Algebra Qual Solutions

Matthew Gherman

March 2019

Be advised there are likely enormous errors. I received help from Alex Wertheim and Harris Khan. I looked at Yacoub Kureh's and Ian Coley's solutions for a couple of the problems.

Contents

Fall 2014

Problem 1. Let G be a finite group. Let $\mathbb{Z}[G]$ be the group algebra of G with augmentation ideal $\mathfrak{a}$. Show that $\mathfrak{a}/\mathfrak{a}^2 \simeq G/G'$ as abelian groups for the derived group G' of G.

View $\mathfrak{a}/\mathfrak{a}^2$ as an abelian group. We will define the group homomorphism $f : G \to \mathfrak{a}/\mathfrak{a}^2$ as $f(g) = [e-g]$. Let $g_i, g_j \in G$. Note that

$$e - g_ig_j = (e-g_i) + (e-g_j) - (e-g_i)(e-g_j)$$

and $(e-g_i)(e-g_j) \in \mathfrak{a}^2$. Thus $f(g_ig_j) = [e-g_ig_j] = [e-g_i] + [e-g_j]$ and f is a group homomorphism. Since $\mathfrak{a}/\mathfrak{a}^2$ is abelian, we have $\overline{f} : G/G' \to \mathfrak{a}/\mathfrak{a}^2$ where $\overline{f}p = f$ for $p : G \to G/G'$ the standard projection.

Let $|G| = n$ and list all of G as $\{g_1, \dots, g_n\}$. Each $a \in \mathfrak{a}$ is $\sum_{i=1}^n (-a_i)g_i$ for $a_i \in \mathbb{Z}$. Since $\sum_{i=1}^n a_i = 0$, we can write a uniquely as $a = \sum_{i=1}^n a_i(e-g_i)$. Then we can define $h : \mathfrak{a} \to G/G'$ as $h(a) = \prod_{i=1}^n g_i^{a_i}$. Take some $b = (e-g_i)(e-g_j) = e - g_i - g_j + g_ig_j$, then $h(b) = [g_i]^{-1}[g_j]^{-1}[g_ig_j] = ([g_i]^{-1}[g_i])([g_j]^{-1}[g_j]) = [e]$ since G/G' is abelian. Thus $\mathfrak{a}^2 \subset \ker(h)$ and h factors through $\mathfrak{a}/\mathfrak{a}^2$ as $\overline{h} : \mathfrak{a}/\mathfrak{a}^2 \to G/G'$. Now $\overline{h}\overline{f}([g]) = \overline{h}[e-g] = [g]$ and $\overline{f}\overline{h}([a]) = \overline{f}(\prod_{i=1}^n [g_i]^{a_i}) = \sum_{i=1}^n a_i\overline{f}([g_i]) = \sum_{i=1}^n a_i[e-g_i]$ for $a = \sum_{i=1}^n a_i(e-g_i)$. We conclude $\mathfrak{a}/\mathfrak{a}^2 \simeq G/G'$.

Problem 2. Let $\mathbb{F}_p$ denote the finite field of p elements. Consider the covariant functor F from the category of commutative $\mathbb{F}_p$-algebras with a multiplicative identity to abelian groups sending a ring R to its p-th roots of unity, that is, $F(R) = \{\zeta \in R | \zeta^p = 1\}$. Answer the following questions and justify your answers.

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

Assume that $p \neq 2$ so $p \geqslant 3$. Let $R := \mathbb{F}_p[x]/(x^3)$ so R is finite. We note that $\mathbb{F}_p[x]$ is a PID and the ideals of R are in bijective correspondence with the ideals of $\mathbb{F}_p[x]$ containing (x^3). Thus the non-trivial, proper ideals of R are principal generated by x or x^2. The ideal (x) is maximal since $R/(x) \simeq \mathbb{F}_p[x]/(x) \simeq \mathbb{F}_p$ is a field and $(x^2) \subset (x)$. Therefore, R is a local ring. Since R has characteristic $p \geqslant 3$, we have

$$(ax^2 + bx + c)^p = (ax^2)^p + (bx)^p + c^p = ax^{2p} + bx^p + c = c.$$

Thus a pth root of unity in R will have $c = 1$. There are p^2 choices for a and b so there are p^2 distinct pth roots of unity in R.

Assume $p = 2$. Let $R := \mathbb{F}_2[x]/(x^4)$. As above, R is a finite local ring. Since R is characteristic 2,

$$(ax^3 + bx^2 + cx + d)^2 = (a^2x^6 + b^2x^4 + c^2x^2 + d^2) = cx^2 + d$$

for $a, b, c, d \in \mathbb{F}_2$. Then $c = 0$ and $d = 1$ gives a second root of unity in R. We have 4 choices for a and b so R has 4 second roots of unity as desired.

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

Let $\mathcal{C}$ be the category of commutative $\mathbb{F}_p$-algebras. We want to show that F is naturally isomorphic to $\mathrm{Hom}_{\mathcal{C}}(R, -)$ for some $R \in \mathrm{Ob}(\mathcal{C})$. Let G be the cyclic group of order p generated by $g \in G$, and define $R := \mathbb{F}_p[G]$ to be the corresponding group ring over $\mathbb{F}_p$. Any $\mathbb{F}_p$-algebra homomorphism $f : R \to A$ satisfies $f(1) = 1$, fixing $\mathbb{F}_p$. We note that f is determined by the image of g. The order of $g \in R$ is p so $f(g)$ must have order dividing p. Thus $f(g) = 1$ or $f(g)$ is a nontrivial element of order p.

For each $A \in \mathrm{Ob}(\mathcal{C})$, we can construct $\eta_A : F(A) \to \mathrm{Hom}_{\mathcal{C}}(R, A)$ by sending $\zeta \in F(A)$ to the $\mathbb{F}_p$-algebra homomorphism $f : R \to A$ given by $f(g) = \zeta$. For an $\mathbb{F}_p$-algebra homomorphism $h : A \to B$, we need to show that the following diagram commutes.

$$\begin{array}{ccc} F(A) & \xrightarrow{\quad h \quad} & F(B) \\ \downarrow{\scriptstyle \eta_A} & & \downarrow{\scriptstyle \eta_B} \\ \mathrm{Hom}_{\mathcal{C}}(R, A) & \xrightarrow{h \circ -} & \mathrm{Hom}_{\mathcal{C}}(R, B) \end{array}$$

Let $\zeta \in F(A)$. We have $\eta_B(h(\zeta)) = f'$ where $f' : R \to B$ is the unique $\mathbb{F}_p$-algebra homomorphism given by $f'(g) = h(\zeta)$. Similarly, $h(\eta_A(\zeta)) = h \circ f$ where $f : R \to A$ is the unique $\mathbb{F}_p$-algebra homomorphism given by $f(g) = \zeta$. The image of g determines the $\mathbb{F}_p$-algebra homomorphisms so $f' = h \circ f$ and $h \circ \eta_A = \eta_B \circ h$. We conclude that η is a natural transformation. Each $\zeta \in F(A)$ determines one and only one $\mathbb{F}_p$-algebra homomorphism $f : R \to A$ with $f(g) = \zeta$. Thus η is a natural isomorphism and F is representable.

We defined $\mathrm{Aut}(F)$ as the set of invertible natural transformations of F into itself, a subset of $\mathrm{Nat}(F, F)$. By above, F is represented by R so $\mathrm{Nat}(F, F) \simeq \mathrm{Nat}(\mathrm{Hom}_{\mathcal{C}}(R, -), F)$. Yoneda Lemma gives a natural bijection between the natural transformations of $\mathrm{Hom}_{\mathcal{C}}(R, -)$ to F and the set $F(R)$. Thus $|\mathrm{Nat}(F, F)| = |F(R)|$. Every element of $R = \mathbb{F}_p[G]$ is of the form $\sum_{i=0}^{p-1} a_i g^i$. Since $\mathbb{F}_p$ is commutative of characteristic p, we have

$$\left(\sum_{i=0}^{p-1} a_i g^i\right)^p = \sum_{i=0}^{p-1} a_i^p (g^i)^p = \left(\sum_{i=0}^{p-1} a_i\right) e.$$

An element $\sum_{i=0}^{p-1} a_i g^i \in R$ is a pth if and only if $\sum_{i=0}^{p-1} a_i = 1$. There are p different possibilities for the sum of the coefficients with $|R| = p^p$. Thus $|F(R)| = p^{p-1}$.

ASK SOMEONE ABOUT THIS PART We will show that $\eta \in \mathrm{Nat}(F, F)$ is an automorphism if and only if $\eta_F(\mathrm{id}_R) \neq 1$. ($\Rightarrow$) If η is an automorphism, then η_R is a bijection between $\mathrm{Hom}_{\mathcal{C}}(R, R)$ and $F(R)$. For $f \in \mathrm{Hom}_{\mathcal{C}}(R, R)$, we have $\eta_R(f) = F(f)(\eta_R(\mathrm{id}_R)) = f(\eta_R(\mathrm{id}_R))$, a pth root of unity of R. Thus $\eta_R(\mathrm{id}_R) \neq 1$

since $f(1) = 1$ for all $f \in \mathrm{Hom}_{\mathcal{C}}(R, R)$. ($\Leftarrow$) The image of the $g \in R$ determines an endomorphism of R, and $g \in F(R)$ must map to another element of $F(R)$. Assume $\eta_R(\mathrm{id}_R) \neq 1$. There is an element $f \in \mathrm{Hom}_{\mathcal{C}}(R, R)$ such that $f(\eta_R(\mathrm{id}_R)) = g$. This implies that η_A is a bijection between $\mathrm{Hom}_{\mathcal{C}}(R, R)$ and $F(R)$. Therefore, $|\mathrm{Aut}(F)| = |F(R)| - 1 = \frac{p^p}{p} - 1 = p^{p-1} - 1$.

Problem 3. Pick a non-zero rational number x. Determine all possibilities for the Galois group G of the normal closure of $\mathbb{Q}[\sqrt[4]{x}]$ over $\mathbb{Q}$, where $\sqrt[4]{x}$ is the root of $X^4 - x$ with maximal degree over $\mathbb{Q}$.

Note that $\mathbb{Q}$ is perfect so all finite extensions of $\mathbb{Q}$ are separable.

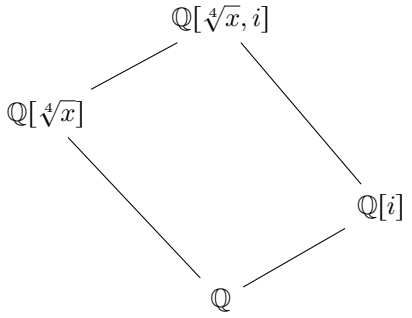
Case 1: Assume $x = y^4$ for some $y \in \mathbb{Q}$, then the roots of $X^4 - x$ are $\{\pm y, \pm yi\}$. A root of maximal degree is yi, and $\mathbb{Q}[yi] = \mathbb{Q}[i]$ is the splitting field of the irreducible polynomial $X^2 + 1$ over $\mathbb{Q}$. Thus $\mathbb{Q}[i]/\mathbb{Q}$ is a Galois extension of degree 2. The only group of order 2 is $\mathbb{Z}/2\mathbb{Z}$ so $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Case 2: Assume $x = y^2$ for some $y \in \mathbb{Q}$ and $x \neq z^4$ for all $z \in \mathbb{Q}$. Then the roots of $X^4 - x$ are $\{\pm\sqrt{y}, \pm\sqrt{y}i\}$ for $\sqrt{y} \in \mathbb{R}$ and $X^4 - x = (X^2 - y)(X^2 + y)$. The two polynomials $X^2 - y$ and $X^2 + y$ are irreducible over $\mathbb{Q}$ since they do not have roots over $\mathbb{Q}$. Thus all of the roots have degree 2 so we can take $\sqrt[4]{x} = \sqrt{y}$. Then $\mathbb{Q}[\sqrt{y}]$ is the splitting field of $X^2 - y$ over $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{y}]/\mathbb{Q}$ is Galois. Once again, the Galois group is order 2 so $\mathrm{Gal}(\mathbb{Q}[\sqrt{y}]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Case 3: Assume $x = -y^2$ for some $y \in \mathbb{Q}$ and $x \neq z^4$ for all $z \in \mathbb{Q}$. Then the roots of $X^4 - x$ are $\{\sqrt{y}\xi_8^j\}$ for ξ_8 a primitive eighth root of unity and $j = 1, 3, 5, 7$. Note that $\xi_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. These roots are not rational so $X^4 - x$ can only factor as a product of quadratics. If $2y$ is the square of a rational number, then $(X - \sqrt{y}\xi_8)(X - \sqrt{y}\xi_8^7) = X^2 - \sqrt{2y}X + y$ and $(X - \sqrt{y}\xi_8^3)(X - \sqrt{y}\xi_8^5) = X - \sqrt{2y}X + y$. The normal closure K is a degree 2 extension of $\mathbb{Q}$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. In all other cases, none of the possible pairings of roots yields a quadratic with coefficients in $\mathbb{Q}$. Thus $X^4 - x$ is irreducible and the normal closure K is the splitting field of $X^4 - x$. It is clear that $K \subset \mathbb{Q}[\sqrt{2y}, i]$. Continuing, $\sqrt[4]{x}\xi_8 = \frac{\sqrt{2y}}{2} + \frac{\sqrt{2y}}{2}i$. We see that $2\sqrt[4]{x}\xi_8 + \sqrt[4]{x}\overline{\xi_8} = \sqrt{2y} \in K$. Then $\frac{2}{y}(\sqrt{2y}\sqrt[4]{x}\xi_8 - \frac{y}{2}) = i \in K$ as well. We conclude $K = \mathbb{Q}[\sqrt{2y}, i]$. Note the polynomials $X^2 - 2y$ and $X^2 + 1$ are irreducible so $\mathbb{Q}[\sqrt{2y}]/\mathbb{Q}$ and $\mathbb{Q}[i]/\mathbb{Q}$ are degree 2 Galois extensions with $\mathbb{Q}[\sqrt{2y}] \cap \mathbb{Q}[i] = \mathbb{Q}$ since $\mathbb{Q}[\sqrt{2y}] \subset \mathbb{R}$. Then $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}[\sqrt{2y}]/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 4: Assume $x \neq y^2$ for all $y \in \mathbb{Q}$ and $x > 0$. The roots are $\{\pm\sqrt[4]{x}, \pm\sqrt[4]{x}i\}$ where we take $\sqrt[4]{x}$ to be the real fourth root of x. By assumption, $X^4 - x$ has no roots in $\mathbb{Q}$. None of the possible pairings of $(x - \alpha)$ for α a root of $X^4 - x$ gives a quadratic with coefficients in $\mathbb{Q}$. Thus $X^4 - x$ is irreducible and all the roots have degree 4, justifying the choice of $\sqrt[4]{x}$ as the real fourth root. Let K be the normal closure of $\mathbb{Q}[\sqrt[4]{x}]/\mathbb{Q}$. Since $X^4 - x$ is irreducible, K will be the splitting field of $X^4 - x$. We note that $K \subset \mathbb{Q}[\sqrt[4]{x}, i]$ since $X^4 - x$ splits in $\mathbb{Q}[\sqrt[4]{x}, i]$. Additionally, $\sqrt[4]{x} \in K$ and $\frac{1}{x}(\sqrt[4]{x})^3(\sqrt[4]{x}i) = i \in K$ so $K = \mathbb{Q}[\sqrt[4]{x}, i]$.

We build the tower of field extensions below. We know that $[\mathbb{Q}[\sqrt[4]{x}] : \mathbb{Q}] = 4$ and $[\mathbb{Q}[i] : \mathbb{Q}] = 2$. Since $\mathbb{Q}[\sqrt[4]{x}] \subset \mathbb{R}$, we have $\mathbb{Q}[\sqrt[4]{x}] \cap \mathbb{Q}[i] = \mathbb{Q}$ and $[\mathbb{Q}[\sqrt[4]{x}, i] : \mathbb{Q}] = 8$, as a result. Note that $\mathbb{Q}[\sqrt[4]{x}]/\mathbb{Q}$ is not a normal extension so $\mathbb{Q}[\sqrt[4]{x}, i]/\mathbb{Q}$ is not an abelian extension. Thus $\mathrm{Gal}(\mathbb{Q}[\sqrt[4]{x}, i]/\mathbb{Q})$ is a nonabelian group of order 8. This leaves the quaternion group or the dihedral group. Complex conjugation τ is an order 2 automorphism. In both D_4 and Q_8, there is an element of order 4. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be such an element. If $\sigma(\sqrt[4]{x}) = -\sqrt[4]{x}$, then $\sigma(\sqrt[4]{x}i) = \sqrt[4]{x}i$ or $\sigma(\sqrt[4]{x}i) = -\sqrt[4]{x}i$. In either case, σ^2 is the identity, a contradiction. Thus $\sigma(\sqrt[4]{x}) = \pm\sqrt[4]{x}i$. The argument will work for either choice so assume $\sigma(\sqrt[4]{x}) = \sqrt[4]{x}i$. We see that $\sigma\tau(\sqrt[4]{x}) = \sigma(\sqrt[4]{x}) = \sqrt[4]{x}i$ and $\tau\sigma(\sqrt[4]{x}) = \tau(\sqrt[4]{x}i) = -\sqrt[4]{x}i$. Thus σ and τ do not commute. The order 2 element -1 in the quaternion group commutes with the order 4 elements. We conclude $\mathrm{Gal}(\mathbb{Q}[\sqrt[4]{x}, i]/\mathbb{Q}) \simeq D_4$.



Case 5: Assume $x \neq y^2$ for all $y \in \mathbb{Q}$ and $x < 0$. Let $z = |x|$. Then the roots of $X^4 - x$ are $\{\sqrt[4]{z}\xi_8^i\}$ for $\sqrt[4]{z}$ the real fourth root and $i \in \{1, 3, 5, 7\}$. The roots are not contained in $\mathbb{Q}$ and none of the possible pairings of roots yields a quadratic with coefficients in $\mathbb{Q}$. Thus $X^4 - x$ is irreducible and the normal closure K is the splitting field

of $X^4 - x$. It is clear that $K \subset \mathbb{Q}[\sqrt[4]{4z}, i]$ since $\sqrt[4]{z}\xi_8 = \sqrt[4]{z}(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)$. But, $\sqrt[4]{z}\xi_8 + \sqrt[4]{z}\xi_8^7 = \sqrt[4]{z}\sqrt{2} = \sqrt[4]{4z} \in K$ and $\sqrt[4]{z}\xi_8^3 + \sqrt[4]{z}\xi_8^5 = \sqrt[4]{z}\sqrt{2}i = \sqrt[4]{4z}i \in K$. Then $(\frac{1}{4z})(\sqrt[4]{4z})^3(\sqrt[4]{4z}i) = i \in K$. We conclude that $K = \mathbb{Q}[\sqrt[4]{4z}, i]$. This is Case 4 since $4z \in \mathbb{Q}$ so $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$.

Problem 4. Let D be a 9-dimensional central division algebra over $\mathbb{Q}$ and $K \subset D$ be a field extension of $\mathbb{Q}$ of degree greater than 1. Show that $K \otimes_{\mathbb{Q}} K$ is not a field and deduce that $D \otimes_{\mathbb{Q}} K$ is no longer a division algebra.

Note K is a finite extension of $\mathbb{Q}$ and $\mathbb{Q}$ is perfect. By the Primitive Element Theorem, $K \simeq \mathbb{Q}[x]/(f)$ for some irreducible polynomial $f \in \mathbb{Q}[x]$. Since f is no longer irreducible in K, (f) is neither a maximal nor a prime ideal of $K[x]$. We conclude $K \otimes_{\mathbb{Q}} K \simeq K[x]/(f)$ is not a field and, further, not a domain. Alternatively, we can factor $f = (x-\alpha)(x-\beta)$ for $\alpha, \beta \in K$, and $K \otimes_{\mathbb{Q}} K \simeq K[x]/(f) \simeq K[x]/(x-\alpha) \times K[x]/(x-\beta)$ by the Chinese Remainder Theorem. (Note that the extension is separable so α and β are distinct.) Therefore, $K \otimes_{\mathbb{Q}} K$ is not even a domain.

Now $K \otimes_{\mathbb{Q}} K$ is a commutative subring of $D \otimes_{\mathbb{Q}} K$ that is not a domain. We conclude that $D \otimes_{\mathbb{Q}} K$ cannot be a division algebra.

Problem 5. Let R be a commutative algebra over $\mathbb{Q}$ of finite dimension n. Let $\rho : R \to M_n(\mathbb{Q})$ be the regular representation, and define $\mathrm{Tr} : R \to \mathbb{Q}$ by the matrix trace of ρ. If the pairing $(x, y) = \mathrm{Tr}(xy)$ is non-degenerate on R, prove that R is semi-simple.

We will show that a non-degenerate trace implies that R has no nontrivial nilpotent elements. Let $r \in R$ be nilpotent with $r^k = 0$. Then $\rho(r)$ is a matrix such that $\rho(r^k) = \rho(r)^k = 0$. Then the minimal polynomial of $\rho(r)$ has the form X^m for some m. We conclude that $\mathrm{Tr}(r) = 0$ since $\mathrm{Tr}(r)$ appears as a non-leading coefficient in the minimal polynomial. In particular, rx is nilpotent for all $x \in R$ since R is commutative. Thus $\mathrm{Tr}(rx) = 0$ for all $x \in R$. If (x, y) is non-degenerate, then R has no nontrivial nilpotent elements. In other words, the nilradical of R is trivial.

Every ideal of R is closed under multiplication by R, which means each ideal is a $\mathbb{Q}$-subspace of a finite-dimensional vector space. Thus R is Artinian by a dimension argument for a descending chain of ideals. In an Artinian commutative ring, each prime is maximal (see Atiyah-MacDonald **ADD A REFERENCE**) so the Jacobson radical and nilradical are equal. Since the nilradical is trivial, the Jacobson radical of A is trivial. A Artinian implies there are finitely many maximal ideal $\{\mathfrak{m}_i\}$ for $1 \leqslant i \leqslant \ell$ (see Atiyah-MacDonald **ADD REFERENCE**). Thus $\cap_{i=1}^{\ell} \mathfrak{m}_i = 0$. By the Chinese Remainder Theorem,

$$A \simeq A/\cap_{i=1}^{\ell} \mathfrak{m}_i \simeq \oplus_{i=1}^{\ell} A/\mathfrak{m}_i.$$

Each $A/\mathfrak{m}_i$ is a simple R-module so R is a semisimple R-module. This shows R is a semisimple ring.

Problem 6. Let G be a finite group and let p be the smallest prime number dividing the order of G. Assume G has a normal subgroup H of order p. Show that H is contained in the center of G.

Conjugating elements of H by G is a group action since H is a normal subgroup. The fixed points of the action are exactly the elements of H in $Z(G)$. Thus $p = |H| = |Z(G) \cap H| + \sum_{h \notin Z(G)} |\mathrm{Orb}(h)|$. The identity is contained in H and $Z(G)$ which implies $|H \cap Z(G)| \geqslant 1$ and $|\mathrm{Orb}(h)| < p$ for all $h \notin Z(G)$. Orbit-Stabilizer gives us $|\mathrm{Orb}(h)| = [G : \mathrm{Stab}(h)]$ so $|\mathrm{Orb}(h)|$ divides $|G|$. Since p is the smallest prime that divides $|G|$, we conclude there are no elements $h \notin Z(G)$. Thus $H \subset Z(G)$.

Problem 7. Let G be a finite group and P a Sylow 2-subgroup of G. Assume P is cyclic, generated by an element x. Show that the signature of the permutation of G given by $g \mapsto xg$ is -1. Deduce that G has a non-trivial quotient of order 2.

Let $|G| = n = 2^k m$ for $\gcd(2, m) = 1$. Then $|P| = 2^k$. Let $\sigma \in S_n$ be the permutation described by left multiplication by x. Then $\sigma(x^i) = x^{i+1}$ for all $0 \leqslant i \leqslant 2^k - 1$. The set of right cosets G/P has order m and each element $g \in G$ appears in one and only one of the cosets. Choose representatives $g_i \in G$ so that $G/P = \{P, Pg_1, \ldots, Pg_{m-1}\}$. Then σ has a unique (up to reordering) representation as a product of disjoint cycles given by

$$\sigma = (e, x, \ldots, x^{2^k-1})(g_1, xg_1, \ldots, x^{2^k-1}g_1) \cdots (g_{m-1}, xg_{m-1}, \ldots, x^{2^k-1}g_{m-1}).$$

Each cycle has length 2^k so each cycle is odd. We have m cycles so there are an odd number of odd cycles. Thus $\operatorname{sgn}(\sigma) = -1$.

Act on G via left multiplication by G. Then define the set H to be all $g \in G$ such that left multiplication by g is an even permutation. Then $e \in H$, H is closed under multiplication, and H is closed under inverses so H is a subgroup of G. Every element either represents an even or odd permutation. By above, $x \notin H$ so $[G : H] = 2$ and H is a normal subgroup of G. We have G/H is a quotient of order 2 as desired.

Problem 8. Let A be a ring. Assume there is an infinite chain of left ideals $I_0 \subset I_1 \subset \cdots \subset A$ with $I_i \neq I_{i+1}$ for $i \geqslant 0$. Show that A has a left ideal that is not finitely generated as a left A-module.

Define $I := \bigcup_{i=0}^{\infty} I_i$. We will show that I is a proper ideal. Let $a, b \in I$. Then $a \in I_k$ for some k and $b \in I_\ell$ for some ℓ. Without loss of generality, assume $k \geqslant \ell$. Then $a, b \in I_k$. Since I_k is an ideal, $a + b \in I_k$ so $a + b \in I$. Similarly, let $r \in A$ and $a \in I$. Then $a \in I_k$ for some k and $ra \in I_k$ since I_k is an ideal. Thus $ra \in I$ and I is an ideal of A. If $1 \in I$, then $1 \in I_k$ for some k. We would have $I_k = I_{k+1} = \cdots = A$, a contradiction. Therefore, I is a proper ideal of A.

Assume for the sake of contradiction that I is finitely generated as a left A-module. Let $\{x_1, \ldots, x_n\}$ be the generating set. Each $x_i \in I_{k_i}$ for some k_i. Define $k := \max_{i=1}^{n} k_i$, then $x_i \in I_k$ for all i. This would imply that $I_k = I_{k+1} = \cdots = A$, a contradiction. Thus I is an ideal of A that is not finitely generated as a left A-module.

Problem 9. Let A be a ring and let $i, j \in A$ such that $i^2 = i$ and $j^2 = j$. Show that the left A-modules Ai and Aj are isomorphic if and only if there are $a, b \in A$ such that $i = ab$ and $j = ba$.

($\Rightarrow$) Assume Ai and Aj are isomorphic. Let $\phi : Ai \to Aj$ be such an isomorphism with inverse $\psi : Aj \to Ai$. Then $\phi(i) = cj$ and $\psi(j) = di$ for some $c, d \in A$. Note that $\phi(i) = \phi(i^2) = i\phi(i) = icj$ and $\psi(j) = \psi(j^2) = j\psi(j) = jdi$. Let $a := icj$ and $b := jdi$. Then

$$ab = (icj)(jdi) = icjdi = ic\psi(j) = \psi(icj) = \psi(\phi(i)) = i$$
$$ba = (jdi)(icj) = jdicj = jd\phi(i) = \phi(jdi) = \phi(\psi(j)) = j$$

as desired.

($\Leftarrow$) Assume $i = ab$ and $j = ba$ for some $a, b \in A$. Then we can define a left A-module homomorphism $\phi : Ai \to Aj$ by $\phi(i) = ia = aj$. Extend ϕ A-linearly. We can also define an A-module homomorphism $\psi : Aj \to Ai$ by extending $\psi(j) = jb = bi$ A-linearly. Let $r \in A$. Then

$$\psi(\phi(ri)) = \psi(r\phi(i)) = \psi(ria) = \psi(raj) = ra\psi(j) = rajb = rabi = ri^2 = ri$$
$$\phi(\psi(rj)) = \phi(r\psi(j)) = \phi(rjb) = \phi(rbi) = rb\phi(i) = rbia = rbaj = rj^2 = rj.$$

We conclude that ϕ is an isomorphism.

This construction is from Yacoub Kureh's solutions.

Problem 10. Let n be a positive integer. Let A_n be the $\mathbb{Q}$-algebra generated by elements $x_1, \ldots, x_n, y_1, \ldots, y_n$ with relations $x_i x_j = x_j x_i$, $y_i y_j = y_j y_i$, and $y_i x_j - x_j y_i = \delta_{ij}$ for $1 \leqslant i, j \leqslant n$. Show that there is a representation of A_n on the vector space $\mathbb{Q}[t_1, \ldots, t_n]$ where x_i acts by multiplication by t_i and y_i acts as $\partial/\partial t_i$.

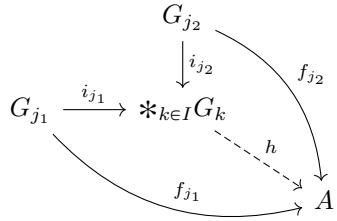
WRITE THIS ONE

Spring 2015

Problem 1. What are the coproducts in the category of groups?

We will define the free product of a family of groups $G_{i\,i\in I}$. As a set, $*_{i\in I} G_i$ is all words on the letters $\bigcup_{i\in I} G_i$. We reduce letters from the same group via the group multiplication. Define the group operation as concatenation. The identity element is the empty word, concatenation is associative, and the inverse of a reduced word $g_1 \cdots g_n$ is $g_n^{-1} \cdots g_1^{-1}$. Thus the free product of a family of groups is a group.

Define the inclusion homomorphisms $i_j : G_j \to *_{k\in I} G_k$ as $i_j(g) = g$. We want to show that $*_{i\in I} G_i$ satisfies the universal property of the coproduct. Let $f_i : G_i \to A$ be a family of group homomorphisms. For the diagram below to commute, $h : *_{k\in I} G_k \to A$ must be defined as $h(g) = f_j(g)$ for $g \in G_j$. Then we extend h to a group homomorphism. For a reduced word $g_1 \cdots g_n \in *_{k\in I} G_k$, we have $h(g_1 \cdots g_n) = h(g_1) \cdots h(g_n) = f_{j_1}(g_1) \cdots f(g_n)$ for $g_i \in G_{j_i}$. Since h is uniquely determined by the $\{f_j\}_{j\in I}$, the free product is the coproduct in the category of groups.



