mathbb{C}\Big\}$$

Now let us consider the localizations $R_{\mathfrak{p}}$ for $\mathfrak{p}$ in the previous list. Recall that localization commutes with quotients in the following way. let $\mathfrak{q}$ be the corresponding prime ideal in $R = \mathbb{C}[X,Y]$, and let $I = (X^2, XY)$. Then we have:

$$R_{\mathfrak{p}} \cong (\mathbb{C}[X,Y]_{\mathfrak{q}})/\tilde{I}$$

where $\tilde{I}$ is the image of I in $\mathbb{C}[X,Y]_{\mathfrak{q}}$. First consider $\mathfrak{p} = (x, y-\alpha)$ for $\alpha \in \mathbb{C}\setminus\{0\}$ or $\mathfrak{p} = (x)$. Then, $\mathfrak{q} = (x, y-\alpha)$ or $\mathfrak{p} = (x)$, and thus $\mathbb{C}[X,Y]_{\mathfrak{q}}$ is the subring of $\mathbb{C}(X,Y)$ of the form $\frac{p(X,Y)}{q(X,Y)}$ for $q \notin \mathfrak{q}$, since $\mathbb{C}[X,Y]$ is a domain. The image $\tilde{I}$ of I in $\mathbb{C}[X,Y]_{\mathfrak{q}}$ is thus the set of elements of the form $\frac{X^2p(X,Y)}{q(X,Y)} + \frac{XYp'(X,Y)}{q'(X,Y)}$ for $q, q' \notin \mathfrak{q}$. In particular, notice that since $Y \notin \mathfrak{q}$, $\frac{XY}{Y} = X \in \tilde{I} = \mathbb{C}[X,Y]_{\mathfrak{q}}I$. Therefore, $\tilde{I}$. Therefore, $\tilde{I}$ is a prime ideal of $\mathbb{C}[X,Y]_{\mathfrak{q}}$ since it corresponds to the prime ideal (X) of $\mathbb{C}[X,Y]$ by the prime ideal correspondence of localization. Therefore, $\mathbb{C}[X,Y]_{\mathfrak{q}}/\tilde{I} \cong R_{\mathfrak{p}}$ is a domain. Now consider the case of $\mathfrak{p} = (x,y)$, so $\mathfrak{q} = (X,Y)$. Then we have that $\mathbb{C}[X,Y]_{\mathfrak{q}}$ is the subring of $\mathbb{C}(X,Y)$ of elements of the form $\frac{p(X,Y)}{q(X,Y)}$ for $q \notin \mathfrak{q}$. $q \notin \mathfrak{q}$ is equivalent to q having a non-zero constant term. Let us show that $\frac{X}{1} \notin \tilde{I}$. It suffices to show that $\frac{X}{1}$ cannot be written as $\frac{X^2p}{q} + \frac{XYp'}{q'}$ for q, q' with having non-constant terms. Assume it could: then we would have

$$\frac{X}{1} = \frac{X^2p}{q} + \frac{XYp'}{q'}$$

$$Xqq' = X^2pq' + XYp'q$$

$$qq' = Xpq' + Yp'q$$

However, $Xpq' + Yp'q$ has a zero constant term in $\mathbb{C}[X,Y]$, but qq' does not. This is a contradiction, so $\frac{X}{1} \notin \tilde{I}$ (notice that cancellation was possible since $\mathbb{C}(X,Y)$ is a domain). Therefore, $\frac{X}{1} \notin \tilde{I}$. However, $\frac{X^2}{1} \in \tilde{I}$, so $\tilde{I}$ is not prime in $\mathbb{C}[X,Y]/_{\mathfrak{q}}$. Therefore,

$$\mathbb{C}[X,Y]_{\mathfrak{q}}/\tilde{I} \cong R_{\mathfrak{p}}$$

is not a domain. □

Exercise 9. Let G be a finite group, F a field, and V a finite dimensional $F-$vector space with $G \xrightarrow{\rho} \mathrm{GL}(V)$ a faithful irreducible representation. Show that the center $Z(G)$ of G is cyclic.

Proof. Notice that the center $Z(G)$ of G is a finite abelian group, and thus of the following form for positive integers $n_r|\ldots|n_2|n_1$:

$$Z(G) \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$$

for $C_n = \mathbb{Z}/n\mathbb{Z}$ the cyclic group with n elements. We ignore the case when $Z(G)$ is trivial, so we may assume that each n_i is greater than 1. Thus, assume $r \geq 2$. Let $g = (1, 0, \ldots, 0)$ and $h = (0, 1, \ldots, 0)$ be generators for C_{n_1}, C_{n_2} respectively. Since g, h are in the center of $Z(G)$, $\rho(g) : V \to V, \rho(h) : V \to V$ are FG-module homomorphisms, since for any $g' \in G$, $\rho(g') \circ \rho(g) = \rho(g) \circ \rho(g')$ and likewise for h. Let $\overline{F}$ be an algebraic closure of F. Fix an F-linear basis of V so

$V \cong F^n$ for some n, so $\rho(g), \rho(h)$ are represented by matrices $A_g, A_h : F^n \to F^n$. We may naturally treat A_g, A_h as $\overline{F}$-linear transformations $\overline{F}^n \to \overline{F}^n$ since they are explicit matrices $F^n \to F^n$. Also since $\rho(g), \rho(h)$ commute, A_g, A_h commute.

Since $\overline{F}$ is algebraically closed, there exists an eigenvalue $\lambda \in \overline{F}$ of A_g. Since A_h commutes with A_g, A_h restricts to a linear transformation on $\ker(A_g - \lambda I_n)$, and thus has a non-zero eigenvector v in $\ker(A_g - \lambda)$. In particular, there is a non-zero $v \in \overline{F}^n$ which is simultaneously an eigenvector of A_g with eigenvalue λ and an eigenvector of A_h with eigenvalue λ'. Also notice that since $A_g^{n_1} = I_n = A_h^{n_2}$, λ is an n_1th root of unity and λ' is an n_2th root of unity. We aim to show that there is some $a \in \mathbb{Z}/n_1\mathbb{Z}, b \in \mathbb{Z}/n_2\mathbb{Z}$ not both equal to 0 such that $\lambda^a \lambda'^b = 1$. If λ is not a primitive n_1th root of unity, this is clearly satisfied for a equal to n_1 divided by the order of n_1. Thus, assume λ is a primitive n_1th root of unity. Then it follows that either $\lambda' = 1$ and we can take $a = 0, b = 1$, or λ' is a non-trivial power of λ. In any of these cases, there exists some $(a, b) \neq (0, 0)$ such that $\lambda^a \lambda'^b = 1$ as desired.

Therefore, $A_g^a A_h^b v = \lambda^a \lambda'^b v = v$, so $A_g^a A_h^b$ has an eigenvalue of 1. Therefore, $\rho(g^a) \circ \rho(h^b) - \mathrm{Id}_V : V \to V$ is an FG-module homomorphism with non-trivial kernel. Therefore since V is irreducible, $\rho(g^a) \circ \rho(b^h) - \mathrm{Id}_V$ is the zero map, so $\rho(g^a) \circ \rho(h^b) = \mathrm{Id}_V$. However, $g^a h^b$ is not the identity in G, so ρ is not faithful. Thus if G has non cyclic center, every irreducible representation is not faithful. □

Exercise 10. Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and suppose that every pair of morphisms in $\mathcal{C}$ admits a coequalizer. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor that preserves coequalizers: i.e., if $f, g : A \to B$ are morphisms in $\mathcal{C}$ and $\pi : B \to \mathrm{coeq}(f, g)$ is the coequalizer morphism, then $F(\pi)$ is a coequalizer morphism for $F(f)$ and $F(g)$. Suppose also that if h is a morphism in $\mathcal{C}$ such that $F(h)$ is an isomorphism, then h is an isomorphism. Show that F is faithful.

Proof. Let $X, Y \in \mathrm{Obj}(\mathcal{C})$ and suppose $f, g \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ such that $F(f) = F(g)$. Let us show that $f = g$. Let $(Z, \pi) = \mathrm{coeq}(f, g)$ for $\pi : Y \to Z$ and Z the coequalizer object. Then by assumption, the pair $(F(Z), F(\pi))$ is the coequalizer of $F(f), F(g)$. Since $F(f) = F(g)$ by assumption, let us show that $F(Y)$ (with the identity map $F(Y) \xrightarrow{\mathrm{id}} F(Y)$) is the coequalizer of $F(f), F(g)$. Since $F(f) = F(g)$, for any object $M \in \mathrm{Obj}(\mathcal{D})$ and morphism $h : F(Y) \to M$, the pair (M, y) is a cocone of the diagram formed by $F(X), F(f), F(g), F(Y)$. Thus, we aim to show that for all (M, y), there exists a unique morphism $Y \to M$ making the following diagram commute:

$$\begin{tikzcd}
F(X) \arrow[r, bend left, "F(f)"] \arrow[r, bend right, "F(g)"'] & F(Y) \arrow[r, "h"] \arrow[dr, "\mathrm{id}"] & M \\
 & & F(Y) \arrow[u, dashed, "\exists!"]
\end{tikzcd}$$

Of course, h makes the diagram commute and is unique since id is an isomorphism. Thus, $(F(Y), \mathrm{id})$ is the coequalizer of $F(X), F(Y)$. Therefore, $F(Y)$ and $F(Z)$ are (uniquely with respect to the diagram) isomorphic by the uniqueness of colimits. In fact we can reprove this by hand, see that the following diagram commutes and by uniqueness we must have $F(\pi) \circ g = \mathrm{id}_Z$:

$$\begin{tikzcd}
 & & F(Z) \\
F(X) \arrow[r, bend left, "F(f)"] \arrow[r, bend right, "F(g)"] & F(Y) \arrow[ur, "F(\pi)"] \arrow[r, "\mathrm{id}"] \arrow[dr, "F(\pi)"] & F(Y) \arrow[u, "F(\pi)"] \\
 & & F(Z) \arrow[u, dashed, "\exists ! g"] \arrow[uu, bend right=60, "\mathrm{id}"]
\end{tikzcd}$$

Therefore, $F(\pi)$ is an isomorphism, so by assumption $\pi : Y \to Z$ is an isomorphism in $\mathcal{C}$. Therefore since $\pi \circ f = \pi \circ g$, $\pi^{-1} \circ \pi \circ f = \pi^{-1} \circ \pi \circ g$ so $f = g$ as desired. □

Spring 2020

Exercise 1. Let G be a group defined by $G = \langle a, b | a^2 = b^2 = 1\rangle$. Determine the order of all non-trivial finite quotient groups.

Proof. First let us show that the order of any non-trivial finite quotient group of G is even. Let $G \xrightarrow{\pi} G/N$ for $N \neq G$. Since G is generated by a, b, G/N is generated by a, b. Therefore, either $\pi(a)$ or $\pi(b)$ is non-zero. Since a, b have order 2, one of $\pi(a), \pi(b)$ has order 2, so 2 divides the order of G/N.

Now let us show that for all even numbers $2n$, there is a quotient G/N of order $2n$. Let D_n be the dihedral group with $2n$ elements, given by $D_n = \langle x, y \mid x^n = 1 = y^2, xyxy = 1\rangle$. Since $y^2 = (xy)^2 = 1$, by the universal property of free groups and quotient groups there is a homomorphism $\rho : G \to D_n$ with $\rho(a) = y$, $\rho(b) = xy$. Since y, xy generate D_n, ρ is surjective. Therefore, $D_n \cong G/\ker\rho$, so $|G/\ker\rho| = 2n$ as desired. □

Exercise 2. Let G be a finite group of order $n > 1$ and consider its group algebra $\mathbb{Z}[G]$ embedded in $\mathbb{Q}[G]$. Let $A = \mathbb{Z}[G]/\mathfrak{a}$ for the ideal $\mathfrak{a}$ generated by $g - 1$ for all $g \in G$.

(a) Prove that the algebra $\mathbb{Q}[G]$ is the product of $\mathbb{Q}$ and $\mathbb{Q} \cdot \mathfrak{a}$, where $\mathbb{Q} \cdot \mathfrak{a}$ is the $\mathbb{Q}$-span of $\mathfrak{a}$ in $\mathbb{Q}[G]$. [Hint: first identify the unit $1_{\mathbb{Q}\cdot\mathfrak{a}}$.]

(b) Let B be the projected image of $\mathbb{Z}[G]$ in $\mathbb{Q} \cdot \mathfrak{a}$. Prove that $A \otimes_{\mathbb{Z}[G]} B \cong G$ as groups if and only if G is a cyclic group.

Proof. (a) Define $e = \frac{1}{|G|}\sum_{g\in G} g$. Notice that e is an idempotent because

$$e \cdot e = \frac{1}{|G|^2}\sum_{g\in G} g \sum_{h\in G} h = \frac{1}{|G|^2}\sum_{g\in G} g \sum_{g^{-1}h\in G} g^{-1}h = \frac{1}{|G|}\sum_{g\in G} g$$

Therefore, as $\mathbb{Q}$-algebras (i.e., as rings), we have

$$\mathbb{Q}[G] \cong e\mathbb{Q}[G] \times (1 - e)\mathbb{Q}[G]$$

With $e\mathbb{Q}[G] \hookrightarrow \mathbb{Q}[G], (1 - e)\mathbb{Q}[G] \hookrightarrow \mathbb{Q}[G]$ the inclusions and $\mathbb{Q}[G] \to e\mathbb{Q}[G], \mathbb{Q}[G] \to (1 - e)\mathbb{Q}[G]$ multiplication by e and $(1-e)$ respectively (this isomorphism holds for any idempotent e of a ring R).

First, let us show that $e\mathbb{Q}[G]$ is canonically isomorphic to $\mathbb{Q}$. Notice that for an arbitrary $\alpha = \sum_g a_g g \in \mathbb{Q}[G]$, we have

$$e \cdot \alpha = \frac{1}{|G|}\sum_{g\in G} g \sum_{g^{-1}h\in G} a_{g^{-1}h} g^{-1}h = \frac{1}{|G|}\sum_{h\in H} h \sum_{g\in G} a_{g^{-1}h} = e \cdot \frac{\sum_{g\in G} a_g}{|G|} = \alpha \cdot e$$

Therefore, $\mathbb{Q}[G] = e \cdot \mathbb{Q}$, so $\mathbb{Q} \cong e\mathbb{Q}[G]$ is an isomorphism by $a \mapsto a \cdot e$. This implies that $(1-e)\mathbb{Q}[G]$ is a dimension $|G|-1$ vector space over $\mathbb{Q}$.

In particular, this also means that $1-g \in (1-e)\mathbb{Q}[G]$ for $g \in G$, since $1-g$ is annihilated by e. Also, $\Big\{1-g \mid g \in G \setminus \{1_G\}\Big\}$ is a $\mathbb{Q}$-linearly independent set of $|G|-1$ elements contained in $(1-e)\mathbb{Q}[G]$. Thus since $\dim_{\mathbb{Q}} \mathbb{Q}[G] = |G|-1$, we have that $(1-e)\mathbb{Q}[G]$ is exactly the $\mathbb{Q}$-span of $g-1$, which is exactly $\mathfrak{a}\mathbb{Q}[G]$. Therefore

$$\mathbb{Q}[G] \cong \mathbb{Q} \times \mathfrak{a} \cdot \mathbb{Q}[G]$$

as desired.

