UCLA Algebra Qualifying Exam Solutions

Ian Coley

August 25, 2014

1 Spring 2014

Problem 1.
Let $L : \mathcal{C} \to \mathcal{D}$ be a functor, left adjoint to $R : \mathcal{D} \to \mathcal{C}$. Show that if the counit $L \circ R \to \mathrm{id}_{\mathcal{D}}$ is a natural isomorphism, then R is fully faithful.

Solution.
R is fully faithful if for every objects X, Y in $\mathcal{D}$, we have $\mathrm{Mor}_{\mathcal{D}}(X, Y) \cong \mathrm{Mor}_{\mathcal{C}}(R(X), R(Y))$. Recall further that L and R being left and right adjoints means that, for every object A in $\mathcal{C}$ and B in $\mathcal{D}$, we have

$$\mathrm{Mor}_{\mathcal{C}}(A, R(B)) \cong \mathrm{Mor}_{\mathcal{D}}(L(A), B).$$

As such, we see, again with X, Y in $\mathcal{D}$,

$$\mathrm{Mor}_{\mathcal{C}}(R(X), R(Y)) = \mathrm{Mor}_{\mathcal{D}}(L \circ R(X), Y) = \mathrm{Mor}_{\mathcal{D}}(X, Y),$$

as required. □

Problem 2.
Let A be a central division algebra (of finite dimension) over a field k. Let $[A, A]$ be the k-subspace of A spanned by the elements $ab - ba$ with $a, b \in A$. Show that $[A, A] \neq A$.

Solution.
Let K be the algebraic closure of k, and consider $B = A \otimes_k K$. Then $B \cong M_n(K)$ for some $n \in \mathbb{N}$, and thus we can understand $[B, B] \cong [A, A] \otimes_k K$. In this case, $[B, B]$ contains only matrices of trace 0, since it is clear that $\mathrm{tr}(XY - YX) = 0$ for every $X, Y \in B$. Therefore $[B, B] \neq B$. As such, we could not have had $[A, A] = A$. □

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

Solution.
We use the following characterisation of the Jacobson radical: $J(R) = \{x \in R : xy - 1 \in$

$R^\times$ for all $y \in R\}$. As such, let $x \in J(A)$. Then consider $\varphi(x)b - 1$ for any $b \in B$. Since φ is surjective, we have $b = \varphi(y)$ for some $y \in A$. Hence we have

$$\varphi(x)b - 1 = \varphi(x)\varphi(y) - 1 = \varphi(xy - 1).$$

Since $xy-1$ is invertible by assumption, $\varphi(xy-1)$ is also invertible, with inverse $\varphi((xy-1)^{-1})$. Therefore $\varphi(x) \in J(B)$, and we are done. □

Problem 4.
Let G be a group and H a normal subgroup of G. Let k be a field and let V be an irreducible representation of G over k. Show that the restriction of V to H is semisimple.

Solution.
This is known as Clifford's theorem, if we assume that V is a finite-dimensional representation (which we do here). The following proof is (crudely) taken from Wikipedia, but a better source likely exists.

Let V_H be the restriction of V to H, and let $U \subset V_H$ be an irreducible $k[H]$-module. For each $g \in G$, $g \cdot U$ is an irreducible $k[H]$-module of V_H. Further, $\sum_{g\in G} g \cdot U$ is a nontrivial $k[G]$-submodule of V, so must be V itself by irreducibility. Therefore $\sum_{g\in G} g \cdot U = V_H$, so V_H is a sum of irreducible submodules. This is one of the equivalent characteristics of a semisimple module, so we are done. □

Problem 5.
Let G be a finite group acting transitively on a finite set X. Let $x \in X$ and let P be a Sylow p-subgroup of the stabiliser of x in G. Show that $N_G(P)$ acts transitively on X^P.

Solution.
Recall that any transitive G-action is G-isomorphic to the action of G by left multiplication on G/H for some subgroup H. As such, we can solve the problem in these terms. First, we need to get a handle on what G_x, the stabiliser of the coset $xH \in G/H$, is. We have

$$\begin{aligned} G_x &= \{g \in G : gxH = xH\} = \{g \in G : x^{-1}gxH = H\} \\ &= \{g \in G : x^{-1}gx \in H\} = \{g \in G : g \in xHx^{-1}\} = xHx^{-1}. \end{aligned}$$