Problem 2. Let $\mathcal{C}$ be the category of groups and $\mathcal{C}'$ be its full subcategory with objects the abelian groups. Let $F : \mathcal{C}' \to \mathcal{C}$ be the inclusion functor. Determine the left adjoint of F and show that F has no right adjoint.

Let $f : G \to H$ be a group homomorphism where H is abelian. The commutator subgroup $[G, G]$ is generated the subgroup generated by $\{g_1 g_2 g_1^{-1} g_2^{-1} \in G \; g_1, g_2 \in G\}$. For $g_1, g_2 \in G$, we have $(g_1[G, G])(g_2[G, G]) = g_1 g_2 [G, G] = g_1 g_2 (g_2^{-1} g_1^{-1} g_2 g_1)[G, G] = g_2 g_1 [G, G] = (g_2[G, G])(g_1[G, G])$. Thus $G/[G, G]$ is an abelian group. Note $f(g_1 g_2) = f(g_1) f(g_2) = f(g_2) f(g_1) = f(g_2 g_1)$ and $f([G, G]) = 0$. Since $[G, G] \subset \ker(f)$, there is a unique abelian group homomorphism $h : G/[G, G] \to H$ such that $ph = f$ for projection $p : G \to G/[G, G]$.

We will define the functor $L : \mathcal{C} \to \mathcal{C}'$ as $L(G) := G/[G, G]$ for $[G, G]$ the commutator subgroup. Note that a morphism of groups $f : G \to H$ gives a unique morphism $\overline{f} : G \to H/[H, H]$ by composing with the projection. Since $H/[H, H]$ is an abelian group, the above argument implies $\overline{f}$ factors uniquely through $G/[G, G]$ as $\overline{f} = pg$ for $p : G \to [G, G]$ the projection. Note that $g(a[G, G]) = f(a)[H, H]$ for $a \in G$. Define $L(f) := g$. Let $1_G : G \to G$ be the identity group homomorphism. Then $\overline{1_G} : G \to G/[G, G]$ factors uniquely as the identity on $G/[G, G]$. We have $L(1_G) = 1_{L(G)}$. Now let $f : G \to H$ and $g : H \to I$ be two group homomorphisms. Then $gf : G \to I$ gives $L(gf) = h$ for $h : G/[G, G] \to I/[I, I]$ an abelian group homomorphism defined as $h(a[G, G]) = (gf)(a)[I, I]$. Now $L(f) : G/[G, G] \to H/[H, H]$ gives $L(f)(a[G, G]) = f(a)[H, H]$ and $L(g) : H/[H, H] \to I/[I, I]$ gives $L(g)(f(a)[H, H]) = g(f(a))[I, I]$. Thus $L(gf) = L(g)L(f)$ and L is a covariant functor.

We want to show that $\mathrm{Hom}_{\mathcal{C}}(A, F(B))$ and $\mathrm{Hom}_{\mathcal{C}'}(L(A), B)$ are in bijective correspondence for $A \in \mathrm{Ob}(\mathcal{C})$ and $B \in \mathrm{Ob}(\mathcal{C}')$ and the bijection is functorial in A and B. As we have seen, some $f \in \mathrm{Hom}_{\mathcal{C}}(A, F(B))$ factors uniquely through $L(A) = A/[A, A]$ since B is an abelian group. Define the natural isomorphism Φ whereby $\Phi_{A,B}(f)$ is this unique morphism. Thus $\mathrm{Hom}_{\mathcal{C}}(A, F(B)) \simeq \mathrm{Hom}_{\mathcal{C}'}(L(A), B)$ via $\Phi_{A,B}$. Let $g : A' \to A$ be a morphism of groups. Then we want to show the diagram below commutes. Note that $g([A, A]) \subset [A', A'] = \ker(A' \to A'/[A', A'])$ so g factors uniquely through $A/[A, A]$. We note that $L(g) : A/[A, A] \to A'/[A', A']$ is this unique morphism. Then $\Phi_{A,B}(f) \circ L(g) : A'/[A', A'] \to B$ descends from $f \circ g : A' \to A \to B$. By construction, $\Phi_{A',B}(f \circ g)$ descends from $f \circ g$. The uniqueness of these morphisms implies $\Phi_{A,B}(f) \circ L(g) = \Phi_{A',B}(f \circ g)$ and we are functorial in A. A similar argument shows the bijection is functorial in B. We conclude that L is a left adjoint to F.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(A, F(B)) & \xrightarrow{\Phi_{A,B}} & \mathrm{Hom}_{\mathcal{C}'}(L(A), B) \\ \downarrow{\scriptstyle -\circ g} & & \downarrow{\scriptstyle -\circ L(g)} \\ \mathrm{Hom}_{\mathcal{C}}(A', F(B)) & \xrightarrow{\Phi_{A',B}} & \mathrm{Hom}_{\mathcal{C}'}(L(A'), B) \end{array}$$

We will show that F does not have a right adjoint. We will first prove that a left adjoint functor F preserves

coproducts. Let G be the right adjoint. Let A_i be objects of $\mathcal{C}$ and B an object of $\mathcal{D}$. Then

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}\left(F\left(\coprod_i A_i\right), B\right) &\simeq \mathrm{Hom}_{\mathcal{D}}\left(\coprod_i A_i, B\right)\\ &\simeq \prod_i \mathrm{Hom}_{\mathcal{D}}(A_i, G(B))\\ &\simeq \prod_i \mathrm{Hom}_{\mathcal{C}}(F(A_i), B)\\ &\simeq \mathrm{Hom}_{\mathcal{C}}\left(\coprod_i F(A_i), B\right).\end{aligned}$$

By Yoneda Lemma, $F\left(\coprod_i A_i\right) \simeq \coprod_i F(A_i)$. The coproduct in the category of groups is the free product while the coproduct in the category of abelian groups is the direct sum. The free product $\mathbb{Z} * \mathbb{Z}$ is not isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$ so F does not have a right adjoint.

Problem 3. Let R be a ring. Show that R is a division ring if and only if all R-modules are free.

($\Rightarrow$) Assume that R is a division ring and let M be a left R-module. Let S be the set of all possible generating sets of M ordered by inclusion. The set S is not empty since $M \in S$. Let $\{x_i\}_{i\in I_0} \supset \{x_i\}_{i\in I_1} \supset \dots$ be a decreasing chain of elements of S. We claim $X := \bigcap_{j=1}^{\infty}\{x_i\}_{i\in I_j}$ is a generating set of M. Assume some $m \in M$ is not in the span of the elements of X. Then there is some index k such that m is not in the span of $\{x_i\}_{i\in I_k}$, contradicting our choices. By Zorn's Lemma, there is a minimal element $\{x_i\}_{i\in I}$ of S. If $\{x_i\}_{i\in I}$ is linearly independent, we are done. Assume otherwise so we have $\sum_{j=1}^{n} r_j x_j = 0$ where we only choose $r_j \neq 0$. Then $x_1 = -r_1^{-1}(\sum_{j=2}^{n} r_j x_j)$ and the set $\{x_i\}_{i\in I}\backslash x_1$ is a strictly smaller generating set. This contradicts our construction, which implies $\{x_i\}_{i\in I}$ is a basis for M. We conclude that all left R-modules are free. We make the same argument for right R-modules.

($\Leftarrow$) We will prove that an injective R-module homomorphism is surjective when R is a left Artinian ring (and thus left Noetherian). We can construct the descending chain $\mathrm{im}(f) \supset \mathrm{im}(f^2) \supset \dots$ of left R-modules. Then the descending chain terminates and $\mathrm{im}(f^k) = \mathrm{im}(f^{k+1})$ for some k. Take $b \in R$. Then $f^k(b) \in \mathrm{im}(f^k) = \mathrm{im}(f^{k+1})$ so there is some $c \in R$ such that $f^{k+1}(c) = f^k(b)$. Then $f^k(b - f(c)) = 0$ and f^k injective implies $b = f(c)$. Thus f is surjective.

Assume that all R-modules are free. Thus all R-modules are projective and R is semisimple. Then R is left Artinian and, consequently, left Noetherian. Right multiplication $f : R \to R$ by some $a \in R$ is a left R-module homomorphism. Since Ra is free as a left R-module, f is an injective R-module homomorphism. By above, f is a surjective left R-module homomorphism. There is some $b \in R$ such that $f(b) = ba = 1$. We conclude that every element $a \in R$ has a left inverse. Let c be the left inverse of b. Then $c = c(ba) = (cb)a = a$ and each element of R has an inverse. We conclude R is a division ring.

Problem 4. Let $M = \mathbb{Z}\left[\frac{1}{p}\right]$ and $N = \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Z}\left[\frac{1}{p}\right] \subset \mathbb{Q}$ is the subring generated by $\frac{1}{p}$ for a prime p. Show

(a) M is an Artinian module but not a Noetherian module

Note that M is the localization of $\mathbb{Z}$ away from the set $S := \{p^k : k \in \mathbb{N}, k \geqslant 1\}$. Let $I_k := \left(\frac{1}{p^k}\right)$ be $\mathbb{Z}$-submodules of M. If $I_k = I_{k+1}$, then there is some $r \in \mathbb{Z}$ such that $\frac{r}{p^k} = \frac{1}{p^{k+1}}$. In other words, there is some $s \in S$ such that $s(rp^{k+1} - p^k) = p^k s(rp - 1) = 0$. Since $\mathbb{Z}$ is an integral domain, this cannot occur. We have an ascending chain $I_1 \subset I_2 \subset \dots$ that does not terminate so M is not Noetherian.

Let $A \subset M$ be a proper $\mathbb{Z}$-submodule. Then there is a maximum $k \in \mathbb{N}$ for which $\frac{a}{p^k} \in A$ for $a \in \mathbb{Z}$ and $\gcd(a, p) = 1$. In this case, $\gcd(a, p^k) = 1$ so there are integers ℓ, m such that $ma + \ell p^k = 1$. Then $m\frac{a}{p^k} = \frac{1-\ell p^k}{p^k} = \frac{1}{p^k} \in M$. Thus $\frac{b}{p^i} \in M$ for all $b \in \mathbb{Z}$ and $i \leqslant k$. In other words, $A = \left(\frac{1}{p^k}\right)$. Take a strict descending chain $A_1 \supset A_2 \supset \dots$ of $\mathbb{Z}$-submodules of M. Then $A_1 = \left(\frac{1}{p^k}\right)$ for some $k \in \mathbb{N}$. Then $\frac{1}{p^j} \notin A_2$ for all natural numbers $j \geqslant k$. Thus $A_2 = \left(\frac{1}{p^i}\right)$ for $i < k$. Continuing this argument, the descending chain must terminate. Thus M is Artinian.

(b) N is neither Noetherian nor Artinian.

The counterexample in (a) proves that N is not Noetherian.

Order the prime numbers $\{p_i\}_{i\in\mathbb{N}}$. Define N_i as the $\mathbb{Z}$-submodule of N generated by $\left\{\frac{1}{p_i}, \frac{1}{p_{i+1}}, \dots\right\}$. Since the $p_i \in Z$ are prime, $\frac{1}{p_{i-1}} \notin N_i$ for each natural number $i \geqslant 2$. Then we can construct a descending chain $N_1 \supset N_2 \supset \dots$ that does not terminate. We conclude that N is not Artinian.

Problem 5. Let K and L be quadratic field extensions of a field k. Prove that $K \otimes_k L$ is an integral domain if and only if the k-algebras K and L are not isomorphic.

($\Rightarrow$) We will prove the contrapositive. Assume $K \simeq L$. We have $K \simeq k[x]/(f(x))$ for an irreducible quadratic $f(x) \in k[x]$. Then $K \otimes_k L \simeq K \otimes_k K \simeq K \otimes_k k[x]/(f(x)) \simeq K[x]/(f(x))$. Note that $f(x)$ has a root in K so $f(x) = (x-a)(x-b)$ for $a, b \in K$. By the Chinese Remainder Theorem, $K[x]/(f(x)) \simeq K[x]/(x-a) \times K[x]/(x-b) \simeq K \times K$. It is clear that $K \times K$ is not an integral domain by taking the elements $(1,0)(0,1) = (0,0)$. We conclude that $K \otimes_k L$ is not an integral domain.

($\Leftarrow$) We will prove the contrapositive. Assume $K \otimes_k L$ is not an integral domain. Since K is a quadratic extension of k, $K \simeq k[x]/(f(x))$ for an irreducible quadratic $f(x) \in k[x]$. We have $K \otimes_k L \simeq k[x]/(f(x)) \otimes_k L \simeq L[x]/(f(x))$. Since $K \otimes_k L$ is not an integral domain, $f(x)$ is not prime in $L[x]$. Note that $L[x]$ is a UFD so $f(x)$ is not irreducible in $L[x]$. Thus $f(x)$ has a root $\alpha \in L$ with $\alpha \notin k$. The field homomorphism $\varphi : K \simeq k[x]/(f(x)) \to L$ given by $\varphi(x) = \alpha$ and $\varphi(a) = a$ for $a \in k$ is well-defined. Any field homomorphism is injective since $\ker(\varphi)$ is an ideal of K. Note that L can be viewed as a 2-dimensional vector space over k with basis $\{1, \alpha\}$. Then φ is surjective since $\varphi(ax + b) = a\alpha + b$ for $a, b \in k$. We conclude that $K \simeq L$.

Problem 6. Let $K \subset L$ be subfields of $\mathbb{C}$ and let p be a prime. Assume K contains a non-trivial p-th root of unity. Show that L/K is a degree p Galois extension if and only if there is an element $a \in K$ that does not admit a p-th root, such that $L = K(\sqrt[p]{a})$.

($\Rightarrow$) Assume that L/K is a degree p Galois extension. Let $G := \mathrm{Gal}(L/K)$. Then G is cyclic, generated by some $\sigma \in G$. Let ξ be a primitive p-th root of unity. Since some primitive p-th root of unity is contained in K, we have all primitive p-th roots of unity in K. Thus $\xi \in K$ and $\sigma(\xi) = \xi$. Since L/K is separable, the Primitive Element Theorem implies $L = K[\beta]$ for some β in the algebraic closure of K. Define $\alpha := \prod_{i=0}^{p-1} \sigma^i(\beta)\xi^{p-i}$. Then

$$\sigma(\alpha) = \sigma\left(\prod_{i=0}^{p-1} \sigma^i(\beta)\xi^{p-i}\right) = \prod_{i=0}^{p-1} \sigma^{i+1}(\beta)\sigma(\xi)^{p-i} = \prod_{i=0}^{p-i} \sigma^{i+1}(\beta)\xi^{p-i} = \prod_{i=1}^{p} \sigma^i(\beta)\xi^{p-i+1} = \alpha\xi$$
$$\sigma(\alpha^p) = \sigma(\alpha)^p = (\alpha\xi)^p = \alpha^p\xi^p = \alpha^p$$

shows that $\alpha \notin K$. Additionally G is cyclic so α^p is fixed by G and $\alpha^p \in K$. Define $a := \alpha^p \in K$. Then the splitting field $M := K[\alpha]$ of $x^p - a$ is a subfield of L that strictly contains K. Then $[M : K] \neq 1$ divides $[L : K] = p$ so $[M : K] = p$. We conclude that $L = M = K[\sqrt[p]{a}]$.

($\Leftarrow$) Assume there is an element $a \in K$ that does not admit a p-th root and $L = K(\sqrt[p]{a})$. Then L is the splitting field of $x^p - a$ over K. The roots of $x^p - a$ are $\{\sqrt[p]{a}\xi^i\}$ for ξ a primitive p-th root of unity and $0 \leqslant i \leqslant p-1$. Since $\mathbb{C}$ is perfect, L/K is a separable and thus Galois extension. Note $\sqrt[p]{a} \notin K$ so there is some $\sigma \in \mathrm{Gal}(L/K)$ that does not fix $\sqrt[p]{a}$. The image of $\sqrt[p]{a}$ is a root which gives $\sigma(\sqrt[p]{a}) = \sqrt[p]{a}\xi^i$ for some $1 \leqslant i \leqslant p-1$. We have $\sigma^p(\sqrt[p]{a}) = \sqrt[p]{a}$ and $\sigma^j(\sqrt[p]{a}) \neq \sqrt[p]{a}$ for all $1 \leqslant j \leqslant p-1$ since p is prime. The order of σ must be at least p. However, L/F Galois implies $p \leqslant |\mathrm{Gal}(L/F)| = [L : F] = [K(\sqrt[p]{a}) : K] \leqslant p$. Thus $[L : K] = p$.

Problem 7. Determine the ring endomorphisms of $\mathbb{F}_2[t, t^{-1}]$, where t is an indeterminate.

Let $R := \mathbb{F}_2[t, t^{-1}]$. For a ring endomorphism $f : R \to R$, we have $f(1) = 1$ so f fixes the base field $\mathbb{F}_2$. Let $a \in R^\times$. We note $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = f(a^{-1})f(a)$ so f will send units to units with $f(a) = f(a)^{-1}$. Each endomorphism of R is thus determined by the image of t since $f(t^{-1}) = f(t)^{-1}$. Take a nonzero $p \in R$. Then there is some $k \in \mathbb{Z}$ such that $t^k p \in \mathbb{F}_2[t]$ and $t^k p$ has a nonzero constant term. If $p \in R^\times$, then $t^k p \in R^\times$ via $(t^k p)(p^{-1}t^{-k}) = 1$. If $t^k p \in R^\times$, then the product of two units $t^{-k}(t^k p) = p$ is also an element of $R^\times$. Thus $t^k p$ is a unit of R if and only if p is a unit of R so it is sufficient to classify $(\mathbb{F}_2[t])^\times$. We show below that $(\mathbb{F}_2[t])^\times = \{1\}$. Thus $R^\times = \{t^k\}$ for $k \in \mathbb{Z}$, and a ring endomorphism $f : R \to R$ will always be defined by $f(t) = t^k$ for some $k \in \mathbb{Z}$.

Let $p(t) = a_0 + \cdots + a_n t^n \in (\mathbb{F}_2[t])^\times$ with $a_n \neq 0$. Then there is some $q(t) = b_0 + \cdots + b_m t^m \in \mathbb{F}_2[t]$ such that $q(t)p(t) = 1$. Distributing the product, the constant term $a_0 b_0 = 1$ so $a_0, b_0 \in \mathbb{F}_2^\times$. Looking at the highest degree term, $a_n b_m = 0$ so $b_m = 0$ since $\mathbb{F}_2$ is an integral domain. Then the next largest term in the expansion yields $a_n b_{m-1} = 0$ so $b_{m-1} = 0$. We can continue this argument to show that $b_i = 0$ for all $i \geqslant 1$. Then $b_0(a_0 + \cdots + a_n t^n) = 1$ implies $n = 0$. In $\mathbb{F}_2[t]$, the set of units is $\{1\}$. (The more general result is $f = a_0 + \ldots a_n t^n \in R[t]$ is a unit if and only if $a_0 \in R^\times$ and a_i is nilpotent for all $i \geqslant 1$.)

Problem 8. Let G be a finite group of order pq, where p and q are distinct primes. Show that

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

Without loss of generality, assume $p > q$. Let m_p denote the number of Sylow p-subgroups of G. By Sylow's Third Theorem, $m_p \equiv 1 \pmod{p}$ and m_p divides q. Since q is prime, m_p is either 1 or q. But $q \not\equiv 1 \pmod{p}$ since $p > q$. Thus $m_p = 1$. Conjugation of a subgroup $H \subset G$ by $g \in G$ is again a subgroup of G of order $|H|$. Thus we will obtain a Sylow p-subgroup of G when we conjugate a Sylow p-subgroup by any element $g \in G$. Since we have a unique Sylow p-subgroup $P \subset G$, $gPg^{-1} = P$ and P is normal in G.

(b) if $p \not\equiv 1 \pmod{q}$ and $q \not\equiv 1 \pmod{p}$, then G is abelian.

Without loss of generality, assume $p > q$. By (a), the Sylow p-subgroup $P \subset G$ is a normal subgroup of G. Sylow's Theorems imply the existence of some Sylow q-subgroup $Q \subset G$. The subgroup $P \cap Q$ is a subgroup of both P and Q. Then $|P \cap Q| = 1$ since $|P|$ and $|Q|$ are relatively prime. All of this implies $G = P \rtimes Q$ for some group homomorphism $\varphi : Q \to \mathrm{Aut}(P)$. We have $\mathrm{Aut}(P) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. The generator $a \in Q$ has order q so it needs to map to an element of order dividing q, leaving 1 or q. By assumption, $p \not\equiv 1 \pmod{q}$ so $\varphi(a)$ is the identity automorphism. Thus $G \simeq P \times Q$ for P, Q cyclic (which implies abelian). We conclude that G is abelian.

Problem 9. Let G be a finite group of order p^n for a prime p. Show that the group ring $\mathbb{F}_p[G]$ over the finite field $\mathbb{F}_p$ with p elements has a unique maximal two-sided ideal.

List the elements of G as $\{g_i\}_{i=1}^{p^n}$ where $e = g_1$. Let $\varepsilon : \mathbb{F}_p[G] \to \mathbb{F}_p$ be the augmentation homomorphism given by $\varepsilon(\sum_{i=1}^{p^n} a_i g_i) = \sum_{i=1}^{p^n} a_i$. It is clear that ε is surjective. Let $I := \ker(\varepsilon)$ be the augmentation ideal. Since $\mathbb{F}_p[G]/I \simeq \mathbb{F}_p$, we note that I is a two-sided maximal ideal of $\mathbb{F}_p[G]$. Thus I contains the Jacobson radical of $\mathbb{F}_p[G]$ which we will denote $J(\mathbb{F}_p[G])$.

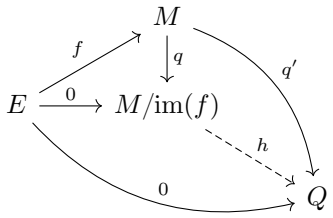
For an element $a \in I$, we can write $a = \sum_{i=1}^{p^n} a_i g_i$ with $\sum_{i=1}^{p^n} a_i = 0$. Then $a = \sum_{i=2}^{p^n} (-a_i)(e - g_i)$ and I is generated by $\{e - g_i\}_{i=2}^{p^n}$. The products I^k for $k \in \mathbb{N}$ are generated by products of k not necessarily distinct choices of $\{e - g_i\}_{i=2}^{p^n}$. We note that $(e - g_i)^{p^n} = 1^{p^n} - g_i^{p^n} = 0$ since $\mathbb{F}_p$ is characteristic p. Thus there is some large $N \in \mathbb{N}$ such that $I^N = 0$ and I is a nilpotent ideal. Every nilpotent ideal is contained in the Jacobson radical so $I \subset J(\mathbb{F}_p[G])$ and $I = J(\mathbb{F}_p[G])$. We conclude that I is the unique two-sided maximal ideal of $\mathbb{F}_p[G]$.

Problem 10. Let E, M and F be finite abelian groups and consider group homomorphisms

$$E \xrightarrow{f} M \xrightarrow{g} F.$$

Assume g is injective. Show that $|\mathrm{coker}(g \circ f)| = |\mathrm{coker}(g)| \cdot |\mathrm{coker}(f)|$ where $|X|$ denotes order of a finite set X.

We will show that in abelian groups, $\mathrm{coker}(f)$ is given by $M/\mathrm{im}(f)$. Note that $\mathrm{im}(f)$ is a normal subgroup of the abelian group M so the quotient $M/\mathrm{im}(f)$ is well-defined. Let $q : M \to M/\mathrm{im}(f)$ be the projection. Then given any abelian group Q for which the diagram below commutes, we want a unique abelian group morphism $h : M/\mathrm{im}(f) \to Q$. Note that $q'(f(e)) = 0$ for all $e \in E$ so $q'(\mathrm{im}(f)) = 0$. In other words, $\mathrm{im}(f) \subset \ker(q')$ and q' factors uniquely through $M/\mathrm{im}(f)$.



Now g injective implies $|\text{im}(g)| = |M|$ and $|\text{im}(gf)| = |\text{im}(f)|$. Thus by the finiteness of the abelian groups in question,

$$|\text{coker}(g \circ f)| = |F|/|\text{im}(gf)| = |F|/|\text{im}(f)| = |F|/|\text{im}(g)| \cdot |M|/|\text{im}(f)| = |\text{coker}(g)| \cdot |\text{coker}(f)|$$

as desired.

Fall 2015

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

We want to show that $f : \mathbb{Z} \to \mathbb{Q}$ is right cancellative. Let $g, h : \mathbb{Q} \to R$ be ring homomorphisms such that $gf = hf$ for R a ring with identity. For $a, b \in \mathbb{Z}$ we have

$$g\left(\frac{a}{b}\right) = g(a)g(b^{-1}) = g(a)g(b)^{-1} = h(a)h(b)^{-1} = h\left(\frac{a}{b}\right)$$

since $g(a) = g(f(a)) = h(f(a)) = h(a)$ for all $a \in \mathbb{Z}$. We conclude $g = h$ and f is an epimorphism

Problem 2. Let R be a principal ideal domain with field of fractions K.

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

We will first prove that the ideals of $R[S^{-1}]$ are in one-to-one correspondence with the ideals of R that are disjoint from S. Let $I \subset R$ be an ideal. We claim $S^{-1}I$ is a proper ideal of $R[S^{-1}]$ when $I \cap S = \varnothing$. Since I is a proper ideal R, $S^{-1}I = R[S^{-1}]$ implies I contains some element of S. Thus $I \cap S = \varnothing$ means $S^{-1}I$ is a proper subset of $R[S^{-1}]$. For $\frac{a}{s}, \frac{b}{t} \in S^{-1}I$, we have $\frac{ta+sb}{st} \in S^{-1}I$ since $ta + sb \in I$ and $st \in S$. For $\frac{r}{t} \in S^{-1}R$ and $\frac{a}{s} \in R[S^{-1}]$, we have $\frac{ra}{st} \in S^{-1}I$ since $ra \in I$ and $st \in S$. Given an ideal $J \subset R[S^{-1}]$, define $I := \{a \in R : \frac{a}{1} \in J\}$. If $\frac{a}{s} \in J$, then $\frac{s}{1}\frac{a}{s} = \frac{a}{1} \in J$ so I is the set of all numerators of J. If $J \subset R[S^{-1}]$ is a proper ideal, then $\frac{1}{1} \notin J$ so $1 \notin I$ is a proper subset of R. Now $ra \in I$ for all $a \in I$ and $r \in R$ since $\frac{r}{1}\frac{a}{1} = \frac{ra}{1} \in J$. For $a, b \in I$ we have $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \in J$ so $a + b \in I$. We conclude that $I \subset R$ is a proper ideal.

Returning to the problem, let $J \subset R[S^{-1}]$ be an ideal. Then the ideal $I \subset R$ of all numerators of J is principal. Let $I = (a)$ for $a \in R$. Then we claim that $J = \left(\frac{a}{1}\right)$. Certainly $J \supset \left(\frac{a}{1}\right)$. Let $\frac{j}{s} \in J$. Then $j = ra$ for some $r \in R$ and $\frac{r}{s}\frac{a}{1} = \frac{ra}{s} = \frac{j}{s}$. We conclude $J = \left(\frac{a}{1}\right)$ and $R[S^{-1}]$ is a principal ideal domain.

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

Let $R \subset T \subset K$ be a subring. Define $S := \{s \in R\backslash\{0\} : \frac{1}{s} \in T\}$. Since $\frac{1}{1} \in T$ we have $1 \in S$. Given $s, t \in S$, we have $\frac{1}{s}\frac{1}{t} = \frac{1}{st} \in T$ so $st \in S$. Thus S is a multiplicatively closed subset of R and $T \supset R[S^{-1}]$. Let $\frac{a}{s} \in T$ and we want to show $\frac{a}{s} \in S^{-1}R$. We can assume $\gcd(a, s) = 1$ since R is a UFD. In the PID R, Bezout's identity implies there are elements $k, \ell \in R$ such that $ka + \ell s = 1$. Thus $\frac{k}{1}\frac{a}{s} + \frac{s}{s}\frac{\ell}{1} = \frac{ka+\ell s}{s} = \frac{1}{s} \in T$ so $\frac{a}{s} \in R[S^{-1}]$. We conclude $T = R[S^{-1}]$ for a multiplicatively closed set S of $R\backslash\{0\}$.

Problem 3. Let k be a field and define $A = k[X, Y]/(X^2, XY, Y^2)$.

(a) What are the principal ideals of A?

Take a polynomial with coefficients in k. We can reduce all terms of degree greater than or equal to 2. Thus the general element of A is $aX + bY + c$ for $a, b, c \in k$. Clearly (0) and (1) = A are principal ideals. A nontrivial, proper principal ideal will have some element $ax + by + c$. Assume $a \neq 0$. Since k is a field, the ideals $(aX + bY + c) = (X + a^{-1}bY + a^{-1}c)$. If $a = 0$, then the element $bY + c$ gives the same principal ideal as $Y + b^{-1}c$ if b is nonzero. If $b = 0$, we see $(c) = (1) = A$ if $c \neq 0$ since c has an inverse in k or $(c) = (0)$ for $c = 0$. Thus all principal ideals have one of the following forms $\{(0), A, (X + aY + b), (Y + c)\}$ for $a, b, c \in k$.

FIX THIS, GUYS WITH NONZERO CONSTANT TERMS ARE UNITS

(b) What are the ideals of A?

Take a nontrivial, proper ideal $I \subset A$. If I is principal, then I is listed above. Assume I is not principal. Then there is some element $aX + bY + c$ for a or b nonzero. First assume $a \neq 0$. Then $(X + a^{-1}bY + a^{-1}c) \in I$ and take $B := a^{-1}b$ and $C := a^{-1}c$ for $B, C \in k$. Since I is not principal, there is some $(dX + eY + f) \in I$

such that $dX + eY + f$ is not a multiple of $X + BY + C$. If $d = 0$, then we have $(Y + F) \in I$ for $F := e^{-1}f$. We find $(X + BY + C) - B(Y + F) = X + (C - BF) \in I$. Given any element $(gX + hY + i) \in I$, we find $(gX + hY + i) - g(X + (C - BF)) - h(Y + F) = (i - g(C - BF) - hF) \in I$. If $i - g(C - BF) - hF \neq 0$, then $I = A$, contradicting our choice. Thus $(gX + hY + i) = g(X + (C - BF)) + h(Y + F)$ and we have $I = (X + (C - BF), Y - F)$.