(b) There is an isomorphism of $\mathbb{Z}$-modules

$$\mathbb{Z}[G]/\mathfrak{a} \otimes_{\mathbb{Z}[G]} B \cong B/\mathfrak{a}B$$

by sending $[a] \otimes b \to [ab]$. Let us prove that $B/\mathfrak{a}B \cong \mathbb{Z}/|G|\mathbb{Z}$ as an abelian group. Then, $A \otimes_{\mathbb{Z}[G]} B \cong G$ if and only if $G \cong \mathbb{Z}/|G|\mathbb{Z}$, i.e., G is cyclic.

Since $\mathbb{Z}[G]$ is generated as an abelian group by $\{g\}_{g\in G}$, B is generated as an abelian group by $\{g(1-e)\}_{g\in G} = \{g-e\}_{g\in G}$. Therefore, $\mathfrak{a} \cdot B$ is generated as an abelian group by

$$\Big\{\Big(g-e\Big)\cdot\Big(1-h\Big)\Big\}_{g,h\in G} = \Big\{g-gh\Big\}_{g,h\in G}$$

using the fact that $g \cdot e = e$ for $g \in G$. Therefore, $\mathfrak{a} \cdot B$ has a $\mathbb{Z}$ generating set

$$T := \{1-g\}_{g\in G\setminus\{1\}}$$

Also, these elements are $\mathbb{Q}$-linearly independent in $\mathbb{Q}[G]$, so $\mathfrak{a} \cdot B \cong \mathbb{Z}^{|G|-1}$ with a $\mathbb{Z}$-basis $\{1-g\}_{g\in G\setminus\{1\}}$.

Pick $g_0 \in G$ not equal to the identity. Since B is generated as an abelian group by $\{g-e\}_{g\in G\setminus\{g_0\}}$, B has a $\mathbb{Z}$-basis $\{g-e\}_{g\in G\setminus\{g_0\}}$ since this set is linearly independent over $\mathbb{Q}$ in $\mathbb{Q}[G]$. Then applying a change of basis, we find that B has a $\mathbb{Z}$-basis

$$S := \{1-e\} \cup \{1-g\}_{g\in G\setminus\{g_0,1\}}$$

by subtracting $g-e$ from $1-e$. Then the inclusion $\mathfrak{a} \cdot B \hookrightarrow B$ with respect to the bases T, S is a matrix $\varphi : \mathbb{Z}^{n-1} \to \mathbb{Z}^{n-1}$.

$$\begin{tikzcd}
\mathfrak{a} \cdot B \arrow[r, hook] \arrow[d, dashed, "\sim"] & B \arrow[d, dashed, "\sim"] \\
\mathbb{Z}^{n-1} \arrow[r, "\varphi"] & \mathbb{Z}^{n-1}
\end{tikzcd}$$

We explicitly compute that

$$\varphi = \begin{bmatrix} -|G| & 0 & 0 & \dots & 0 \\ -1 & 1 & 0 & & \vdots \\ -1 & 0 & 1 & & \\ \vdots & & & \ddots & \\ -1 & \dots & & & 1 \end{bmatrix}$$

since

$$1 - g_0 = |G|(e-1) + \sum_{g \in G \setminus \{g_0, 1\}} 1 - g$$

In particular, $B/\mathfrak{a} \cdot B \cong \operatorname{coker} \varphi = \mathbb{Z}/|G|\mathbb{Z}$ as desired.

□

Exercise 3. Prove that a noetherian commutative ring A is a finite ring if the following two conditions are satisfied:

(a) the nilradical of A vanishes

(b) localization at every maximal ideal is a finite ring

Proof. **Note:** there are much easier ways to do this problem if you have more technology.
First we show that A has Krull dimension 0, so every prime ideal is maximal. Let $\mathfrak{p}$ be a prime ideal of A, and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. The ring $A_\mathfrak{m}$ is finite by assumption (b). There is a correspondence between prime ideals contained in $\mathfrak{m}$ and prime ideals of $A_\mathfrak{m}$, so the ideal $\tilde{\mathfrak{p}}$ generated by $\eta_\mathfrak{m}(\mathfrak{p})$ in $A_\mathfrak{m}$ is prime. Furthermore, $A/\mathfrak{p} \cong A_\mathfrak{m}/\tilde{\mathfrak{p}}$ as rings. Since $\tilde{\mathfrak{p}}$ is a prime ideal of $A_\mathfrak{m}$, $A_\mathfrak{m}/\tilde{\mathfrak{p}}$ is a domain and thus a field since it is finite. Therefore, $A/\mathfrak{p}$ is field, so $\mathfrak{p}$ is maximal by definition.

Now let $\mathfrak{m}$ be a maximal ideal of A. Let S be the set of ideals defined by:

$$S_\mathfrak{m} := \{\operatorname{Ann}(m) \mid m \in A \setminus \mathfrak{m}\}$$

where

$$\operatorname{Ann}(x) := \{a \in A \mid ax = 0\}$$

Since A is Noetherian, there exists an $x \in A \setminus \mathfrak{m}$ such that $\operatorname{Ann}(x)$ is maximal in S. Now let us show that $\operatorname{Ann}(x)$ contains every other $\operatorname{Ann}(y)$ for $y \in A \setminus \mathfrak{m}$. Let $y \in A \setminus \mathfrak{m}$. Then notice that $\operatorname{Ann}(xy) \supseteq \operatorname{Ann}(x) \cup \operatorname{Ann}(y)$, since if $ax = ay = 0$, then $axy = 0$. Furthermore by maximality of $\operatorname{Ann}(x)$ and because $A \setminus \mathfrak{m}$ is closed under multiplication, $\operatorname{Ann}(xy) \supseteq \operatorname{Ann}(x)$ implies that $\operatorname{Ann}(xy) = \operatorname{Ann}(x)$, so $\operatorname{Ann}(y) \subseteq \operatorname{Ann}(x)$. Thus, $\operatorname{Ann}(x)$ contains every $\operatorname{Ann}(y)$ for $y \in A \setminus \mathfrak{m}$.

For each maximal ideal $\mathfrak{m}$ of A, let $x_\mathfrak{m}$ be chosen as discussed above so $\operatorname{Ann}(x_\mathfrak{m})$ is maximal in $S_\mathfrak{m}$. let $I = (x_\mathfrak{m})_\mathfrak{m}$ be the ideal generated by $x_\mathfrak{m}$ for each maximal ideal $\mathfrak{m}$ of A. Since A is Noetherian, I is finitely generated by some $x_{\mathfrak{m}_1}, \dots, x_{\mathfrak{m}_k}$. Let us show that

$$\eta : A \to \prod_{i=1}^{n} A_{\mathfrak{m}_i}$$

is an injection (induced by the localization maps $\eta_{\mathfrak{m}_i} : A \to A_{\mathfrak{m}_i}$ and the universal property of the product). Let $\mathfrak{m}$ be any maximal ideal. The kernel of $\eta_\mathfrak{m}$ is all of the elements $x \in A$ such that there exists $a \in A \setminus \mathfrak{m}$ such that $xa = 0$. In particular, $x \in I$ for some $I \in S_\mathfrak{m}$, i.e., $x \cdot a_\mathfrak{m} = 0$. Now take any $x \in A$ not equal to 0. Since $x \neq 0$, $\operatorname{Ann}(x) \neq A$ and is thus contained in some maximal ideal $\mathfrak{m}$. Then $x \notin \ker \eta_\mathfrak{m}$, so $a_\mathfrak{m} x \neq 0$. Since $(x_{\mathfrak{m}_1}, \dots, x_{\mathfrak{m}_k})$ generate I, there exists $a_1, \dots, a_k \in A$ such that $a_\mathfrak{m} = x_{\mathfrak{m}_1} a_1 + \dots + x_{\mathfrak{m}_k} a_k$. Thus,

$$(x_{\mathfrak{m}_1} a_1 + \dots + x_{\mathfrak{m}_k} a_k) x \neq 0$$

Therefore, there is some $1 \leq i \leq n$ such that $x_{\mathfrak{m}_i} a_i x \neq 0$, and thus $x \notin \ker \eta_{\mathfrak{m}_i}$. Thus, η is an injection. First we show that A has Krull dimension 0, so every prime ideal is maximal. Let $\mathfrak{p}$ be a prime ideal of A, and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. The ring $A_\mathfrak{m}$ is finite by assumption (b). There is a correspondence between prime ideals contained in $\mathfrak{m}$ and prime ideals of $A_\mathfrak{m}$, so the ideal $\tilde{\mathfrak{p}}$ generated by $\eta_\mathfrak{m}(\mathfrak{p})$ in $A_\mathfrak{m}$ is prime. Furthermore, $A/\mathfrak{p} \cong A_\mathfrak{m}/\tilde{\mathfrak{p}}$ as rings. Since $\tilde{\mathfrak{p}}$ is a prime ideal of $A_\mathfrak{m}$, $A_\mathfrak{m}/\tilde{\mathfrak{p}}$ is a domain and thus a field since it is finite. Therefore, $A/\mathfrak{p}$ is field, so $\mathfrak{p}$ is maximal by definition.

Now let $\mathfrak{m}$ be a maximal ideal of A. Let S be the set of ideals defined by:

$$S_\mathfrak{m} := \{\operatorname{Ann}(m) \mid m \in A \setminus \mathfrak{m}\}$$

where

$$\operatorname{Ann}(x) := \{a \in A \mid ax = 0\}$$

Since A is Noetherian, there exists an $x \in A \setminus \mathfrak{m}$ such that $\operatorname{Ann}(x)$ is maximal in S. Now let us show that $\operatorname{Ann}(x)$ contains every other $\operatorname{Ann}(y)$ for $y \in A \setminus \mathfrak{m}$. Let $y \in A \setminus \mathfrak{m}$. Then notice that $\operatorname{Ann}(xy) \supseteq \operatorname{Ann}(x) \cup \operatorname{Ann}(y)$, since if $ax = ay = 0$, then $axy = 0$. Furthermore by maximality of $\operatorname{Ann}(x)$ and because $A \setminus \mathfrak{m}$ is closed under multiplication, $\operatorname{Ann}(xy) \supseteq \operatorname{Ann}(x)$ implies that $\operatorname{Ann}(xy) = \operatorname{Ann}(x)$, so $\operatorname{Ann}(y) \subseteq \operatorname{Ann}(x)$. Thus, $\operatorname{Ann}(x)$ contains every $\operatorname{Ann}(y)$ for $y \in A \setminus \mathfrak{m}$.

For each maximal ideal $\mathfrak{m}$ of A, let $x_\mathfrak{m}$ be chosen as discussed above so $\operatorname{Ann}(x_\mathfrak{m})$ is maximal in $S_\mathfrak{m}$. let $I = (x_\mathfrak{m})_\mathfrak{m}$ be the ideal generated by $x_\mathfrak{m}$ for each maximal ideal $\mathfrak{m}$ of A. Since A is Noetherian, I is finitely generated by some $x_{\mathfrak{m}_1}, \dots, x_{\mathfrak{m}_k}$. Let us show that

$$\eta : A \to \prod_{i=1}^{n} A_{\mathfrak{m}_i}$$

is an injection (induced by the localization maps $\eta_{\mathfrak{m}_i} : A \to A_{\mathfrak{m}_i}$ and the universal property of the product). Let $\mathfrak{m}$ be any maximal ideal. The kernel of $\eta_\mathfrak{m}$ is all of the elements $x \in A$ such that there exists $a \in A \setminus \mathfrak{m}$ such that $xa = 0$. In particular, $x \in I$ for some $I \in S_\mathfrak{m}$, i.e., $x \cdot a_\mathfrak{m} = 0$. Now

take any $x \in A$ not equal to 0. Since $x \neq 0$, $\mathrm{Ann}(x) \neq A$ and is thus contained in some maximal ideal $\mathfrak{m}$. Then $x \notin \ker \eta_{\mathfrak{m}}$, so $a_{\mathfrak{m}} x \neq 0$. Since $(x_{\mathfrak{m}_1}, \ldots, x_{\mathfrak{m}_k})$ generate I, there exists $a_1, \ldots, a_k \in A$ such that $a_{\mathfrak{m}} = x_{\mathfrak{m}_1} a_1 + \cdots + x_{\mathfrak{m}_k} a_k$. Thus,

$$(x_{\mathfrak{m}_1} a_1 + \cdots + x_{\mathfrak{m}_k} a_k) x \neq 0$$

Therefore, there is some $1 \leq i \leq n$ such that $x_{\mathfrak{m}_i} a_i x \neq 0$, and thus $x \notin \ker \eta_{\mathfrak{m}_i}$. Thus, η is an injection. □

Exercise 4. Compute the dimension of the tensor products of two algebras $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{R}$ over $\mathbb{R}$. Is $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{R}$ finite dimensional over $\mathbb{R}$?

Proof. Let us show that for $\mathbb{Q}$-algebras A, B, that $A \otimes_{\mathbb{Z}} B$ is naturally isomorphic to $A \otimes_{\mathbb{Q}} B$. It suffices to show that for every $\mathbb{Q}$-bilinear function $\psi : A \times B \to M$ for M a $\mathbb{Q}$-algebra that ψ is $\mathbb{Q}$-balanced if and only if it is $\mathbb{Z}$-balanced. In this case, both $\mathbb{Q}$-algebras satisfy the same universal property and are thus (uniquely) isomorphic. It is clear that any such $\mathbb{Q}$-balanced ψ is also $\mathbb{Z}$ balanced. Thus assume $\psi : A \times B \to M$ is $\mathbb{Z}$ balanced, so $\psi(ma, b) = \psi(a, mb)$ for all $m \in \mathbb{Z}$. Then, let $m/n \in \mathbb{Q}$ be any non-zero rational number. Then we have that:

$$\psi(ma/n, b) = \psi(ma/n, (bn/n)) = \psi(ma, b/n) = \psi(a, mb/n)$$

by $\mathbb{Z}$-balance, so ψ is $\mathbb{Q}$-balanced. Thus, we have

$$\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}] \cong (\mathbb{Q}^{\oplus 2} \otimes \mathbb{Q}^{\oplus 2}) \cong \mathbb{Q}^{\oplus 4}$$

So $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Q}[\sqrt{2}]$ is dimension 4 over $\mathbb{Q}$. Furthermore, we have:

$$\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{Q}^{\oplus 2} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{\oplus 2}$$

as an $\mathbb{R}$ module, so $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{R}$ is dimension 2 over $\mathbb{R}$. Finally, we have:

$$\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{R} \cong (\mathbb{Q}^{\aleph_1} \otimes_{\mathbb{Q}} \mathbb{R}) \cong \mathbb{R}^{\oplus \aleph_1}$$

so $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{R}$ is not finite dimensional over $\mathbb{R}$. □

Exercise 5. If $K \neq \mathbb{Q}$ appears as a subfield (sharing the identity) of some central simple algebra over $\mathbb{Q}$ of $\mathbb{Q}$-dimension 9, determine (isomorphism classes of) the groups appearing as the Galois group of the Galois closure of K over $\mathbb{Q}$.