Hence P is a Sylow p-subgroup of xHx^{-1}. Further, X^P is given by

$$\begin{aligned} X^P &= \{yH \in G/H : pyH = yH \text{ for all } p \in P\} = \{xH \in G/H : y^{-1}pyH = H \text{ for all } p\} \\ &= \{yH \in G/H : y^{-1}py \in H \text{ for all } p\} = \{yH \in G/H : p \in yHy^{-1} \text{ for all } p\} \\ &= \{yH \in G/H : P \subset yHy^{-1}\}. \end{aligned}$$

In particular, we see that $xH \in X^P$. We will show that, for any coset $yH \in X^P$, there exists $p \in P$ so that $pxH = yH$, which will prove transitivity. Indeed, since we have $P \subset xHx^{-1}$ and $P \subset yHy^{-1}$, we have $x^{-1}Px, y^{-1}Py \subset H$. These are two Sylow p-subgroups of H, so they are conjugate by some $h \in H$. Hence

$$hx^{-1}Pxh^{-1} = y^{-1}Py \implies yhx^{-1}Pxh^{-1}y^{-1} = P \implies yhx^{-1} \in N_G(P).$$

This is the required element, as

$$yhx^{-1} \cdot xH = yh \cdot H = yH.$$

Hence the action of $N_G(H)$ is transitive. □

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

Solution.
This question has been asked in various forms time and time again. See, for example, Fall 2013 #9, whose argument boils down to this statement. □

Problem 7.
Let G be a finite group and let $s, t \in G$ be two distinct elements of order 2. Show that the subgroup of G generated by s and t is a dihedral group. (Recall that the dihedral groups are the groups $D_{2m} = \langle g, h : g^2 = h^2 = (gh)^m = 1 \rangle$ for some $m \geq 2$.)

Solution.
The definition given here is by no means standard, and makes the problem fairly trivial. First, let H denote the subgroup in question. We know that $|st| = n < \infty$ for some $n \in \mathbb{N}$ since G is finite. Moreover, because $|s| = 2$, $s^{-1} = s$, so in particular $s^{-1} \neq t$ so $st \neq 1$. Therefore $n \geq 2$, which gives a surjection $f : H \to D_{2n}$, where $f(s) = g, f(t) = h$. We need only show it is injective. Note that $|ts| = |st|$ since

$$t = t(st)^n = (ts)^n t \implies 1 = (ts)^n$$

and if $|ts| < n$ we would have a contradiction by the same reasoning. Thus without loss of generality assume $(st)^k s \in \ker f$ for $k < n$. Then we have

$$f((st)^k s) \cdot f(s) = f((st)^k) = g \implies f((st)^{2k}) = 1.$$

Additionally,

$$f((st)^k s) \cdot f(t) = f((st)^{k+1}) = h \implies f((st)^{2k+2}) = 1.$$

This implies that $f((st)^2) = 1$. Therefore since $(st)^k s \in \ker f$ as well, this implies that either sts or s is in $\ker f$, depending on the parity of k. The second case is impossible. For the first case, this implies that

$$ghgh = f(stst) = f(t) = h,$$

which is also a contradiction. Therefore f is injective as well, and we are done. □

Problem 8.
Let F be a finite field. Without using any of the theorems on finite fields, show that F has a field extension of degree 2.

Solution.
It suffices to construct an irreducible quadratic polynomial. If f is such a polynomial, then $F[X]/(f)$ is a priori a 2-dimensional algebra over F. Since $F[X]$ is a PID, any irreducible element is prime, and any (nonzero) prime ideal is maximal. Hence $F[X]/(f)$ is a field of degree 2 over F.

Now, let $S = \{X^2 + aX + b : a, b \in F\}$, the set of all monic quadratic polynomials in $F[X]$. Further, let $T = \{(X - a)(X - b) : a, b \in F\}$, the set of reducible monic quadratic

polynomials. We use the fact that a quadratic polynomial is reducible over F if and only if it has a root in F. Clearly $T \subset S$. By direct calculation, if $|F| = q$, then $|S| = q^2$ and $|T| = \binom{q}{2} + q$, which correspond to when $a \neq b$ and $a = b$, respectively. Hence $|S| > |T|$ for any $q > 1$, so there are more monic quadratic polynomials than reducible ones, whence one must be irreducible. This completes the proof. □

Problem 9.
Let G be a finite group. Show that there exist fields $F \subset E$ such that E/F is Galois with group G.