If $d \neq 0$, we have $(X + EY + F) \in I$ for $E := d^{-1}e$ and $F := d^{-1}f$. Reducing, $(X + EY + F) - (X + BY + C) = (E - B)Y + (F - C) \in I$ and we know $(E - B)Y + (F - C) \neq 0$ by construction. If $E - B = 0$, then $F - C \neq 0$ and $I = A$, contradicting our choice. Thus $E - B \neq 0$ and we have $Y + (E - B)^{-1}(F - C) \in I$. We are now in the case of $d = 0$ so $I = (X + J, Y + (E - B)^{-1}(F - C))$ for $J \in k$.

We now take $a = 0$. Then we have $(Y + b^{-1}c) \in I$. Let $C := b^{-1}c$. Take $(dX + eY + f) \in I$ such that $dX + eY + f$ is not a multiple of $Y + C$. We have $(dX + eY + f) - e(Y + C) = (dX + (f - eC)) \in I$. We cannot have $d = 0$ since I is proper. Then $I = (X + D, Y + C)$ for $D := d^{-1}(f - eC)$ as above. Thus all ideals of A are of the form $\{(0), A, (X + aY + b), (Y + c), (X + d, Y + e)\}$ for $a, b, c, d, e \in k$.

Problem 4. Let K be a field and let L be the field $K(X)$ of rational functions over K.

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

We define $f : L \to L$ as $f(k) = k$ for $k \in K$ and $f(X) = X^{-1}$. Then extend f to a K-homomorphism. Similarly, $g : L \to L$ is defined as $g(k) = k$ for $k \in K$ and $g(X) = 1 - X$. Then we extend g to a K-homomorphism. We will now show that f and g are automorphisms of L. Since L is a field, f and g are injective. Take $\frac{p(X)}{q(X)} \in L$ for $p(X), q(X) \in K[X]$. Then $f\left(\frac{p(X^{-1})}{q(X^{-1})}\right) = \frac{f(p(X^{-1}))}{f(q(X^{-1}))} = \frac{p(X)}{q(X)}$. Thus f is a K-automorphism. Similarly, $g\left(\frac{p(1-X)}{q(1-X)}\right) = \frac{p(X)}{q(X)}$ so g is a K-automorphism.

Note that $f \neq g$ via the image of X. Then G contains at least $\{e, f, g\}$ where e is the identity K-automorphism. Now $gf(X) = g(X^{-1}) = \frac{1}{1-X}$ and $fg(X) = f(1 - X) = 1 - X^{-1} = \frac{X-1}{X}$. If $\frac{1}{1-X} = \frac{X-1}{X}$, then $\frac{X+(1-X)^2}{X(1-X)} = 0$ and X would be algebraic over K, a contradiction. Thus $gf \neq fg$ as K-automorphisms. A similar argument shows that both gf and fg are distinct from e, f, and g. Thus G contains at least $\{e, f, g, fg, gf\}$ and $|G| > 3$.

It will be important later to show that $|G| \geqslant 6$. Take $fgf(X) = f\left(\frac{1}{1-X}\right) = \frac{1}{1-X^{-1}} = \frac{X}{X-1}$. Then a similar argument to above shows that fgf is distinct from e, f, g, fg, and gf. Thus $|G| \geqslant 6$.

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

We want to show that P is fixed under f and g action.

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

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

Thus $P \in L^G$.

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

We construct a polynomial with coefficients in $K(P)$ for which X is a root. Define

$$p(T) := (T^2 - T + 1)^3 - P(T^2(T-1)^2)$$

for $p(T) \in K(P)[T]$ so $p(X) = 0$. Since p is degree 6, $[L : K(P)] \leqslant 6$. Note that $P \in L^G$ by (b) so $K(P) \subset L^G \subset L$. By the final argument of (a), we have $6 \leqslant [L : L^G] \leqslant [L : K(P)] \leqslant 6$. Therefore, $L/K(P)$ is a finite extension of degree 6.

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

The chain of inequalities in (c) implies $[L : L^G] = 6$. By Artin's Theorem, L/L^G is a Galois extension with Galois group $\mathrm{Gal}(L/L^G) \simeq G$. The finite Galois extension satisfies $|G| = [L : L^G] = 6$. By (a), it is clear that G is not abelian. The only nonabelian group of order 6 is S_3. Thus $G \simeq S_3$.

Problem 5.

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

By Sylow's Third Theorem, the number of Sylow p-subgroups m_p satisfies $m_p \equiv 1 \pmod{p}$ and m_p divides v. Thus $m_p = kp + 1$ for $k \geqslant 0$. However, $p > v$ and $m_p | v$ implies $k = 0$. We conclude $m_p = 1$. Let P be the unique Sylow p-subgroup of G. As in Spring 2015 Problem 8, conjugation of P by an element $g \in G$ is another Sylow p-subgroup. Thus $gPg^{-1} = P$ and P is a normal Sylow p-subgroup of G.

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

Let H be a nontrivial finite p-group. Thus $|H| = p^k$ for $k > 0$. Act on the set H by H via conjugation. An element is fixed by conjugation if and only if the element is in the center of H. The class equation implies

$$|H| = |Z(H)| + \sum_{h \in H, h \notin Z(H)} |\mathrm{Orb}(h)|.$$

We have $p||H|$ and $|\mathrm{Orb}(h)| = [G : \mathrm{Stab}(h)]$ by Orbit-Stabilizer. Thus $p||\mathrm{Orb}(h)|$ for each $h \notin Z(H)$. We conclude that p divides $|Z(G)| = |H| - \sum_{h \in H, h \notin Z(H)} |\mathrm{Orb}(h)|$. Note $|Z(H)| > 1$ since the identity of H is contained in the center. Thus $|Z(H)| \geqslant p$ so H has a nontrivial center.

Problem 6. Let F be a field of characteristic not 2. Let a and b be nonzero elements of F. Let R be the F-algebra $R = F\langle i, j\rangle/(i^2 - a, j^2 - b, ij + ji)$, the quotient of the free associative algebra on 2 generators by the given two-sided ideal.

(a) Let $\overline{F}$ be the algebraic closure of F. Show that $R \otimes_F \overline{F}$ is isomorphic as an $\overline{F}$-algebra to the matrix algebra $\mathrm{M}_2(\overline{F})$.

Let $\alpha \in \overline{F}$ be such that $\alpha^2 = a$ and $\beta \in \overline{F}$ such that $\beta^2 = b$. Define the F-algebra homomorphism $f : F\langle i, j\rangle \otimes_F \overline{F} \to \mathrm{M}_2(\overline{F})$ by $f(1 \otimes 1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $f(i \otimes 1) = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$, and $f(j \otimes 1) = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}$.

$$f\left(i \otimes \frac{\alpha^{-1}}{2} + 1 \otimes \frac{1}{2}\right) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$f\left(i \otimes \frac{\alpha^{-1}}{2} - 1 \otimes \frac{1}{2}\right) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} - \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$$

$$f\left(\frac{1}{2}(i \otimes \alpha^{-1})(j \otimes \beta^{-1}) + j \otimes \frac{\beta^{-1}}{2}\right) = \begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} + \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$f\left(\frac{1}{2}(i \otimes \alpha^{-1})(j \otimes \beta^{-1}) - j \otimes \frac{\beta^{-1}}{2}\right) = \begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} - \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$$

We see that f is surjective since the above matrices generate $\mathrm{M}_2(\overline{F})$ as an $\overline{F}$-algebra. By construction, $(i \otimes 1)^2 - (a \otimes 1)$, $(j \otimes 1)^2 - (b \otimes 1)$, and $(i \otimes 1)(j \otimes 1) + (j \otimes 1)(i \otimes 1)$ are all elements in the kernel of f. With the above relationships, we can reduce all other elements to the form $c_1(i \otimes 1) + c_2(j \otimes 1) + c_3(i \otimes 1)(j \otimes 1) + c_4(1 \otimes 1)$.

$$f(c_1(i \otimes 1) + c_2(j \otimes 1) + c_3(i \otimes 1)(j \otimes 1) + c_4(1 \otimes 1)) = c_1 \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix} + c_2 \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} + c_3 \begin{pmatrix} 0 & \alpha\beta \\ -\alpha\beta & 0 \end{pmatrix} + c_4 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

If the above is zero, we need $c_i = 0$ for all $1 \leqslant i \leqslant 4$. Thus $\ker(f)$ is the normal subgroup of $F\langle i, j\rangle \otimes_F \overline{F}$ generated by $\{(i \otimes 1)^2 - (a \otimes 1), (j \otimes 1)^2 - (b \otimes 1), (i \otimes 1)(j \otimes 1) + (j \otimes 1)(i \otimes 1)\}$. Then $\overline{f} : (F\langle i, j\rangle \otimes_F \overline{F})/\ker(f) \simeq R \otimes_F \overline{F} \to \mathrm{M}_2(\overline{F})$ is an isomorphism.

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

By (a), $R \otimes_F \overline{F} \simeq \mathrm{M}_2(\overline{F})$ is a central simple $\overline{F}$-algebra. Note $F \subset Z(R)$. If $Z(R) \neq F$, then it is a k-dimensional vector space over F for some k. Thus $Z(R) \otimes_F \overline{F} \simeq \bigoplus_{i=1}^{k} \overline{F}$. But, $Z(R \otimes_F \overline{F}) = Z(R) \otimes_F Z(\overline{F}) = Z(R) \otimes_F \overline{F} = \overline{F}$. Thus $Z(R) = F$. If R is not simple, then there is a two-sided ideal $I \subset R$. Then $I \otimes_F \overline{F}$ would be a proper two-sided ideal of $R \otimes_F \overline{F}$. Since $R \otimes_F \overline{F}$ is simple, R is simple. Thus R is a central simple F-algebra and $\dim_F(R) = \dim_{\overline{F}}(R \otimes_F \overline{F}) = \dim_{\overline{F}}(\mathrm{M}_2(\overline{F})) = 4$.

By the argument in (a), we have that $\{1 \otimes 1, i \otimes 1, j \otimes 1, ij \otimes 1\}$ is linearly independent in $R \otimes_F \overline{F}$ as an $\overline{F}$-vector space. Thus $\{1, i, j, ij\}$ is a linearly independent set and a basis of R as an F-vector space.

Problem 7. Show the symmetric group S_4 has exactly two isomorphism classes of irreducible complex representations of dimension 3. Compute the characters of these two representations.

We will first show that the abelianization $S_4/[S_4, S_4]$ has order 2. The commutator subgroup $[S_4, S_4]$ is generated by elements $ghg^{-1}h^{-1} \in S_4$. Each $ghg^{-1}h^{-1}$ is an even permutation so $[S_4, S_4] \subset A_4$. The nonidentity elements of A_4 are of the form $(ij)(k\ell)$ or (ijk) for $1 \leqslant i, j, k, \ell \leqslant 4$. Without loss of generality, we will show $(123), (14)(23) \in [S_4, S_4]$. Notice $(23)(12)(23)(12) = (123) \in [S_4, S_4]$ and $(123)(234)(132)(243) = (14)(23) \in [S_4, S_4]$ as desired. Thus $[S_4, S_4] = A_4$ and $|S_4/[S_4, S_4]| = 2$.

Each one-dimensional representation of S_4 is a group homomorphism $\rho : S_4 \to \mathbb{C}^\times$. Since $\mathbb{C}^\times$ is an abelian group, ρ factors uniquely through the abelian group $S_4/[S_4, S_4]$. If two one-dimensional representations are equal on $S_4/[S_4, S_4]$, then they were equal as homomorphisms from S_4. Thus the number of one-dimensional representations of $S_4/[S_4, S_4]$ is equal to the number of one-dimensional representations of S_4. By above, $S_4/[S_4, S_4]$ has two conjugacy classes so it has two one-dimensional irreducible representations. We conclude that S_4 should have two one-dimensional representations. (This works for one-dimensional irreducible representations of any group.)

Now the trivial representation and the sign representation, $\text{sgn} : S_4 \to \mathbb{C}^\times$, are the two one-dimensional representations of S_4. The conjugacy classes of S_4 are based on cycle type of which there are five. Since $|S_4| = 24$, we have $24 = 1 + 1 + a^2 + b^2 + c^2$ for $a, b, c \in \mathbb{N}$ representing the dimensions of the three other irreducible representations. If we take $c \geqslant 4$, we are left with $a^2 + b^2 = 6$, which cannot occur. Thus $1 < a, b, c \leqslant 3$. We cannot have $a = b = c = 2$ so, without loss of generality, take $c = 3$. Then we need $13 = a^2 + b^2$ so the only option is $a = 2$ and $b = 3$. Thus S_4 has two 3-dimensional irreducible representations.

We will realize the two irreducible representations in question. Define the vector space $V := \{(v_i) \in \mathbb{R}^4 : \sum_{i=1}^4 v_i = 0\}$. Then V has a left S_4 action via $\sigma(v_i) = (v_{\sigma(i)})$ for $\sigma \in S_4$. Then $\{(-1, 1, 0, 0), (-1, 0, 1, 0), (-1, 0, 0, 1)\}$ is a basis for V. The action described gives an irreducible representation for S_4 since $(23)(-1, 1, 0, 0) = (-1, 0, 1, 0)$ and $(24)(-1, 1, 0, 0) = (-1, 0, 0, 1)$. In other words, there is no S_4-invariant subspace of V. Let $\rho : S_4 \to M_3(\mathbb{C})$ be the described irreducible representation.

	e	(12)	(123)	(12)(34)	(1234)
χ_{sgn}	1	-1	1	1	-1
χ_ρ	3	1	0	-1	-1

Now $\rho \otimes \text{sgn}$ is an irreducible representation of $S_4 \times S_4$. Include S_4 along the diagonal of $S_4 \times S_4$ to make $\rho \otimes \text{sgn}$ a representation of S_4. The character $\chi_{\rho\otimes\text{sgn}}(g) = \chi_\rho(g)\chi_{\text{sgn}}(g)$ which gives the following row of the character table.

	e	(12)	(123)	(12)(34)	(1234)
$\chi_{\rho\otimes\text{sgn}}$	3	-1	0	-1	1

We have an inner product on the space of class functions such as $\langle \chi_\mu, \chi_\nu \rangle = \frac{1}{|G|} \sum_{g\in G} \chi_\mu(g)\chi_\nu(g^{-1})$. We know that $\langle \chi_{\rho\otimes\text{sgn}}, \chi_{\rho\otimes\text{sgn}} \rangle = 1$ if and only if $\rho \otimes \text{sgn}$ is an irreducible representation. We note that the number of elements in each conjugacy class are $1, 6, 8, 3, 6$ respectively. Since g^{-1} and g are in the same conjugacy class for all $g \in S_4$,

$$\langle \chi_{\rho\otimes\text{sgn}}, \chi_{\rho\otimes\text{sgn}} \rangle = \frac{1}{24}(1(9) + 6(1) + 8(0) + 3(1) + 6(1)) = 1.$$

Thus $\rho \otimes \text{sgn}$ is the other irreducible representation of S_4.

Problem 8. Let F be a field. Show that the group $\text{SL}(2, F)$ is generated by the matrices $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$ for elements e in F.

The group $\text{SL}(2, F)$ is all 2×2 contains matrices with determinant one. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a general matrix in $\text{SL}(2, F)$. Case 1: If $a = 0$ or $d = 0$, then $c = -b^{-1}$. Case 2: If $b = 0$ or $c = 0$, then $d = a^{-1}$. Case 3: Assuming nonzero $a, b, c, d \in F$, then $A = \begin{pmatrix} d^{-1}(1 + bc) & b \\ c & d \end{pmatrix}$. We will show that we can construct each of these cases with

the matrices $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$. Let $a, b, e, f \in F$. Case 1 is given by the following.

$$\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -e^{-1} & 1 \end{pmatrix} = \begin{pmatrix} 0 & e \\ -e^{-1} & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & e \\ -e^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & e(1-a) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & e \\ -e^{-1} & a \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ -e^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & e \\ -e^{-1} & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & e(1-a) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & e \\ -e^{-1} & 0 \end{pmatrix} = \begin{pmatrix} a & e \\ -e^{-1} & 0 \end{pmatrix}$$

Case 2 can be constructed by the following.

$$\begin{pmatrix} 0 & -be \\ e^{-1}b^{-1} & 0 \end{pmatrix}\begin{pmatrix} 0 & e \\ -e^{-1} & -e^{-1}b^{-1}a \end{pmatrix} = \begin{pmatrix} b & a \\ 0 & b^{-1} \end{pmatrix}$$
$$\begin{pmatrix} 0 & -e^{-1} \\ e & -e^{-1}b^{-1}a \end{pmatrix}\begin{pmatrix} 0 & e^{-1}b^{-1} \\ -be & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ a & b^{-1} \end{pmatrix}$$

Let $c, d \in F$. Case 3 begins as follows.

$$\begin{pmatrix} b & a \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} c & 0 \\ d & c^{-1} \end{pmatrix} = \begin{pmatrix} bc+ad & ac^{-1} \\ b^{-1}d & b^{-1}c^{-1} \end{pmatrix}$$

Then $(b^{-1}c^{-1})^{-1}(1+(ac^{-1})(b^{-1}d)) = bc(1+ab^{-1}c^{-1}d) = bc+ad$, the first row, first column entry above. We can generate every matrix in Cases 1, 2, and 3. We conclude $\mathrm{SL}(2,F)$ is generated by $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$.

Problem 9.

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

Let $x \in J(R)$ such that $x \neq 0$. Thus $x \notin F$. By finite dimension, $\{1, x, \ldots, x^n\}$ is a linearly dependent set for some $n \in \mathbb{N}$. Choose n minimal. If $x^n = 0$, we are done so assume otherwise. Then $x^n = \sum_{i=0}^{n-1} a_i x^i$ and $0 = x^n - \sum_{i=0}^{n-1} a_i x^i$. Factor out x^j for maximal j which implies $a_j \neq 0$. Define $b_i := a_j^{-1} a_i$ so $b_j = 1$. Then

$$0 = a_j x^j \left(a_j^{-1} x^{n-j} - \sum_{i=j}^{n-1} b_i x^{i-j} \right) = a_j x^j \left(1 - \left(\sum_{i=j+1}^{n-1} (b_i x^{i-j-1}) - a_j^{-1} x^{n-j-1} \right) x \right).$$

Since $x \in J(R)$, we have $\left(1 - \left(\sum_{i=j+1}^{n-1}(b_i x^{i-j-1}) - a_j^{-1}x^{n-j-1}\right)x\right) \in R^\times$ so $a_j x^j = 0$. Then $a_j \in R^\times$ implies $x^j = 0$, contradicting the minimality of n. We conclude that $x^n = 0$ for some n. Therefore, every element of the Jacobson radical is nilpotent.

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

In Problem 2, we derived the correspondence of ideals in a localization. We want to show that a prime ideal of R maps to a prime ideal of $S^{-1}R$ for S a multiplicatively closed subset of $R\backslash\{0\}$ with $1 \in S$ under this correspondence. Let $\mathfrak{p} \subset R$ be a prime ideal. Let $\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \in S^{-1}\mathfrak{p}$. Then $ab \in \mathfrak{p}$ so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Thus $\frac{a}{s} \in S^{-1}\mathfrak{p}$ or $\frac{b}{t} \in S^{-1}\mathfrak{p}$. Note that $\frac{1}{1} \in S^{-1}\mathfrak{p}$ implies there is some $\frac{a}{1} \in S^{-1}\mathfrak{p}$ such that $sa = 1$ for $a \in \mathfrak{p}$. Thus $1 \in \mathfrak{p}$, a contradiction. We conclude $S^{-1}\mathfrak{p}$ is proper and, as a result, $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}R$.

An element of the Jacobson radical is not always nilpotent. In commutative rings, the nilradical, the set of all nilpotent elements, is the intersection of all prime ideals of the ring. The Jacobson radical is the intersection of all maximal ideals of R. The ring $\mathbb{Z}[x]$ has maximal ideal $(2, x)$. Let $R = \mathbb{Z}[x]_{(2,x)}$ be the localization of $\mathbb{Z}[x]$ with $S = \mathbb{Z}[x]\backslash(2, x)$. Then R is local with $J(R) = S^{-1}(2, x)$. Note $Z[x]/(2) \simeq (\mathbb{Z}/2\mathbb{Z})[x]$, which is an integral domain. Thus (2) is a prime ideal of $\mathbb{Z}[x]$. Similarly, $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$, an integral domain. Thus (x) is a prime

ideal of $\mathbb{Z}[x]$. By the argument above, $S^{-1}(2)$ and $S^{-1}(x)$ are prime ideals of R. We see that $S^{-1}(2) \cap S^{-1}(x)$ is a strict subset of the Jacobson radical $S^{-1}(2, x)$. Take for instance $\frac{2+x}{1} \in J(R)$ but $\frac{2+x}{1}$ is not nilpotent.

A nilpotent element is not always in the Jacobson radical of a ring R. Let $R = \mathrm{M}_2(\mathbb{C})$ and $A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathrm{M}_2(\mathbb{C})$. It is clear that A^2 is the zero matrix so A is nilpotent. Then we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

The result is not invertible so $A \notin J(R)$.

Problem 10. Let p be a prime number. For each abelian group K of order p^2, how many subgroups H of $\mathbb{Z}^3$ are there with $\mathbb{Z}^3/H$ isomorphic to K.

Note that $\mathbb{Z}^3$ is abelian so each subgroup $H \subset \mathbb{Z}^3$ is normal. Let S be the set of surjective group homomorphisms $f : \mathbb{Z}^3 \to K$ and T be the set of all subgroups H of $\mathbb{Z}^3$ for which $\mathbb{Z}^3/H \simeq K$. Then define a set map $\Phi : S \to T$ by $\Phi(f) = \ker(f)$. Let $\mathrm{Aut}(K)$ be the group automorphism of K, and $\mathrm{Aut}(K)$ acts on S by post-composition. Denote by $S/\mathrm{Aut}(K)$ the set of orbits of S under the action by $\mathrm{Aut}(K)$. Let $\sigma \in \mathrm{Aut}(K)$, then $\ker(\sigma \circ f) = \ker(f)$ since σ is injective. As a result, $\overline{\Phi} : S/\mathrm{Aut}(K) \to T$ is a well-defined set map. Surjectivity of $\overline{\Phi}$ follows from the fact that each subgroup H for which $\mathbb{Z}^3/H \simeq K$ defines a surjective group homomorphism $f : \mathbb{Z}^3 \to \mathbb{Z}^3/H \simeq K$.

We want to show that $\overline{\Phi}$ is injective. Let $f, g \in S$ such that $\ker(f) = \ker(g)$. By the universal property of quotients, f factors through $\mathbb{Z}^3/\ker(f)$, and there is some isomorphism $\alpha : \mathbb{Z}^3/\ker(f) \to K$ such that $\alpha \circ \pi = f$ for $\pi : \mathbb{Z}^3 \to \mathbb{Z}^3/H$ the canonical quotient homomorphism. Similarly, $\beta \circ \pi = g$ for an isomorphism $\beta : \mathbb{Z}^3/\ker(g) \to K$. Then $f = (\alpha \circ \beta^{-1}) \circ g$ where $(\alpha \circ \beta^{-1}) \in \mathrm{Aut}(K)$, and f and g are in the same $\mathrm{Aut}(K)$-orbit of S. We conclude that $\overline{\Phi}$ is a bijection.

It is sufficient to find the number of surjective group homomorphisms $f : \mathbb{Z}^3 \to K$ for each K. There are only two abelian groups of order p^2: $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Case 1: Let $K = \mathbb{Z}/p^2\mathbb{Z}$. We need only find images for the 3 generators of the free abelian group $\mathbb{Z}^3$. Let $x, y \in \mathbb{Z}/p^2\mathbb{Z}$ be non-generating elements. They are classes represented by integers divisible by p. Then representatives of $x + y$ are divisible by p and $x + y$ does not generate $\mathbb{Z}/p^2\mathbb{Z}$. Thus at least one of the generators of $\mathbb{Z}^3$ must map to a generator of $\mathbb{Z}/p^2\mathbb{Z}$ in order for the homomorphism to be surjective. There are $\phi(p^2) = p^2 - p$ generators of $\mathbb{Z}/p^2\mathbb{Z}$ for Euler's totient function φ. There are p^6 total homomorphisms and p^3 homomorphisms that are not surjective. Since $|\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})| = \varphi(\mathbb{Z}/p^2\mathbb{Z}) = p^2 - p$, there are $\frac{p^6-p^3}{p^2-p} = p^4 + p^3 + p^2$ total subgroups H of $\mathbb{Z}^3$ for which $\mathbb{Z}^3/H \simeq \mathbb{Z}/p^2\mathbb{Z}$.

Case 2: Let $K = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Once again, we need only find images for the 3 generators of the free abelian group $\mathbb{Z}^3$. Note that K is no longer generated by just one element. For the homomorphism to be surjective, we need the image of at least two of the generators of $\mathbb{Z}^3$ to map to generators of K. This equates to sending one generator to a nontrivial element $a \in K$ and sending a second to an element outside the subgroup generated by a in K. The subgroup generated by a will have order p. We have three scenarios. If the first generator is sent to a nonzero $a \in K$, we have $(p^2 - 1)(p^2 - p)(p^2) + (p^2 - 1)(p)(p^2 - p)$ options depending on the image of the second generator. If the first generator is sent to zero, we have $(p^2 - 1)(p^2 - p)$ options. In total, we have $p^6 - p^4 - p^3 + p$ surjective homomorphisms. There are $(p^2 - 1)(p^2 - p) = p^4 - p^3 - p^2 + p$ automorphisms of K which implies $\frac{p^6-p^4-p^3+p}{p^4-p^3-p^2+p} = p^2 + p + 1$ subgroups H of $\mathbb{Z}^3$ such that $\mathbb{Z}^3/H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Spring 2016

Problem 1.

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

Let $A := \mathbb{Z}[x]$. We know that A is a UFD by an application of Gauss's Lemma. Let $I := (2, x)$ and we claim that I is not a principal ideal. We will first show that I is a proper ideal of A. For $1 \neq 2a + bx$, we would need $b = 0$. Then there are no possible choices for a since $1 \notin 2\mathbb{Z}$. Thus $1 \notin I$ and I is a proper ideal of A.

Assume $I = (p)$ for some $p \in A$. Then there is an $r \in A$ such that $rp = 2$. Since $\mathbb{Z}$ is an integral domain, $0 = \deg(rp) = \deg(r) + \deg(p)$ so $\deg(p) = 0$. Thus $p \in \mathbb{Z}$ and the only integer divisors of 2 are $\pm 1, \pm 2$. Since I is a proper ideal, $p = \pm 2$. We note $(2) = (-2)$ so take $p = 2$. Now there is some $s \in A$ such that $sp = x$. However, $2s = x$ cannot occur. We conclude that I is not principal.

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

Let $a \in \mathfrak{p}$ be some nonzero element. Since R is a UFD, we can factor a as a product of irreducible elements $a = \prod_{i=1}^{n} p_i^{k^i}$. In a UFD, irreducible implies prime so each p_i is prime in R. Since $a \in \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, one of the $p_i \in \mathfrak{p}$. Thus $(p_i) \subset \mathfrak{p}$. Since (p_i) is a prime ideal, we must have $(p_i) = \mathfrak{p}$ and $\mathfrak{p}$ is principal.

Problem 2. Consider the functor F from commutative rings to abelian groups that takes a commutative ring R to the group R^* of invertible elements. Does F have a left adjoint? Does F have a right adjoint? Justify your answers.

We will show that F has a left adjoint. Define the functor $L : \text{AbGroup} \to \text{CRing}$ as $L(A) = \mathbb{Z}[A]$, the group ring over $\mathbb{Z}$. For an abelian group morphism $f : X \to Y$, we define $L(f) : \mathbb{Z}[X] \to \mathbb{Z}[Y]$ as $L(f)(x) = f(x)$ and extend $\mathbb{Z}$-linearly. Note that $L(f)$ is well-defined since $x \in X$ is a unit in $\mathbb{Z}[X]$ and it maps to a unit in $\mathbb{Z}[Y]$. Additionally, $L(f)$ is a unique commutative ring morphism that agrees with f on X since $\mathbb{Z}$ is initial in CRings. Let $1_X : X \to X$ be the identity morphism. Then $L(1_X)(\sum_{x\in X} a_x x) = \sum_{x\in X} a_x x$ and $L(1_X) = 1_{L(X)}$ for $a_x \in \mathbb{Z}$. Let $f : X \to Y$ and $g : Y \to Z$ be two abelian group morphisms. Then $L(gf)(\sum_{x\in X} a_x x) = \sum_{x\in X} a_x g(f(x)) = L(g)(\sum_{x\in X} a_x f(x)) = L(g)(L(f)(\sum_{x\in X} a_x x))$ for $a_x \in \mathbb{Z}$. Thus $L(gf) = L(g)L(f)$ and L is a functor.