Proof. □

Exercise 6. Let $\mathbb{F}$ be a finite field with at least 3 elements. Show that $\mathrm{SL}_2(\mathbb{F})$ has order divisible by 12.

Proof. Let $|\mathbb{F}| = q$ a prime power greater than 2. Let us explicitly compute $|\mathrm{SL}_2(\mathbb{F})|$. Consider an arbitrary element of $M_2(\mathbb{F})$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

There are $q^2 - 1$ ways to choose $v_1 = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix}$ to be a non-zero vector. For any such choice, there are $q^2 - q$ ways to choose the column $v_2 \begin{bmatrix} a_{12} \\ a_{21} \end{bmatrix}$ to be non-colinear to the first column, so A has non-zero determinant. Fix any such v_1, v_2. Notice that since det is bilinear,

$$\{\det \begin{bmatrix} v_1 & av_2 \end{bmatrix} \mid a \in \mathbb{F}^\times\} = \mathbb{F}^\times$$

Therefore, among the $q^2 - q$ ways to choose the column v_2 so A has non-zero determinant, exactly $(q^2 - q)/|\mathbb{F}^\times| = (q^2 - q)/(q - 1) = q$ of those choices yield a matrix with determinant 1. Since all elements of $\mathrm{SL}_2(\mathbb{F})$ can be constructed uniquely in this way (picking $v_1 \neq 0$ and then picking v_2 to not be colinear),

$$|\mathrm{SL}_2(\mathbb{F})| = (q^2 - 1)q = q(q - 1)(q + 1)$$

Now let us show that $12|(q(q - 1)(q + 1))$. Since $(q - 1), q, (q + 1)$ are three colinear positive integers, exactly one of them is divisible by 3. If q is odd, then both $q - 1, q + 1$ are even and thus $12|(q - 1)q(q + 1)$. If q is even, then q is a power of 2 greater than or equal to 4 so $4|q$, so $12|(q - 1)q(q + 1)$. □

Exercise 7. Let G be a p-group and $1 \neq N \trianglelefteq G$ be a non-trivial normal subgroup.

(a) Show that N contains a non-trivial element of the center $Z(G)$ of G.

(b) Give an example where $Z(N) \not\subseteq Z(G)$

Proof. (a) Since $N \trianglelefteq G$, G acts on N by conjugation, say by $\psi : G \to \mathrm{Aut}_{\mathbf{Set}}(N)$ by $\psi(g)(n) = gng^{-1}$. By the orbit stabilizer theorem,

$$|N| = \sum_{n \in \mathrm{Orbit}(\psi)} [G : \mathrm{stab}_\psi(n)]$$

Since G is a p-group, $[G : \mathrm{stab}_\psi(n)]$ is either 1 or a power of p. And since N is a non-trivial subgroup of G, p divides the order of N. Thus taking mod$p$ of both sides, we have:

$$0 \equiv \sum_{n \in \psi\text{-stable}} 1 \bmod p$$

Thus, the number of ψ-stable elements in N is divisible by p. There is at least one ψ-stable element, the identity $e \in N$, so there is another non-identity $n \in N$ which is ψ stable. This means that $\psi(g)(n) = gng^{-1} = n$ for all $g \in G$, so $n \in Z(G)$ as desired.

(b) Let G be the quaternion group with 8 elements. Then $\langle i \rangle \cong \mathbb{Z}/4\mathbb{Z}$ is a normal subgroup of G, but $Z(N) = N \not\subseteq Z(G) = \{\pm 1\}$.

□

Exercise 8. Let R be a ring.

(a) Show that an R-module X is indecomposable if $\mathrm{End}_R(X)$ is local.

(b) Suppose that every finitely generated R-module M is isomorphic to $X_1 \oplus \cdots \oplus X_m$ with all $\mathrm{End}_R(X_i)$ local. Show that such a decomposition is unique up to isomorphism and permutation of terms.

(c) Given an example of an isomorphism $X_1 \oplus X_2 \cong Y_1 \oplus Y_2$ with $\mathrm{End}(X_i)$ and $\mathrm{End}(Y_i)$ local that is not the direct sum of any isomorphisms $X_i \cong Y_i$, even up to renumbering the Y_i.

Proof. (a) Suppose that $\mathrm{End}_R(X)$ is local and $X \cong M \oplus N$. Then, we have endomorphisms $\pi_1, \pi_2 \in \mathrm{End}_R(M \oplus N)$ by $\pi_1(m,n) = (m,0)$ and $\pi_2(m,n) = (0,n)$. Their sum $\pi_1 + \pi_2$ is the identity on $\mathrm{End}_R(M \oplus N)$. Since $\mathrm{End}_R(M \oplus N) \cong \mathrm{End}_R(X)$ is local, this implies that either π_1 or π_2 is invertible, since the sum of non-invertible elements in a local ring is non-invertible. Therefore, either $M = 0$ or $N = 0$.

(b) Suppose that

$$X_1 \oplus X_2 \oplus \cdots \oplus X_m \cong Y_1 \oplus Y_2 \oplus \cdots \oplus Y_n$$

for R-modules X_i, Y_j each with $\mathrm{End}_R(X_i)$, $\mathrm{End}_R(Y_i)$ local (and each X_i, Y_j non-zero). Let $\psi : \bigoplus_{i=1}^{n} X_i \to \bigoplus_{j=1}^{m} Y_j$ be an R-module isomorphism with two sided inverse φ. Since finite coproducts coincide with finite products in R-**Mod**, $\mathrm{Hom}_R(\bigoplus_{i=1}^{m} X_i, \bigoplus_{j=1}^{n} X_j) \cong \bigoplus_{i=1,j=1}^{m,n} \mathrm{Hom}_R(X_i, Y_j)$. Let $\psi_{ab} : X_a \to Y_b$ and $\varphi_{ba} : Y_b \to X_a$ be the corresponding maps under this identification (which can be concretely defined as $X_a \hookrightarrow \bigoplus_{i=1}^{m} X_i \xrightarrow{\psi} \bigoplus_{j=1}^{n} Y_j \twoheadrightarrow Y_b$). Thus, ψ is of the form

$$\begin{bmatrix} \psi_{11} & \dots & \psi_{1m} \\ \vdots & & \vdots \\ \psi_{n1} & \dots & \psi_{nm} \end{bmatrix}$$

and similarly for φ. Therefore, since $\varphi \circ \psi = \mathrm{id}_{\bigoplus X_i}$, for all $1 \le a \le m$, we have

$$\varphi_{a1}\psi_{1a} + \varphi_{a2}\psi_{2a} + \cdots + \varphi_{an}\psi_{na} = \mathrm{id}_{X_a}$$

Similarly, for all $1 \le b \le n$,

$$\psi_{b1}\varphi_{1b} + \psi_{b2}\varphi_{2b} + \cdots + \psi_{bm}\varphi_{mb} = \mathrm{id}_{Y_b}$$

Since End_{X_a} is local, at least one of the $\varphi_{aj}\psi_{ja}$ is invertible since their sum is. After relabelling, we can assume without loss of generality that $\psi_{11} \circ \varphi_{11} = \mathrm{id}_{X_1}$. Therefore, this implies that the there is a retraction of the following short exact sequence and therefore it splits:

$$\begin{tikzcd} 0 \arrow[r] & X_1 \arrow[r, hook, "\psi_{11}"] & Y_1 \arrow[r] \arrow[l, bend left, "\varphi_{11}"] & \operatorname{coker}\psi_{11} \arrow[r] & 0 \end{tikzcd}$$

Thus, X_1 is a direct summand of Y_1 so by part (a) we have that ψ_{11} is an isomorphism. Since ψ_{11} is invertible, after performing row and column reductions (i.e., composing with automorphisms of $X_1 \oplus \cdots \oplus X_n$, $Y_1 \oplus \cdots \oplus Y_n$), we have that there are isomorphisms $\rho_1 : X_1 \oplus \cdots \oplus X_n \to X_1 \oplus \cdots \oplus X_n$, $\rho_2 : Y_1 \oplus \cdots \oplus Y_n \to Y_1 \oplus \cdots \oplus Y_n$ such that:

$$\rho_2 \circ \psi \circ \rho_1 = \begin{bmatrix} \psi_{11} & \begin{bmatrix} 0 & \dots & 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} & A \end{bmatrix}$$

for an isomorphism $A : X_2 \oplus \cdots \oplus X_n \to Y_1 \oplus \cdots \oplus Y_n$. Therefore by induction, we have that the set of X_i are isomorphic pairwise with the set of Y_j.

(c) Let $R = \mathbb{Q}$ and $X_1 = X_2 = Y_1 = Y_2 = \mathbb{Q}$ as left $\mathbb{Q}$-modules in the natural way. Then, define $\psi : X_1 \oplus X_2 \to Y_1 \oplus Y_2$ by $\psi(a, b) = (a, a + b)$. Also notice that $\operatorname{End}_R(X_i) = \operatorname{End}_R(Y_j) = \mathbb{Q}$ which is a field and thus local. Furthermore, for any $\rho_1 : X_1 \to Y_1, \rho_2 : X_2 \to Y_2$ $\mathbb{Q}$-module isomorphisms (i.e., multiplication by an element of $\mathbb{Q}$), it is clear that $\psi \neq \rho_1 \oplus \rho_2$. By symmetry, this will not change if we permute Y_1, Y_2.

□

Exercise 9. Let R be a commutative ring and $S \subset R$ a multiplicative subset. Construct a natural transformation (in either direction) between the functors $\operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ and $S^{-1}\operatorname{Hom}_R(M, N)$, considered as functors of R-modules M and N, and prove it is an isomorphism if M is finitely presented.

Proof. Let us define a natural transformation $\alpha : S^{-1}\operatorname{Hom}_R(-,-) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}-, S^{-1}-)$. The data of such a natural transformation is for every R-module pair M, N, an R-module homomorphism $\alpha_{MN} : S^{-1}\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$. Notice that there is a natural R-module homomorphism $\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ by the functoriality of the tensor product (and recalling that $S^{-1}M \cong S^{-1}R \otimes_R M$). Furthermore, S acts invertibly on the R-module $\operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ since this is naturally an $S^{-1}R$ module, so by the universal property of localization there is an induced homomorphism from $S^{-1}\operatorname{Hom}_R(M, N)$.

$$\begin{tikzcd}
S^{-1}\operatorname{Hom}_R(M,N) \arrow[dr, dashed, "\alpha_{MN}"] & \\
\operatorname{Hom}_R(M,N) \arrow[u, "\eta"] \arrow[r, "S^{-1}R\otimes_R"] & \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)
\end{tikzcd}$$

Thus, as the diagram suggests, define α_{MN} to be this induced R-module homomorphism. Now let us argue that α is natural in M, N. First notice that the natural transformation $\beta : \operatorname{Hom}_R(-,-) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}-, S^{-1}-)$ is natural by the functoriality of the tensor product. But since $\eta : R\text{-}\mathbf{Mod} \to S^{-1}R\text{-}\mathbf{Mod}$ by $M \to S^{-1}M$ is essentially surjective and full, and $\alpha\eta = \beta$ by definition, the naturality of α is induced from the naturality of β.

Now let us show that if M is finitely presented, α_{MN} is an isomorphism (for all N). Since M is finitely presented, there is a short exact sequence:

$$0 \to R^k \to R^m \to M \to 0 \tag{4}$$

Tensoring with $S^{-1}R$ is exact, so we have an exact sequence:

$$0 \to S^{-1}R^k \to S^{-1}R^m \to S^{-1}M \to 0$$

and taking $\operatorname{Hom}_{S^{-1}R}(-, S^{-1}N)$ we have an exact sequence of $S^{-1}R$-modules, which can be treated as an exact sequence of R modules by restriction of scalars:

$$0 \to 0 \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \to (S^{-1}N)^n \to (S^{-1}N)^k$$

If we apply the left exact functor $S^{-1}\operatorname{Hom}_R(-, N)$ to equation 4, we instead have:

$$0 \to 0 \to S^{-1}\operatorname{Hom}_R(M, N) \to (S^{-1}N)^n \to (S^{-1}N)^k$$

Thus, let us show the following diagram is commutative and then by the 5 lemma we are done:

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & S^{-1}\operatorname{Hom}_R(M,N) \arrow[r] \arrow[d, "\alpha_{MN}"] & (S^{-1}N)^n \arrow[r] \arrow[d, "\mathrm{id}"] & (S^{-1}N)^k \arrow[d, "\mathrm{id}"] \\
0 \arrow[r] & 0 \arrow[r] & \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \arrow[r] & (S^{-1}N)^n \arrow[r] & (S^{-1}N)^k
\end{tikzcd}$$

This is a routine check. □

Exercise 10. Let R be a commutative ring and M a left R-module. Let $f : M \to M$ be a surjective R-linear endomorphism. [Hint: let $R[x]$ act on M via f]

(a) Suppose that M is finitely generated. Show that f is an isomorphism and that f^{-1} can be described as a polynomial in f.

(b) Show that this fails if M is not finitely generated.

Proof. (a) M is naturally an $R[x]$ module by letting x act by f. Furthermore, since M is finitely generated over R, it is finitely generated over $R[x]$. Let $I = (x)$ be the principal ideal generated by x. Since $f \cdot M = M$, $I \cdot M = M$. Therefore by Nakayama's lemma, there exists $p \in I$ such that $p \cdot m = m$ for all $m \in M$. Since $p \in I$, p is of the form $p(x) = xq(x)$ for some q. Then it follows that $f^{-1} = q(f)$, since for all $m \in M$,

$$q(f)f(m) = p(x) \cdot m = m$$

and $q(f) \circ f = f \circ q(f)$.

(b) Let $R = \mathbb{Z}$ and let $M = \bigsqcup_{\mathbb{Z}^+} \mathbb{Z}$. Then let $f : M \to M$ by $f(e_i) = f(e_{i-1})$ for $i \geq 2$ and $f(e_1) = 0$. Notice that this definition induces a unique $\mathbb{Z}$-linear endomorphism $M \to M$ by the universal property of the coproduct, so f uniquely exists as defined. Furthermore, $e_1, e_2, \ldots,$ are in the image of f, so f is surjective since $e_1, e_2, \ldots,$ form a $\mathbb{Z}$ generating set for M. However, f is not an isomorphism since f has non-zero kernel.

□

Fall 2019

Exercise 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?

Proof. Let G be a group of order 315 and let n_3, n_5, n_7 be the number of 3-Sylows, 5-Sylows, 7-Sylows respectively. By the Sylow theorems and some basic arithmetic, $n_3 \in \{1, 7\}, n_5 \in \{1, 21\}, n_7 \in \{1, 15\}$. Let H_3 be a 3-Sylow of G. Since the number of 3-Sylows is either 1 or 7 and G acts transitively on the 3-Sylows by conjugation, $K = N_G(H_3)$ is either order 315 or $315/7 = 45$ by the orbit stabilizer theorem. In either case, K contains a 5-Sylow H_5 which is also a 5-Sylow of G. Since H_5 normalizes H_3, $H_5H_3 < G$ is a subgroup of G of order 45. Let us show as a lemma that every group of order 45 is Abelian so H_5, H_3 commute.