We want to show that L is a left adjoint to F. Let $f : A \to F(B)$ be an abelian group morphism for $A \in \text{Ob}(\text{AbGroup})$ and $B \in \text{Ob}(\text{CRing})$. Define a natural transformation $\Phi_{A,B} : \text{Hom}_{\text{AbGroup}}(A, F(B)) \to \text{Hom}_{\text{CRing}}(L(A), B)$ by $\Phi_{A,B}(f)(x) = f(x)$ and extend $\mathbb{Z}$-linearly. By above, this is well-defined and the unique commutative ring morphism that agrees with f on X. Since units must map to units in a commutative ring morphism, every $h \in \text{Hom}_{\text{CRing}}(L(A), B)$ restricts to a morphism in $\text{Hom}_{\text{AbGroup}(A,F(B))}$. Thus $\Phi_{A,B}$ is a bijection. We want to show that the bijection is functorial in A and B. Let $g : A' \to A$ be a morphism of abelian groups. We want the diagram below to commute. Let $f \in \text{Hom}_{\text{AbGroup}}(A, F(B))$ as before. Then $\Phi_{A,B}(f) \circ L(g) : L(A') \to B$ extends the morphism $f \circ g : A' \to F(B)$. By definition, $\Phi_{A',B}(f \circ g)$ is also a morphism that extends $f \circ g$. The uniqueness in our choices of this morphism implies $\Phi_{A,B}(f) \circ L(g) = \Phi_{A',B}(f \circ g)$ and the diagram commutes. The argument for B is similar so the bijection is functorial in A and B. Therefore, L is a left adjoint to F.

$$\begin{array}{ccc} \text{Hom}_{\text{AbGroup}}(A, F(B)) & \xrightarrow{\Phi_{A,B}} & \text{Hom}_{\text{CRing}}(L(A), B) \\ \downarrow{\scriptstyle -\circ g} & & \downarrow{\scriptstyle -\circ L(g)} \\ \text{Hom}_{\text{AbGroup}}(A', F(B)) & \xrightarrow{\Phi_{A',B}} & \text{Hom}_{\text{CRing}}(L(A'), B) \end{array}$$

We will now show that left adjoints preserve initial objects. Let $L : \mathcal{C} \to \mathcal{D}$ and $R : \mathcal{D} \to \mathcal{C}$ be an adjoint pair. Let $A \in \text{Ob}(\mathcal{C})$ be an initial object. Then $\text{Hom}_{\mathcal{D}}(L(A), B) \simeq \text{Hom}_{\mathcal{C}}(A, R(B))$ for any $B \in \text{Ob}(\mathcal{D})$. But A initial in $\mathcal{C}$ implies $\text{Hom}_{\mathcal{C}}(A, R(B))$ has only one element. We conclude that $\text{Hom}_{\mathcal{D}}(L(A), B)$ has only one element and $L(A)$ is initial in $\mathcal{D}$.

In this problem, we want to show that F does not have a right adjoint. Assume F has a right adjoint G for the sake of contradiction. We will prove that F preserves initial objects. Let I be an initial object of $\mathcal{C}$ and B any object in $\mathcal{D}$. Then

$$\text{Hom}_{\mathcal{D}}(F(I), B) \simeq \text{Hom}_{\mathcal{D}}(I, G(B))$$

and $\text{Hom}_{\mathcal{D}}(I, G(B))$ is one element by the definition of an initial object. Thus $F(I)$ is initial in $\mathcal{D}$. We note that $\mathbb{Z}$ is initial in CRings, but $F(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ since ± 1 are the only units in $\mathbb{Z}$. The abelian group $\mathbb{Z}/2\mathbb{Z}$ is not initial since $\text{Hom}_{\text{AbGroup}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ has two elements, the trivial morphism and an isomorphism. Thus F cannot have a right adjoint.

Problem 3. Let R be a ring which is left Artinian (that is, Artinian with respect to left ideals). Suppose that R is a domain, meaning that $1 \neq 0$ in R and $ab = 0$ implies $a = 0$ or $b = 0$ in R. Show that R is a division ring.

Let the ring homomorphism $f : R \to R$ be right multiplication by some nonzero $a \in R$. Then $f(b) = 0$ implies $ba = 0$ so $a = 0$ or $b = 0$ by R a domain. Since $a \neq 0$, we have $b = 0$ and f is injective. Note that this means f^k is injective for all k. We have the chain of decreasing left R-modules,

$$\text{im}(f) \supset \text{im}(f^2) \supset \dots$$

Since R is Artinian, the chain terminates so $\mathrm{im}(f^k) = \mathrm{im}(f^{k+1})$ for some $k \in \mathbb{N}$. Let $b \in R$ be any element. Then $f^k(b) \in \mathrm{im}(f^k)$ so there is some $c \in R$ such that $f^{k+1}(c) = f^k(b)$. Rearranging, $f^k(f(c) - b) = 0$ and $f(c) = b$ by injectivity of f^k. We conclude that f is surjective. Then $f(b) = 1$ for some $b \in R$ which implies $ba = 1$. We have shown that every nonzero element $a \in R$ has a left inverse. In particular, b has a left inverse, say, $c \in R$. Then $a = (cb)a = c(ba) = c$ so $ba = ab = 1$. Thus every nonzero $a \in R$ is invertible. We conclude R is a division ring.

Problem 4. Let A be a commutative ring, S a multiplicatively closed subset of A, $A \to A[S^{-1}]$ the localization.

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

An element $a \in A$ maps to $\frac{a}{1} \in A[S^{-1}]$. If $\frac{a}{1} = 0$, then there is some $s \in S$ such that $sa = 0$. Thus $0 \in Sa$ for the set $Sa = \{sa : s \in S\}$. All elements $a \in A$ such that $0 \in Sa$ map to zero in the localization so this classifies all elements of A that map to zero.

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

Denote the image of $\mathfrak{p}$ in $A[S^{-1}]$ by $S^{-1}\mathfrak{p}$. ($\Rightarrow$) Assume $\mathfrak{p} \cap S \neq \varnothing$ and we will prove the contrapositive. Let $s \in \mathfrak{p} \cap S$, then $\frac{s}{1} \in S^{-1}\mathfrak{p}$ so $\frac{s}{1}\frac{1}{s} = \frac{1}{1} \in S^{-1}\mathfrak{p}$. Thus $S^{-1}\mathfrak{p} = A[S^{-1}]$ and the image of $\mathfrak{p}$ in $A[S^{-1}]$ is not a prime ideal. ($\Leftarrow$) Assume $\mathfrak{p} \cap S = \varnothing$. Then $S^{-1}\mathfrak{p}$ is a prime ideal by the arguments in Fall 2015 Problems 2(a) and 9(b).

Problem 5. Let A be the ring $\mathbb{C}\langle u, v\rangle/(uv - vu - 1)$, the quotient of the free associative algebra on two generators by the given two-sided ideal.

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

Assume that M is a finite dimensional $\mathbb{C}$-vector space. Pick a basis β. We note that left multiplication by u is a $\mathbb{C}$-linear transformation of M. Thus there is a matrix A in the basis β such that $Ax = ux$. Let B be the matrix that represents left multiplication by v. We have $AB - BA = I$. However, $\mathrm{Trace}(AB - BA) = 0$ and $\mathrm{Trace}(I) \neq 0$, a contradiction. We conclude that M is infinite dimensional as a $\mathbb{C}$-vector space.

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

Take $\sum_{i=0}^{\infty} c_i(v^i y) = 0$ for only finitely many nonzero $c_i \in \mathbb{C}$. Take N to be the maximal i for which $c_i \neq 0$. Left multiplication by u gives $u\left(\sum_{i=0}^{N} c_i(v^i y)\right) = \sum_{i=1}^{N} c_i(iv^{i-1}y + v^i uy) = \sum_{i=1}^{N} ic_i v^{i-1}y$ where the initial term is sent to zero. Then we have

$$0 = u^N \left(\sum_{j=1}^{N} c_i(v^i y)\right) = (N! c_N)y.$$

Since $y \neq 0$, we have $c_N = 0$. Continue this process by multiplying by u^{N-1} and so on. We conclude that $c_i = 0$ for all $0 \leqslant i$ so $\{y, vy, v^2y, \dots\}$ is linearly independent.

Problem 6. Let K be a field of characteristic $p > 0$. For an element $a \in K$, show that the polynomial $P(X) = X^p - X + a$ is irreducible over K if and only if it has no root in K. Show also that, if P is irreducible, then any root of it generates a cyclic extension of K of degree p.

($\Rightarrow$) We will prove the contrapositive. Assume P has a root $\alpha \in K$. We can immediately conclude that P is not irreducible in K since $P = (X - \alpha)g$ for some $g \in K[X]$.

($\Leftarrow$) We will prove the contrapositive. Assume P is reducible so $P = \prod_{i=1}^{k} g_i$ for irreducible $g_i \in K[X]$ with $\deg(g_i) < p$. Let $\alpha \in \overline{K}$ be a root of $g := g_1$. Then α is a root of P and $\alpha^p - \alpha + a = 0$. Since K is a field of characteristic p, we have $\mathbb{F}_p \subset K$ for $\mathbb{F}_p$ the field of p elements. Let $k \in \mathbb{F}_p$. Then

$$(\alpha + k)^p - (\alpha + k) + a = \alpha^p + k^p - \alpha - k + a = \alpha^p + k - \alpha - k + a = \alpha^p - \alpha + a = 0.$$

We conclude that the set of roots of P is $\{\alpha + k : k \in \mathbb{F}_p\} \subset K[\alpha]$, which implies P is separable over K. Further, $K[\alpha]$ is the splitting field of P so $K[\alpha]/K$ is a Galois extension. Let $G := \mathrm{Gal}(K[\alpha]/K)$ and take $\sigma \in G$. Then $\sigma(\alpha) = \alpha + k$ for $k \in \mathbb{F}_p$. We see that $\sigma^\ell(\alpha) = \alpha + k\ell$. Assume that $k \neq 0$. Then $k\ell = 0$ in $\mathbb{F}_p$ implies $k = 0$ in $\mathbb{F}_p$ or $p|\ell = 0$ in $\mathbb{Z}$. Thus the order of σ is at least p. Since $\sigma^p(\alpha) = \alpha$, we know the order of σ is p. Then $|G| \geqslant p$,

contradicting our assumption that $\deg(g) < p$. We have $\sigma(\alpha) = \alpha$ and $|G| = 1$. Thus $g = (X - \alpha)$, which implies P has a root in K.

Assume P is irreducible. Let $\alpha \in \overline{K}$ be a root of P. By above, the roots of the separable polynomial P are $\{\alpha + k : k \in \mathbb{F}_p\}$ so P splits in $K[\alpha]$. Then $K[\alpha]/K$ is Galois with $[K[\alpha] : K] = p$. The Galois group $\mathrm{Gal}(K[\alpha]/K)$ is order p and, thus, cyclic. We conclude that any root of P generates a cyclic extension of K of degree p.

The polynomial in question is an example of an Artin-Schreier polynomial.

Problem 7. Show that for every positive integer n, there exists a cyclic extension of $\mathbb{Q}$ of degree n which is contained in $\mathbb{R}$.

By Dirichlet's Theorem, there is some odd prime integer p such that $p \equiv 1 \pmod{2n}$. Let ξ be a primitive pth root of unity. We know that $\mathbb{Q}[\xi]/\mathbb{Q}$ is a Galois extension with $[\mathbb{Q}[\xi] : \mathbb{Q}] = \varphi(p) = p - 1$ for $\varphi : \mathbb{Z} \to \mathbb{Z}$ Euler's totient function. The Galois group $G := \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, which is cyclic. Complex conjugation $\tau : \mathbb{Q}[\xi] \to \mathbb{Q}[\xi]$ is an order two $\mathbb{Q}$-automorphism of $\mathbb{Q}[\xi]$. Let H be the order two subgroup of G generated by τ and $K := \mathbb{Q}[\xi]^H$. We have $K \subset \mathbb{R}$ since K is fixed by complex conjugation. (For a more explicit description, $K = \mathbb{Q}[\xi + \xi^{-1}]$.) Then Artin's Theorem implies $\mathbb{Q}[\xi]/K$ is Galois with $[\mathbb{Q}[\xi] : K] = 2$. As a result, $[K : \mathbb{Q}] = \frac{p-1}{2} = n$. Since $\mathbb{Q}[\xi]/\mathbb{Q}$ is cyclic, H is a normal subgroup of G so $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G/H$. The group G/H is cyclic so $K/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$ of degree n with $K \subset \mathbb{R}$.

Problem 8. Determine the character table of S_4, the symmetric group on 4 letters. Justify your answer.

In Fall 2015 Problem 7, we started the character table for representations of S_4 over $\mathbb{C}$. The only remaining row of the character table corresponds to the 2-dimensional irreducible representation which we denote $\mu : S_4 \to M_2(\mathbb{C})$. We will use column orthogonality to complete the table below.

	e	(12)	(123)	(12)(34)	(1234)
χ_{trivial}	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_μ	2	0	-1	2	0
χ_ρ	3	1	0	-1	-1
$\chi_{\rho\otimes\text{sgn}}$	3	-1	0	-1	1

Problem 9. Show that if G is a finite group acting transitively on a set X with at least two elements, then there exists $g \in G$ which fixes no point of X.

Let $n := |G|$ and $k := |X| \geqslant 2$. Note that $|\mathrm{Stab}(x)|$ is all $g \in G$ such that $gx = x$. For each $g \in \mathrm{Stab}(x)$, we have $x \in \mathrm{Fix}(g) = \{x \in X : gx = x\}$ and visa versa. We conclude $\sum_{x\in X} |\mathrm{Stab}(x)| = \sum_{g\in G} |\mathrm{Fix}(g)|$. By Orbit-Stabilizer and $|G|$ finite, $|\mathrm{Stab}(x)| = |G|/|\mathrm{Orb}(x)|$ for all $x \in X$. But G acts transitively on X so $|\mathrm{Orb}(x)| = |X| = k$ and $|\mathrm{Stab}(x)| = \frac{n}{k}$. Then $\sum_{g\in G} |\mathrm{Fix}(g)| = \sum_{x\in X} \frac{n}{k} = n$. Since $|\mathrm{Fix}(e)| = k \geqslant 2$, we have $\sum_{g\in G, g\neq e} |\mathrm{Fix}(g)| < n - 1$. If all non-identity $g \in G$ have $|\mathrm{Fix}(g)| = 1$, we would have $\sum_{g\in G, g\neq e} |\mathrm{Fix}(g)| = n - 1$. By the pigeonhole principle, there is some g such that $|\mathrm{Fix}(g)| = 0$ as desired.

Problem 10.

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

We determine the Galois group of $X^4 - 2$ over $\mathbb{Q}$ in Case 4 of Fall 2014 Problem 3. We find $\mathrm{Gal}(X^4 - 2) \simeq D_4 = \langle r, s : r^4 = s^2 = e, rs = sr^3\rangle$. The roots of $X^4 - 2$ are $\{\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i\}$ so identify these as roots 1, 2, 3, and 4 respectively. Then D_4 as a subgroup of S_4 is the subgroup generated by $\{(1234), (24)\}$.

(b) Determine the Galois group of the polynomial $X^3 - 3X - 1$ over $\mathbb{Q}$. (Hint: for polynomials of the form $X^3 + aX + b$, the quantity $\Delta = -4a^3 - 27b^2$, known as the discriminant, plays a key theoretical role.) Explain your answer.

Let K be the splitting field of an irreducible polynomial in $F[x]$ with roots $\{\alpha_1, \ldots, \alpha_n\}$. Define $\delta := \prod_{i<j}(\alpha_i - \alpha_j)$, and the discriminant $\Delta := \delta^2$. For $\sigma \in \mathrm{Gal}(f)$, $\sigma(\delta) = \mathrm{sign}(\sigma)\delta$ **SHOW THIS** so $\sigma(\Delta) = \Delta$ for all

$\sigma \in \mathrm{Gal}(f)$. Thus $\Delta \in F$, and each $\sigma \in \mathrm{Gal}(f)$ such that $\sigma(\delta) = \delta$ must be an even permutation of the roots of f. If $\delta \in F$, then $\mathrm{Gal}(f)$ must be a subgroup of A_n.

For a degree 3 polynomial, there will be at least one real root. The other roots could both be real or could be a conjugate pair of complex roots. Let the roots of f be $\{x, a+bi, a-bi\}$ for $a, b, x \in \mathbb{R}$, then

$$\delta = (x-(a+bi))(x-(a-bi))(a+bi-(a-bi)) = 2bi(x^2 - 2x + (a^2+b^2)).$$

Note $\Delta = \delta^2 < 0$. In this problem, $\Delta = -4a^3 - 27b^2 = -4(-3)^3 - 27(-1)^2 = 81 > 0$ so the roots of f are real. Since $\Delta = 9^2$, we have $\delta \in \mathbb{Q}$. By above, $\mathrm{Gal}(f)$ embeds in A_3, and $|\mathrm{Gal}(f)| \leqslant |A_3| = 3$. By the rational root test, f is irreducible over $\mathbb{Q}$. Then $[F[\alpha] : F] = 3 = |\mathrm{Gal}(f)| = |A_3|$ for some $\alpha \in \mathbb{R}$ a root of f. We conclude $\mathrm{Gal}(f) \simeq A_3$.

Fall 2016

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

We claim $G \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$, the free product of the additive group of order two with itself. Let the first copy of $\mathbb{Z}/2\mathbb{Z}$ have generator 1 and the second copy have generator $1'$. Define the set map $f : \{a, b\} \to \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ as $f(a) = 1$ and $f(b) = 1'$. By the universal property of free groups, there is a unique group homomorphism $f : F \to \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ such that $f(a) = 1$ and $f(b) = 1'$ where F is the free group on the generators $\{a, b\}$. By construction, f is surjective and $a^2, b^2 \in \ker(f)$. Let N be the normal subgroup of F generated by $\{a^2, b^2\}$ so $N \subset \ker(f)$. Thus f descends to a unique group homomorphism $\overline{f} : F/N \to \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. Take an element $w \in \ker(\overline{f})$. If w is the empty word in F/N, then $w \in N$ so we may assume that w is a reduced non-empty word. Without loss of generality, $w = a^{k_1}b^{\ell_1} \cdots a^{k_n}b^{\ell_n}$ where the integers $k_i = 1$ for $1 < i \leqslant n$ and the integers $\ell_j = 1$ for $1 \leqslant j < n$. The same argument will work if w starts with b^{ℓ_1}. We have

$$0 = \overline{f}(w) = \overline{f}(a^{k_1}b^{\ell_1} \cdots a^{k_n}b^{\ell_n}) = \overline{f}(a)^{k_1}\overline{f}(b)^{\ell_1} \cdots \overline{f}(a)^{k_n}\overline{f}(b)^{\ell_n} = (k_1 \cdot 1)(\ell_1 \cdot 1') \cdots (k_n \cdot 1)(\ell_n \cdot 1').$$

This can only occur if $n = 1$ and $\ell_n = 0$. In this case, $w = aga^{-1}$ for $g \in N$. Since N is normal in F, $w \in N$, contradicting the choice of w. We conclude that $\ker(\overline{f})$ contains only the empty word and $G \simeq F/N \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ by the First Isomorphism Theorem.

Problem 2. Let K be a semi-simple quadratic extension over $\mathbb{Q}$ and consider the regular representation $\rho : K \to M_2(\mathbb{Q})$. Compute the index of $\rho(K^\times)$ in the normalizer of $\rho(K^\times)$ in $GL_2(\mathbb{Q})$, and justify your answer.

By Artin-Wedderburn, K is isomorphic to a product of matrix algebras over division rings. Since $\dim_{\mathbb{Q}}(K) = 2$, the only options are $K \simeq \mathbb{Q} \times \mathbb{Q}$ or $K \simeq \mathbb{Q}[\alpha]$ for α a root of an irreducible quadratic in $\mathbb{Q}[x]$.

Case 1: Let $K \simeq \mathbb{Q} \times \mathbb{Q}$. Then $\{(1,0),(0,1)\}$ is a basis of K as a $\mathbb{Q}$-vector space. Let $(x, y) \in K$ for $x, y \in \mathbb{Q}\backslash\{0\}$ and we will construct $\rho(x, y)$ by multiplying the basis elements by (x, y).

$$(x,y)(1,0) = (x,0)$$
$$(x,y)(0,1) = (0,y)$$
$$\rho(x,y) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$$

Let $A \in \mathrm{GL}_2(\mathbb{Q})$ so $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $a, b, c, d \in \mathbb{Q}$ and $ad - bc \neq 0$. Then

$$A\rho(x,y)A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} adx - bcy & ab(y-x) \\ cd(x-y) & -bcx + ady \end{pmatrix}.$$

For A to be in the normalizer of $\rho(K^\times)$, we need $ab(y-x)$ and $cd(x-y) = 0$. Since x and y can be distinct this implies one of a or b must be zero and one of c or d is zero. By assumption, A is invertible so $a = 0$ implies $d = 0$ and $b = 0$ implies $c = 0$. We conclude that an element A in the normalizer of $\rho(K^\times)$ will be of the form

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \text{ or } \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$$

for nonzero $a, b, c, d \in \mathbb{Q}$. Therefore, the index of $\rho(K^\times)$ in the normalizer is 2.

Case 2: We note that the root of an irreducible quadratic has the form $\alpha = \frac{-b+\sqrt{b^2-4ac}}{2a}$ for $a, b, c \in \mathbb{Q}$. Thus $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{b^2-4ac}]$. Let $r := b^2 - 4ac$ and r is not a square in $\mathbb{Q}$ since $K/\mathbb{Q}$ is a degree 2 extension. Then $K \simeq \mathbb{Q}[\sqrt{r}]$ which has basis $\{1, \sqrt{r}\}$ as a $\mathbb{Q}$-vector space. We construct $\rho(x + y\sqrt{r})$ for $x, y \in \mathbb{Q}$ as follows.

$$\begin{aligned}(x + y\sqrt{r})1 &= x + y\sqrt{r} = (x, y)\\ (x + y\sqrt{r})\sqrt{r} &= ry + x\sqrt{r} = (ry, x)\\ \rho(x, y) &= \begin{pmatrix} x & y \\ ry & x \end{pmatrix}\end{aligned}$$

Let $A \in \mathrm{GL}_2(\mathbb{Q})$ so $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $a, b, c, d \in \mathbb{Q}$ and $ad - bc \neq 0$. Then

$$\begin{aligned}A\rho(x, y)A^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ ry & x \end{pmatrix} \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\\ &= \frac{1}{ad-bc} \begin{pmatrix} ax + by & ary + bx \\ cd + dy & cry + dx \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\\ &= \frac{1}{ad-bc} \begin{pmatrix} (ad-bc)x + (bd-acr)y & -b^2y + a^2ry \\ d^2y - c^2ry & (ad-bc)x + (acr-bd)y. \end{pmatrix}\end{aligned}$$

For A to be in the normalizer of $\rho(K^\times)$, we need the following equations to be satisfied. Take $y \in \mathbb{Q}$ to be non-zero.

$$\begin{aligned}(ad-bc)x + (bd-acr)y &= (ad-bc)x + (acr-bd)y\\ (bd-acr)y &= (acr-bd)y\\ bd - acr &= 0\\ bd &= acr\end{aligned}$$

$$\begin{aligned}r(d^2y - c^2ry) &= -b^2y + a^2ry\\ (b^2 + (d^2-a^2)r - c^2r^2)y &= 0\\ b^2 + (d^2-a^2)r - c^2r^2 &= 0\end{aligned}$$

If $b = 0$, then $acr = 0$. Since A is invertible, $a \neq 0$ and $c = 0$. From the second equation, $(d^2 - a^2)r = 0$ and $r \neq 0$ implies $d = \pm a$. Assume $b \neq 0$. Then $d = \frac{acr}{b}$ and, substituting into the second equation,

$$\begin{aligned}0 &= b^2 + \left(\left(\frac{acr}{b}\right)^2 - a^2\right) r - c^2r^2\\ &= (b^2 - c^2r^2) - \frac{a^2r}{b^2}\left(b^2 - c^2r^2\right)\\ &= (b^2 - c^2r^2)\left(1 - \frac{a^2r}{b^2}\right).\end{aligned}$$

As a result, either $b = \pm cr$ or $b = \pm a\sqrt{r}$. We cannot have $b = a\sqrt{r}$ since $a, b \in \mathbb{Q}$ and $\sqrt{r} \notin \mathbb{Q}$ by assumption. If $b = \pm cr$, we have $d = \frac{acr}{\pm cr} = \pm a$. Note that the matrices A such that $b = 0$ is a subset of this type of normalizer. The case $b = cr$ implies $A \in \rho(K^\times)$ whereas $b = -cr$ produces the coset $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\rho(K^\times)$. We conclude that $\rho(K^\times)$ has index 2 in the normalizer.

Problem 3. Let A be an integral domain with field of fractions F. For an A-ideal $\mathfrak{a}$, prove that $\mathfrak{a}$ is an A-projective ideal finitely generated over A if there exists an A-submodule $\mathfrak{b}$ of F such that $\mathfrak{ab} = A$, where $\mathfrak{ab}$ is an A-submodule of F generated by ab for all $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

We will first show that $\mathfrak{a}$ is a finitely generated ideal of A. Since $\mathfrak{ab} = A$, there is a finite sum $\sum_{i=1}^n a_ib_i = 1$ for $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Let $a \in A$, then $a = a(\sum_{i=1}^n a_ib_i) = \sum_{i=1}^n a_i(ab_i)$. Since $\mathfrak{ab} = A$, we have $ab_i \in A$ for all $1 \leqslant i \leqslant n$. Thus $\{a_i\}_{i=1}^n$ is a generating set of A as an A-module.

Now we will show that $\mathfrak{a}$ is a projective ideal of A. Since $\mathfrak{a}$ is finitely generated by $\{a_i\}_{i=1}^n$, there is a short exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow A^n \xrightarrow{f} \mathfrak{a} \longrightarrow 0$$

with $f(e_i) = a_i$ for $\{e_i\}_{i=1}^n$ the standard generating set of A^n. Define the A-module homomorphism $h : \mathfrak{a} \to A^n$ by $h(a) = \sum_{i=1}^n (ab_i e_i)$. Then $f(h(a)) = f(\sum_{i=1}^n (ab_i e_i)) = \sum_{i=1}^n ab_i f(e_i) = \sum_{i=1}^n ab_i a_i = a$. We conclude that h is a splitting and $A^n \simeq \mathfrak{a} \oplus \ker(f)$. Since $\mathfrak{a}$ is a direct summand of a free A-module, $\mathfrak{a}$ is a projective A-module.

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

Let $D := \langle r, s : r^p = s^2 = e, rs = sr^{-1} \rangle$ be the dihedral group of order $2p$. We will find the commutator subgroup $[D, D] \subset D$. Any element of the commutator subgroup is of the form $(r^i s)(r^j s)(r^i s)^{-1}(r^j s)^{-1}$ for some $0 \leqslant i, j \leqslant p-1$. Reducing this, we end up with r^{2i-2j}. Further, $r^{\frac{p+1}{2}} s r^{p-\frac{p+1}{2}} s^{-1} = r^{\frac{p+1}{2}} r^{\frac{p+1}{2}} ss = r^{\frac{2p+2}{2}} = r \in [D, D]$. Thus $[D, D]$ is the subgroup of D generated by r and $|D/[D, D]| = 2$. Thus there are two non-isomorphic classes of one-dimensional representations of D.

We now classify the conjugacy classes of D_p. Note that it is sufficient to conjugate each element only by the generators r and s. The identity makes up one conjugacy class. When we conjugate s we notice $r^i s r^{p-i} = r^{2i} s$. Since p is odd, we can continue this process to obtain the conjugacy class $\{s, rs, \ldots, r^{p-1}s\}$. When we conjugate r^i we have $sr^i s^{-1} = sr^i s = r^{p-i}$ for $1 \leqslant i \leqslant p-1$. Conjugating by s again yields $sr^{p-i}s^{-1} = sr^{p-i}s = r^i$. Thus we have the conjugacy classes $\{r^i, r^{p-i}\}$ for $1 \leqslant i \leqslant \frac{p-1}{2}$. In total, this is $\frac{p+3}{2}$ conjugacy classes.

Using the intuition of D as permutations of vertices of a regular p-gon, we can construct the classes of 2-dimensional irreducible representations. We can construct $\phi_k : D \to M_2(\mathbb{C})$ as $\phi_k(r) = \begin{pmatrix} \cos(2\pi k/p) & -\sin(2\pi k/p) \\ \sin(2\pi k/p) & \cos(2\pi k/p) \end{pmatrix}$, the rotation by $\frac{2\pi k}{p}$ counterclockwise in the plane, and $\phi_k(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ for $1 \leqslant k \leqslant \frac{p-1}{2}$, the reflection about the x-axis in the plane. Each ϕ_k is an irreducible representation of D since there are no subspaces of $\mathbb{C}^2$ invariant under these transformations. Further, these are non-isomorphic irreducible representations since the characters $\chi_{\phi_k}(r) = 2\cos(2\pi k/p)$ differ for each k.

The sum of the squares of the dimensions of these representations is $1 + 1 + \left(\frac{p-1}{2}\right) 2^2 = 2 + (2p - 2) = 2p$, the order of the group. Thus these are all isomorphism classes of irreducible representations of D over $\mathbb{C}$. We conclude that there are two one-dimensional and $\frac{p-1}{2}$ two-dimensional isomorphism classes of irreducible complex representations of D.

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

Note that K/F is a Galois extension since f is separable and K is the splitting field of f. Let $\alpha \in K$ be a root of f. Then $F[\alpha]/F$ is a field extension with $[F[\alpha] : F] = p$ since f is irreducible. Then $K/F[\alpha]/F$ is a tower of field extensions so $p = [F[\alpha] : F] | [K : F]$. Now $|\mathrm{Gal}(K/F)| = [K : F]$ since K/F is a finite Galois extension of F. Thus $p | |\mathrm{Gal}(K/F)|$ and Cauchy's Theorem implies there is some element $\sigma \in \mathrm{Gal}(K/F)$ of order p. We know σ permutes the roots of f, of which there are p, so σ must permute the roots cyclically.

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

Let $\alpha \in \overline{F}$ be some pth root of a in the algebraic closure of F. Then $x^p - a = (x - \alpha)^p$ since F is characteristic p. If $\alpha \in F$, we conclude that f splits into a product of linear factors. Thus assume $\alpha \notin F$ and we want to show that f is irreducible over F. We can factor $f = \prod_{i=1}^n g_i$ into irreducible $g_i \in F[x]$. Each g_i must be of the form $g_i = (x - \alpha)^{k_i}$ for some integer k_i satisfying $1 < k_i \leqslant p$. In this case, $[F[\alpha] : F] = k_i$ and $k_i = k_j$ for all $1 \leqslant i, j \leqslant n$. However, $p = \deg(f) = \sum_{i=1}^n k_i = nk_1$ implies $k_1 = 1$ or $k_1 = p$. Since $k_1 > 1$ by assumption, $k_1 = p$ and f is irreducible.

Problem 7. Let $f \in \mathbb{Q}[X]$ and $\xi \in \mathbb{C}$ a root of unity. Show that $f(\xi) \neq 2^{1/4}$.

We will assume that $f(\xi) = 2^{1/4}$ for some $f \in \mathbb{Q}[X]$ and draw a contradiction. We know that $\mathbb{Q}[\xi]/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ for ξ a primitive nth root of unity. In particular, $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ is abelian so $\mathbb{Q}[\xi]/\mathbb{Q}$ is an abelian Galois extension. By assumption $f(\xi) = 2^{1/4}$ so $2^{1/4} \in \mathbb{Q}[\xi]$ and $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ is a subextension of $\mathbb{Q}[\xi]/\mathbb{Q}$. By the Galois correspondence, $\mathbb{Q}[2^{1/4}] = (\mathbb{Q}[\xi])^H$ for some subgroup $H \subset \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ and $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ should be a normal extension since any subgroup of an abelian group is normal. The minimal polynomial of $2^{1/4}$ over $\mathbb{Q}$ is $x^4 - 2$ (which is irreducible by Eisenstein's Criterion). But $x^4 - 2$ does not split in $\mathbb{Q}[2^{1/4}]$ so $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ is not a Galois extension, contradicting our assumption. We conclude that $f(\xi) \neq 2^{1/4}$ for all $f \in \mathbb{Q}[X]$.

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

Let $L : \mathrm{Sets} \to \mathcal{C}$ be the left adjoint to F. Then we know that $\Phi_{A,B} : \mathrm{Hom}_{\mathcal{C}}(L(A), B) \simeq \mathrm{Hom}_{\mathrm{Sets}}(A, F(B))$ for some natural isomorphism Φ and $A \in \mathrm{Ob}(\mathrm{Sets})$ and $B \in \mathrm{Ob}(\mathcal{C})$. Let $A := \{*\}$ be a set with one element. Then $\mathrm{Hom}_{\mathrm{Sets}}(A, F(B)) \simeq F(B)$ as sets via the morphism $h_B : \mathrm{Hom}_{\mathrm{Sets}}(A, F(B)) \to F(B)$ with $h_B(\alpha) := \alpha(*)$. Thus $\mathrm{Hom}_{\mathcal{C}}(L(A), B) \simeq \mathrm{Hom}_{\mathrm{Sets}}(A, F(B)) \simeq F(B)$ for all $B \in \mathrm{Ob}(\mathcal{C})$.

Define a natural transformation $\eta_B : \mathrm{Hom}_{\mathcal{C}}(L(A), B) \to F(B)$ by $\eta_B(f) := \Phi_{A,B}(f)(*)$. Since $\Phi_{A,B}$ is an isomorphism and $\mathrm{Hom}_{\mathrm{Sets}}(A, F(B)) \simeq F(B)$ by choosing the image of $* \in A$, we conclude that η_B is an isomorphism for each $B \in \mathrm{Ob}(\mathcal{C})$. Let $f \in \mathrm{Hom}_{\mathcal{C}}(L(A), B)$, and let $g : B \to C$ be a morphism in $\mathcal{C}$ for $C \in \mathrm{Ob}(\mathcal{C})$. We want to show the diagram below commutes. Since Φ is a natural transformation, the square on the left commutes. The square on the right commutes since $F(g)(h_B(\alpha)) = F(g)(\alpha(*))$ and $h_C(F(g) \circ \alpha) = (F(g) \circ \alpha)(*)$ for $\alpha \in \mathrm{Hom}_{\mathrm{Sets}}(A, F(B))$. Therefore, the diagram commutes. We conclude that F is represented by $L(A) \in \mathrm{Ob}(\mathcal{C})$.

$$\begin{array}{ccccc}
 & & \overset{\eta_B}{\frown} & & \\
\mathrm{Hom}_{\mathcal{C}}(L(A), B) & \xrightarrow{\Phi_{A,B}} & \mathrm{Hom}_{\mathrm{Sets}}(A, F(B)) & \xrightarrow{h_B} & F(B) \\
\downarrow{\scriptstyle g\circ -} & & \downarrow{\scriptstyle F(g)\circ -} & & \downarrow{\scriptstyle F(g)} \\
\mathrm{Hom}_{\mathcal{C}}(L(A), C) & \xrightarrow{\Phi_{A,C}} & \mathrm{Hom}_{\mathrm{Sets}}(A, F(C)) & \xrightarrow{h_C} & F(C) \\
 & & \underset{\eta_C}{\smile} & &
\end{array}$$

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

In the category of F-algebras, F is initial. Thus a morphism from the F-algebra $A := F[B_1, B_2, C_1, C_2]/(B_1C_1 + aB_2C_2 - 1, B_1C_2 - B_2C_1)$ is determined by the image of B_i and C_j for $1 \leqslant i, j \leqslant 2$. We can define a natural transformation $\eta_R : \mathrm{Hom}_{F\text{-alg}}(A, R) \to R^4$ via $\eta_R(f) := (f(B_1), f(B_2), f(C_1), f(C_2))$. Let $g : R \to S$ be an F-algebra homomorphism of commutative F-algebras R and S. Let $f \in \mathrm{Hom}_{F\text{-alg}}(A, R)$. Then $\eta_S(g \circ f) = (gf(B_1)), gf(B_2), gf(C_1), gf(C_2))$ and $(g, g, g, g) \circ \eta_R(f) = (gf(B_1)), gf(B_2), gf(C_1), gf(C_2))$. Thus the diagram below commutes.

$$\begin{array}{ccc}
\mathrm{Hom}_{F\text{-alg}}(A, R) & \xrightarrow{\eta_R} & R^4 \\
\downarrow{\scriptstyle g\circ -} & & \downarrow{\scriptstyle (g,g,g,g)} \\
\mathrm{Hom}_{F\text{-alg}}(A, S) & \xrightarrow{\eta_S} & S^4
\end{array}$$

We have $R^2 \simeq R[X]/(X^2 - a)$ as R-modules via the isomorphism $f(b, c) = (bX + c)$. If $(b_1, b_2) \in R^2$ maps to a unit in $R[X]/(X^2 - a)$, then there is some $(c_1, c_2) \in R^2$ such that $b_1c_1 + ab_2c_2 = 1$ and $b_1c_2 - b_2c_1 = 0$. Similarly, the existence of such a (c_1, c_2) implies (b_1, b_2) maps to a unit of $R[X]/(X^2 - a)$. Therefore, η_R is an isomorphism between $\mathrm{Hom}_{F\text{-alg}}(A, R)$ and $F(R)$ for each commutative F-algebra R. Further, the set of units of a ring S is naturally isomorphic to the set $\{(x, y) \in S^2 : xy = 1\}$. Thus we have a natural isomorphism $\mu : \mathrm{Hom}_{F\text{-alg}}(A, -) \to F$. We conclude that A represents the functor F.

ADD SOME CONTEXT FOR THIS PROBLEM FROM ALEX

Problem 10. Let F be a field and A a simple subalgebra of a finite dimensional F-algebra B. Prove that $\dim_F(A)$ divides $\dim_F(B)$.

This problem is incorrect as written. A counterexample is $B = M_2(F) \oplus M_3(F)$ where $A = M_2(F)$. Then A is a simple subalgebra of a finite-dimensional F-algebra B. However, $\dim_F(A) = 4$ does not divide $\dim_F(B) = 13$.

Spring 2017

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

Each conjugacy class of matrices in $\mathrm{GL}(2, \mathbb{R})$ has a unique representative in rational canonical form. For 2×2 matrices, the invariant factors of $A \in \mathrm{GL}(2, \mathbb{R})$ could be $\{f\}$ for $f = x^2 - ax - b \in \mathbb{R}[x]$ or $\{g, h\}$ where $g|h$. Since the sum of the degrees of g and h is 2, we see that $\deg(g) = \deg(h) = 1$. We can take g and h monic so $g = h = x - c$ for some $c \in \mathbb{R}$. Thus the possible rational canonical forms for a matrix in $\mathrm{GL}(2, \mathbb{R})$ are

$$\begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} \text{ or } \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

for $a, b, c \in \mathbb{R}$. Each conjugacy classes of $\mathrm{GL}(2, \mathbb{R})$ has a representative of the form above.

Problem 2. Let G be the group with presentation $\langle x, y : x^4 = 1, y^5 = 1, xyx^{-1} = y^2 \rangle$, which has order 20. Find the character table of G.

We will first find the conjugacy classes of G. Note that we only need to check conjugation by the generators x and y. Since $xy = y^2x$, we can write each element of G as $y^i x^j$ for some $0 \leqslant i < 5$ and $0 \leqslant j < 4$. Additionally,

$$(y^i x^j)(y^k x^\ell)(y^i x^j)^{-1} = y^{i+2^j k} x^{j+\ell} x^{-j} y^{-i} = y^{i+2^j k} x^\ell y^{-i} = y^{-i+2^j k} x^\ell$$

so the exponent of x remains unchanged by conjugation. By the formula above, conjugating $y^k x^\ell$ by y will result in $y^{k-1} x^\ell$. Thus the conjugacy classes are

$$\{1\}, \{y, y^2, y^3, y^4\}\{x, yx, y^2x, y^3x, y^4x\}, \{x^2, yx^2, y^2x^2, y^3x^2, y^4x^2\}, \{x^3, yx^3, y^2x^3, y^3x^3, y^4x^3\},$$

which implies 5 isomorphism classes of irreducible representations. We will now find the commutator subgroup $[G, G]$. The generators of $[G, G]$ have the form $(y^i x^j)(y^k x^\ell)(y^i x^j)^{-1}(y^k x^\ell)^{-1} = (y^{-i+2^j k} x^\ell) x^{-\ell} y^{-k} = y^{-i+(2^j-1)k}$. We can pick $i = 4$, $j = 0$, $k = 0$, and $\ell = 1$, which implies $[G, G]$ is the cyclic subgroup of G generated by y. Then the number of isomorphism classes of one-dimensional representations is $|G/[G, G]| = 4$ by the argument in Fall 2015 Problem 7. There are 4 one-dimensional representations and 5 conjugacy classes. Since the order of G is the sum of the squares of the dimensions of the irreducible representations, $20 = 1^2 + 1^2 + 1^2 + 1^2 + k^2$ so $k = 4$.

We will now determine the 4 one-dimensional representations. Since x is order 4, it must map to $\pm 1, \pm i$ in $\mathbb{C}^\times$. Similarly, y is order 5 so y must map to a fifth root of unity in $\mathbb{C}^\times$. The character is equal to the representation in the one-dimensional case so the representation is the same on each conjugacy class. Let $\rho_i : G \to \mathbb{C}^\times$ be one-dimensional representations for $1 \leqslant i \leqslant 3$ and $\mu : G \to \mathrm{GL}_4(\mathbb{C})$ be the 4-dimensional irreducible representation. For $\rho_i : G \to \mathbb{C}^\times$, $\rho_i(y) = \rho_i(y^2) = \rho_i(y)^2$ so $\rho(y) = 1$. We can fill in the character table below based on the image of x. The last row of the table is found by column orthogonality.

	1	y	x	x^2	x^3
χ_{trivial}	1	1	1	1	1
χ_{ρ_1}	1	1	i	-1	$-i$
χ_{ρ_2}	1	1	-1	1	-1
χ_{ρ_3}	1	1	$-i$	-1	i
χ_μ	4	-1	0	0	0

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

Let $X = \{1, 2, 3\}$ be a set of order 3. Assume there is a transitive group action of F_2 on X. Then Stab(1) is a subgroup of G with $[G : \text{Stab}(1)] = |\text{Orb}(1)| = 3$ by Orbit-Stabilizer. Now assume H is an index 3 subgroup of F_2. Then the set F_2/H of left cosets has order 3. We have a transitive group action of F_2 on the set F_2/H given by left multiplication. Let $g \in F_2$. We have $g \cdot H = H$ if and only if $g \in H$. As a result, $\text{Stab}(H) = H$. The two situations describe a bijection between index 3 subgroups of G and stabilizers of transitive group actions on sets of three elements.

We will find the number of transitive group actions of F_2 on the set $X = \{1, 2, 3\}$ with $H := \text{Stab}(1)$. In the case of $|X| = 3$, this is equivalent to finding a homomorphism $\phi : F_2 \to S_3$ whose image contains a 3-cycle. The image of u and v under ϕ uniquely determines ϕ by the universal property of free groups. We will break into cases. Note that 2 and 3 can are interchangeable so $\phi(u) = (13)$ cases produce the same stabilizers of 1 as the $\phi(u) = (12)$ cases. Similarly, we do not have to consider $\phi(u) = (132)$.

$$\begin{aligned}
&\phi(u) = e \text{ implies } \phi(v) \in \{(123), (132)\}\\
&\phi(u) = (12) \text{ implies } \phi(v) \in \{(13), (23), (123), (132)\}\\
&\phi(u) = (23) \text{ implies } \phi(v) \in \{(12), (13), (123), (132)\}\\
&\phi(u) = (123) \text{ implies } \phi(v) \in \{e, (12), (13), (23), (123), (132)\}
\end{aligned}$$

The symmetry of 2 and 3 also allows us to remove the cases $\{\phi(u) = e, \phi(v) = (132)\}$, $\{\phi(u) = (23), \phi(v) = (13)\}$, and $\{\phi(u) = (23), \phi(v) = (132)\}$. We are left with 13 suitable group homomorphisms $\phi : F_2 \to S_3$ for which Stab(1) determines all distinct subgroups of F_2 of index 3.

Problem 4. Show that the ring $R = \mathbb{C}[x, y]/(y^2 - x^3 + 1)$ is a Dedekind domain. (Hint: Compare R with the subring $\mathbb{C}[x]$.)

It is sufficient to show that R is the integral closure of $\mathbb{C}[x]$ in the fraction field of R, $\mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$. Let $\alpha \in \mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$ be integral over $\mathbb{C}[x]$. The set $\{1, y\}$ is a basis for $\mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$ as a $\mathbb{C}(x)$-vector space. Thus $\alpha = p + qy$ for $p, q \in \mathbb{C}(x)$. If $q = 0$, $\alpha \in \mathbb{C}[x] \subset R$ so we may assume $q \neq 0$. Let $m = T^2 - 2pT + (p^2 + q^2(x^3 - 1)) \in \mathbb{C}(x)[T]$ be the minimal polynomial of α over $\mathbb{C}(x)$. Since $\mathbb{C}[x]$ is a UFD, Gauss's Lemma implies that $m \in \mathbb{C}[x][T]$. Then $2p \in \mathbb{C}[x]$ gives $p \in \mathbb{C}[x]$. Since $p^2 + q^2(x^3 - 1) \in \mathbb{C}[x]$, we have $q^2(x^3 - 1) \in \mathbb{C}[x]$. From $x^3 - 1$ square-free in $\mathbb{C}[x]$, we conclude $q \in \mathbb{C}[x]$ and $\alpha \in R$. Therefore, R is the integral closure of $\mathbb{C}[x]$ in $\mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$, which implies R is a Dedekind domain.

Problem 5. Let S be a multiplicatively closed subset of a commutative ring R. For a prime ideal I in R with $I \cap S = \varnothing$, show that the ideal $I \cdot R[S^{-1}]$ in the localized ring $R[S^{-1}]$ is prime. Also, show that sending I to $I \cdot R[S^{-1}]$ gives a bijection between the prime ideals in R that do not meet S and the prime ideals in the localized ring $R[S^{-1}]$.

We want to show that a prime ideal of R maps to a prime ideal of $R[S^{-1}]$ for S a multiplicatively closed subset of $R\backslash\{0\}$ with $1 \in S$ under this correspondence. Let $\mathfrak{p} \subset R$ be a prime ideal. Let $\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \in S^{-1}\mathfrak{p}$. Then $ab \in \mathfrak{p}$ so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Thus $\frac{a}{s} \in S^{-1}\mathfrak{p}$ or $\frac{b}{t} \in S^{-1}\mathfrak{p}$. Note that $\frac{1}{1} \in S^{-1}\mathfrak{p}$ implies there is some $\frac{a}{1} \in S^{-1}\mathfrak{p}$ such that $sa = 1$ for $a \in \mathfrak{p}$. Thus $1 \in \mathfrak{p}$, a contradiction. We conclude $S^{-1}\mathfrak{p}$ is proper and, as a result, $S^{-1}\mathfrak{p}$ is a prime ideal of $R[S^{-1}]$.

Let $S^{-1}\mathfrak{p} \in R[S^{-1}]$ be a prime ideal. Then the set $\mathfrak{p}' = \{r \in R : \frac{r}{1} \in S^{-1}\mathfrak{p}\}$ is a proper ideal of R by Fall 2015 Problem 2(a). Let $ab \in \mathfrak{p}'$ for $a, b \in R$. Then $\frac{ab}{1} \in \mathfrak{p}$ which implies $\frac{a}{1} \in \mathfrak{p}$ or $\frac{b}{1} \in \mathfrak{p}$ by primality of $\mathfrak{p}$ in $R[S^{-1}]$. Thus $a \in \mathfrak{p}'$ or $b \in \mathfrak{p}'$ and $\mathfrak{p}'$ is a prime ideal of R. Note that $S^{-1}\mathfrak{p}' = \mathfrak{p}$ and we have constructed a bijection between the prime ideals in R that do not meet S and the prime ideals in the localized ring $R[S^{-1}]$.

Problem 6. Prove the following generalization of Nakayamas Lemma to noncommutative rings. Let R be a ring with 1 (not necessarily commutative) and suppose that $J \subset R$ is a left ideal contained in every maximal left ideal of R. If M is a finitely generated left R-module such that $JM = M$, prove that $M = 0$.

We will prove that if x is contained in each left maximal ideal of a ring R, then $1 - rx$ is left invertible for all $r \in R$. Assume x is contained in each left maximal ideal of a ring R. For the sake of contradiction, assume $1 - rx$ is not left invertible for some $r \in R$. Then $1 - rx$ is contained in some left maximal ideal $\mathfrak{m} \subset R$ by a Zorn's Lemma

argument. But $x \in \mathfrak{m}$ so $(1-rx)+rx = 1 \in \mathfrak{m}$, a contradiction. We conclude that $1-rx$ is left invertible for each $r \in R$.

Let $\{x_1, \ldots, x_n\}$ be a minimal generating set of M as a left R-module. Then $x_i = \sum_{j=1}^n a_{ij}x_j$ for $a_{ij} \in J$ by assumption. For x_1, we have $(1-a_{11})x_1 = \sum_{j=2}^n a_{1j}x_j$. Note that J is a subset of the intersection of all left maximal ideals so $1-a_{11}$ is left invertible by above. Thus

$$x_1 = \sum_{j=2}^{n}((1-a_{11})^{-1}a_{1j})x_j,$$

contradicting the minimality of the generating set. We conclude that there is cannot be a nontrivial generating set so $M = 0$.

Problem 7. Find $[K : \mathbb{Q}]$ where K is a splitting field of $X^6 - 4X^3 + 1$ over $\mathbb{Q}$.

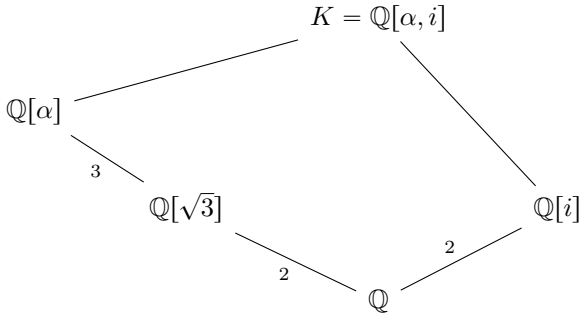
Let $f = X^6 - 4X^3 + 1$. Using the quadratic formula for X^3, we find the roots of f are $\{\sqrt[3]{2 \pm \sqrt{3}}\xi^i\}$ for $0 \leqslant i \leqslant 2$ where ξ is a primitive third root of unity. Let $\alpha := \sqrt[3]{2+\sqrt{3}}$ be the real third root. We have $\frac{1}{\alpha} = \sqrt[3]{2-\sqrt{3}}$ after simplification and $\alpha^3 - 2 = \sqrt{3} \in K$. Thus $\alpha, \sqrt[3]{2-\sqrt{3}}, \xi \in \mathbb{Q}[\alpha, i]$ so $K \subset \mathbb{Q}[\alpha, i]$. Then

$$\alpha^2(\alpha\xi) - \left(1 + \frac{\sqrt{3}}{2}\right) = (2+\sqrt{3})\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) - \left(1 + \frac{\sqrt{3}}{2}\right) = \left(\sqrt{3} + \frac{3}{2}\right)i \in K$$

$$\frac{4\left(\sqrt{3} - \frac{3}{2}\right)}{3}\left(\sqrt{3} + \frac{3}{2}\right)i = \frac{4\left(3 - \frac{9}{4}\right)i}{3} = i \in K.$$

Since $\alpha, i \in K$, we have $K \supset \mathbb{Q}[\alpha, i]$ and $K = \mathbb{Q}[\alpha, i]$,

We construct the tower of fields below. We know $\mathbb{Q}[i] \not\subset \mathbb{Q}[\alpha]$ since $\mathbb{Q}[\alpha] \subset \mathbb{R}$ by choice of α. Additionally, $\mathbb{Q}[i] \cap \mathbb{Q}[\alpha]$ is a subfield of $\mathbb{Q}[i]$ so $\mathbb{Q}[i] \cap \mathbb{Q}[\alpha] = \mathbb{Q}[i]$ or $\mathbb{Q}[i] \cap \mathbb{Q}[\alpha] = \mathbb{Q}$. We have $\mathbb{Q}[i] \cap \mathbb{Q}[\alpha] = \mathbb{Q}$. Since $\mathbb{Q}[i]/\mathbb{Q}$ is a normal extension, $\mathbb{Q}[i]$ and $\mathbb{Q}[\alpha]$ are linearly disjoint. This implies that $[K : \mathbb{Q}] = [\mathbb{Q}[i] : \mathbb{Q}][\mathbb{Q}[\alpha] : \mathbb{Q}] = 2[\mathbb{Q}[\alpha] : \mathbb{Q}]$. Assume $\alpha \in \mathbb{Q}[\sqrt{3}]$ so $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}]$. Then $G := \mathrm{Gal}(K/\mathbb{Q})$ has order 4. However, G needs to define a transitive group action on the set of 6 roots of $X^6 - 4X^3 + 1$. Neither the cyclic group of order 4 nor $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ would satisfy this condition. Therefore, $\alpha \notin \mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{3}] \subset \mathbb{R}$ imply the degree 3 polynomial $X^3 - (2+\sqrt{3}) \in \mathbb{Q}[\sqrt{3}][X]$ is irreducible. We conclude that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}[\sqrt{3}]][\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 6$ and $[K : \mathbb{Q}] = 12$.



Problem 8. Let M be an abelian group (written additively). Prove that there is a functor F from the opposite of the category of rings to the category of sets taking a ring R to the set of all left R-module structures on M. Is the functor F representable?

A left R-module structure on M is equivalent to a ring morphism $f : R \to \mathrm{End}(M)$ with scalar multiplication defined as $r \cdot m = f(r)(m)$. Thus define $F : \mathrm{Rings}^{\mathrm{op}} \to \mathrm{Sets}$ as $F(R) := \mathrm{Hom}_{Rings^{op}}(\mathrm{End}(M), R)$ and $F(g) : F(R) \to F(S)$ as $F(g)(f) = g \circ f \in \mathrm{Hom}_{\mathrm{Rings}^{op}}(\mathrm{End}(M), S)$ for $g \in \mathrm{Hom}_{\mathrm{Rings}^{op}}(R, S)$ and $f \in F(R)$. Then $F(1_R)(f) = f$ for all $f \in F(R)$ so $F(1_R) = 1_{F(R)}$. Let $g \in \mathrm{Hom}_{\mathrm{Rings}^{op}}(R, S)$ and $h \in \mathrm{Hom}_{\mathrm{Rings}^{op}}(S, T)$, then $F(h \circ g)(f) = (h \circ g) \circ f = F(h)(g \circ f) = (F(h) \circ F(g))(f)$. Therefore, F is a functor from the opposite category of rings to the category of sets.

We define a natural transformation $\eta_R : \mathrm{Hom}_{Rings^{op}}(R, \mathrm{End}(M)) \to F(R)$ as $\eta_R(f) := f$. Let $g : R \to S$ be a morphism in the opposite category of rings. We want to show that the diagram below commutes. By our construction, it is trivial. We have $F(g)(\eta_R(f)) = g \circ f$ and $\eta_S(g \circ f) = g \circ f$. Therefore, the functor F is representable.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathrm{Rings}^{\mathrm{op}}}(\mathrm{End}(M), R) & \xrightarrow{\eta_R} & F(R) \\ \downarrow{\scriptstyle g\circ -} & & \downarrow{\scriptstyle F(g)} \\ \mathrm{Hom}_{\mathrm{Rings}^{\mathrm{op}}}(\mathrm{End}(M), S) & \xrightarrow{\eta_S} & F(S) \end{array}$$

Problem 9. Let R be a ring. Prove that if the left free R-modules R^n and R^m are isomorphic for some positive integers n and m, then R^n and R^m are isomorphic as right R-modules.

Let $\phi : R^n \to R^m$ be a left R-module isomorphism with inverse $\psi : R^m \to R^n$. Pick the standard basis $\{e_1, \ldots, e_n\}$ for R^n and $\{f_1, \ldots, f_m\}$ for R^m. Then $\phi(e_i) = \sum_{j=1}^m a_{ij} f_j$ for each $1 \leqslant i \leqslant n$ and $a_{ij} \in R$. Multiplication by the $n \times m$ matrix $A = (a_{ij})$ represents ϕ. Similarly, $\psi(f_k) = \sum_{\ell=1}^n b_{k\ell} e_\ell$ for each $1 \leqslant k \leqslant m$ and $b_{k\ell} \in R$ gives an $n \times m$ matrix $B = (b_{k\ell})$. Since $\psi \circ \phi = \mathrm{id}_{R^n}$ and $\phi \circ \psi = \mathrm{id}_{R^m}$, we have $BA = I_n$ and $AB = I_m$. Left multiplication by A is a right R-module homomorphism since $A(xr) = (Ax)r$ for $x \in R^n$ and $r \in R$. We conclude that $R^n \simeq R^m$ as right R-modules.

Problem 10. Let K/F be a (finite) Galois field extension with $G = \mathrm{Gal}(K/F)$ and let $H \subset G$ be a subgroup. Determine in terms of H and G the group $\mathrm{Gal}(K^H/F)$ of all field automorphisms of K^H over F.

Note that K/F Galois implies that K^H/F is a separable extension. By the Primitive Element Theorem, $K^H = F[\alpha]$ for some $\alpha \in K$. For an automorphism $\tau \in \mathrm{Gal}(K^H/F)$, there is an extension $\sigma : K \to K$ such that $\sigma(\alpha) = \tau(\alpha)$ and $\sigma(x) = x$ for $x \in F$. Thus $\sigma \in G$, which implies that each $\tau \in \mathrm{Gal}(K^H/F)$ can be viewed as a restriction of an element in G.

Take an element $\sigma \in G$. We want to show that $\sigma|_{K^H} \in \mathrm{Gal}(K^H/F)$ if and only if $\sigma \in N_G(H)$. ($\Rightarrow$) Assume $\sigma|_{K^H} \in \mathrm{Gal}(K^H/F)$ so $\sigma(K^H) \subset K^H$. Let $h \in H$ and $x \in K^H$. Then $\sigma h \sigma^{-1}(x) = \sigma(h(\sigma^{-1}(x))) = \sigma(\sigma^{-1}(x)) = x$ since $\sigma^{-1}(x) \in K^H$. We note $\sigma h \sigma^{-1}$ fixes all $x \in K^H$ so $\sigma h \sigma^{-1} \in H$. Thus $\sigma \in N_G(H)$. ($\Leftarrow$) We will prove the contrapositive. Assume $\sigma|_{K^H} \notin \mathrm{Gal}(K^H/F)$. Then there is some $y \in K^H$ for which $\sigma(y) = z \notin K^H$. Thus there is some $h \in H$ such that $h(z) \neq z$ so $\sigma^{-1}(h(\sigma(y))) = \sigma^{-1}(h(z)) \neq y$. As a result, $\sigma(h(\sigma^{-1}(x))) \notin H$ and $\sigma \notin N_G(H)$.

The above result allows us to define the restriction homomorphism $r : N_G(H) \to \mathrm{Gal}(K^H/F)$ by $r(\sigma) = \sigma|_{K^H}$. The first argument shows that r is surjective. It is clear that $H \subset \ker(r)$ since $h \in H$ fixes all elements of K^H. Take $\sigma \in \ker(r)$ so σ fixes each $x \in K^H$. Then the subgroup $I \subset G$ generated by $H \cup \{\sigma\}$ has $K^I \supset K^H$. This implies $I \subset H$ and, by construction, $I \supset H$ so $H = I$. Thus $\sigma \in H$. We conclude that $\ker(f) = H$ and $\mathrm{Gal}(K^H/F) \simeq N_G(H)/H$ by the First Isomorphism Theorem.

Fall 2017

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

Let G act on a set X with $g \cdot x = y$ for $g \in G$ and $x, y \in X$. We want to show that $\mathrm{Stab}(Y) = g\mathrm{Stab}(x)g^{-1} \subset G$. Let $h \in \mathrm{Stab}(y)$. Then $g^{-1}hg \cdot x = g^{-1}h \cdot y = g^{-1} \cdot y = x$ so $g^{-1}hg \in \mathrm{Stab}(x)$. We have $g^{-1}\mathrm{Stab}(y)g \subset \mathrm{Stab}(x)$. Next let $k \in \mathrm{Stab}(x)$. Then $gkg^{-1} \cdot y = gk \cdot x = g \cdot x = y$ and $g\mathrm{Stab}(x)g^{-1} \subset \mathrm{Stab}(y)$. Since conjugation by an element of a group is an invertible operation, $\mathrm{Stab}(y) = g\mathrm{Stab}(x)g^{-1}$.