Lemma: Let H be a group of order 45. Then H is Abelian.
The number of 5-Sylows in H is equal to 1 by the Sylow theorems, since both $3, 9$ are not congruent to 1 mod 5. Therefore, $H \cong \mathbb{Z}/5 \rtimes L$ for L a group of order 9. Since $\text{Aut}(\mathbb{Z}/5) \cong \mathbb{Z}/4$, there are no non-trivial group homomorphisms $L \to \mathbb{Z}/4$ since there are no subgroups of L of even order. Therefore, $H \cong \mathbb{Z}/5 \times L$. Furthermore, any group L of order 9 is Abelian since L has non-trivial center, so $H = \mathbb{Z}/5 \times L$ is Abelian.

Therefore, H_5, H_3 commute, so $H_3 < N_G(H_5)$. If $n_5 = 21$, then by the orbit stabilizer theorem with respect to the action of G on the set of 5-Sylows we must have $|N_G(H_5)| = 315/21 = 15$. However since $H_3 < N_G(H_5)$, we must have $9 = |H_3|$ dividing $|N_G(H_5)|$. Therefore, $n_5 = 1$. Let H_7 be a 7-Sylow of G. Since $n_5 = 1$, H_7 normalizes H_5, so $H_5H_7 < G$ is a subgroup of order 35. Every group of order 35 is Abelian so H_5 normalizes H_7. If $n_7 = 15$, then we have $N_G(H_7) = 315/15 = 21$ which 5 does not divide, which is impossible. Thus, $n_7 = 1$.

Since $n_7 = 1$, $H_7 \trianglelefteq G$, so $N = H_7H_3$ is a subgroup of G. Also since H_5 commutes with H_7 and H_3, H_5 commutes with N. Therefore NH_5 is a subgroup of G of order 315 and is thus equal to G. Furthermore, $N \cap H_5 = \{e\}$ by order considerations. Therefore, $G \cong N \times H_5$. Furthermore since $H_7 \trianglelefteq G$, $H_7 \trianglelefteq N$, so $N \cong H_7 \rtimes H_3$ for a 3-Sylow H_3. The only groups of order 9 are $\mathbb{Z}/9$ and $\mathbb{Z}/3 \times \mathbb{Z}/3$, and $\text{Aut}(\mathbb{Z}/7) \cong \mathbb{Z}/6$. Thus, there are 4 groups of order 63 up to isomorphism:

$$\mathbb{Z}/7 \times \mathbb{Z}/9 \qquad \mathbb{Z}/7 \rtimes \mathbb{Z}/9 \qquad \mathbb{Z}/7 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \qquad \mathbb{Z}/7 \rtimes \mathbb{Z}/3 \times \mathbb{Z}/3$$

Where the above semidirect products are with respect to the non-trivial automorphism - i.e., defined by $\mathbb{Z}/9 \to \mathbb{Z}/6$ by $1 \mapsto 2$ and $\mathbb{Z}/3 \times \mathbb{Z}/3 \to \mathbb{Z}/6$ by $(1, 0) \mapsto 2$. Any other choice of group homomorphism yields an isomorphic semidirect product. □

Exercise 2. Let L be a finite Galois extension of a field K inside an algebraic closure $\overline{K}$ of K. Let M be a finite extension of K. Show that the following are equivalent:

(a) $L \cap M = K$.

(b) $[LM : K] = [L : K][M : K]$

(c) every K-linearly independent subset of L is M linearly independent.

Proof. Since L is a finite Galois extension of K, L is a finite simple extension, so $L = K(x)$ for some x with minimal polynomial $p(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ which splits in L, and $ML = M(x)$.

(a) ⇒ (b) We have:

$$[M(x) : K] = [M(x) : M][M : K]$$

Thus it suffices to show that the minimal polynomial of x over M is still p. Let $q \in M[T]$ be the (monic) minimal polynomial for x, so $q(T) = T^m + b_{n-1}T^{m-1} + \cdots + b_0$ for some $b_{n-1}, \dots, b_0 \in M$. Since p splits in L, all of the coefficients $b_{n-1}, \dots, b_0$ are in L. Since $L \cap M = K$, we thus must have $b_{n-1}, \dots, b_0 \in K$. Thus, $q \in K[T]$, so $q = p$ by the uniqueness of minimal polynomials. Thus, $[M(x) : M] = [L : K]$.

(b) ⇒ (c) Let $S = \{r_1, \dots, r_k\}$ be a K-linearly independent subset of L so $k \leq n$. Notice that $\{1, \dots, x^{n-1}\}$ forms a K basis for $L = K(x)$ and $\{1, \dots, x^{n-1}\}$ forms an M basis for $M(x)$ since $[M(x) : M] = [K(x) : K]$ which follows from

$$[M(x) : M][M : K] = [M(x) : K] = [K(x) : K][M : K]$$

and the fact that $[M : K]$ is finite. S can be extended to a K basis $r_1, \dots, r_k, r_{k+1}, \dots, r_n$ of L. Then, $\{1, x, \dots, x^{n-1}\} \subset \langle r_1, \dots, r_n \rangle_K \subset \langle r_1, \dots, r_n \rangle_M$. Thus, $\{r_1, \dots, r_{n-1}\}$ spans $M(x) = ML$ as an M-vector space, and since $\dim_M M(x) = n$, $r_1, \dots, r_n$ is an M basis of $M(x)$. Therefore, $r_1, \dots, r_k$ are M-linearly independent.

(c) ⇒ (a) Let $a \in L \setminus K$. Then $\{1, a\}$ is linearly independent over K since $a \notin K$. Thus by assumption $\{1, a\}$ is M linearly independent over M so $a \notin M$. Thus $(L \setminus K) \cap M = \emptyset$.

□

Exercise 3. Let I be the ideal $(x^2 - y^2 + z^2, (xy + 1)^2 - z, z^3)$ of $R = \mathbb{C}[x, y, z]$. Find the maximal ideals of R/I, as well as all of the points on the variety

$$V(I) = \{(a, b, c) \in \mathbb{C}^3 \mid f(a, b, c) = 0 \text{ for all } f \in I\}$$

Proof. The maximal ideals of R/I are in correspondence with the maximal ideals of R containing I. Furthermore by the Nullstellensatz, the maximal ideals of R are in correspondence with the points of the variety $V(I)$. Thus, let us compute $V(I)$. Let $a, b, c \in \mathbb{C}$. Then $(a, b, c) \in I$ if and only if $f(a, b, c) = 0$ for all $f \in I$. Thus, $(a, b, c) \in I$ if and only if $c^3 = 0$, $a^2 - b^2 + c^2 = 0, (ab+1)^2 - c^2 = 0$. Since $c^3 = 0$ implies $c = 0$, this simplifies to the equations $c = 0, a^2 - b^2 = 0, ab = -1$. Since $a^2 - b^2 = 0$, either $a = -b$ or $a = b$. Thus, the equations split into two possibilities:

$$c = 0, a = b, a^2 = -1 \qquad\qquad c = 0, b = -a, a^2 = 1$$

In the first case, the only solutions in $\mathbb{C}^3$ are $(0, i, i)$ and $(0, -i, -i)$, and in the second case the only solutions are $(0, 1, -1)$ and $(0, -1, 1)$. Thus, $V(I)$ is the set of these 4 points, and the maximal ideals of R/I are in correspondence by $(a, b, c) \mapsto (x - a, y - b, z - c)$. □

Exercise 4. Find all isomorphism classes of simple (i.e., irreducible) left modules over the ring $M_n(\mathbb{Z})$ of n-by-n matrices with $\mathbb{Z}$-entries with $n \geq 1$.

Proof. Notice that a module being simple is an additive categorical property, in the sense that a module $M \in R$-**Mod** is simple if and only if every every homomorphism $N \to M$ is either an epimorphism or the zero map. By Morita equivalence, $M_n(\mathbb{Z})$-**Mod** $\cong \mathbb{Z}$-**Mod**. In particular, there is an equivalence of categories $\mathbb{Z}$-**Mod** $\xrightarrow{F}$ $M_n(\mathbb{Z})$-**Mod** by $F(-) = \mathbb{Z}^n \otimes_{\mathbb{Z}} -$ where $\mathbb{Z}^n$ has a natural $M_n(\mathbb{Z})$ left module structure. The simple modules of $\mathbb{Z}$ are all of the form $\mathbb{Z}/\mathfrak{m}$ for $\mathfrak{m}$ a maximal left module of $\mathbb{Z}$ and thus of the form $\mathbb{Z}/p\mathbb{Z}$ for p a prime. Therefore since F is an equivalence of additive categories, $F(\mathbb{Z}/p\mathbb{Z})$ is simple in $M_n(\mathbb{Z})$-**Mod** for all primes p and since F is essentially surjective every simple $M_n(\mathbb{Z})$-module is isomorphic to $F(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^n$ for some prime p. □

Exercise 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.

Proof. By the tensor-hom adjunction, t_B has a right adjoint by $\mathrm{Hom}_R(B, -)$. Since left adoints preserve colimits, t_B thus preserves colimits. For any R-module B, let B be an R-module which is not finitely generated - i.e., $B = R^{\mathbb{N}}$. If $\otimes_R B$ preserved limits, then the following natural map would be an isomorphism:

$$B \otimes \prod_{b \in B} R \xrightarrow{\varphi} \prod_{b \in B} B \qquad b \otimes (r_c)_{c \in B} \mapsto \Big(br_c\Big)_{c \in B}$$

Let $\iota \in \prod_{b \in B} B = B^B$ be the element $(b)_{b \in B}$ which represents the identity element of B^B. If φ were an isomorphism, then it would be surjective so there would exist some $b_1, \ldots, b_n \in B$ and $(r^1_c)_{c \in B}, \ldots, (r^n_c)_{c \in B}$ such that $\varphi(b_1 \otimes r^1 + \cdots + b_n \otimes r^n) = \iota$. If this equality were true, we would have

$$\varphi(b_1 \otimes r^1 + \cdots + b_n \otimes r^n) = \sum_{i=1}^{n} \varphi(b_i \otimes r^i) = \Big(\sum_{i=1}^{n} b_i r^i_c\Big)_{c \in B} = \Big(c\Big)_{c \in B}$$

In particular, B would be finitely generated as an R module by $b_1, \ldots, b_n$, which is a contradiction. □

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

Proof. Let $\langle\ ,\ \rangle : (\mathbb{R}^2 \times \mathbb{R}^2) \to \mathbb{R}$ be the usual inner product by dot products and let $H < \mathrm{GL}(2, \mathbb{R})$ be a finite group. Define a new inner product $\langle\ ,\ \rangle_H : (\mathbb{R}^2 \times \mathbb{R}^2) \to \mathbb{R}$ by

$$\langle u, v \rangle_H = \frac{1}{|H|} \sum_{A \in H} \langle Au, Av \rangle$$

Since $\langle u, v \rangle_H$ is (a non-zero) $\mathbb{R}$-linear combination of $\mathbb{R}$-inner products on $\mathbb{R}$ (and since each A is $\mathbb{R}$-linear), $\langle\ ,\ \rangle_H$ is in fact an inner product on $\mathbb{R}^2$. With respect to this inner product, every element of H is orthogonal since for all $B \in H$,

$$\langle Bu, Bv \rangle_H = \frac{1}{|H|} \sum_{A \in H} \langle ABu, ABv \rangle = \frac{1}{|H|} \sum_{A \in H} \langle Au, Av \rangle = \langle u, v \rangle_H$$

Since every inner product on $\mathbb{R}^2$ is isomorphic by a change of basis so up to conjugacy we may assume that $H < O(2, \mathbb{R})$. Since every element of H is finite order, each element of H has determinant ± 1. Let $N = \det^{-1}(1) \cap H$, which is a normal subgroup of H since $\det|_H : H \to \{\pm 1\}$ is a group homomorphism. Therefore, N is a finite subgroup of $SO_2(\mathbb{R}) \cong S^1$ with the usual multiplicative structure on S^1 as a subset of $\mathbb{C}^\times$. In particular, it is clear that any finite subgroup of S^1 is cyclic since it is generated by $e^{2\pi i/n}$ for n minimal. Thus, $N \cong \mathbb{Z}/n\mathbb{Z}$ for some n. Thus, either $H \cong \mathbb{Z}/n\mathbb{Z}$, or H contains $N = \mathbb{Z}/n\mathbb{Z}$ as an index 2 subgroup. In the latter case since every element in $O_2(\mathbb{R})$ with determinant -1 is a reflection, $H \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = D_n$. Thus, the finite subgroups of $\mathrm{GL}(2, \mathbb{R})$ are $\mathbb{Z}/n\mathbb{Z}$ (as a subgroup of $SO_2(\mathbb{R}) \cong S^1$) or D_n (as a subgroup $O_2(\mathbb{R})$) up to conjugacy. □

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

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

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.