We can define an N-action on S via conjugation. Define $\mathrm{Stab}(X) := \bigcap_{x \in X} \mathrm{Stab}(x) \subset G$. Since $X, Y \subset Z(S)$, we have $S \subset \mathrm{Stab}(X)$ and $S \subset \mathrm{Stab}(Y)$. Note that S is a Sylow p-subgroup of $\mathrm{Stab}(X)$ and $\mathrm{Stab}(Y)$. By the result above applied to each $y \in Y$, we have $\mathrm{Stab}(Y) = g\mathrm{Stab}(X)g^{-1}$. Conjugation preserves the order of subgroups so $gSg^{-1} \subset \mathrm{Stab}(Y)$ is a Sylow p-subgroup of $\mathrm{Stab}(Y)$. By Sylow's Second Theorem, the two Sylow p-subgroups S and gSg^{-1} are conjugate in $\mathrm{Stab}(Y)$. Thus there exists an $h \in \mathrm{Stab}(Y)$ such that $h(gSg^{-1})h^{-1} = S$. We note that $hg \in N$. Additionally, $(hg) \cdot x = h \cdot (gxg^{-1}) = gxg^{-1}$ since $h \in \mathrm{Stab}(Y)$. Let $n := hg \in N$ and $nxn^{-1} = gxg^{-1}$ for all $x \in X$.

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

Let G be a p-group that acts on a finite set X. We will first show that $|X^G| \equiv |X| \pmod{p}$ where $X^G = \{x \in X : |\mathrm{Orb}(x)| = 1\}$. The orbits partition X so

$$|X| = |X^G| + \sum_{x \in X, x \notin X^G} |\mathrm{Orb}(x)|.$$

By Orbit-Stabilizer, $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|$ by $|G|$ finite. For $x \notin X^G$, we have $|\mathrm{Orb}(x)| = |G|/|\mathrm{Stab}(y)| > 1$ so p will divide $|G|/|\mathrm{Stab}(y)| = |\mathrm{Orb}(x)|$. Therefore, $|X| \equiv |X^G|$ modulo p.

Let $|G| = p^k$. Let $H \subset G$ be a maximal proper subgroup of G so $|H| = p^{k-1}$. Let H act on G/H by left multiplication. If $aH \in X^H$, then $b(aH) = aH$ for all $b \in H$. Thus $aba^{-1} \in H$ and $a \in N_G(H)$. Similarly, taking some $a \in N_G(H)$ gives $aH \in X^H$. Therefore, $X^H = [N_G(H) : H]$ and the above result implies $[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$. We conclude $[N_G(H) : H] = p$ and $N_G(H) = G$ since $|H| = p^{k-1}$. Now that H is a normal subgroup of G, the set G/H is a group of order p. The only such group is the cyclic group $\mathbb{Z}/p\mathbb{Z}$ so $G/H \simeq \mathbb{Z}/p\mathbb{Z}$. If $g \notin H$ for $g \in G$, then the left cosets gH and H are not equal. Thus gH is a generator of G/H so $(gH)^p = g^pH = H$. Further, G/H is abelian so the canonical projection $p : G \to G/H$ factors through $\pi : G/[G, G]$ for $[G, G]$ the commutator subgroup. Thus $\ker(\pi) = [G, G] \subset \ker(p) = H$ and H contains all elements of the form $ghg^{-1}h^{-1}$ for $g, h \in H$. Therefore, $\Phi(G)$ is contained in the intersection of the maximal proper subgroups of G.

Now we will show that for each $g \notin \Phi(G)$, there is some maximal proper subgroup M of G such that $g \notin M$. In particular, $g \notin [G, G]$ so $g[G, G] \in G/[G, G]$ is a non-trivial element of an abelian group. Since G is finite, $G/[G, G]$ is a finite abelian group. Our classification of finitely generated $\mathbb{Z}$-modules implies $G/[G, G] \simeq \bigoplus_{i=1}^{\ell} \mathbb{Z}/p_i^{k_\ell}\mathbb{Z}$. Since $g \notin \Phi(G)$, it cannot be a product of a pth power of some $h \in G$ and an element of $[G, G]$. Thus the element $g[G, G]$ has to be a generator for one of the direct summands. By reordering the summands, assume $g[G, G]$ generates the first. Let $S := \{g_i\}_{i=2}^{\ell}$ be a set of elements $g_i \in G$ such that $g_i[G, G]$ generates the ith direct summand. Let T be a set of generators for $[G, G]$. Then the set $S \cup T \cup \{g^n\}$ generates a subgroup M of G. By construction, $g \notin M$ so M is proper. M is maximal in G since G would be generated by $\{g\} \cup M$ and $g^p \in M$. We conclude that $\Phi(G)$ is the intersection of the maximal proper subgroups of G.

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

We want to show that M is the sum of all of the simple modules of A. Let N be a simple left A-module. Then $J(A)N = 0$ by the definition of the Jacobson radical as the annihilator of all simple left A-modules. Since $t(xn) = 0$ for $n \in N$ and all $x \in J(A)$, we have $N \subset M$. Thus M contains the sum of all the simple left A-submodules of A.

Take a descending chain of left ideals of A. Each left ideal is a finite-dimensional k-vector space. Thus the chain must terminate, and A is left Artinian as a left A-module. The same argument works for right ideals so A is Artinian as a ring. Consequently, $A/J(A)$ is an Artinian ring. Since $J(A)$ is a two-sided ideal of A, we have $J(A)M$ is a left ideal contained in $\ker(t)$. We assume $\ker(t)$ contains no non-zero left ideal so $J(A)M = 0$. Thus M has the structure of a left $A/J(A)$-module. Now $A/J(A)$ is Artinian and has trivial Jacobson radical so $A/J(A)$ is a semisimple ring. We conclude that M is a semisimple left $A/J(A)$-module. In other words, M is the direct sum of simple left $A/J(A)$-modules. These simple $A/J(A)$-modules are simple as A-modules so M is a semisimple left A-module. Since M contains the sum of all simple left A-modules, M is the largest semisimple left A-submodule of A.

Problem 4. Let R be a commutative Noetherian ring and A a finitely generated R-algebra (not necessarily commutative). Let B be an R-subalgebra of the center $Z(A)$. Assume A is a finitely generated B-module. Show that B is a finitely generated R-algebra.

Let $\{x_1, \ldots, x_m\}$ generate A as a C-algebra and $\{y_1, \ldots, y_n\}$ generated A as a B-module. Then $x_i = \sum_{j=1}^{n} b_{ij}y_j$ and $y_iy_j = \sum_{k=1}^{n} b_{ijk}y_k$ for some $b_{ij}, b_{ijk} \in B$. Let B_0 be the R-algebra generated by the set $\{b_{ij}, b_{ijk}\}$. Since R is Noetherian and B_0 is finitely generated as an R-algebra, B_0 is a Noetherian as a ring. Every element of C is

a polynomial in the x_i, which we can write in terms of the y_j. Then $B \subset Z(A)$ and $y_i y_j = \sum_{k=1}^n b_{ijk} y_k$ allow us to reduce this expression to a linear combination of the y_j with coefficients in B_0. Thus A is a finitely generated B_0-module, which implies A is a Noetherian B_0-module. Initially, B is an R-subalgebra of A and $B_0 \subset B$ so B has the structure of a B_0-submodule of A. Thus B is finitely generated as a B_0-module. B_0 is finitely generated as an R-algebra so B is finitely generated as an R-algebra.

This proof is based on that of Proposition 7.8 in Atiyah MacDonald.

Problem 5. Let A be a ring and M an A-module that is a finite direct sum of simple A-modules. Let $f \in \mathrm{End}_{\mathbb{Z}}(M)$. Assume $f \circ g = g \circ f$ for all $g \in \mathrm{End}_A(M)$. Consider a positive integer n.

(a) Show that the map $f_n : M^n \to M^n$ defined by $f_n(m_1, \ldots, m_n) = (f(m_1), \ldots, f(m_n))$ commutes with all elements of $\mathrm{End}_A(M^n)$.

Note that $\mathrm{End}_A(M^n) = \mathrm{Hom}_A\left(\bigoplus_{i=1}^n M, \bigoplus_{j=1}^n M\right) \simeq \bigoplus_{i,j=1}^n \mathrm{Hom}_A(M, M)$. Let $g \in \mathrm{End}_A(M^n)$ so we can identify g with the matrix (g_{ij}) for $1 \leqslant i, j \leqslant n$ and $g_{ij} \in \mathrm{Hom}_A(M, M)$. Then

$$\begin{aligned} g(f_n(m_1, \ldots, m_n)) &= g(f(m_1), \ldots, f(m_n)) \\ &= \left(\sum_{i=1} g_{i1}(f(m_1)), \ldots, \sum_{i=1}^n g_{in}(f(m_n)) \right) \\ &= \left(\sum_{i=1} f(g_{i1}(m_1)), \ldots, \sum_{i=1}^n f(g_{in}(m_n)) \right) \\ &= f_n\left(\sum_{i=1} g_{i1}(m_1), \ldots, \sum_{i=1}^n g_{in}(m_n) \right) \\ &= f_n(g(m_1, \ldots, m_n)). \end{aligned}$$

Therefore, f commutes with all elements of $\mathrm{End}_A(M^n)$.

(b) Deduce that given any family $(m_1, \ldots, m_n) \in M^n$, there exists $a \in A$ such that $(f(m_1), \ldots, f(m_n)) = (am_1, \ldots, am_n)$.

DEFINITELY DOESN'T FEEL RIGHT

Let $M = \bigoplus_{i=1}^k L_i$ for L_i the distinct simple A-modules. Let $\{e_1, \ldots, e_n\}$ be the corresponding central idempotents for $e_i \in M$. Then

$$\mathrm{End}_A(M) = \mathrm{Hom}_A\left(\bigoplus_{i=1}^k L_i, \bigoplus_{i=1}^k L_i \right) \simeq \bigoplus_{i,j=1}^k \mathrm{Hom}_A(L_i, L_j) \simeq \bigoplus_{i=1}^k \mathrm{Hom}_A(L_i, L_i)$$

since each L_i is a simple A-module. Each L_i is cyclic, generated by e_i, so $f \in \bigoplus_{i=1}^n \mathrm{Hom}_A(L_i, L_i)$ is defined by the image of the e_i. We have $f(e_i) = a_i e_i$ for some $a_i \in A$ since e_i must map to an element of Ae_i. Define $a := \sum_{i=1}^n a_i e_i$, then $f(x) = ax = \sum_{i=1}^n a_i e_i x$. We conclude that $f_n(m_1, \ldots, m_n) = (am_1, \ldots, am_n)$.

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

We will show that $m = 0$ if and only if $\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subset R$. If $m = 0$, the result is clear. Assume $m \neq 0$ and we will show that there is some prime $\mathfrak{p} \subset R$ for which $\frac{m}{1} \neq 0$. Since $m \neq 0$, the ideal $\mathrm{Ann}(m) \subset R$ is proper. By a Zorn's Lemma argument, $\mathrm{Ann}(m)$ is contained in some maximal and, thus, prime ideal $\mathfrak{p} \subset R$. We have $\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ only when there is some $s \in S$ such that $sm = 0$. But $s \notin \mathrm{Ann}(m)$ for all $s \in R \backslash \mathfrak{p}$ so $\frac{m}{1} \neq 0 \in M_{\mathfrak{p}}$.

($\Rightarrow$) We will prove the contrapositive. Assume $\frac{r}{s}\frac{m}{t} = 0$ in $M_{\mathfrak{p}}$ for some $r \in R$, $s, t \in S$, and non-zero $m \in M$. Then there is some $k \in S$ such that $(kr)m = 0$ for $kr \in R$ which implies that M is not torsion-free.

($\Leftarrow$) Let $f : M \to N$ be a left R-module homomorphism. If f is not injective, there is some non-zero $x \in \ker(f)$. Then $\frac{x}{1}$ is non-zero in $M_{\mathfrak{p}}$ for some $\mathfrak{p}$ by above. Thus $\ker(f) = 0$ if and only if $(R \backslash \mathfrak{p})^{-1} \ker(f) \subset M_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subset R$. Assume $M_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-torsion-free for all prime ideals $\mathfrak{p} \subset R$. Define the left R-module homomorphism $\ell_r : M_{\mathfrak{p}} \to M_{\mathfrak{p}}$ as left multiplication by $\frac{r}{1}$. Since $M_{\mathfrak{p}}$ is torsion-free, ℓ_r is injective for each prime ideal $\mathfrak{p} \subset R$. Therefore, $\ell_r : M \to M$ given by left multiplication by $r \in R$ is injective for any $r \in R$. We conclude that M is torsion-free.

Problem 7.

(a) Show that there is at most one extension $F(\alpha)$ of a field F such that $\alpha^4 \in F$, $\alpha^2 \notin F$, and $F(\alpha) = F(\alpha^2)$.

We have that α is a root of $f := x^4 - \alpha^4 \in F[x]$. Similarly, α^2 is a root of $x^2 - \alpha^4$ so $[F[\alpha^2] : F] = 2$. Assume first that char $= 2$. Then $x^4 - \alpha^4 = x^4 + \alpha^4 = (x + \alpha)^4$. Since $[F[\alpha] : F] = [F[\alpha^2] : F] = 2$, the minimal polynomial of α must be $(x + \alpha)^2$, which implies $\alpha^2 \in F$, a contradiction.

Assume $\text{char}(F) \neq 2$. Then $f' = 4x^3 \neq 0$, which is relatively prime to f. Then f is separable and the roots are $\{\pm\alpha, \pm\alpha\gamma\}$ for $\gamma^2 = -1$. We have two cases for the minimal polynomial of α, denoted $m_\alpha \in F[x]$. If $m_\alpha = (x - \alpha)(x + \alpha)$, then $\alpha^2 \in F$, a contradiction. If $m_\alpha = (x \pm \alpha)(x \pm \alpha\gamma)$, then $\alpha^2\gamma \in F$. Note $\gamma \in F$ would imply $\alpha^2 \in F$ so $\gamma \notin F$. But $\alpha^2(\alpha^2\gamma) = \alpha^4\gamma \in F[\alpha^2] = F[\alpha]$ so $\gamma \in F[\alpha]$. We have the tower of fields $F[\alpha]/F[\gamma]/F$ with $[F[\alpha] : F] = 2$. Since $\gamma \notin F$, we conclude $F[\alpha] = F[\gamma]$. Therefore, there is at most one field extension like $F[\alpha]$ since it would equal $F[\gamma]$.

(b) Find the isomorphism class of the Galois group of the splitting field of $x^4 - a$ for $a \in \mathbb{Q}$ with $a \notin \pm\mathbb{Q}^2$.

FINISH THIS

By Fall 2014 Problem 3 Case 4, we have $G \simeq D_4$ for $a > 0$. Additionally by Fall 2014 Problem 3 Case 5, we have $G \simeq D_4$ for $a < 0$ and $a \neq -2y^2$ for $y \in \mathbb{Q}$. Finally, we need to check the case when $a = -2y^2$ for $y \in \mathbb{Q}$. The roots of $X^4 - a$ are $\{\sqrt{2}y\xi_8^i\}$ for $i \in \{1, 3, 5, 7\}$.

Problem 8. Let F be a field, and let $f, g \in F[x]\backslash\{0\}$ be relatively prime and not both constant. Show that $F(x)$ has finite degree $d = \max(\deg(f), \deg(g))$ over its subfield $F\left(\frac{f}{g}\right)$. (Hint: If the degree were less than d, show that there exists a nonzero polynomial with coefficients in $F[x]$ of degree less than d having $\frac{f}{g}$ as a root.)

Note that $\frac{f}{g}$ is a root of the irreducible polynomial $p = gy - f$ for $p \in (F[x])[y]$. Since f and g are relatively prime, p is primitive. The polynomial $q = \frac{f}{g}g(T) - f(T) \in (F[x])[T]$ is degree d and has x as a root. Thus $\left[F(x) : F\left(\frac{f}{g}\right)\right] \leqslant d$ and $F(x)$ is a finite extension of $F\left(\frac{f}{g}\right)$. Let $m = a_kT^k + a_{k-1}T^{k-1} + \cdots + a_0 \in F\left(\frac{f}{g}\right)[T]$ be the minimal polynomial of x over $F\left(\frac{f}{g}\right)$. By clearing denominators, we may assume that each $a_i \in F\left[\frac{f}{g}\right]$. Then $m = b_n\left(\frac{f}{g}\right)^n + b_{n-1}\left(\frac{f}{g}\right)^{n-1} + \cdots + b_0$ for $b_i \in F[T]$. After writing each b_i as an element of $F[x]$, $M := b_ny^n + b_{n-1}y^{n-1}\cdots + b_0$ is a polynomial in $(F[x])[y]$ with $\frac{f}{g}$ as a root. Thus p divides M in $(F[x])[y]$. Since p is primitve, g divides b_n and f divides b_0. We have $\deg(b_n) \geqslant \deg(g)$ and $\deg(b_0) \geqslant \deg(f)$ so $\deg(m) \geqslant d$. Therefore, $\left[F(x) : F\left(\frac{f}{g}\right)\right] = d$.

Problem 9. Let R be a commutative ring, and let A, B, and C be R-modules. Suppose that A is finitely presented over R and C is flat over R. Show that

$$\text{Hom}_R(A, B \otimes_R C) \simeq \text{Hom}_R(A, B) \otimes_R C.$$

Since A is finitely presented, there is an exact sequence $R^m \to R^n \to A \to 0$ with $g : R^n \to A$ and $h : R^m \to A$. Apply the left exact functor $\text{Hom}_R(-, B)$ to obtain the exact sequence $0 \to \text{Hom}_R(A, B) \to \text{Hom}_R(R^n, B) \to \text{Hom}_R(R^m, B)$ with morphisms $- \circ g : \text{Hom}_R(A, B) \to \text{Hom}_R(R^n, B)$ and $- \circ h : \text{Hom}_R(R^n, B) \to \text{Hom}_R(R^m, B)$. We assume C is flat so $0 \to \text{Hom}_R(A, B) \otimes_R C \to \text{Hom}_R(R^n, B) \otimes_R C \to \text{Hom}_A(R^m, B) \otimes_R C$ is exact. Similarly, apply the functor $\text{Hom}_R(-, B \otimes_R C)$ to the original exact sequence. Define the morphism $\phi_A : \text{Hom}_R(A, B) \otimes_R C \to \text{Hom}_R(A, B \otimes_R C)$ by $\phi(f \otimes c) = (a \mapsto f(a) \otimes c)$. Then ϕ_A is an R-module homomorphism via $\phi_A(r \cdot f \otimes c) = \phi_A(f \otimes (rc)) = (a \mapsto f(a) \otimes (rc)) = r(a \mapsto f(a) \otimes c)$. Let $f \in \text{Hom}_R(A, B) \otimes_R C$. Then

$$\phi_{R^n}((f \circ g) \otimes 1_C) = (a \mapsto (fg)(a) \otimes c) = (\phi_A(f)) \circ g$$

and a similar argument for the other square give the commutative diagram below. As R-modules, $\text{Hom}_R(R^n, B) \simeq \prod_{i=1}^n \text{Hom}_R(R, B) \simeq B^n$ so $\text{Hom}_R(R^n, B) \otimes_R C \simeq B^n \otimes_R C \simeq \text{Hom}_R(R^n, B \otimes_R C)$ with ϕ_{R^n} the isomorphism for

all $n \geqslant 1$. By the Five Lemma, ϕ_A is an isomorphism.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & \mathrm{Hom}_R(A,B)\otimes_R C & \xrightarrow{-\circ g\otimes 1_C} & \mathrm{Hom}_R(R^n,B)\otimes_R C & \xrightarrow{-\circ h\otimes 1_C} & \mathrm{Hom}_A(R^m,B)\otimes_R C \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle \phi_A} & & \downarrow{\scriptstyle \phi_{R^n}} & & \downarrow{\scriptstyle \phi_{R^m}} \\
0 & \longrightarrow & 0 & \longrightarrow & \mathrm{Hom}_R(A, B\otimes_R C) & \xrightarrow{-\circ g} & \mathrm{Hom}_R(R^n, B\otimes_R C) & \xrightarrow{-\circ h} & \mathrm{Hom}_R(R^m, B\otimes_R C)
\end{array}$$

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

(a) Find a left adjoint to F.

Let $C, D \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$. Define $L : \mathcal{C} \to \mathcal{C}^2$ as $L(C) := (C, C)$ and $L(f) : L(C) \to L(D)$ as (f, f). Then $L(1_C) = (1_C, 1_C) = 1_{L(C)}$. Additionally, $L(gf) = (gf, gf) = (g, g) \circ (f, f) = L(g)L(f)$ for a morphism $g \in \mathrm{Hom}_{\mathcal{C}}(D, E)$ and $E \in \mathrm{Ob}(\mathcal{C})$. Thus L is a functor.

By the universal property of the direct product, there is a unique morphism $h : C \to A \prod B$ for each pair of morphisms $(f, g) : (C, C) \to (A, B)$ such that $\mathrm{pr}_A \circ h = f$ and $\mathrm{pr}_B \circ h = g$. Define a natural transformation $\Phi : \mathrm{Hom}_{\mathcal{C}^2}(L(-), -) \to \mathrm{Hom}_{\mathcal{C}^2}(-, F(-))$ so that $\Phi_{C,(A,B)} : \mathrm{Hom}_{\mathcal{C}}(L(C), (A, B)) \to \mathrm{Hom}_{\mathcal{C}^2}(C, F(A, B))$ gives $\Phi_{C,(A,B)}(f, g) := h$. Let $k \in \mathrm{Hom}_{\mathcal{C}}(C', C)$ for $C' \in \mathrm{Ob}(\mathcal{C})$. We want to show the diagram below commutes. Let $(f, g) \in \mathrm{Hom}_{\mathcal{C}}(L(C), (A, B)) = \mathrm{Hom}_{\mathcal{C}}((C, C), (A, B))$. We have $\Phi_{C,(A,B)}(f, g) \circ k$ is a morphism from C' to $A \prod B$ for which $\mathrm{pr}_A \circ (\Phi_{C,(A,B)}(f, g) \circ k) = f \circ k$ and $\mathrm{pr}_B \circ (\Phi_{C,(A,B)}(f, g) \circ k) = g \circ k$. We have $\Phi_{C',(A,B)}(f \circ k, g \circ k)$ is the unique morphism $C' \to A \prod B$ that commutes with $f \circ k$ and $g \circ k$ under projection morphisms. Thus the universal property of the direct product implies $\Phi_{C,(A,B)}(f, g) \circ k = \Phi_{C,(A,B)}(f, g) \circ k$ and the diagram commutes. By a similar argument, we obtain naturality in (A, B). We conclude that L is a left adjoint to F.

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(L(C), (A,B)) & \xrightarrow{\Phi_{C,(A,B)}} & \mathrm{Hom}_{\mathcal{C}^2}(C, F(A,B)) \\
\downarrow{\scriptstyle (-\circ k, -\circ k)} & & \downarrow{\scriptstyle -\circ k} \\
\mathrm{Hom}_{\mathcal{C}}(L(C'), (A,B)) & \xrightarrow{\Phi_{C',(A,B)}} & \mathrm{Hom}_{\mathcal{C}^2}(C', F(A,B))
\end{array}$$

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

Since abelian groups is an abelian category, finite products and coproducts are isomorphic. Define $R : \mathcal{C} \to \mathcal{C}^2$ as $R(C) := (C, C)$ and $R(f) := (f, f)$ for $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$. Then $R(1_C) = (1_C, 1_C) = 1_{R(C)}$. Additionally, $R(gf) = (gf, gf) = (g, g) \circ (f, f) = R(g)R(f)$ for a morphism $g \in \mathrm{Hom}_{\mathcal{C}}(D, E)$ and $E \in \mathrm{Ob}(\mathcal{C})$. Thus R is a functor.

By the universal property of the coproduct, there is a unique morphism $h : A \coprod B \to C$ for each pair $(f, g) : (A, B) \to (C, C)$ such that $h \circ i_A = f$ and $h \circ i_B = g$. Define the natural transformation $\Phi : \mathrm{Hom}_{\mathcal{C}^2}(-, R(-)) \to \mathrm{Hom}_{\mathcal{C}}(F(-), -)$ as $\Phi_{(A,B),C}(f, g) := h$. As in (a), the universal property of the coproduct implies naturality in (A, B) and C. We conclude that R is a right adjoint to F.

Spring 2018

Problem 1. Let $\alpha \in \mathbb{C}$. Suppose that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite and prime to $n!$ for an integer $n > 1$. Show that $\mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$.

The field $\mathbb{Q}(\alpha^n)$ is a subfield of $\mathbb{Q}(\alpha)$. In fact, α is a root of $f = x^n - \alpha^n$ over $\mathbb{Q}(\alpha^n)$. Thus the minimal polynomial of α over $\mathbb{Q}(\alpha^n)$, $m_\alpha \in \mathbb{Q}(\alpha^n)[x]$, must divide f. As a result, $\deg(m_\alpha) \leqslant n$ and $\deg(m_\alpha) | (n!)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)][\mathbb{Q}(\alpha^n) : \mathbb{Q}] = \deg(m_\alpha)[\mathbb{Q}(\alpha^n) : \mathbb{Q}]$ is relatively prime to $n!$, we conclude that $\deg(m_\alpha) = 1$. Therefore, $\mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$.

Problem 2. Let $\zeta^9 = 1$ and $\zeta^3 \neq 1$ with $\zeta \in \mathbb{C}$.

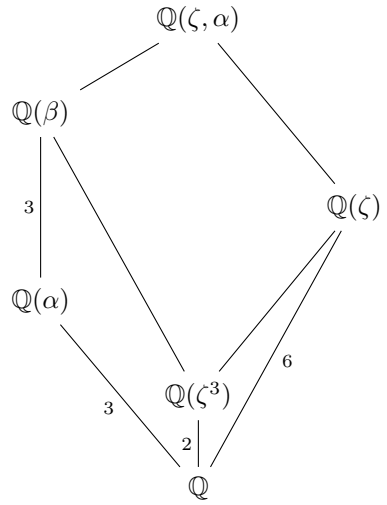
(a) Show that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$.

For the sake of contradiction, assume that $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$. Note that ζ is a primitive ninth root of unity. Then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/9\mathbb{Z})^\times$. In particular, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian. The polynomial $f = x^3 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with roots $\{\sqrt[3]{3}\zeta^{3i}\}_{i=0}^2$ for $\sqrt[3]{3} \in \mathbb{R}$. Thus $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$ is not the splitting field of f, the minimal polynomial of $\sqrt[3]{3}$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is abelian, $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ is a normal extension, a contradiction. We conclude that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$.

(b) If $\alpha^3 = 3$, show that α is not a cube in $\mathbb{Q}(\zeta, \alpha)$.

Assume that $\beta^3 = \alpha$ and $\beta \in \mathbb{Q}(\zeta, \alpha)$ for the sake of contradiction. Then $\mathbb{Q}(\zeta, \alpha)$ is the splitting field of $m_\beta = x^9 - 3$ over $\mathbb{Q}$. By Eisenstein's Criterion, m_β is irreducible in $\mathbb{Q}[x]$ so $[\mathbb{Q}(\beta) : \mathbb{Q}] = 9$. Since $\mathbb{Q}$ is perfect, $\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}$ is a Galois extension. We have the tower of fields shown below. We know that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta)$ is a subfield of a degree 3 extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. Thus $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}(\alpha)$ or $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$. By (a), $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ and $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois implies $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta)$ are linearly disjoint. Thus the degree of their compositum over $\mathbb{Q}$ is $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\zeta) : \mathbb{Q}] = 18$.

Since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta)$ are linearly disjoint and $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, we know that $\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\alpha)$ is Galois. Additionally, the restriction map from $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\alpha))$ to $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is an isomorphism. As before, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian so $\mathbb{Q}(\beta)/\mathbb{Q}(\alpha)$ must be a Galois extension. The polynomial $g = x^3 - \alpha$ has no roots in $\mathbb{Q}(\alpha)$ and, as a degree 3 polynomial, is irreducible over $\mathbb{Q}(\alpha)$. With g the minimal polynomial of β over $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)/\mathbb{Q}(\alpha)$ Galois, g must split in $\mathbb{Q}(\beta)$. Thus the roots $\{\beta\zeta^{3i}\}_{i=0}^2$ of g are elements of $\mathbb{Q}(\beta)$. Proceeding, $\beta^2(\beta\zeta^3) \in \mathbb{Q}(\beta)$ so $\mathbb{Q}(\zeta^3)$ is a subfield of $\mathbb{Q}(\beta)$. However, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 9$ and $[\mathbb{Q}(\zeta^3) : \mathbb{Q}] = \varphi(3) = 2$ for φ Euler's totient function, a contradiction. Therefore, α does not have a third root in $\mathbb{Q}(\zeta, \alpha)$.



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

We will classify the non-zero left ideals $I \subset M_n(\mathbb{Z})$. Since I is non-zero, there is an element $A \in I$ with a non-zero column. Without loss of generality, assume the first column is non-trivial. By left multiplication with elementary matrices, we can perform row operations on I. Since $\mathbb{Z}$ is a PID, Bezout's identity allows us to obtain the greatest common divisor of the entries in the first column of A. By row switches, put the greatest common divisor in the first row. Repeat this process for each matrix $B \in I$ with at least one non-zero entry in the first column. Then Bezout's identity allows us to obtain a matrix in I with the greatest common divisor $d_1 \in \mathbb{Z}$ of all non-zero entries of the first column of elements of I. There cannot be a matrix in I whose first column entries are not divisible by d_1 by construction. Thus the first columns of elements of I are of the form $d_1\mathbb{Z}^n$ for some $d_1 \in \mathbb{Z}$. Once we have the matrix with d_i in the first column, we can produce any matrix with multiples of d_i in the first column. Repeat this process for each column. As a result, the left ideals of $M_n(\mathbb{Z})$ are all matrices where elements of the ith column are multiples of some $d_i \in \mathbb{Z}$.

Let $D_1 \in I$ be the matrix with d_i in the first row and zero in each other row for the columns $1 \leqslant i \leqslant n$. By choosing $v \in \mathbb{Z}^n$ based on Bezout's identity, we have $D_1 v$ is the vector with $d := \gcd(d_1, \ldots, d_n)$ in the first row

and zeros in rows $2 \leqslant j \leqslant n$. The same argument allows us to produce any multiple of d in each row. In fact, every element of αv for $\alpha \in I$ must be divisible by d since the entries of α are all divisible by d. We conclude that $I\mathbb{Z}^n = (d\mathbb{Z})^n$ which has finite index in $\mathbb{Z}^n$.

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

We will first show that $K \otimes_k K$ has zero divisors. Let $m_\alpha \in k[x]$ be the minimal polynomial of α over k. Then $K \otimes_k K = k[x]/(m_\alpha) \otimes_k K = K[x]/(m_\alpha)$. Since K contains a root of m_α, $m_\alpha = \prod_{i=1}^m g_i$ for some irreducible polynomials $g_i \in K[x]$. Therefore, $K[x]/(m_\alpha) = K[x]/(\prod_{i=1}^m g_i) \simeq \prod_{i=1}^m K[x]/(g_i)$ by the Chinese Remainder Theorem. It is clear that $\prod_{i=1}^m K[x]/(g_i)$ has zero divisors for $m \geqslant 2$.

Now $K \otimes_k K$ is a subring of $D \otimes_k K$. Since $K \otimes_k K$ has zero divisors, we conclude that $D \otimes_k K$ is not a division ring. Note that $Z(D \otimes_k K) = Z(D) \otimes_k Z(K) = k \otimes_k K = K$. The tensor product of a central simple algebra and a simple algebra is simple. Therefore, $D \otimes_k K$ is a central simple K-algebra. By Artin-Wedderburn, $D \otimes_k K$ is the product of matrix algebras over division rings. However, $\dim_K(D \otimes_k K) = \dim_k(D) = p^2$ so either $D \otimes_k K$ is a division algebra or $D \otimes_k K \simeq M_p(K)$. By above, we have $D \otimes_k K \simeq M_p(K)$.

Problem 5. Let $\mathbb{C}$ be a category. A morphism $f : A \to B$ in $\mathbb{C}$ is called an epimorphism if for any two morphisms $g, h : B \to X$ in $\mathbb{C}$, $g \circ f = h \circ f$ implies $g = h$. Let ALG be the category of $\mathbb{Z}$-algebras, and let MOD be the category of $\mathbb{Z}$-modules.

(a) Prove that in MOD, $f : M \to N$ is an epimorphism if and only if f is a surjection.

($\Rightarrow$) We will prove the contrapositive. Assume that $f : M \to N$ is not surjective. Then $\mathrm{im}(f) \subset N$ is a proper $\mathbb{Z}$-submodule. We define $\pi : N \to N/\mathrm{im}(f)$ the canonical projection and $g : N \to N/\mathrm{im}(f)$ the zero $\mathbb{Z}$-module homomorphism. Then gf and πf are zero maps so $gf = \pi f$. Let $n \in N$ such that $n \notin \mathrm{im}(f)$. Then $g \neq \pi$ since $g(n) = 0 + im(f)$ while $g(n) = n + \mathrm{im}(f) \neq 0 + \mathrm{im}(f)$. We conclude that f is not an epimorphism

($\Leftarrow$) Let $f : M \to N$ be surjective. Let $g, h : N \to P$ be $\mathbb{Z}$-module homomorphisms such that $gf = hf$. Let $n \in N$, then $n = f(m)$ for some $m \in M$. As a result, $g(n) = g(f(m)) = h(f(m)) = h(n)$ so $g = h$. We conclude that f is right-cancellative and f is an epimorphism.

(b) In ALG, does the equivalence of epimorphism and surjection hold? If yes, prove the equivalence, and if no, give a counterexample (as simple as possible).

Let $i : \mathbb{Z} \to \mathbb{Q}$ be the canonical inclusion morphism of $\mathbb{Z}$-algebras. By Fall 2015 Problem 1, this morphism is a non-surjective epimorphism.

Problem 6. Let G be a group with a normal subgroup $N = \langle y, z \rangle$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Suppose that G has a subgroup $Q = \langle x \rangle$ isomorphic to the cyclic group $\mathbb{Z}/3\mathbb{Z}$ such that the composition $Q \subset G \to G/N$ is an isomorphism. Finally, suppose that $xyx^{-1} = z$ and $xzx^{-1} = yz$. Compute the character table of G.

We will find the conjugacy classes of G. Since $xy = zx$ and $xz = yzx$, we can write every element of G as $y^i z^j x^k$ for $0 \leqslant i, j \leqslant 1$ and $0 \leqslant i \leqslant 2$. The relations allow reduction to the form $y^i z^j x^k$ without changing the x exponent. As a result, conjugation by any element will preserve the x exponent of any element. We will show that the conjugacy classes are based on the exponent of x. The relations of G produce the conjugacy class $\{y, z, yz\}$. In the equations below, we start with x.

$$\begin{aligned} yxy^{-1} &= yxy = zx \\ y(zx)y^{-1} &= yz^2x = yx \\ z(zx)z^{-1} &= xz = yzx \end{aligned}$$

A similar argument starting with x^2 gives the conjugacy class breakdown below.

$$\{e\}, \{y, z, yz\}, \{x, yx, zx, yzx\}, \{x^2, yx^2, zx^2, yzx^2\}$$

Note that $|G| = 12$. Thus the sum of 1 and three squares needs to be $|G| = 12$. We cannot have an irreducible representations of dimension higher than three. The only option is $12 = 1^2 + 1^2 + 1^2 + 3^2$ so there should be three

isomorphism classes of one-dimensional representations and one isomorphism class of 3-dimensional irreducible representations.

We will first classify the characters of the one-dimensional irreducible representations. Let $\rho_i : G \to \mathbb{C}^\times$ for $1 \leqslant i \leqslant 3$ be the one-dimensional representations. Since y and z are order 2 elements of G, they must map to ± 1 in $\mathbb{C}^\times$. Similarly, x will be sent to a third root of unity. The group $\mathbb{C}^\times$ is abelian so $\rho(z) = \rho(xyx^{-1}) = \rho(x)\rho(y)\rho(x)^{-1} = \rho(y)$ and $\rho(yz) = \rho(xzx^{-1}) = \rho(x)\rho(z)\rho(x)^{-1} = \rho(z)$. Let ξ be a primitive third root of unity. We find the final row of the character table by column orthogonality and the identity $\sum_{i=1}^{3} \xi^i = 0$.

	1	y	x	x^2
χ_{trivial}	1	1	1	1
χ_{ρ_1}	1	1	ξ	ξ^2
χ_{ρ_2}	1	1	ξ^2	ξ
χ_μ	3	-1	0	0

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

WE NEVER FIGURED THIS ONE OUT

Problem 8. Let F be a field that contains the real numbers $\mathbb{R}$ as a subfield. Show that the tensor product $F \otimes_{\mathbb{R}} \mathbb{C}$ is either a field or isomorphic to the product of two copies of F, $F \times F$.

We note that $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$ so $F \otimes_{\mathbb{R}} \mathbb{C} \simeq F \otimes_{\mathbb{R}} \mathbb{R}[x]/(x^2+1) \simeq F[x]/(x^2+1)$. If x^2+1 is irreducible in $F[x]$, then $F[x]/(x^2+1)$ is a field. If x^2+1 has a root in F, then $F[x]/(x^2+1) \simeq F[x]/(x-\alpha) \times F[x]/(x-\beta) \simeq F \times F$ by the Chinese Remainder Theorem. Therefore, $F \otimes_{\mathbb{R}} \mathbb{C}$ is either a field or isomorphic to $F \times F$.

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

As in Spring 2015 Problem 8, conjugation of a Sylow p-subgroup by an element $g \in G$ is another Sylow p-subgroup. If there is only one Sylow p-subgroup, then the Sylow p-subgroup is normal in G.

Let G be a group with order $616 = 2^3 \cdot 7 \cdot 11$. By Sylow's Third Theorem, the number of Sylow 11-subgroups $m_1 1$ divides 56 and is congruent to 1 modulo 11. Thus we could have $m_1 1 = 1$ or $m_1 1 = 56$. As we will show, $m_1 1 = 1$ implies the Sylow 11-subgroup is normal in G. Thus, assume $m_1 1 = 56$. Next, the number of Sylow 7-subgroups m_7 divides 88 and is congruent to 1 modulo 7. We could have $m_7 = 1, 8, 22, 88$. The argument will work for larger choices for m_7 so assume $m_7 = 8$. The intersection of a Sylow 7-subgroup and Sylow 11-subgroup must be trivial by an order consideration. Thus the Sylow subgroups chosen account for $(11 + 55(10)) + (8(6)) = 609$ elements. A Sylow 2-subgroup of G will have order 8. As a result, there can be at most one Sylow 2-subgroup. Sylow's Theorems imply the existence of a Sylow 2-subgroup so $m_j = 1$ for some $j \in \{2, 7, 11\}$. By the above argument, we conclude that G has a normal subgroup and G is not simple.

Problem 10. By one definition, a Dedekind domain is a commutative Noetherian integral domain R, integrally closed in its fraction field, such that R is not a field and every nonzero prime ideal in R is maximal. Let R be a Dedekind domain, and let S be a multiplicatively closed subset of R. Show that the localization $R[S^{-1}]$ is either the zero ring, a field, or a Dedekind domain.

If $0 \in S$, then $R[S^{-1}]$ is the zero ring. If $S = R \backslash \{0\}$, then $R[S^{-1}]$ is a field. Assume $0 \notin S$ and $S \neq S \backslash \{0\}$. It is clear that $R[S^{-1}]$ is a commutative integral domain. By Fall 2015 Problem 2(a), there is a bijective correspondence between the ideals of $\mathfrak{p} \subset R$ that intersect trivially with S and the ideals of $S^{-1}\mathfrak{p} \subset R[S^{-1}]$. Let

$$S^{-1}I_1 \subset S^{-1}I_2 \subset \dots$$

be an increasing chain of ideals in $R[S^{-1}]$. Then $I_1 \subset I_2 \subset \dots$ is an increasing chain of ideals in R for $I_j := \{r \in R : \frac{r}{1} \in S^{-1}I\}$. Since R is Noetherian, the chain terminates so $I_k = I_{k+i}$ for all $i \in \mathbb{N}$. As a result $S^{-1}I_k = S^{-1}I_{k+i}$ for all $i \in \mathbb{N}$ and the chain in $R[S^{-1}]$ terminates. We conclude that $R[S^{-1}]$ is Noetherian.

By Spring 2016 Problem 4(b), we have a correspondence between prime ideals $\mathfrak{p} \subset R$ that do not intersect S and prime ideals $S^{-1}\mathfrak{p} \subset R[S^{-1}]$. Take a chain of prime ideals

$$0 \subset S^{-1}\mathfrak{p}_1 \subset S^{-1}\mathfrak{p}_2 \subset \dots$$

which corresponds to a chain of prime ideals $0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots$ of R. Each non-zero prime ideal of R is maximal so $\mathfrak{p}_i = \mathfrak{p}_1$ for all $i \in \mathbb{N}$. Thus $S^{-1}\mathfrak{p}_i = S^{-1}\mathfrak{p}_1$ for all $i \in \mathbb{N}$. We conclude that each non-zero prime ideal of $R[S^{-1}]$ is maximal.

We will show that $R[S^{-1}]$ is integrally closed in its fraction field. Let K be the fraction field of R and $R[S^{-1}]$ is a subring of K. Let $\frac{r}{s} \in K$ be integral over $R[S^{-1}]$. If $\frac{r}{s} \in R$, then $\frac{r}{s} \in R[S^{-1}]$ so assume $\frac{r}{s} \notin R$. There is a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[S^{-1}][x]$ such that $f(\frac{r}{s}) = 0$. Each $a_i = \frac{r_i}{s_i}$ for $r_i \in R$ and $s_i \in S$. Define $t := \prod_{i=1}^{n-1} s_i \in S$ so

$$\begin{aligned} 0 &= \left(\frac{r}{s}\right)^n + \frac{r_{n-1}}{s_{n-1}}\left(\frac{r}{s}\right)^{n-1} + \dots + \frac{r_0}{s_0} \\ &= t^n\left(\frac{r}{s}\right)^n + t^n\frac{r_{n-1}}{s_{n-1}}\left(\frac{r}{s}\right)^{n-1} + \dots + t^n\frac{r_0}{s_0} \\ &= \left(\frac{tr}{s}\right)^n + \frac{tr_{n-1}}{s_{n-1}}\left(\frac{tr}{s}\right)^{n-1} + \dots + \frac{t^n r_0}{s_0}. \end{aligned}$$

Note that $\frac{t^i r_{n-i}}{s_{n-i}} \in R$ by the choice of $t \in S$. Thus $\frac{tr}{s}$ is a root of a monic polynomial in $R[x]$. Since R is integrally closed, $\frac{tr}{s} \in R$. Then $\frac{r}{s} = \frac{r'}{t} \in R[S^{-1}]$ for some $r' \in R$. We conclude that $R[S^{-1}]$ is integrally closed in K. As a result, $R[S^{-1}]$ is a Dedekind domain.

Fall 2018

Problem 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.

Let $H \subset Q_8$ be a non-trivial subgroup. If $-1 \in H$, then we are done. Otherwise, one of $\{\pm i, \pm j, \pm k\}$ is in H. But $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1 \in H$. Therefore, each 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).

Let $\phi : Q_8 \to S_7$ be an injective group homomorphism. This defines a group action of Q_8 on the set $X = \{x_1, \dots, x_7\}$ via $g \cdot x_i = x_{\phi(g)(i)}$ for $g \in Q_8$. The orbits of the action partition X so $|X| = \sum_{x \in X} |\mathrm{Orb}(x)|$. By Orbit-Stabilizer, $|\mathrm{Orb}(x)| = [Q_8 : \mathrm{Stab}(x)] = |Q_8|/|\mathrm{Stab}(x)|$ by $|Q_8|$ finite. Note $|\mathrm{Stab}(x)| \neq 1$ for all $x \in X$ since $|Q_8|/|\mathrm{Stab}(x)| = 8 > 7$, a contradiction. Thus $\mathrm{Stab}(x)$ is a non-trivial subgroup of Q_8 for all $x \in X$. By (a), $-1 \in \mathrm{Stab}(x)$ for all $x \in X$ so $\phi(-1) = e$. This contradicts the injectivity of ϕ. Therefore, there is no embedding of Q_8 into S_7.

Problem 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.

There are finite groups for which the statement does not hold. Conjugation by an element of a group is an automorphism of the group (called an inner automorphism). Thus every characteristic subgroup of a group is normal. The finite group A_5 is simple and thus contains no non-trivial characteristic subgroups. Assume G is infinite.

Let $H \subset G$ be a subgroup of index n. Then G acts on the set of left cosets $G/H = \{g_1H, g_2H, \dots, g_nH\}$ via left multiplication. This defines a group homomorphism $\phi : G \to S_n$ such that $g \cdot g_iH = g_{\phi(g)(i)}H$. Note that $g \cdot H = H$ if and only if $g \in H$. Thus $\mathrm{Stab}(H) = H$ implying a one-to-one correspondence between the index n subgroups of G and homomorphisms $\phi : G \to S_n$. Let G be finitely generated by $\{x_1, \dots, x_k\}$, say. Then the image of each x_i in S_n determine uniquely each homomorphism $\phi : G \to S_n$. There are $n!$ choices for the image of each x_i so there are finitely many homomorphisms $\phi : G \to S_n$. We conclude there are finitely many index n subgroups of G.

Let $\sigma \in \mathrm{Aut}(G)$ and $H \subset G$ be the index n subgroup in the problem statement. Now $\sigma(H)$ is a subgroup of G since σ is an automorphism. Note that the cosets are $\sigma(G)/\sigma(H) = G/\sigma(H) = \{\sigma(g_1)\sigma(H), \ldots, \sigma(g_n)\sigma(H)\}$ so $\sigma(H)$ is an index n subgroup of G. Define $N := \bigcap_{\sigma \in \mathrm{Aut}(G)} \sigma(H)$. There are finitely many index n subgroups of G so $N = \bigcap_{i=1}^{m} H_i$ for some index n subgroups $H_i \subset G$. We want to show that N is a proper characteristic subgroup of finite index in G. It is clear that N is a subgroup that is fixed under all automorphisms of G. We can define a group action of G on $\prod_{i=1}^{m} G/H_i$ by component-wise left multiplication. Then $\mathrm{Stab}(H_1, H_2, \ldots, H_m) = \bigcap_{i=1}^{m} H_i = N$ since $gH_i = H_i$ if and only if $g \in H_i$. By Orbit-Stabilizer,

$$[G : N] = [G : \mathrm{Stab}(H_1, H_2, \ldots, H_m)] = |\mathrm{Orb}(H_1, H_2, \ldots, H_m)| \leqslant |\mathrm{Orb}(H_1)| \cdots |\mathrm{Orb}(H_n)| = [G : H_1] \cdots [G : H_m].$$

Since each H_i is of finite index, $[G : N]$ is finite. Therefore, N is a characteristic subgroup of G of finite index. Note that N cannot be all of G since it is a subgroup of a H and N is not trivial since it is a finite index subgroup of an infinite group.

Problem 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 $x \in K$.

If F is a finite field, then K is also a finite field of the same characteristic. We know $K^\times$ is cyclic so $K = F(x)$ for some $x \in K$.

Assume F is not finite. Let $\alpha, \beta \in K$. By assumption, there are only a finite number of distinct fields $F(\alpha + c\beta)$ for all $c \in F$. Since F is infinite, there are $c_1, c_2 \in F$ with $c_1 \neq c_2$ such that $E := F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Thus $(c_1 - c_2)\beta \in E$ and $\beta \in E$. Further, $\alpha \in E$ and the field $F(\alpha, \beta)$ can be generated by one element. By an inductive argument, for $E = F(\alpha_1, \ldots, \alpha_n)$ there are corresponding $c_1, \ldots, c_n$ such that $E = F(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$. Since K/F is a finite field extension, $K = F(\alpha_1, \ldots, \alpha_n)$ so $K = F(x)$ for some $x \in K$.

This proof is based on that of the Primitive Element Theorem found in Lang Section 5.4.

Problem 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.

Note that $\mathrm{char}(K) = 0$ so each finite field extension is separable. Let $r, s \in \mathbb{R}$ be the two distinct real roots of f. Let $\alpha \in \mathbb{C}$ be a complex root of f so $\overline{\alpha}$ is the final root of f. Since f is irreducible, $[K[r] : K] = 4$. Case 1: Assume $s \in K[r]$. Then $f = (x - r)(x - s)h$ for $h \in (F[r])[x]$ and $\deg(h) = 2$. Note that $K[r] \subset \mathbb{R}$ but $\alpha \notin \mathbb{R}$. Thus the quadratic h is irreducible over $K[r]$. We conclude $[K[r, \alpha] : K] = [K[r, \alpha] : K[r]][K[r] : K] = 8$ where $K[r, \alpha]$ is the splitting field of f over K. Then $K[r, \alpha]/K$ is Galois and $|\mathrm{Gal}(f)| = 8$.

Case 2: Assume $s \notin K[r]$. Then $f = (x - r)g$ with $g \in (K[r])[x]$ and $\deg(g) = 3$. Since $K[r] \subset \mathbb{R}$ and $s \notin K[r]$, the cubic g is irreducible over $K[r]$. Then $[K[r, s] : K] = 12$ and $f = (x - r)(x - s)h$ for $h \in (K[r, s])[x]$ and $\deg(h) = 2$. Since $K[r, s] \subset \mathbb{R}$, the quadratic h will be irreducible over $K[r, s]$. We have $K[r, s, \alpha]$ is the splitting field of f over K so $K[r, s, \alpha]/K$ is Galois. Additionally, $[K[r, s, \alpha] : K] = |\mathrm{Gal}(K[r, s, \alpha]/K)| = 24$. The Galois group defines a group action on the set of four roots of f. Therefore, we have an injective group homomorphism $\phi : \mathrm{Gal}(K[r, s, \alpha]/K) \to S_4$. By an order argument, ϕ is surjective and $\mathrm{Gal}(K[r, s, \alpha]/K) \simeq S_4$.

Problem 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 $R \backslash S$ is a union of prime ideals.

Let $a \in R$ be a non-unit. Define the set Ω of all prime ideals $\mathfrak{p} \subset R$ such that $a \in \mathfrak{p}$. Note that Ω is non-empty since a is contained in some maximal ideal of R. Take a totally ordered subset, $\{\mathfrak{p}_i\}_{i \in I}$, of decreasing elements of Ω. We want to show that $\mathfrak{q} := \bigcap_{i \in I} \mathfrak{p}_i$ is an element of Ω. Since $a \in \mathfrak{p}_i$ for all $i \in I$, $a \in \mathfrak{q}$ so $\mathfrak{q}$ is non-empty. Let $bc \in \mathfrak{q}$ for $b, c \in R$. Then $bc \in \mathfrak{p}_i$ for all $i \in I$. If $b, c \in \mathfrak{p}_i$ for all $i \in I$, then we are done. Thus assume $c \notin \mathfrak{p}_j$ for some $j \in I$. Then $c \notin \mathfrak{p}_i$ for all $\mathfrak{p}_i \subset \mathfrak{p}_j$. Thus $b \in \mathfrak{p}_i$ for all $\mathfrak{p}_i \subset \mathfrak{p}_j$. Since the subset is totally ordered, $b \in \mathfrak{p}_i$ for all $i \in I$ and $b \in \mathfrak{q}$. By Zorn's Lemma, there exists a minimal element $\mathfrak{p} \in \Omega$ by inclusion.

Note that $R^\times \subset S$ since $1 \in S$. Let $a \in R \backslash S$, and let $\mathfrak{p}_a$ be a minimal prime ideal containing a. Assume $\mathfrak{p}_a \cap S \neq \varnothing$. Then $S^{-1}\mathfrak{p}_a \subset S^{-1}R$ is not a prime ideal of $S^{-1}R$. By the prime ideal correspondence and the minimality of $\mathfrak{p}_a$, $\frac{a}{1}$ is not contained in a prime ideal of $S^{-1}R$ so $\frac{a}{1}$ is a unit of $S^{-1}R$. Then there is some $\frac{r}{s} \in S^{-1}R$ such that $\frac{r}{s}\frac{a}{1} = \frac{1}{1}$. For $k \in S$, $k(ra) = (kr)a = s \in S$. Since S is saturated, $a \in S$, a contradiction. Therefore, $\mathfrak{p}_a \cap S = \varnothing$ and $R \backslash S \subset \bigcup_{a \in R \backslash S} \mathfrak{p}_a$. By construction, $R \backslash S \supset \bigcup_{a \in R \backslash S} \mathfrak{p}_a$ and $R \backslash S$ is a union of prime ideals.

(b) If R is a domain, show that R is a UFD if and only if every non-zero prime ideal in R contains a non-zero principal prime ideal.

($\Rightarrow$) Let $\mathfrak{p} \subset R$ be a prime ideal in a UFD R. Then for $a \in \mathfrak{p}$, we have a factorization of a into irreducible and, thus, prime elements, $a = \prod_{i=1}^{n} p_i^{k_i}$. Since $\prod_{i=1}^{n} \in \mathfrak{p}$ and $\mathfrak{p}$ is prime, $p_i \in \mathfrak{p}$ for some $1 \leqslant i \leqslant n$. Thus $(p_i) \subset \mathfrak{p}$.

($\Leftarrow$) Suppose that every non-zero prime ideal in R contains a non-zero principal prime ideal. Let S be the set of all finite products of prime elements in R. It is clear that S is mulitplicatively closed and $0 \notin S$. Further, units in R are empty products of primes so $R^\times \subset S$. We will show that S is saturated. If $a, b \in S$, then $ab \in S$ by mulitplying the two factorizations. Let $a, b \in R$ such that $ab \in S$. If both a and b are units, we are done so let a be a non-unit. Then $ab = \prod_{i=1}^{n} p_i$ for prime elements $p_i \in R$. If $n = 1$, we have $ab = p_1$ so either a or b is a unit by the irreducibility of primes. By assumption b is a unit and $a, b \in S$. Assume the statement is true for all $n < m$. Take $ab = \prod_{i=1}^{m} p_i$. Each p_i divides either a or b. First, assume some p_i divides b. Then there is some $c \in R$ such that $b = p_i c$. By renumbering the primes, $ac = \prod_{i=1}^{m-1} p_i$. The inductive hypothesis implies $a, c \in S$ and $b = p_i c \in S$. Next, if no p_i divides b, we have $(\prod_{i=1}^{m} p_i)\, x = a$ for some $x \in R$. Then $xb = 1$ and $b \in R^\times \subset S$. Similarly, x is a unit so $a \in S$. We conclude that S is saturated.

Let $a \in R$ be a non-zero non-unit. Either $(a) \cap S \neq \varnothing$ or $(a) \cap S = \varnothing$. If $(a) \cap S \neq \varnothing$, then there is some $b \in R$ such that $ab \in S$. By above, $a \in S$ so a is a product of prime elements of R. If $(a) \cap S = \varnothing$, then $(a) \subset R \backslash S$ so $(a) \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset R$ by part (a). There is a principal prime ideal $(p) \subset \mathfrak{p}$, but $(p) \subset R \backslash S$ contradicts our choice of S. Therefore, every non-zero non-unit $a \in R$ has a factorization into a finite product of prime and, thus, irreducible elements. Since an irreducible element will be a product of prime elements, it must be a product of one prime element. Irreducible elements of R are prime so R is a UFD.

Problem 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.

Since K/F is a separable field extension, trace defines a non-degenerate bilinear form on K. Thus there exists a basis $\{y_1, \ldots, y_n\}$ for K as an F-vector space such that $\mathrm{Tr}_{K/F}(x_i y_j) = \delta_{ij}$ for all i, j.

(b) If B is the integral closure of A in K, show that B is a finitely generated A-module.

Each $x_i \in L$ is algebraic over K. Thus x_i satisfies an equation $a_r x_i^r + a_{r-1} x_i^{r-1} + \cdots + a_0 = 0$ for $a_i \in A$. Multiply by a_r^{r-1} so that $a_r x_i$ is a root of a monic polynomial with coefficients in A. Since B is the integral closure of A in K, we have $a_r x_i \in B$. Let $\{u_1, \ldots, u_n\}$ be a basis for K as an F-vector space with $u_i \in B$ for $1 \leqslant i \leqslant n$.

By (a), there is a dual basis $\{v_1, \ldots, v_n\}$ for K as an F-vector space such that $\mathrm{Tr}_{K/F}(x_i y_j) = \delta_{ij}$. Let $x \in B$, then $x = \sum_{j=1}^{n} x_j v_j$ for $x_j \in K$. Since $u_i \in B$, we have $x u_i \in B$. Now $\mathrm{Tr}_{K/F}(x u_i)$ appears as a multiple of a coefficient in the minimal polynomial of $x u_i$ so $\mathrm{Tr}_{K/F}(x u_i) \in A$. Thus

$$\mathrm{Tr}_{K/F}(x u_i) = \sum_{j=1}^{n} \mathrm{Tr}_{K/F}(x_j u_i v_j) = \sum_{j=1}^{n} x_j \mathrm{Tr}_{K/F}(u_i v_j) = \sum_{j=1}^{n} x_j \delta_{ij} = x_i \in A.$$

We conclude that $B \subset \sum_{j=1}^{n} A v_j$. **WHY DOES THIS GIVE FINITELY GENERATED AS AN A-MODULE. THE Vj MIGHT NOT BE IN B**

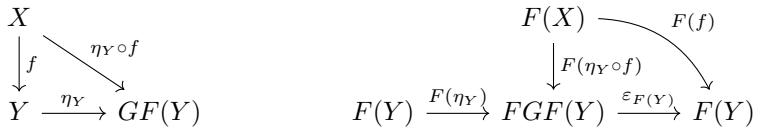
This is the proof of Proposition 5.17 in Atiyah-MacDonald.

Problem 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.

Let $\varepsilon : GF \to 1_{\mathcal{D}}$ be the counit of the adjunction. ($\Rightarrow$) Assume F is fully faithful. We will show that $\eta_Y : Y \to GF(Y)$ is an isomorphism. Let $f, g : X \to Y$ be morphisms in $\mathcal{C}$ such that $\eta_Y \circ f = \eta_Y \circ g$. By the adjunction, $\mathrm{Hom}_{\mathcal{C}}(X, GF(Y)) \simeq \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ so $\eta_Y \circ f$ and $\eta_Y \circ g$ map to the same morphism $h : F(X) \to F(Y)$. Since F is fully faithful, $F_{X,Y} : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$. Thus $f = g$ and η_Y is left cancellative. Since F is full, we have $h : GF(X) \to X$ such that $F(h) = \varepsilon_{F(X)}$ for each $X \in \mathrm{Ob}(\mathcal{C})$. Then $\varepsilon_{F(X)} \circ F(\eta_X \circ h) =$

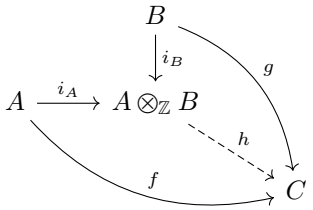
$(\eta_{F(X)} \circ F(\eta_X)) \circ F(h) = F(h) = \varepsilon_{F(X)} = \varepsilon_{F(X)} \circ F(1_X)$ for all $X \in \mathrm{Ob}(\mathcal{C})$. Note that F is faithful so $\eta_X \circ h = 1_X$ and η_X is right cancellative. We conclude η is an isomorphism.

($\Leftarrow$) Assume η is an isomorphism. Let $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$. Since η_Y is an isomorphism, $\eta_Y \circ -$ is a natural isomorphism $\mathrm{Hom}_{\mathcal{C}}(X, Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, GF(Y))$. Via the adjunction, $\varepsilon_{F(Y)} \circ F(\eta_Y \circ f) = \varepsilon_{F(Y)} \circ F(\eta_Y) \circ F(f) = F(f)$. As a result, $\mathrm{Hom}_{\mathcal{C}}(X, Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, GF(Y)) \simeq \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ via $F_{X,Y}$ and F is fully faithful.



Problem 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).

We will show that the coproduct of two commutative rings is the tensor product over $\mathbb{Z}$. Let A, B, C be commutative rings with ring homomorphisms $f : A \to C$ and $g : B \to C$. We need $h(i_A(a)) = h(a \otimes 1) = f(a)$ and $h(i_B(b)) = h(1 \otimes b) = g(b)$ for $a \in A$ and $b \in B$. Extend h to a commutative ring morphism so $h(a \otimes b) = f(a)g(b)$ for $a \otimes b \in A \otimes_{\mathbb{Z}} B$. Thus h is the unique commutative ring morphism that causes the diagram to commute.