Proof. Notice that $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\psi \mathbb{Z}/4\mathbb{Z}$ with $\psi(1) = (a \mapsto 2a)$. Thus, $G = \{1, h, h^2, g, hg, h^2g, g^2, hg^2, h^2g^2, g^3, hg^3, h^2g^3\}$. Notice that $\{h, h^2\}$ is a conjugacy class of G since $ghg^{-1} = h^2$ and $xhx^{-1} \in \{h, h^2\}$ for all $x \in G$ by casework. Similarly, we compute the other conjugacy classes of G, so the following is the character table of G:

$\{1\}$	$\{h, h^2\}$	$\{g, hg, h^2g\}$	$\{g^2\}$	$\{hg^2, h^2g^2\}$	$\{g^3, hg^3, h^2g^3\}$

First let us find the one dimensional representations of G. Thus, let us compute $[G, G]$. Notice that $h = ghg^{-1}h^{-1} \in [G, G]$, so $[G, G] \supset \langle h \rangle$. Furthermore, there is a group homomorphism $\mathbb{Z}/3\mathbb{Z} \rtimes_\psi \mathbb{Z}/4\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/4\mathbb{Z}$ by projection onto the second coordinate, and since $\mathbb{Z}/4\mathbb{Z}$ is abelian, φ factors through $[G, G]$. Since $\ker \varphi = \mathbb{Z}/3\mathbb{Z}$, $[G, G] \subset \langle h \rangle$. Thus, $[G, G] = \langle h \rangle$, so $G/[G, G] = \mathbb{Z}/4\mathbb{Z}$. Thus, the one dimensional representations are given by the group homomorphisms $\mathbb{Z}/4\mathbb{Z} \to \mathbb{C}^\times$:

$\{1\}$	$\{h, h^2\}$	$\{g, hg, h^2g\}$	$\{g^2\}$	$\{hg^2, h^2g^2\}$	$\{g^3, hg^3, h^2g^3\}$
1	1	1	1	1	1
1	1	i	-1	-1	$-i$
1	1	-1	1	1	-1
1	1	$-i$	-1	-1	i

Let a, b be the dimensions of the last two representations. We must have $a^2 + b^2 + 4 = 12$ and a, b positive integers, so $a = b = 2$. Also by column orthogonality, in each conjugacy class C with 3 elements and $x \in C$, we must have

$$\sum_{i=1}^{6} \chi_i(x) = \frac{|G|}{|C|} = 4$$

for $\chi_1, \ldots, \chi_6$ the irreducible representations of G. Therefore, the remaining two rows must have 0 in these columns. Notice that tensoring an irreducible representation with a one dimensional representation preserves irreducibility. Let χ_5, χ_6 be the two dimensional irreducible representations. By column orthogonality, at least one of $\chi_5(g^2), \chi_6(g^2)$ is non-zero. Without loss of generality, assume $\chi_5(g^2) = a \neq 0$. Thus, $\chi_3 \otimes \chi_5(g^2) = \chi_3(g^2) \cdot \chi_5(g^2) = -a$ is a differerent two dimensional irreducible representation of G, and is thus equal to χ_6. Thus, $\chi_5 \otimes \chi_3 = \chi_6$, so the last two rows of the character table are of the form $2|a|0|b|c|0$ and $2|a|0|-b|-c|0$. Finally by column orthogonality between columns 1 and 2 we must have $a = -1$, and by similar logic we find that $b = \pm 2$ and $c = \pm 1$, so the character table is:

$\{1\}$	$\{h, h^2\}$	$\{g, hg, h^2 g\}$	$\{g^2\}$	$\{hg^2, h^2 g^2\}$	$\{g^3, hg^3, h^2 g^3\}$
1	1	1	1	1	1
1	1	i	-1	-1	$-i$
1	1	-1	1	1	-1
1	1	$-i$	-1	-1	i
2	-1	0	2	-1	0
2	-1	0	-2	1	0

□

Exercise 8. Let M be a finitely generated module over an integral domain R. Show that there is a nonzero element $u \in R$ such that the localization $M[1/u]$ is a free module over $R[1/u]$.

Proof. Let $K = \text{Frac}(R)$ and let $S = R \setminus \{0\}$ so $K = S^{-1}R$. Since M is finitely generated over R, $S^{-1}M$ is finitely generated over K and is thus a finite dimensional K vector space. Thus, there is an isomorphism

$$K^n \xrightarrow{\tilde{\varphi}} S^{-1}M \qquad \tilde{\varphi}\left(\begin{bmatrix} k_1 \\ \vdots \\ k_n \end{bmatrix} \right) = k_1 \frac{m_1}{a_1} + \cdots + k_n \frac{m_n}{a_n}$$

for some $n \in \mathbb{N}$ and $m_1, \ldots, m_n \in M$, $a_1, \ldots, a_n \in R \setminus \{0\}$. Let $u = a_1 a_2 \ldots a_n$. Then define $\varphi : R[1/u]^n \to M[1/u]$ by $\varphi = \begin{bmatrix} \frac{m_1}{a_1} & \cdots & \frac{m_n}{a_n} \end{bmatrix}$, so φ is just the restriction of $\tilde{\varphi}$ to $R[1/u]^n \subset K^n$, which is well defined since $\frac{m_i}{a_i} \in M[1/u]$ for each i. Since φ is a restriction of $\tilde{\varphi}$ and $\tilde{\varphi}$ is an isomorphism, φ has trivial kernel. Thus, we have a short exact sequence

$$0 \longrightarrow R[1/u]^n \xrightarrow{\varphi} M[1/u] \longrightarrow \operatorname{coker} \varphi \longrightarrow 0$$

Since M is finitely generated over R, $M[1/u]$ is finitely generated over $R[1/u]$, so $\operatorname{coker} \varphi$ is also finitely generated over $R[1/u]$. Thus, let $x_1, \ldots, x_m \in \operatorname{coker} \varphi$ generate $\operatorname{coker} \varphi$ as an $R[1/u]$ module. By exactness of localization and since $\tilde{\varphi}$ is an isomorphism, $S^{-1} \operatorname{coker} \varphi = 0$. Therefore, $\operatorname{coker} \varphi$ is torsion, since for all $x \in \operatorname{coker} \varphi$, $\frac{x}{1} = 0$ in $S^{-1} \operatorname{coker} \varphi$ implies there is some $a \in R \setminus \{0\}$ such that $ax = 0$. In particular, there exists $a_1, \ldots, a_m \in R \setminus \{0\}$ such that $a_1 x_1 = 0, a_2 x_2 = 0, \ldots, a_m x_m = 0$. Let $v = a_1 \ldots a_m$. Then $\operatorname{coker} \varphi[1/v] = 0$. Therefore by exactness of localization (and that $R[1/u][1/v] = R[1/(uv)]$), we have the following exact sequence:

$$0 \longrightarrow R[1/(uv)]^n \xrightarrow{\varphi'} M[1/(uv)] \longrightarrow 0$$

Thus, $M[1/(uv)]$ is free over $R[1/(uv)]$ as desired. □

Exercise 9. Let A be a unique factorization domain which is a $\mathbb{Q}$-algebra. Let K be the fraction field of A. Let L be a quadratic extension field of K. Show that the integral closure of A in L is a finitely generated free A-module.

Exercise 10. Compute the Galois groups of the Galois closures of the following field extensions:

(a) $\mathbb{C}(x)/\mathbb{C}(x^4+1)$

(b) $\mathbb{C}(x)/\mathbb{C}(x^4+x^2+1)$.

where $\mathbb{C}(y)$ denotes the field of rational functions over $\mathbb{C}$ in a variable y.

Proof. (a) Let y be a formal variable (representing x^4+1) and let $F=\mathbb{C}(y)$. Then let $K=F[T]/(T^4+1-y)$. Let us find the Galois closure of K over F and $\mathrm{Gal}(K/F)$. Consider the polynomial $T^4+1-y\in F[T]$, and notice that $F=\mathrm{Frac}\mathbb{C}[y]$. Therefore by Gauss' lemma, the polynomial T^4+1-y is irreducible in $F[T]$ if and only if it is irreducible in $\mathbb{C}[y]$. Furthermore, T^4+1-y is irreducible in $\mathbb{C}[y]$ by Eisenstein and $1-y$ being a prime. Therefore, $K=F[T]/(T^4+1-y)$ is a field of degree 4 over F. Furthermore since F has four distinct 4th roots of unity, for any root x of T^4+1-y in K, $ix,-x,-ix$ are also roots of T^4+1-y. Therefore, K is a splitting field for T^4+1-y, with splitting $(T-x)(T-ix)(T+x)(T+ix)$. Therefore (since the characteristic is zero, K/F is automatically separable), K/F is a Galois extension of degree 4. Furthermore, notice by the transitivity of the Galois group that there is a F-homomorphism $\sigma\in\mathrm{Aut}_F(K)$ such that $\sigma(x)=ix$. By linearity, we thus have $\sigma^2(x)=-x$ and $\sigma^4(x)=x$. Therefore, $\mathrm{Gal}(K/F)=\mathrm{Aut}_F(K)$ is an order 4 group with an element of order 4 and is thus congruent to $\boxed{\mathbb{Z}/4\mathbb{Z}}$

(b) Let y be a formal variable (representing x^4+x^2+1) and let $F=\mathbb{C}(y)$. Then let $K=F[T]/(T^4+T^2+1-y)$. By Gauss' lemma, to show T^4+T^2+1-y is irreducible over F it suffices to show it is irreducible as a polynomial in T over $\mathbb{C}[y]$. It is equivalent to show that the polynomial $y-T^4-T^2-1$ is irreducible as a polynomial in y over $\mathbb{C}[T]$, which is clear since it is linear. Thus, T^4+T^2+1-y is irreducible so K is a field of degree 4 over F. Let x represent a formal root of T^4+T^2+1-y in K. Notice that since $y=x^4+x^2+1$ and y is algebraically independent over $\mathbb{C}$, x is also algebraically independent over $\mathbb{C}$ in K. Therefore, there is a field homomorphism $\mathbb{C}(T)\xrightarrow{\varphi}K$ by $T\mapsto x$. Furthermore, F is in the image of φ since y is, so φ is surjective and thus $K\cong\mathbb{C}(x)$ with $y=x^4+x^2+1$. In K, the polynomial T^4+T^2+1-y factors as $(T-x)(T+x)(T^2+x^2+1)$. Let us show T^2+x^2+1 is irreducible in $K[T]$. Since $K\cong\mathbb{C}(x)$, by Gauss' lemma it suffices to show that T^2+x^2+1 is irreducible in $\mathbb{C}[x]$, which is true by Eisenstein. Therefore, K/F is not Galois, but letting $E=K[T]/(T^2+x^2+1)$, E/F is the splitting field of T^4+T^2+1-y and is thus Galois. Let $z\in E$ be a formal root of T^2+x^2+1 so $z^2=-x^2-1$. Notice that T^2+x^2+1 factors as $(T-z)(T+z)$ in E. Since E/F is Galois and degree 8, $\mathrm{Gal}(E/F)$ is an order 8 group. By the Galois correspondence, since K/F is not a normal extension $[E:K]=2$, $\mathrm{Gal}(E/F)$ is not Abelian contains a non-normal subgroup of order 2. The only order 8 subgroup with a non-normal subgroup of order 2 is D_4, so $\mathrm{Gal}(E/F)\cong D_4$.

□

Spring 2019

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

Proof. Let $1 \neq N \trianglelefteq G$ be a minimal normal subgroup. Notice that N cannot have any non-trivial characteristic subgroups. Therefore since $[N : N]$ char N, either $[N : N] = N$ or $[N : N] = 1$. Since G is solvable and thus so is N, $[N : N] = N$ is impossible, so $[N : N] = 1$. Therefore, N is Abelian.

Therefore by the classification of finite abelian groups,

$$N \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}$$

for primes $p_1, \ldots, p_r$ and positive integers $m_1, \ldots, m_r$. Let M be the set of elements in N of order p_1 (along with the identity). Let us show that M char N. Let $\psi : N \to N$ be an automorphism. Automorphisms preserve the order of elements, so $\psi(M) \subseteq M$. Furthermore, M is a subgroup since N is abelian. Therefore, M is characteristic, so either $M = 1$ or $M = N$. Since $(1, 0, \ldots, 0) \in M$, we cannot have $M = 1$, so $M = N$. Therefore, every element of N is order 1 or p_1, so N must be of the form $\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$. □

Exercise 2. An additive group (abelian group written additively) Q is called divisible if any equation $nx = y$ with $0 \neq n \in \mathbb{Z}$, $y \in Q$ has a solution $x \in Q$. Let Q be a divisible group and A is 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 $B \to Q$.

Proof. Let $A \xrightarrow{\varphi} Q$ be an abelian group homomorphism and $A \subset B$. Define the set S of ordered pairs (C, ψ) for C a ($\mathbb{Z}$)-submodule of B and $\psi : C \to Q$ an abelian group homomorphism such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, hook, "\iota"] & Q \\
C \arrow[ur, "\psi"] &
\end{tikzcd}$$

$$S := \{(C, \psi) \mid A \subseteq C \subseteq B \text{ a submodule and } \psi : C \to Q \text{ commuting with } \varphi\}$$

Give S a partial order by $(C, \psi) \preceq (C', \psi')$ if $C \subset C'$ and $\psi'|_C = \psi$. Consider a totally ordered chain in S:

$$(C_1, \psi_1) \preceq (C_2, \psi_2) \preceq \ldots$$

Then, notice that $C = \bigcup_{i=1}^{\infty} C_i$ is a $\mathbb{Z}$-submodule of B and we can define $\psi : C \to Q$ by $\psi(c) = \psi_i(c_i)$ for i the smallest index such that $c \in C_i$. This is an abelian group homomorphism since each ψ_i agrees on their shared domains. Therefore, (C, ψ) is maximal in this totally ordered subset. Thus by Zorn's Lemma, there is a maximal element (C, ψ) of S. Let us show that C is necessarily equal to B.

It suffices to show that for any $C \subsetneq B$ and $\psi : C \to Q$ commuting with φ that (C, ψ) is not maximal in S. Thus, take any such C, ψ and let $x \in B \setminus C$. Let us show that there exists $\psi' : C + x\mathbb{Z} \to Q$ which commutes with φ. We have a short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \ker \pi \arrow[r, hook] & C \oplus \mathbb{Z} \arrow[r, "\pi"] & C + x\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

Let $(a, n) \in \ker \pi$ such that $n \in \mathbb{Z}^+$ is minimal. If no such (a, n) exists, then $\ker \pi = 0$ since $(a, 0) \in \ker \pi$ implies $a = 0$. We claim that $\ker \pi = (a, n)\mathbb{Z}$. Let $(b, m) \in \ker \pi$. By $\mathbb{Z}$ division in the second coordinate, there exists $p, q \in \mathbb{Z}$ non-zero such that

$$p(a, n) + q(b, m) = (a', \gcd(m, n)) \in \ker \pi$$

for some $a' \in A$. By minimality of n, $\gcd(m, n) = n$. Therefore, $a' = a$ since $(a' - a, 0) \in \ker \pi$, so (b, m) is a $\mathbb{Z}$ multiple of (a, n) as desired. Since Q is divisible, there exists an element $y \in Q$ such that $ny = \psi(a)$. Define $\xi : C \oplus \mathbb{Z} \to Q$ by $(b, m) \mapsto (\psi(b) - my)$. Notice that $\xi((a, n)) = \psi(a) - ny = 0$. By the first isomorphism theorem, this map then factors through $C \oplus \mathbb{Z}/\ker \pi \cong C + x\mathbb{Z}$ as $\psi' : C + x\mathbb{Z} \to Q$, defined on C by ψ and on $x\mathbb{Z}$ by $\psi(x) = y$. Therefore, $(C, \psi) \preceq (C + x\mathbb{Z}, \psi')$, so (C, ψ) is not maximal. Therefore the only maximal element of S must be of the form (B, Ψ), so φ extends to a group homomorphism Ψ commuting with φ and the inclusion. □

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

Proof. Recall that we have a multiplicative function $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{N}$ by $N(a + b\sqrt{-d}) = a^2 + db^2$. Thus to show that 2 is irreducible, it suffices to show that every element of norm 1 in $\mathbb{Z}[\sqrt{-d}]$ is a unit and there are no elements of norm 2. First, suppose that $x = a + b\sqrt{-d}$ satisfies $N(x) = 1$. Then we must have $b = 0$ since $d > 2$, so $a = \pm 1$. Thus, $x = \pm 1$. Similarly if $N(x) = 2$, then $b = 0$ since $d > 2$, but there is no square root of 2 in $\mathbb{Z}$ so there are no elements of norm 2. Therefore, 2 is irreducible in $\mathbb{Z}[\sqrt{-d}]$.

Now let us show that the ideal (2) is not a prime ideal by finding elements $a, b \notin (2)$ such that $ab \in (2)$. First notice that

$$(2) = \left\{ a + b\sqrt{-d} \mid a, b \in 2\mathbb{Z} \right\}$$

Since $(2) = \{2x \mid x \in \mathbb{Z}[\sqrt{-d}]\}$.

Now we have two cases. If d is odd, then notice that

$$(1+\sqrt{-d})(1-\sqrt{-d}) = 1 + d^2 \in (2)$$

but $1 \pm \sqrt{-d} \notin (2)$. If d is even, then we have that

$$(2+\sqrt{-d})(2+\sqrt{-d}) = (4-d) + 4\sqrt{-d} \in (2)$$

but $2 \pm \sqrt{-d} \notin (2)$. Therefore, (2) is not a prime ideal in $\mathbb{Z}[\sqrt{-d}]$ as desired. □

Exercise 4. Let R be a commutative local ring and P a finitely generated projective R-module. Prove that P is free over R.

Proof. See Spring 2024 problem 5 (commutative not necessary). □

Exercise 5. Let π_n denote the nth cyclotomic polynomial in $\mathbb{Z}[x]$ and let a be a positive integer and p a positive prime not dividing n. Prove that if $p|\pi_n(a)$ in $\mathbb{Z}$, then $p \equiv 1 \bmod n$.

Proof. Let $n > 1$ an integer. Let us show that if p is a prime not dividing n and $p \not\equiv 1 \bmod n$, then $\pi_n(x)$ has no roots in $\mathbb{Z}/p[x]$. This will imply that if a prime q not dividing n satisfies $q|\pi_n(a)$ for some $a \in \mathbb{Z}^+$, then a is a root of $\pi_n(x)$ in $\mathbb{Z}/q[x]$, so $q \equiv 1 \bmod n$, as desired.

Thus let p prime, $p \nmid n$, and $p \not\equiv 1 \bmod n$. Notice that the polynomial $f(x) = x^{n(p-1)} - 1$ in $\mathbb{Z}/p[x]$ has no repeated roots since $f'(x) = n(p-1)x^{n(p-1)-1}$ and $f(x)$ have no shared roots (since $p \nmid n$). Therefore, f has exactly $p-1$ roots counted with multiplicity, since zero is not a root of f but each element of $\mathbb{Z}/p^\times$ is a root of f by Fermat's little theorem. Notice that

$$f(x) = (x^{p-1} - 1)(x^{(p-1)(n-1)} + x^{(p-1)(n-2)} + \cdots + x^{p-1} + 1)$$

And $x^{p-1} - 1$ has exactly $p-1$ roots, so $g(x) = (x^{(p-1)(n-1)} + x^{(p-1)(n-2)} + \cdots + x^{p-1} + 1)$ has no roots in $\mathbb{Z}/p[x]$. Furthermore since $x^m - 1 = \prod_{d|m} \pi_d(x)$ for all m, we have:

$$\prod_{d|(p-1)n} \pi_d = f(x) = (x^{p-1} - 1)(x^{(p-1)(n-1)} + x^{(p-1)(n-2)} + \cdots + x^{p-1} + 1) = \prod_{d|(p-1)} \pi_d \prod_{d|(p-1)n, d\nmid(p-1)} \pi_d$$

Since $p \not\equiv 1 \bmod n$ by assumption, n does not divide $p-1$. Therefore since π_n appears a single time in the above product of $x^{n(p-1)}$, $\pi_n(x)$ divides $g(x)$. But we already observed that $g(x)$ has no roots in $\mathbb{Z}/p[x]$, so $\pi_n(x)$ has no roots in $\mathbb{Z}/p[x]$, as desired. □

Exercise 6. Let $\mathbb{F}$ be a field of characteristic $p > 0$ and $a \in \mathbb{F}^\times$. Prove that if the polynomial $f = x^p - a$ has no root in $\mathbb{F}$, then f is irreducible over $\mathbb{F}$.

Proof. Suppose that $f = x^p - a$ has no root in $\mathbb{F}$. Let $\mathbb{F}[\alpha] = \mathbb{F}[x]/(x^p - a)$ be a field extension of $\mathbb{F}$ with a root α of f. Notice that in $\mathbb{F}[\alpha]$, f splits as:

$$f(x) = x^p - a = (x - \alpha)^p$$

Therefore, if f were to factor nontrivially into monic polynomials as $f = g \cdot h$ in $\mathbb{F}[x]$, then $g(x) = (x-\alpha)^q$ in $\mathbb{F}[\alpha][x]$ and $h(x) = (x-\alpha)^{p-q}$ for some $0 < q < p$ by unique factorization. In particular, notice that q treated as an element of $\mathbb{F}$ is invertible. By binomial expansion we have:

$$g(x) = (x - \alpha)^q = x^q - q\alpha x^{q-1} + \cdots \pm \alpha^q$$

Thus if $g(x) \in \mathbb{F}[x]$, then $q\alpha \in \mathbb{F}$, so $\alpha \in \mathbb{F}$. This is a contradiction since f has no root in $\mathbb{F}$ by assumption. Therefore, f is irreducible over $\mathbb{F}$. □

Exercise 7. Let $\mathbb{F}$ be a field and let R be the ring of 3×3 matrices over $\mathbb{F}$ with $(3,1)$ and $(3,2)$ entry equal to 0. Thus,

$$R := \begin{bmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{bmatrix}$$

(a) Determine the Jacobson radical J of R.

(b) Is J a minimal left (respectively right) ideal?

Proof. (a) Recall that the Jacobson radical is the intersection of the maximal left ideals of R (equivalently, right ideals, equivalently, the set of elements $x \in R$ such that $\mathrm{id} - axb$ is invertible for all $a, b \in R$). First notice that $L = \begin{bmatrix} \mathbb{F} & \mathbb{F} & \mathbb{F} \\ \mathbb{F} & \mathbb{F} & \mathbb{F} \\ 0 & 0 & 0 \end{bmatrix}$ is a left ideal of R. Furthermore, it is maximal since any left ideal of R properly containing L contains a matrix with a non-zero entry in the lower rightmost corner, and since $\mathbb{F}$ is a field, thus contains all of R. Now let I be any left ideal of R not contained in L, and thus contains a matrix $A = \{a_{ij}\}$ with $a_{33} \neq 0$. Then letting $B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{1}{a_{33}} \end{bmatrix} \in R$, we have that $BA = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in I$. Then it is easy to see that

$$S = \begin{bmatrix} 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \end{bmatrix} \subset I$$

Now let us show that for each left ideal $J \subset M_2(\mathbb{F})$ that

$$\hat{J} := \begin{bmatrix} J & \begin{bmatrix}\mathbb{F}\\ \mathbb{F}\end{bmatrix} \\ \begin{bmatrix}0 & 0\end{bmatrix} & \mathbb{F} \end{bmatrix}$$

is a left ideal of R. $\hat{J}$ is clearly an additive subgroup of R. To show it is closed under left multiplication by R is a straighforward matrix computation: let $A \in M_2(\mathbb{F}), v \in \mathbb{F}^2, r \in \mathbb{F}$, $B \in J$, $w \in \mathbb{F}^2$, and $s \in \mathbb{F}$:

$$\begin{bmatrix} A & v \\ \begin{bmatrix}0 & 0\end{bmatrix} & r \end{bmatrix} \cdot \begin{bmatrix} B & w \\ \begin{bmatrix}0 & 0\end{bmatrix} & s \end{bmatrix} = \begin{bmatrix} AB & Aw + sv \\ \begin{bmatrix}0 & 0\end{bmatrix} & sr \end{bmatrix} \in \begin{bmatrix} J & \begin{bmatrix}\mathbb{F}\\ \mathbb{F}\end{bmatrix} \\ \begin{bmatrix}0 & 0\end{bmatrix} & \mathbb{F} \end{bmatrix}$$

Recall that the Jacobson radical of $M_2(\mathbb{F})$ is zero (for instance by explicitly identifying the maximal left ideals of $M_2(\mathbb{F})$ with matrices which vanish on a one dimensional space), so

$$J(R) \subset L \cap \begin{bmatrix} J(M_2(\mathbb{F})) & \begin{bmatrix}\mathbb{F}\\ \mathbb{F}\end{bmatrix} \\ \begin{bmatrix}0 & 0\end{bmatrix} & \mathbb{F} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \end{bmatrix}$$

But also notice that by our previous analysis that every maximal left ideal of R is either L or contains S. Thus, $J(R) \supset \begin{bmatrix} 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \end{bmatrix}$, so $J(R) = \begin{bmatrix} 0 & 0 & \mathbb{F} \\ 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \end{bmatrix}$.

(b) $J(R)$ is not a minimal right ideal since $\begin{bmatrix} 0 & 0 & \mathbb{F} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is a right ideal of R. $J(R)$ is a minimal left ideal since any non-zero left ideal $I \subset J(R)$, I contains a non-zero matrix $\begin{bmatrix} 0 & 0 & a \\ 0 & 0 & b \\ 0 & 0 & 0 \end{bmatrix}$, and then multiplying by $\begin{bmatrix} a^{-1} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 & 0 \\ a^{-1} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ on the left, or by $\begin{bmatrix} 0 & b^{-1} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 & 0 \\ 0 & b^{-1} & 0 \\ 0 & 0 & 0 \end{bmatrix}$ if $a = 0$, yields a basis for $J(R)$, so $I \supset J(R)$.

□

Exercise 8. Prove that every finite group of order n is isomorphic to a subgroup of $\mathrm{GL}_{n-1}(\mathbb{C})$.

Proof. Let G be a finite non-abelian group of order n. Let C be the number of conjugacy classes of G and let $V_1, \ldots, V_C$ be the irreducible $\mathbb{C}$ representations of G up to isomorphism. Let $V \cong \mathbb{C}^n$ be the regular representation of G: i.e., $V = \mathbb{C}^n$ with basis elements e_g indexed by the elements $g \in G$, and G acts on V by $h(e_g) = e_{hg}$. Let $\rho_V : G \to \mathrm{GL}(V)$ be the group homomorphism associated to the regular representation. Recall that as a G representation,

$$V \cong \bigoplus_{i=1}^{C} V_i^{\oplus \dim V_i}$$

Consider the representation W of G:

$$W = \bigoplus_{i=1}^{n} V_i$$

Let us show that the homomorphism $\rho_W : G \to \mathrm{GL}(W)$ is injective. Notice that $\rho_V : G \to \mathrm{GL}(V)$ is injective from the definition of the regular representation. Let $\rho_i : G \to \mathrm{GL}(V_i)$ be the group homomorphism of the G action on V_i. The kernel of ρ_V is the set of elements $g \in G$ which act trivially on V, i.e., the set of elements $g \in G$ which act trivially on each irreducible component V_i. Therefore,

$$0 = \ker \rho_V = \bigcap_{i=1}^{C} \bigcap_{j=1}^{\dim V_i} \ker \rho_i = \bigcap_{i=1}^{C} \ker \rho_i = \ker \rho_W$$

Therefore, $\ker \rho_W = 0$. Since G is nonabelian and $\sum_{i=1}^{C} (\dim V_i)^2 = n$, there is some $j \in [1, C]$ such that $\dim V_j > 1$. Therefore, $\dim W < n$. Therefore (since $W \cong \mathbb{C}^m$ for some $m < n$), we have an injective group homomorphism $\rho : G \to \mathrm{GL}(\mathbb{C}^m)$ for $m < n$, and thus we can compose with the inclusions $\mathrm{GL}(\mathbb{C}^m) \hookrightarrow \mathrm{GL}(\mathbb{C}^{n-1})$ to obtain an injective group homomorphism $\rho' : G \to \mathrm{GL}(\mathbb{C}^{n-1})$ as desired.

It remains to show that the statement holds for G abelian. By the classification of finite abelian groups,

$$G = \prod_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$$

for unique integers $a_1 | a_2 | \ldots | a_m$ each greater than 1. $\mathbb{Z}/a_i\mathbb{Z}$ embeds into $\mathrm{GL}(\mathbb{C})$ by $[1] \mapsto e^{2\pi i/a_i}$. Thus there is an injective group homomorphism of G into $\mathrm{GL}(\mathbb{C}^m)$. Since each $a_i > 1$ and $|G| = \prod_{i=1}^{m} a_i$, $m < n$, so by composing with the inclusion $\mathrm{GL}(\mathbb{C}^m) \to \mathrm{GL}(\mathbb{C}^{n-1})$, there is an injective group homomorphism of G into $\mathrm{GL}(\mathbb{C}^{n-1})$. □

Exercise 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 **CRing** be the category of commutative rings. Prove that the functor **CRing** $\to$ **Set** taking a commutative ring to R to the set of all pairs $(a, b) \in R^2$ such that $aR + bR = R$ is not representable.

Proof. (a) Let $R = \mathbb{Z}[x]$ and let $a = 2$, $b = x$. Notice that $R[1/a]$ consists of elements of the form $\frac{p(x)}{2^m}$ for $p \in \mathbb{Z}[x]$ and $m \in \mathbb{N}$, and similarly $R[1/b]$ consists of elements of the form $\frac{q(x)}{x^n}$. Since $\mathbb{Z}[x]$ is a UFD, if $\frac{p(x)}{2^m} = \frac{q(x)}{x^n}$, we must have 2^m divide $p(x)$ and x^n divide $q(x)$, i.e., after reducing, $x = n = 0$. Therefore, $\mathbb{Z}[x][1/a] \cap \mathbb{Z}[x][1/b] = \mathbb{Z}[x]$. However, $2\mathbb{Z}[x] + x\mathbb{Z}[x] \neq \mathbb{Z}[x]$.