We will now show that the tensor product over $\mathbb{Z}$ is not the coproduct in the category of rings. Let $A = B = C = M_2(\mathbb{Q})$ and take $f = g = \mathrm{id}_{M_2(\mathbb{Q})}$. Then $h : M_2(\mathbb{Q}) \otimes_{\mathbb{Z}} M_2(\mathbb{Q}) \to M_2(\mathbb{Q})$ can be defined as $h(a \otimes b) = ab$ or $h(a \otimes b) = ba$. These two ring morphisms are not equal since $M_2(\mathbb{Q})$ is not commutative. Thus $M_2(\mathbb{Q}) \otimes_{\mathbb{Z}} M_2(\mathbb{Q})$ does not satisfy the universal property of the coproduct.

Problem 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.]

Since $\mathrm{id}_M - gf : M \to M$ is invertible, there is some R-module homomorphism $c : M \to M$ such that $c(\mathrm{id}_M - gf) = \mathrm{id}_M = (\mathrm{id}_M - gf)c$. Note that $cgf = c - \mathrm{id}_M$ and $gfc = c - \mathrm{id}_M$. We claim the R-module homomorphism $\mathrm{id}_N + fcg : N \to N$ is the inverse of $\mathrm{id}_N - fg : N \to N$.

$$\begin{aligned}
(\mathrm{id}_N + fcg)(\mathrm{id}_N - fg) &= \mathrm{id}_N - fg + fcg - f(cgf)g \\
&= \mathrm{id}_N - fg + fcg - f(c - \mathrm{id}_M)g \\
&= \mathrm{id}_N - fg + fcg - fcg + fg \\
&= \mathrm{id}_N \\
(\mathrm{id}_N - fg)(\mathrm{id}_N + fcg) &= \mathrm{id}_N + fcg - fg - f(gfc)g \\
&= \mathrm{id}_N + fcg - fg - f(c - \mathrm{id}_M)g \\
&= \mathrm{id}_N + fcg - fg - fcg + g \\
&= \mathrm{id}_N.
\end{aligned}$$

Problem 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 Mobius band.)

(a) Show that there is an A-linear isomorphism $A^2 \to M \oplus M$ mapping the canonical basis to $(1 + x, y)$ and $(-y, 1 + x)$.

Let $f : A^2 \to M \oplus M$ be the A-linear homomorphism defined by $f(1,0) = (1+x, y)$ and $f(0,1) = (-y, 1+x)$. We will show that f is injective. The ideal $(X^2 + Y^2 - 1) \subset \mathbb{R}[X,Y]$ is a prime ideal since $X^2 + Y^2 - 1$ is irreducible and $\mathbb{R}[X,Y]$ is a UFD. Thus A is an integral domain, and we can embed A into its quotient field F. Let $(a,b) \in \ker(f)$ for $a, b \in A$. Then $a(1+x) - by = 0$ and $ay + b(1+x) = 0$ as elements of A. We need $a = \frac{by}{1+x} \in F$ from the first equation and, substituting into the second equation, $\frac{by^2}{1+x} + b(1+x) = 0$. Note $by^2 + b(1+x)^2 = by^2 + bx^2 + 2bx + b = 2b(x+1)$ via the relation of A so $b = 0$. Next, $a = 0$ and f is injective.

We will show that f is surjective. Note

$$f(1-x, 0) = ((1+x)(1-x), y(1-x)) = (1-x^2, y(1-x)) = (y^2, y(1-x))$$
$$f(0,y) = (-y^2, y(1+x))$$

implies $f(1-x,0) + f(0,y) = (0, 2y)$. Then $(0,y)$ is contained in the image of f. Similarly, $f(0,1-x) + f(-y,0) = (-2y, 0)$ so $(y,0)$ is contained in the image of f. Continuing,

$$f(1+x, 0) = (1 + 2x + x^2, y(1+x))$$
$$f(0,-y) = (y^2, -y(1+x)) = (1-x^2, -y(1+x))$$

and $f(1+x,0) + f(0,-y) = (2+2x, 0)$. Similarly, $f(0,1+x) + f(y,0) = (0, 2+2x)$ so $(1+x,0)$ and $(0,1+x)$ are contained in the image of f. Since M is generated by $\{1+x, y\}$ as an A-module, f is surjective.

(b) Show that there is an A-linear isomorphism $A \to M \otimes_A M$ mapping 1 to $((1+x) \otimes (1+x)) + (y \otimes y)$.

FIGURE OUT Injectivity

Let $f : A \to M \otimes_A M$ be the A-linear homomorphism defined by $f(1) = ((1+x) \otimes (1+x)) + (y \otimes y)$. A general element of $M \otimes_A M$ is of the form $(p_1(1+x) + q_1 y) \otimes (p_2(1+x) + q_2 y) = (p_1(1+x)) \otimes (p_2(1+x)) + (p_1())$. Thus $(1+x) \otimes (1+x)$, $y \otimes y$, $(1+x) \otimes y$, and $y \otimes (1+x)$ generate $M \otimes_A M$ as an A-module. Note that

$$\begin{aligned} f(y) &= y(((1+x) \otimes (1+x)) + (y \otimes y)) = (y(1+x)) \otimes (1+x) + y \otimes y^2 = y \otimes (1+x)^2 + y \otimes (1-x^2) \\ &= y \otimes (1 + 2x + x^2) + y \otimes (1-x^2) = y \otimes (2+2x) \\ f(y) &= y(((1+x) \otimes (1+x)) + (y \otimes y)) = (1+x) \otimes (y(1+x)) + y^2 \otimes y = (1+x)^2 \otimes y + (1-x^2) \otimes y \\ &= (1 + 2x + x^2) \otimes y + (1-x^2) \otimes y = (2+2x) \otimes y \end{aligned}$$

so $y \otimes (1+x)$ and $(1+x) \otimes y$ are in the image of f. Similarly,

$$\begin{aligned} f(1-x) &= ((1-x)(1+x)) \otimes (1+x) + y \otimes (1-x)y = y^2 \otimes (1+x) + y \otimes (1-x)y \\ &= y \otimes (y + xy) + y \otimes (y - xy) = y \otimes (2y) \end{aligned}$$

implies $y \otimes y$ and, consequently, $f(1) - y \otimes y = (1+x) \otimes (1+x)$ are contained in image of f. We conclude that f is surjective.

Problem 11. Let G be a finite group, ω be a primitive 3rd root of 1 in $\mathbb{C}$ and suppose that the complex character table 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.

Note that the number of columns, four, determines the number of conjugacy classes of G and the number of isomorphism classes of irreducible representations. The first row of the character table corresponds to the trivial representation. Let $\rho : G \to \mathbb{C}$ be the one-dimensional representation described in the row given. Then we can construct a one-dimensional representation $\rho \otimes \rho : G \times G \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \simeq \mathbb{C}$. By including G in $G \times G$ via the diagonal homomorphism, we find $\rho \otimes \rho$ describes a one-dimensional representation with $\chi_{\rho\otimes\rho}(g) = \chi_\rho(g)^2$. Since the characters $\chi_{\rho\otimes\rho}$ differ from the current rows, $\rho \otimes \rho$ describes a distinct isomorphism class of one-dimensional representations.

By orthogonality of the second/third column and the first column, we find the zeros in the fourth row. Let $a := \chi_\mu(e)$ and $b := \chi_\mu(g)$ for $g \in C_4$. Then $ab = -3$ by the orthogonality of columns one and four. Since a represents the dimension of the irreducible representation $\mu : G \to M_a(\mathbb{C})$, $a > 0$ is an integer so $b \in \mathbb{Q}$. With $|G|$

finite, the trace of $\mu(g)$ is the sum of eigenvalues that are all roots of unity. Thus $b \in \mathbb{Q}$ is an algebraic integer so $b \in \mathbb{Z}$. We conclude that $a = 1$ and $b = -3$ or $a = 3$ and $b = -1$. If $a = 1$, then $|G| = 4$. The order of some $g \in C_2$ must be divisible by 3 since $\rho(g^3) = \rho(g)^3 = 1$. This contradicts the order of G so $a \neq 1$. Thus $a = 3$ and $b = -1$.

As a result, $|G| = 1^2 + 1^2 + 1^2 + 3^2 = 12$. The rows are orthonormal under the inner product $\langle v, w \rangle = \frac{1}{|G|} \sum_{i=1}^{4} |C_i| v_i \overline{w_i}$. Row three implies $1 = \frac{9+|C_4|}{12}$ and $|C_4| = 3$. The inner product of rows two and one gives $0 = \frac{1+|C_2|\omega+|C_3|\omega^2+3}{12}$. Similarly, the inner product of rows three and one gives $0 = \frac{1+|C_2|\omega^2+|C_3|\omega+3}{12}$. Thus $|C_2| = |C_3|$ with 8 elements between the two conjugacy classes. We conclude $|C_2| = |C_3| = 4$.

	$C_1 = \{e\}$	C_2	C_3	C_4
χ_{trivial}	1	1	1	1
χ_ρ	1	ω	ω^2	1
$\chi_{\rho\otimes\rho}$	1	ω^2	ω	1
χ_μ	3	0	0	-1

Problem 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.

Let L/F be an algebraic extension. Then for each $\alpha \in L$, we have a finite extension $F[\alpha]/F$. Then $F[\alpha]$ is the finite field of order q for q some power of a prime. Then $(F[\alpha])^\times$ is cyclic of order $q-1$. Thus $K[\alpha]$ is a subfield of K for each $\alpha \in L$ so L is a subfield of K. We conclude that K is the algebraic closure of F. By Artin-Wedderburn, a simple finite dimensional K-algebra A is a matrix algebras with coefficients in division rings over K. However, if $\dim_K(D)$ is finite, we must have $D \subset K$ by K algebraically closed. Thus $A \simeq M_n(K)$ for some integer $n \geqslant 1$.

Spring 2019

Problem 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.

https://math.stackexchange.com/questions/4051604/
given-a-finite-solvable-group-g-prove-that-a-minimal-normal-subgroup-h-is-a

Since G is solvable, N is solvable as well. The derived series of N will eventually reach the trivial subgroup which implies that $[N, N]$ is not all of N. Every characteristic subgroup of a normal subgroup of G is normal in G (**PROVE THIS**). Thus $[N, N]$ is normal in G. By assumption, N is minimal normal in G so $[N, N]$ is the trivial subgroup of G. We find that N is abelian.

For a prime p dividing the order of N, Cauchy's Theorem implies that N has an element of order p. Since N is abelian, the subgroup $\{n \in N : n^p = 1\}$ is a non-trivial characteristic subgroup of N. Every characteristic subgroup of a normal subgroup of G is normal in G so $N = \{n \in N : n^p = 1\}$. The classification of finite abelian groups proves that N is cyclic of order p or a direct sum of cyclic order p groups.

Problem 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 $B \to Q$.

https://planetmath.org/ExampleOfInjectiveModule

Problem 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.

Define the norm $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{Z}_{\geqslant 0}$ as $N(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2 d$. We can show algebraically that the norm is multiplicative. Further, we will show $N(a + b\sqrt{-d}) = 1$ if and only if $a + b\sqrt{-d}$ is a unit in $\mathbb{Z}[\sqrt{-1}]$. ($\Rightarrow$) Assume $N(a + b\sqrt{-d}) = 1$. Then $(a + b\sqrt{-d})(a - b\sqrt{-d}) = 1$ and $a + b\sqrt{-d}$ is a unit. ($\Leftarrow$) Assume $a + b\sqrt{-d}$ is a unit. Then there is some element $a' + b'\sqrt{-d}$ for which $(a + b\sqrt{-d})(a' + b'\sqrt{-d}) = 1$. By multiplicativity of the norm, $N(a + b\sqrt{-d})$ divides $N(1) = 1$. We conclude that $N(a + b\sqrt{-d}) = 1$.

We will first show that 2 is irreducible in $\mathbb{Z}[\sqrt{-d}]$. Let $a+b\sqrt{-d}$ be a non-unit factor of 2. Then $N(a+b\sqrt{-d}) = a^2 + b^2 d$ divides $N(2) = 4$. If $N(a + b\sqrt{-d}) = 1$ or $N(a + b\sqrt{-d}) = 4$, the factorization of 2 includes a unit. Thus $N(a + b\sqrt{-d}) = 2$ or $a^2 + b^2 d = 2$. Since $d > 2$, we must have $b = 0$. Then $a^2 = 2$ for integer a, which is not possible. No such non-trivial factor of 2 exists.

We will now show that (2) is not prime in $\mathbb{Z}[\sqrt{-d}]$. If d is even, 2 divides $-d$ but 2 does not divide either factor in $-d = \sqrt{-d}\sqrt{-d}$. If d is odd, 2 divides $1 + d$ but 2 does not divide either factor of $1 + d = (1 + \sqrt{-d})(1 - \sqrt{-d})$. Thus (2) is not a prime ideal. Note that this argument proves that $\mathbb{Z}[\sqrt{-d}]$ is not a UFD since irreducible and prime are equivalent notions in a UFD.

Problem 4. Let R be a commutative local ring and P a finitely generated projective R-module. Prove that P is R-free.

DO THIS ONE

Problem 5. Let Φ_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 $p|\Phi_n(a)$ in $\mathbb{Z}$,then $p \equiv 1 \bmod n$.

Problem 6. Let F be a field of characteristic $p > 0$ and $a \in F^\times$. Prove that if the polynomial $f = X^p - a$ has no root in F, then f is irreducible over F.

Problem 7. Let F be a field and let R be the ring of 3×3 matrices over F with (3,1) and (3,2) entry equal to 0. Thus,

$$R = \begin{pmatrix} F & F & F \\ F & F & F \\ 0 & 0 & F \end{pmatrix}.$$

(a) Determine the Jacobson radical J of R.

(b) Is J a minimal left (respectively right) minimal ideal?

Problem 8. Prove that every finite group of order n is isomorphic to a subgroup of $\mathrm{GL}_{n-1}(\mathbb{C})$.

By Cayley's Theorem, there is an injective homomorphism from G to S_n. There is an injective homomorphism S_n to $\mathrm{GL}_n(\mathbb{C})$ given by permuting the elements of $\mathbb{C}^n$ once a basis has been chosen. Let $v \in \mathbb{C}^n$ be the vector of all 1s, which is an eigenvector for each permutation matrix. Each permutation matrix in the basis $\beta = \{v, e_2, \ldots, e_n\}$ for $\mathbb{C}^n$ will be a block matrix of (1) and a permutation matrix in $\mathrm{GL}_{n-1}(\mathbb{C})$. Thus there is an injective homomorphism of S_n to $\mathrm{GL}_{n-1}(\mathbb{C})$. Compose this with the injection from Cayley's Theorem to prove the claim.

Problem 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 $aR + bR \neq R$.

DO THIS ONE

Problem 10. Let $\mathcal{C}$ be an abelian category. Prove TFAE:

(1) Every object of $\mathcal{C}$ is projective.

(2) Every object of $\mathcal{C}$ is injective.

(1) $\Rightarrow$ (2): Assume that every object is projective. Let $m : X \to Y$ be a monomorphism for which there is a morphism $g : X \to Q$. We can build the short exact sequence

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{q} C \longrightarrow 0$$

where $C = \text{coker}(m)$. By assumption, C is projective so the short exact sequence splits. In an abelian category left and right split are equivalent so there is a morphism $s : Y \to X$ such that $s \circ m = 1_X$. Define $h = g \circ s$ and $h \circ m = (g \circ s) \circ m = g \circ (s \circ m) = g$. Thus Q is injective.

(1) $\Leftarrow$ (2): Similar argument.

Fall 2019

Problem 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?

How do we show that there is only one Sylow 5-subgroup?

Assume that there is a normal Sylow 5-subgroup denoted P_5. Let H be the product of a Sylow 3-subgroup and Sylow 7-subgroup of G. By order considerations, the intersection of any Sylow 3-subgroup and Sylow 7-subgroup is trivial so $|H| = 63$. Similarly, $|P_5 \cap H| = 1$ and $G = P_5H$. With P_5 normal in G, we have $G \simeq P_5 \rtimes_\psi H$. Since 5 is prime, P_5 is cyclic and $\text{Aut}(P_5) \simeq \mathbb{Z}/4\mathbb{Z}$. The image of any $h \in H$ via $\psi : H \to \text{Aut}(P_5)$ is trivial since its order must divide 63 and 4. We conclude that $G \simeq P_5 \times H$.

We would like to classify all groups H of order 63. By Sylow's Third Theorem, the number of distinct Sylow 7-subgroups in H satisfies $n_7 \equiv 1 \pmod 7$ and $n_7|9$. Thus $n_7 = 1$ and there is a unique normal Sylow 7-subgroup denoted P_7. Let P_3 be some Sylow 3-subgroup of H. By order considerations, $|P_3 \cap P_7| = 1$ so $|H| = |P_3P_7|$ and $H = P_3P_7$. Since P_7 is normal in H, $H \simeq P_7 \rtimes_\varphi P_3$. Again by Sylow's Third Theorem, the number of distinct Sylow 3-subgroups in H satisfies $n_3 \equiv 1 \pmod 3$ and $n_3|7$ so $n_3 = 1$ or $n_3 = 7$.

Case 1: If $n_3 = 1$, then $H \simeq P_7 \times P_3$. Note that 7 is prime so $P_7 \simeq \mathbb{Z}/7\mathbb{Z}$ is cyclic of order 7. Further, $P_3 \simeq \mathbb{Z}/9\mathbb{Z}$ or $P_3 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. There are 2 isomorphism classes.

Case 2: If $n_3 = 7$, then $\varphi : P_3 \to \text{Aut}(P_7)$ is non-trivial. Since P_7 is cyclic of order 7, $\text{Aut}(P_7) \simeq \mathbb{Z}/6\mathbb{Z}$. Then the image of φ is the unique order 3 subgroup of $\text{Aut}(P_7)$. There are 2 isomorphism classes.

We conclude that $G \simeq P_5 \times (P_7 \rtimes P_3)$. There are 4 isomorphism classes.

Problem 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 in $\overline{K}$. 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.

Problem 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

$$V(I) = \{(a, b, c) \in \mathbb{C}^3 : f(a, b, c) = 0 \text{ for all } f \in I\}.$$

By ideal correspondence, the maximal ideals of R/I are in bijection with the ideals of R containing I. Hilbert Nullstellensatz reveals that the maximal ideals of R are of the form $(x - a, y - b, z - c)$ for $a, b, c \in \mathbb{C}$. Let $\mathfrak{m}$ be a maximal ideal. Since $\mathfrak{m}$ contains z^3, it must contain z. We reduce the other relations to $x^2 - y^2$ and $(xy + 1)^2$. If $\mathfrak{m}$ contains $x^2 - y^2$, then it contains either $x - y$ or $x + y$. If $\mathfrak{m}$ contains $(xy + 1)^2$, then it contains $xy + 1$. Case 1: Assume $\mathfrak{m}$ contains $x - y$. Multiply by $-y$ to obtain $-xy + y^2$ in $\mathfrak{m}$. Then $y^2 + 1$ is in $\mathfrak{m}$ so either $y + i$ or $y - i$ is in $\mathfrak{m}$. Case 2: Assume $\mathfrak{m}$ contains $x + y$. Then $-xy - y^2$ is in $\mathfrak{m}$ and so is $1 - y^2$. Thus either $y + 1$ or $y - 1$ is in $\mathfrak{m}$. The maximal ideals of R containing I are $(x - 1, y + 1, z)$, $(x + 1, y - 1, z)$, $(x - i, y - i, z)$, and $(x + i, y + i, z)$ which correspond to the points $(1, -1, 0)$, $(-1, 1, 0)$, $(i, i, 0)$, and $(-i, -i, 0)$ in the variety.

Problem 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 $n \geqslant 1$.

DO THIS ONE

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

See Spring 2017 Problem 1.

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

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

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

The final relation of G implies that $gh = h^2g$ and $gh^2 = hg$. We can use these relations to write every element of G as g^ih^j for $0 \leqslant i \leqslant 3$ and $0 \leqslant j \leqslant 2$. Further, we have the relations $h^2g^3 = g^3h$ and $hg^3 = g^3h^2$ by inverting the above relations. Clearly, $C_1 = \{e\}$ is a conjugacy class. The relations

$$\begin{aligned} ghg^{-1} &= ghg^3 = h^2 \\ gh^2g^{-1} &= gh^2g^3 = h \end{aligned}$$

show that $C_2 = \{h, h^2\}$ is a conjugacy class. We find

$$\begin{aligned} hgh^{-1} &= hgh^2 = gh \\ h(gh)h^{-1} &= gh^2 \\ g(gh)g^{-1} &= g^2hg^3 = gh^2 \\ h(gh^2)h^{-1} &= hgh = g \\ g(gh^2)g^{-1} &= g^2h^2g^3 = gh \end{aligned}$$

so $C_3 = \{g, gh, gh^2\}$ is a conjugacy class. By similar computation, we have conjugacy class $C_4 = \{g^3, g^3h, g^3h^2\}$. The equations

$$\begin{aligned} hg^2h^{-1} &= hg^2h^2 = gh^2gh^2 = g^2 \\ h(g^2h)h^{-1} &= hg^2 = gh^2g = g^2h \\ g(g^2h)g^{-1} &= g^3hg^3 = g^2h^2 \\ h(g^2h^2)h^{-1} &= hg^2h = gh^2gh = g^2h^2 \\ g(g^2h^2)g^{-1} &= g^3h^2g^3 = g^2h \end{aligned}$$

prove that $C_5 = \{g^2\}$ and $C_6 = \{g^2h, g^2h^2\}$ are conjugacy classes. All elements of G have been placed in conjugacy classes.

The commutator $[G, G]$ has elements of the form $ghg^{-1}h^{-1} = ghg^3h^2 = h$. Thus $\langle h \rangle \subset [G, G]$. We see that $G/\langle h \rangle$ is cyclic of order 4 and, thus, abelian. We conclude $[G, G] = \langle h \rangle$ and there are $|G/[G, G]| = 4$ one-dimensional non-isomorphic irreducible representations of G. Each one-dimensional $\rho_i : G \to \mathbb{C}^\times$ sends h to 1. The image of g must be a fourth root of unity. Further, $12 = 4 + a^2 + b^2$ for a and b the dimensions of the other irreducible representations of G. We see that $a < 3$ and $b < 3$ so $a = b = 2$ so we obtain the following character table.

	e	h	g	g^2	g^3	g^2h
χ_1	1	1	1	1	1	1
χ_2	1	1	i	-1	$-i$	-1
χ_3	1	1	-1	1	-1	1
χ_4	1	1	$-i$	-1	i	-1
χ_5	2					
χ_6	2					

We will construct a two-dimensional irreducible representation of G over $\mathbb{C}$. Define a set map μ on the generators

$$\mu(g) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$\mu(h) = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}}. \end{pmatrix}$$

Then the image of g has order 4 in $\mathrm{GL}_2(\mathbb{C})$ and the image of h has order 3 in $\mathrm{GL}_2(\mathbb{C})$. Further,

$$\begin{aligned} \mu(ghg^{-1}) &= \mu(g)\mu(h)\mu(g)^{-1} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} e^{\frac{4\pi i}{3}} & 0 \\ 0 & e^{\frac{2\pi i}{3}} \end{pmatrix} \\ &= \mu(h)^{-1} \end{aligned}$$

so $\mu : G \to \mathrm{GL}_2(G)$ is a group homomorphism as desired. There is no non-trivial, proper G-invariant subspace of $\mathbb{C}^2$ which proves μ is irreducible. Compute the characters χ_5 by taking the traces of the relevant matrices. We can complete the final row of the character table by column orthogonality of column j with column 1.

	e	h	g	g^2	g^3	g^2h
χ_1	1	1	1	1	1	1
χ_2	1	1	i	-1	$-i$	-1
χ_3	1	1	-1	1	-1	1
χ_4	1	1	$-i$	-1	i	-1
χ_5	2	-1	0	-2	0	1
χ_6	2	-1	0	2	0	-1

Problem 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 $R[1/u]$.

DO THIS ONE

Problem 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.

Problem 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.

Spring 2020

Problem 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.

Problem 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 $A \otimes_{\mathbb{Z}[G]} B \simeq G$ as groups if and only if G is a cyclic group.

Problem 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.

DO THIS ONE

Problem 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 $\mathbb{R}$?

DO THIS ONE

Problem 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 $\mathbb{Q}$.

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

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

Let G be a nontrivial p-group, and P the set of order-p elements of N. We have seen that P is non-empty, and indeed that $|P|$ is congruent to -1 mod p. Now consider the action of G on P by conjugation. The stabilizer under this action of any x in P is the centralizer $C(x)$ of x, which is the subgroup of G consisting of all elements that commute with x. The orbit of x then has size $[G : C(x)]$. But G is a p-group, so $[G : C(x)]$ is a power of p. Hence $[G : C(x)]$ is either 1 or a multiple of p. Since $|P|$ is not a multiple of p, it follows that at least one of the orbits is a singleton. Then $C(x) = G$, which is to say that x commutes with every element of G. We have thus found a nontrivial element x of the center of G.

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

Take $G = D_4$, the dihedral group of order 8. Let $N = \langle r \rangle$ be the cyclic subgroup of G generated by rotation by $\frac{\pi}{2}$ counter-clockwise. Then $Z(N) = N$ but $Z(G) = \langle r^2 \rangle$.

Problem 8. Let R be a ring.

(a) Show that an R-module X is indecomposable if $\mathrm{End}_R(X)$ is local. (Recall that a ring is local if the sum of non-invertible elements remains non-invertible).

DO THIS ONE

(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: If $X_1 \oplus \cdots \oplus X_m \simeq Y_1 \oplus \cdots \oplus Y_n$ then $m = n$ and there is a bijection $\sigma \in S_n$ and isomorphisms $X_i \simeq Y_{\sigma(i)}$.

DO THIS ONE

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

DO THIS ONE

Problem 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.

DO THIS ONE

(b) Show that this fails if M is not finitely generated.

DO THIS ONE

Fall 2020

Problem 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.

We will first prove that G is not simple. Let n_p be the number of distinct Sylow p-subgroups, n_q be the number of distinct Sylow q-subgroups, and n_r be the number of distinct Sylow r-subgroups. By Sylow's Third Theorem, we know the following

$$\begin{aligned} n_p &\equiv 1 \pmod{p},\ n_p | qr \\ n_q &\equiv 1 \pmod{q},\ n_q | pr \\ n_r &\equiv 1 \pmod{r},\ n_r | pq. \end{aligned}$$

We conclude that $n_r = 1, p, q, pq$. Since $r > p$ and $r > q$, p and q can't be congruent to 1 modulo r. Thus $n_r = 1$ or $n_r = pq$. If $n_r = 1$, we're done so assume $n_r = pq$. Every Sylow r-subgroup contains the identity and $r-1$ order r elements of G. Thus there are $pq(r-1) = pqr - pq$ order r elements of G. Similarly, $n_q = 1, p, r, pr$. Since $q > p$, p can't be congruent to 1 modulo q. If $n_q = 1$, we're done so assume that $n_q = r$, the smallest other possibility. As above, there are $r(q-1) = rq - r$ elements of order q in G. We have $n_p = 1, q, r, qr$ so assume that $n_p = q$. Then there are $q(p-1) = pq - q$ elements of order p in G. In total this accounts for

$$(pqr - pq) + (rq - r) + (pq - q) + 1 = pqr + rq - r - q + 1$$

elements of G. Since r and q are greater than 1, $rq \geqslant r + q$ and this exceeds the order of G. Thus there is some normal Sylow subgroup and G is not simple.

Let N be a normal Sylow subgroup of G. If $|N| = r$, we are done so assume $|N| = q$ without loss of generality. Then G/N is a group of order pr, which implies that G/N has a normal subgroup of order r. By the subgroup correspondence, there is a normal subgroup H of G containing N for which H/N is order r. Thus $|H| = qr$ and H contains a normal subgroup of order r denoted P_r. We want to prove that P_r is normal in G. Let $g \in G$. Then $|gP_rg^{-1}| = r$ and $gP_rg^{-1} \subset H$ since H is normal in G. Since P_r is a normal Sylow r-subgroup of H, P_r is the unique Sylow r-subgroup of H. We conclude that $gP_rg^{-1} = P_r$ and P_r is normal in G.

Problem 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.

Let G be a group of order 231 with P_3 a Sylow 3-subgroup, P_7 a Sylow 7-subgroup, and P_{11} a Sylow 11-subgroup. Since $|P_i \cap P_j| = 1$ for distinct i and j in $\{3, 7, 11\}$, we conclude that $|G| = |P_3P_7P_{11}|$ and $G = P_3P_7P_{11}$. By Fall 2020 Problem 1, P_{11} is normal in G. Let n_7 be the number of distinct Sylow 7-subgroups in G. Sylow's Third Theorem proves that $n_7 \equiv 1 \pmod 7$ and $n_7 | 33$. The only option is $n_7 = 1$ and P_7 is normal in G. Thus the cyclic subgroup P_7P_{11} of order 77 is normal in G and $G \simeq P_7P_{11} \rtimes_\varphi P_3$. We have $\mathrm{Aut}(P_7P_{11}) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and P_3 cyclic of order 3. Therefore, $\varphi : P_3 \to \mathrm{Aut}(P_7P_{11})$ is either trivial or sends a generator of P_3 to an order 3 element of $\mathbb{Z}/6\mathbb{Z}$. The cases of the latter produce isomorphic semidirect products so there are only two groups of order 231 up to isomorphism.

Problem 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.

Problem 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-homomorphisms $f_i : M \to R$ for each $i \in I$ such that the sets $\{m_i : i \in I\}$ and $\{f_i : i \in I\}$ 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 $m = \sum_{i \in I} f_i(m) m_i$.

DO THIS ONE

Problem 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: $F = \mathbb{Q}, \mathbb{F}_5, \mathbb{F}_7$.

Problem 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 $\mathrm{Gal}(L/K_1)$.

Problem 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.

DO THIS ONE

(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 $I + xJ = R$.

DO THIS ONE

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

DO THIS ONE

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