(b) Let $F : \mathbf{CRing} \to \mathbf{Set}$ be the described functor on objects. It extends to a functor on morphisms by $F\varphi : FR \to FS$ with $F\varphi((a, b)) = (\varphi(a), \varphi(b))$ for $\varphi : R \to S$ a ring homomorphism. Suppose that F was representable, so there existed some $R \in \mathbf{CRing}$ and a natural isomorphism $\Phi : \mathrm{Hom}(R, -) \Rightarrow F(-)$. By the Yoneda lemma, natural transformations $\mathrm{Hom}(R, -) \Rightarrow F(-)$ are in a natural correspondence with elements of $F(R)$. Thus, take any $(a, b) \in F(R)$ (so $aR + bR = R$), and by the Yoneda lemma $\Phi : \mathrm{Hom}(R, -) \Rightarrow F(-)$ is defined by

$$\Phi_S : \mathrm{Hom}(R, S) \to F(S)$$

$$\Phi_S(\varphi) = F\varphi((a, b)) = (\varphi(a), \varphi(b))$$

Let us show that for any choice of (R, φ), Φ_S is not an isomorphism, so F is not representable. Assume for the sake of contradiction that Φ_S is bijective for all S. Then consider $\Phi_{\mathbb{Z}[x][1/2]} : \mathrm{Hom}(R, \mathbb{Z}[x][1/2]) \to F(\mathbb{Z}[x][1/2])$. Since 2 is invertible in $\mathbb{Z}[x][1/2]$, $2\mathbb{Z}[x][1/2] + x\mathbb{Z}[x][1/2] = \mathbb{Z}[x][1/2]$, so there is a unique ring homomorphism (by assumption of Φ an isomorphism) $\varphi_1 : R \to \mathbb{Z}[x][1/2]$ such that $\varphi_1(a) = 2, \varphi_1(b) = x$. Similarly, there is a unique ring homomorphism $\varphi_2 : R \to \mathbb{Z}[x][1/x]$ such that $\varphi_2(a) = 2, \varphi_2(b) = x$ since $(2, x) \in F(\mathbb{Z}[x][1/2])$. Additionally, there is a unique ring homomorphism $\varphi_3 : R \to \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Z}[x])$ such that $\varphi_3(a) = 2, \varphi_3(b) = x$. Furthermore, for the inclusions $\iota_1 : \mathbb{Z}[x][1/2] \hookrightarrow \mathbb{Q}(x)$ and $\iota_2 : \mathbb{Z}[x][1/x] \hookrightarrow \mathbb{Q}(x)$, we have $\iota_1 \circ \varphi_1$ agrees with φ_3 on a, b, and similarly for $\iota_2 \circ \varphi_2$. Therefore by uniqueness, $\iota_1 \circ \varphi_1 = \iota_2 \circ \varphi_2 = \varphi_3$. In particular,

$$\mathrm{Im}\varphi_3 = \Big(\mathrm{Im}(\iota_1 \circ \varphi_1) \cap \mathrm{Im}(\iota_2 \circ \varphi_2)\Big) \subset \Big(\mathbb{Z}[x][1/2] \cap \mathbb{Z}[x][1/x]\Big) = \mathbb{Z}[x]$$

$$\begin{tikzcd}
 & \mathbb{Z}[x][1/2] \arrow[dr, "\subseteq"] & & \\
R \arrow[ur, "\exists!\varphi_1"] \arrow[rr, "\exists!\varphi_3"] \arrow[dr, "\exists!\varphi_2"] \arrow[rrr, dashed, bend right=50, "\psi"'] & & \mathbb{Q}(x) & \mathbb{Z}[x] \arrow[l, hook', "\supseteq"'] \\
 & \mathbb{Z}[x][1/x] \arrow[ur, "\subseteq"] & &
\end{tikzcd}$$

Therefore since $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}(x)$ and $\operatorname{im}\varphi_3 \subset \mathbb{Z}[x]$, φ_3 induces a ring homomorphism $\psi : R \to \mathbb{Z}[x]$ defined by $\psi(r) = \varphi_3(r)$. In particular, $\psi(a) = 2$, $\psi(b) = x$. Since $aR + bR = R$, there exist $r \in R, s \in R$ such that $ar + bs = 1$. Then $1 = \varphi_3(ar) + \varphi_3(bs) = 2\varphi_3(r) + x\varphi_3(b)$, which is a contradiction since $2\mathbb{Z}[x] + x\mathbb{Z}[x] \neq \mathbb{Z}[x]$. Thus, Φ_S is not an isomorphism.

□

Exercise 10. Let $\mathcal{C}$ be an abelian category. Prove that the following are equivalent:

(a) Every object of $\mathcal{C}$ is projective.

(b) Every object of $\mathcal{C}$ is injective.

Proof. Let us first show that (a) $\Rightarrow$ (b). Let X, Y, Z objects of C, $\psi : Y \hookrightarrow Z$ a monomorphism and $\varphi : Y \to X$ a morphism. Let us show that there exists a morphism $\Psi : Z \to X$ such that $\Psi \circ \psi = \varphi$ (i.e., X is injective, so every object of $\mathcal{C}$ is injective). Since $\mathcal{C}$ is abelian, we have cokernels, and since every object of $\mathcal{C}$ is projective (in particular $\operatorname{coker} \psi$), the following diagram is satisfied:

$$\begin{tikzcd}
 & Z \arrow[r, two heads] & \operatorname{coker} \psi \\
X & Y \arrow[l, "\varphi"] \arrow[u, hook, "\psi"] & \operatorname{coker} \pi \arrow[u, "\operatorname{id}"'] \arrow[ul, dashed, "\exists"]
\end{tikzcd}$$

In particular, the exact sequence $Y \xrightarrow{\psi} Z \to \operatorname{coker} \psi$ splits, so Z is isomorphic to $Y \oplus \operatorname{coker} \psi$. In particular, there is a section $\iota : Z \to Y$ of ψ. Therefore, we define $\Psi : Y \oplus \operatorname{coker} \psi \to X$ by $\varphi \oplus 0$ which clearly satisfies the following commutative diagram:

$$\begin{tikzcd}
Y \oplus \operatorname{coker} \psi \arrow[d, dashed, "\varphi \oplus 0"] & Z \arrow[l, "\iota \oplus \pi"] \\
X & Y \arrow[l, "\varphi"] \arrow[u, "\psi"]
\end{tikzcd}$$

Therefore, X is injective.

(There is an alternate argument for (b) $\Rightarrow$ (a) pointed out to me by Rhea, using that if X is a projective/injective object of $\mathcal{C}$, then X is an injective/projective object of $\mathcal{C}^{\mathrm{op}}$. If every object of $\mathcal{C}$ is injective, then every object of $\mathcal{C}^{\mathrm{op}}$ (which is still an abelian category) is projective, so by (a) $\Rightarrow$ (b), every object of $\mathcal{C}^{\mathrm{op}}$ is injective. So every object of $\mathcal{C}$ is projective).

Now let us show that (b) $\Rightarrow$ (a). Let X, Y, Z be objects of C, $\psi : Y \twoheadrightarrow Z$ an epimorphism and $\varphi : X \to Z$ a morphism. Let us show that there exists a morphism $\Psi : X \to Y$ such that $\psi \circ \Psi = \varphi$. Since every object of $\mathcal{C}$ is injective by assumption, $\ker \psi$ is injective, so the following diagram is satisfied:

$$\begin{tikzcd}
 & Z & \ker \psi \\
X \arrow[ur, "\varphi"] & Y \arrow[u, two heads, "\psi"] \arrow[ur, dashed, "\exists"] & \ker \psi \arrow[l, hook'] \arrow[u, "\operatorname{id}"']
\end{tikzcd}$$

in particular, the exact sequence $\ker \psi \hookrightarrow Y \xrightarrow{\psi} Z$ splits, so $Y \cong \ker \psi \oplus Z$. Therefore, we define $\Psi : X \to \ker \psi \oplus Z$ by $\Psi(x) = (0, \varphi(x))$ which clearly satisfies the following commutative diagram:

$$\begin{tikzcd}
 & Z \\
X \arrow[ur, "\varphi"] \arrow[r, dashed, "0 \oplus \varphi"] & \ker \psi \oplus Z \arrow[u, "\tilde{\psi}"]
\end{tikzcd}$$

Therefore, X is projective, so every object of $\mathcal{C}$ is projective. □

Fall 2018

Exercise 1. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order 8.

(a) Show that every non-trivial subgroup of Q_8 contains -1.

(b) Show that Q_8 does not embed in the symmetric group S_7 as a subgroup.

Proof. (a) Any non-trivial subgroup of Q_8 contains one of $\pm i, \pm j, \pm k$ or -1, and thus contains their square which is -1 (or already contains -1).

(b) Suppose $\psi : Q_8 \to S_7$ were an injective homomorphism ab absurdo. Then ψ preserves orders, so $\psi(i)$ is an order 4 element of S_7 and thus has cycle type either $(abcd)(ef)$ or $(abcd)$ for distinct integers $1 \leq a, b, c, d, e, f \leq 7$. Without loss of generality by applying an isomorphism to S_7, assume that $\psi(i) = (1234)$ or $\psi(i) = (1234)(56)$. In either case, $\psi(i^2) = \psi(j^2) = \psi(k^2) = (13)(24)$. Therefore since both $\psi(j), \psi(k)$ have cycle type $(abcd)(ef)$ or $(abcd)$ and

$$\Big((abcd)(ef)\Big)^2 = (ac)(bd) = \Big((abcd)(ef)\Big)^2$$

in S_7, we have that one of the following holds for $5 \leq a, b \leq 7$ distinct integers:

$$\psi(j) = \begin{cases} (1234) & \text{Case 1} \\ (1432) & \text{Case 2} \\ (1234)(ab) & \text{Case 3} \\ (1432)(ab) & \text{Case 4} \end{cases}$$

In Case 1 or 2 or if $\psi(i) = (1234)$, $\psi(j)$ commutes with $\psi(i)$, which is a contradiction since i, j don't commute in Q_8. Thus we may assume that $\psi(i) = (1234)(56)$ and $\psi(j) = (1234)(ab)$ or $\psi(j) = (1432)(ab)$. These two cases are equivalent by replacing j with $-j$, so assume without loss of generality that $\psi(j) = (1432)(ab)$. Then $\psi(i)\psi(j) = (ab)(56)$. In particular, $\psi(i)\psi(j)$ is an element of S_3, the symmetric group on the set $\{5, 6, 7\}$. Therefore, $\psi(i)\psi(j)$ is not order 4: but this is a contradiction with ψ being an injection, since this implies that $\psi(k) = \psi(i)\psi(j)$ is not order 4.

□

Exercise 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.

Proof. Let $H \leq G$ be of index n, and let $\psi_H : G \to S_n$ be the action of G on the left cosets G/H of H. Without loss of generality, order the cosets of G/H so the first coset is $eH = H$, so in particular $\mathrm{Stab}_{\mathrm{id}_{S_n}}(\psi_H) = H$. Therefore, there is a surjective map $\mathrm{Hom}(G, S_n) \to S$, where S is the set of subgroups of index n or smaller in G by $\psi \mapsto \mathrm{Stab}_{\mathrm{id}_{S_n}}(\psi)$. Therefore, it suffices to show that $\mathrm{Hom}(G, S_n)$ is finite. Let $\{x_1, \ldots, x_k\}$ be a finite generating set of G. Every homomorphism $\psi : G \to S_n$ is determined by its action on the set $\{x_i\}$. Furthermore, $|S_n| = n!$, so there are at most $n!$ choices of the image of each x_i. Therefore, $|\mathrm{Hom}(G, S_n)| \leq (n!)^k < \infty$, so there are finitely many subgroups of index n.

Let $H_1, \ldots, H_r$ be all of the subgroups of index n in G, and let $N = \bigcap_{i=1}^r H_i$. Any automorphism $\varphi : G \to G$ permutes the set $\{H_1, \ldots, H_r\}$. Therefore,

$$H(N) = \varphi(H_1 \cap \cdots \cap H_r) = \varphi(H_1) \cap \cdots \cap \varphi(H_r) = H_1 \cap \cdots \cap H_r = N$$

so N is characteristic. Let us show that N is finite index by showing that the intersection of two finite index subgroups in G is finite index. Let $H, H' \leq G$ be of finite index. Let G act on $G/H, G/H'$ by left translation (on each factor). Then the stabilizer of (H, H') is $H \cap H'$, and by the orbit stabilizer theorem $[G : H \cap H'] \leq [G : H][G : H'] < \infty$. (Also notice that $[G : H], [G : H']\Big|[G : H \cap H']$ since $[G : H \cap H'] = [G : H][H : H \cap H']$ and vice versa). □

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

Proof. K is a finite algebraic extension over F and thus has a finite generating set $x_1, \ldots, x_n$, and without loss of generality take n minimal among such sets. Assume for the sake of contradiction that $n > 1$ so there does not exist $y \in K$ such that $F(x_1, x_2) \subset F(y)$. Let us consider the subextensions $K \subset F(\alpha x_1 + x_2) \subset F(x_1, x_2)$ for $\alpha \in K$. Notice that F is not finite, since otherwise F would be perfect and thus K would be a finite separable extension and thus simple. Therefore, there are infinitely many choices of α. Since there are only finitely many intermediate extensions $F \subseteq E \subseteq K$, there is some $\alpha \neq \beta \in F$ such that $F(\alpha x_1 + x_2) = F(\beta x_1 + x_2)$. Thus, this extension contains $(\alpha - \beta)x_1$. Since $\alpha \neq \beta$, we divide by $\alpha - \beta$ so this extension contains x_1. But then this extension also contains x_2, and thus $F(\alpha x_1 + x_2) = F(\beta x_1 + x_2) = F(x_1, x_2)$. This is a contradiction, so K is simple over F. □

Exercise 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.

Proof. Let L be the splitting field of f over K, so $\mathrm{Gal}(L/K) = G$ is the Galois group of f. Let f have roots $r_1, r_2, r_3, r_4 \in L$, and assume r_1, r_2 are the real roots. We have an injective group homomorphism $G \xrightarrow{\psi} S_4$ by sending an element $\sigma \in G$ to its action on the roots $\{r_1, r_2, r_3, r_4\}$. Since f is irreducible, ψ is a transitive action on r_1, r_2, r_3, r_4. Therefore, $|\mathrm{Orb}_\psi(r_1)| = 4$. Recall that there is a complex conjugation action $\tau \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C})$. Since $K \subseteq \mathbb{R}$ and $L \subseteq \mathbb{C}$, τ restricts to an element $\tau' \in G$ which fixes r_1, r_2 and does not fix r_3, r_4 (since $\mathbb{R}$ is the fixed field of τ, and $r_3, r_4 \notin \mathbb{R}$ by assumption). Furthermore, τ is order 2, so τ' is order 1 or 2, but since it does not fix r_3, it must be order 2 in g. Therefore, $\sigma' \in \mathrm{Stab}_\psi(r_1)$, so $\mathrm{Stab}_\psi(r_1)$ is a subgroup of G containing an element of order 2. Therefore, $|\mathrm{Stab}_\psi(r_1)| = 2k$ for some $k \in \mathbb{N}$, so

$$|G| = |\mathrm{Orb}_\psi(r_1)||\mathrm{Stab}_\psi(r_1)| = 8k$$

also, the order of G divides $|S_4| = 24$, so either $|G| = 24$ and ψ is an isomorphism or $|G| = 8$, as desired. □

Exercise 5. Let R be a commutative ring. Show the following:

(a) Let S be a non-empty saturated multiplicative set in R, i.e., if $a, b \in R$, then $ab \in S$ if and only if $a, b \in S$. Show that $R \cap S$ 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 non-zero principal prime ideal.

Proof. (a) Notice that S contains 1 since it is nonempty, and thus contains all units of R. Let $\eta : R \to S^{-1}R$ the canonical morphism for the localization by S. There is an inclusion preserving correspondence of prime ideals of $S^{-1}R$ and prime ideals of R disjoint from S by $\mathfrak{p} \mapsto \eta^{-1}(\mathfrak{p})$. Take any $x \in R \setminus S$. Let us show that $\eta(x)$ is not a unit in $S^{-1}R$. Suppose for contradiction there existed r/s such that $x/1 \cdot r/s = 1/1$ in $S^{-1}R$. Then, there would exist $t \in S$ such that

$$t(xr - s) = 0 \qquad txr = st \in S$$

But $x \notin S$ and S is saturated, which is a contradiction. Thus, $\eta(x)$ is not invertible, and thus generates a proper ideal I of $S^{-1}R$ which is contained in a maximal (and thus prime) ideal $\mathfrak{p}$ of $S^{-1}R$. $\mathfrak{q}_x := \eta^{-1}(\mathfrak{p})$ is thus a prime ideal of R containing x and is disjoint from S. Therefore, $R/S = \bigcup_{x \in R/S} \mathfrak{q}_x$ as desired.

(b) Let S be the set of elements in R which can be expressed as a (finite) product of non-zero primes and units in S. S is clearly multiplicative. Let us show that S is saturated. Suppose $ab \in S$ for $a, b \in R$. Then $ab = up_1 \dots p_r$ for a unit u and primes $p_1, \dots, p_r$. By primality, p_r divides one of a, b. Say p_r divides a, so $a = a_1 p_r$ for $a_1 \in R$. Let $b_1 = b \in R$. Then $a_1 b_1 = up_1 \dots p_{r-1}$, and p_{r-1} divides one of $a_1 b_1$. Repeating this process, we have $a_r b_r = u$, so both a_r, b_r are units. Furthermore, we have that $a = \prod_{l \in S} p_l a_r$ for a finite subset S of $\{1, 2, \dots, r\}$, and $b = \prod_{l \in S^c} p_l a_r$. Therefore, a and b can be expressed as a finite product of primes and units and are thus in S.

Let $x \in R \setminus S$. Let us show that $x = 0$, which will imply that R is a UFD. Suppose for the sake of contradiction that $x \neq 0$. Since $R \setminus S$ is a union of prime ideals by part (a), there is a non-zero prime ideal $\mathfrak{p}$ containing x. By assumption, $\mathfrak{p}$ contains a principal prime ideal (p), so $p \in (p) \subset \mathfrak{p} \subset R \setminus S$. But $p \in S$ since it can be expressed as a finite product of primes (namely, $p = 1 \cdot p$). This is a contradiction, so $R \setminus S = \{0\}$ as desired.

□

Exercise 6. Let A be an integrally closed Noetherian domain with quotient field F and K/F be a finite separable field extension.

(a) If $\{x_1, \ldots, x_n\}$ is a basis for K as an F-vector space, show that there exists $\{y_1, \ldots, y_n\}$ in K such that $\mathrm{Tr}_{K/F}(x_i y_j) = \delta_{i,j}$ for all i, j.

(b) If B is the integral closure of A in K, show that B is a finitely generated A-module.

Proof. □

Exercise 7. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor with a 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.

Proof. Let $\epsilon : FG \to \mathrm{Id}_{\mathcal{D}}$ be the counit of the adjunction. Consider the following diagram in **Set** for $X, Y \in \mathcal{C}$:

$$\begin{tikzcd}
\mathrm{Mor}_{\mathcal{C}}(X,Y) \arrow[r, "\eta_Y^*"'] \arrow[rrr, bend left, "F_*"] & \mathrm{Mor}_{\mathcal{C}}(X,GFY) \arrow[r, "F_*"'] \arrow[rr, bend right, "\sim"'] & \mathrm{Mor}_{\mathcal{D}}(FX,FGFY) \arrow[r, "\epsilon_{FY}^*"'] & \mathrm{Mor}_{\mathcal{D}}(FX,FY)
\end{tikzcd} \tag{5}$$

Where η_Y^* and ϵ_{FY}^* are defined by post composition with η_Y, ϵ_{FY}:

$$\begin{tikzcd}
Y \arrow[r, "\eta_Y"'] & GFY & FGFY \arrow[r, "\epsilon_{FY}"'] & FY
\end{tikzcd}$$

Notice that the composition
$$\begin{tikzcd}
\mathrm{Mor}_{\mathcal{C}}(X,GFY) \arrow[r, "F_*"'] \arrow[rr, bend right, "\sim"'] & \mathrm{Mor}_{\mathcal{D}}(FX,FGFY) \arrow[r, "\epsilon_{FY}^*"'] & \mathrm{Mor}_{\mathcal{D}}(FX,FY)
\end{tikzcd}$$
is the usual morphism of hom-sets by the adjunction of F and G, and in particular is an isomorphism.

Diagram 5 commutes, i.e., $F_* = \eta^*_{FY} \circ F_* \circ \eta^*_Y : \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{D}}(FX, FY)$ by the unit-counit relation:

$$\begin{tikzcd}
FY \arrow[r, "F\eta_Y"'] \arrow[rr, bend left, "\mathrm{Id}_{FY}"] & FGFY \arrow[r, "\epsilon_{FY}"'] & FY
\end{tikzcd}$$

Therefore, $F_* : \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{D}}(FX, FY)$ is an isomorphism for some X, Y if and only if η^*_Y is an isomorphism. Therefore, F is fully faithful if and only if η^*_Y is an isomorphism for all Y. By Yoneda, F is thus fully faithful if and only if η is an isomorphism. □

Exercise 8. Give an example of a diagram of commutative rings whose colimit in the category of commutative rings is different from its colimit in the larger category of rings (and ring homomorphisms).

Proof. $\mathbb{Z}[x]$ is the free ring with one variable and also the free commutative ring with one variables. Let I be the diagram

$$\mathbb{Z}[x] \qquad \mathbb{Z}[x]$$

so $\underrightarrow{\operatorname{colim}}_I = \mathbb{Z}[x] \sqcup \mathbb{Z}[x]$ is the coproduct of $\mathbb{Z}[x]$ with itself (in the corresponding categories). In **CRing**, $\mathbb{Z}[x] \sqcup \mathbb{Z}[x] \cong \mathbb{Z}[x, y]$ since $\mathbb{Z}[x, y]$ is the free commutative ring in 2 variables. To show that $\mathbb{Z}[x, y] \neq \mathbb{Z}[x] \sqcup_{\mathbf{Ring}} \mathbb{Z}[x]$, it suffices to show that there is ring R and morphisms $\varphi_1 : \mathbb{Z}[x] \to R, \varphi_2 : \mathbb{Z}[x] \to R$ such that for any ring homomorphisms $\iota_1, \iota_2 : \mathbb{Z}[x] \to \mathbb{Z}[x, y]$, there is no ψ making the following diagram commute:

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[dr, "\iota_1"] \arrow[ddr, bend right, "\varphi_1"] & & \mathbb{Z}[x] \arrow[dl, "\iota_2"'] \arrow[ddl, bend left, "\varphi_2"'] \\
& \mathbb{Z}[x, y] \arrow[d, dotted, "\nexists\psi"] & \\
& R &
\end{tikzcd}$$

Let R be any noncommutative ring with $a, b \in R$ such that $ab - ba \neq 0$. Define $\varphi_1, \varphi_2 : \mathbb{Z}[x] \to R$ by $\varphi_2(x) = a, \varphi_2(x) = b$. In order for the diagram to commute, $\psi(\iota_1(x)\iota_2(x) - \iota_2(x)\iota_1(x)) = ab - ba \neq 0$, but since $\mathbb{Z}[x, y]$ is commutative this is impossible. □

Exercise 9. Let $f : M \to N$ and $g : N \to M$ be two R-linear homomorphisms of R-modules such that $\mathrm{id}_M - gf$ is invertible. Show that $\mathrm{id}_N - fg$ is invertible as well and give a formula for its inverse. [Hint: You may use Analysis to make a guess.]

Proof. Using analysis as an intuition, we write the nonsense equations

$$\frac{1}{\mathrm{id}_M - gf} = \mathrm{id}_M + gf + gfgf + \dots$$

$$\frac{1}{\mathrm{id}_N - fg} = \mathrm{id}_N + fg + fgfg + \dots$$

Letting $h = \frac{1}{\mathrm{id}_M - gf}$, we thus write

$$\mathrm{id}_N + fhg = \mathrm{id}_N + fg + fgfg + \dots = \frac{1}{\mathrm{id}_N - fg}$$

It is straight forward to check that $\mathrm{id}_N + fhg$ is in fact $(\mathrm{id}_N - fg)^{-1}$:

$$(\mathrm{id}_N - fg)(\mathrm{id}_N + fhg) = \mathrm{id}_N - fg + f(h(gf - \mathrm{id}_M))g = \mathrm{id}_N$$

$$(\mathrm{id}_N + fhg)(\mathrm{id}_N - fg) = \mathrm{id}_N - fg + f((gf - \mathrm{id}_M)h)g = \mathrm{id}_N$$

□

Exercise 10. Consider the real algebra $A = \mathbb{R}[x, y] = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ where x and y are the classes of X and Y respectively. Let $M = A(1 + x) + Ay$ be the ideal generated by $1 + x$ and y. (This is the Möbius band.)

(a) Show that there is an A-linear isomorphism $A^2 \xrightarrow{\sim} M \oplus M$ mapping the canonical basis to $(1 + x, y)$ and $(-y, 1 + x)$.

(b) Show that there is an A-linear isomorphism $A \xrightarrow{\sim} M \otimes_A M$ mapping 1 to $((1+x)\otimes(1+x))+y\otimes y$.

Proof. (a) The existence of such an A-linear homomorphism ψ is immediate from the universal property of A^2 as a free A-module. Thus, it remains to show it is an isomorphism onto its image. First we show that ψ. Notice that A is an integral domain since $X^2 + Y^2 - 1$ is irreducible by Eisenstein (considering $X^2 + Y^2 - 1$ as a polynomial in X and that $Y - 1$ is a prime in $\mathbb{R}[Y]$ dividing the constant term once). Let $a, b \in A$, and suppose that $\psi(a, b) = (0, 0)$. This implies that $a(1 + x) + by = 0$ and $-ay + b(1 + x) = 0$. Multiplying both equations by $1 + x, y$ yields the equations

$$(1) : by(1 + x) = -a(1 + x)^2 \qquad (2) : ay(1 + x) = -by^2$$

$$(3) : ay(1 + x) = b(1 + x)^2 \qquad (4) : by(1 + x) = ay^2$$

Combining equations $(1), (4)$, we have:

$$-a(1 + x)^2 = ay^2$$

If $a \neq 0$, then this implies $(1+x)^2 = -y^2$ since A is a domain. Equivalently, that $Y^2 + X^2 + 2X + 1 \in (X^2 + Y^2 - 1) \subset \mathbb{R}[X,Y]$. But this is not true, for instance by plugging in $X = 1$ and $Y = 0$. Therefore $a = 0$. Similarly, combining equations (2) and (3) yields

$$-by^2 = b(1+x)^2$$

If b were not zero, then since A is a domain this would imply $y^2 = -(1+x)^2$. But by the same reasoning this is not true, so $b = 0$. Thus, ψ is injective.

To show ψ is surjective it suffices to show that $(1+x,0)$, $(y,0)$, $(0,1+x), (0,y)$ are in its image. Since $(1+x,y), (-y,1+x)$ are clearly in the image of ψ, it suffices to show that $(y,0)$ and $(0,y)$ are in the image of ψ. Notice that:

$$\psi((y,x-1)) = (y(1+x), y^2) + (-y(x-1), x^2-1) = (y + yx - xy + y, y^2 + x^2 - 1) = (2y, 0)$$

$$\psi((x-1,-y)) = (x^2-1, y(x-1)) + (y^2, -y(1+x)) = (x^2+y^2-1, xy - xy - 2y) = (0, -2y)$$

Thus (by multiplying by $1/2, -1/2$), $(y,0), (0,y)$ are in the image of ψ so ψ is surjective.

(b) The existence of such an A-linear homomorphism φ is immediate since A is free as a module over itself. Thus, we only need to show that it is an isomorphism. First we show that φ is a surjection. Notice that since M is generated as an A-module by $1+x$ and y, $M \otimes_A M$ is generated by $(1+x) \otimes y = y \otimes (1+x), y \otimes y$ and $(1+x) \otimes (1+x)$. Let us show that $1 \otimes (1+x) \in M \otimes_A M$. We have:

$$\varphi(1) = (1+x)\otimes(1+x) + y\otimes y = 1\otimes(1+x)^2 + 1\otimes y^2 = 1\otimes\Big(1+2x+x^2+y^2\Big) = 1\otimes\Big(2+2x\Big) = 2\cdot\Big(1\otimes(1+x)\Big)$$

This computation showed us two things: $(1+x) \otimes 1 \in M \otimes_A M$ and that $y \otimes y$ is in the span of $(1+x) \otimes 1 \in M$. Therefore, all the generators of $M \otimes_A M$ are in $\langle (1+x) \otimes 1 \rangle$, so $M \otimes_A M = \langle (1+x) \otimes 1 \rangle$. Therefore, ψ is surjective. Furthermore, $M \otimes_A M$ is naturally an A-submodule of $A \otimes_A A$, and $A \otimes_A A \xrightarrow{\sim} A$ by the homomorphism $\rho(a \otimes b) = ab$. We have that the composition

$$A \xrightarrow{\varphi} M \otimes_A M \hookrightarrow A \otimes_A A \to A$$

is defined by $1 \mapsto 2 \cdot (1+x)$ and is therefore injective. In particular, φ is injective, so φ is an isomorphism.

□

Exercise 11. Let G be a finite group, ω be a primitive 3rd root of 1 in $\mathbb{C}$ and suppose that the complex able of G contains the row

$$1 \quad \omega \quad \omega^2 \quad 1$$

Determine the whole complex character table of G, the order of the group and the order of its conjugacy classes.

Proof. Let χ_1 be the irreducible character of above. Then $\chi_1 \otimes \chi_1$ gives another character, and we have the trivial character. By column orthogonality, the last row is of the form $a\ 0\ 0\ -3/a$ for $a \in \mathbb{Z}^+$ the dimension. Since each entry of the character table is an algebraic integer, we must have $a = 1$ or $a = 3$. But $a \neq 1$ since the value of the character at 1 must bound the other values of the character on other group elements in absolute value. Thus, $|G|$ is the sum of the squares of dimensions of the irreducibles, and is therefore $1 + 1 + 1 + 3^2 = 12$. Furthermore using column orthogonality, the size of the conjugacy classes are $1, 4, 4, 3$ (going left to right). One can show that $G \cong A_4$ using the facts that $G/[G, G] \cong \mathbb{Z}/3$ and there are 4 conjugacy classes of G. □

Exercise 12. Let F be a finite field and $K \subset \overline{F}$ the subfield of an algebraic closure generated by all roots of unity. Find all simple finite dimensional K-algebras.

Proof. First we show that $K = \overline{F}$. Let $\alpha \in \overline{F}$ and let $f(x)$ be its irreducible polynomial over $\overline{F}$. Let $L = F(\alpha)$ so $[L : F]$ is finite and $\alpha \in L$. Let $n = [L : F]$ so $|L| = q^n$, where $q = |F|$. Then $L^\times$ is a finite group of order $q^n - 1$, so since $\alpha \in L^\times$, $\alpha^{q^n-1} = 1$. Therefore, α is a root of unity, so $x \in K$. Therefore, $\overline{F} = K$.

Now let S be a simple finite dimensional K-algebra. By Wedderburn, $S \cong M_n(D)$ for a division K-algebra D with $[D : K]$ finite. Since K is algebraically closed, there are no finite extensions D/K for D a division algebra, so $S \cong M_n(K)$ for some n. Thus, these are the only simple finite dimensional K-algebras. □