Solution.
There is a usual way of performing this construction. Let $|G| = n$. Let $E = \mathbb{C}(X_1, \ldots, X_n)$, the field of rational functions in n variables. Let $k = \mathbb{C}(s_1, \ldots, s_n)$, the subfield generated by the symmetric polynomials, which are defined by

$$s_k = \sum_{1 \leq j_1 < \cdots < j_k \leq n} X_{j_1} \cdots X_{j_k}.$$

E/F is separable since $\operatorname{char} k = 0$. We need only show that it is a (finite) normal extension. But this is clear, since E is the splitting field of

$$g(Y) = \prod_{i=1}^{n} (Y - X_i) \in k[Y],$$

whose coefficients are easily seen to lie in k because of the inherent symmetry of $g(Y)$. Therefore E/k is Galois, and by construction has $\operatorname{Gal}(E/k) = S_n$. We have a canonical embedding of G into S_n by the group action of G on itself by left multiplication. Let $H \subset S_n$ be the image of that embedding. By Galois correspondence, there exists an intermediate field F so that $\operatorname{Gal}(E/F) = H$. Since $H \cong G$, we are done. □

Problem 10.
Let F be a field. Show that the polynomial ring $F[X]$ has infinitely many prime ideals. Also prove that algebraically closed fields are infinite.

Solution.
Since $F[X]$ is a PID, we need to show that there are infinitely many irreducible polynomials in the polynomial ring of a field. If F itself were infinite, then the set of polynomials $\{X - \alpha : \alpha \in F\}$ is infinite, and all of these are irreducible since they are monic of degree 1.

If F is finite, then let $|F| = q = p^n$. Then we may consider the field extensions $\mathbb{F}_{q^k}/F$ for each $k \in \mathbb{N}$. These are finite separable extensions, so they are simple, so let $\mathbb{F}_{q^k} = F(\alpha_k)$. Then the (irreducible) minimal polynomial of α_k over F is of degree k. Hence there are infinitely many irreducible polynomials over a finite field as well.

Let K be an algebraically closed field. Let $F \subset K$ be its prime field. In particular, K contains (an embedded copy of) the algebraic closure of F, so K contains (an embedded copy of) the roots of every irreducible polynomial in $F[X]$. By the above, there are infinitely many such polynomials, so there are infinitely many distinct roots. Hence K is infinite. □

2 Fall 2013

Problem 1.
How many groups are there up to isomorphism of order pq where $p < q$ are prime integers?

Solution.
Let n_q denote the number of Sylow q-subgroups (and respectively n_p). Then by the Sylow theorems, $n_q \mid p$ and $n_q \equiv 1 \mod q$. since $q + 1 > p$, we must have $n_q = 1$, so every group G with $|G| = pq$ has a normal Sylow q-subgroup, which we denote $Q \triangleleft G$. Now for the p-subgroups of G, by the Sylow theorems, $n_p \mid q$ and $n_p \equiv 1 \mod p$. Since $n_p \mid q$, we have $n_p = 1$ or q. We always have $1 \equiv 1 \mod p$, but we do not always have $q \equiv 1 \mod p$.

Let P be a Sylow p-subgroup of G. Since P and Q have coprime orders, they have trivial intersection. Hence

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = pq.$$

which implies that $G = Q \rtimes_\varphi P$, for some map $\varphi : P \to \operatorname{Aut} Q$. Since $P \cong \mathbb{Z}/p\mathbb{Z}$, we have $\operatorname{Aut} Q \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Further, since P has no proper subgroups, φ is injective or trivial. Suppose that $p \nmid q - 1$. Then φ must be trivial, since $|\varphi(P)|$ must divide the order of $\operatorname{Aut} Q$. Therefore $G = Q \times P$ is a proper direct product, so $G \cong \mathbb{Z}/pq\mathbb{Z}$ is the only group of order pq.

Otherwise, if $p \mid q - 1$, then there is a unique subgroup of $\operatorname{Aut} Q$ of order p by the fundamental theorem of cyclic groups. We may map the generator of P to any element of this subgroup, for a total of p different homomorphisms φ, one of which is the trivial homomorphism. This yields p groups of order pq of the form $G = Q \rtimes_\varphi P$ for each φ. However, for any two nontrivial $\varphi, \psi : P \to \operatorname{Aut} Q$, we can construct an isomorphism of $Q \rtimes_\varphi P$ and $Q \rtimes_\psi P$ via an automorphism of P, since P is cyclic. Hence there are two nonisomorphic groups of order pq, which correspond to a trivial φ and a nontrivial φ. □

Problem 2.
Show that there are up to isomorphism exactly two nonabelian groups G of order 8. Prove that each of them has an irreducible complex representation of dimension 2.

Solution.
First, suppose that no element of G has order 4. Then every nonidentity element has order 2, which implies that G is abelian. Therefore G contains an element of order 4, say $a \in G$. Suppose there exists $b \in G$ of order 4 so that $ba \neq ab$. Then let $A, B \subset G$ be the subgroups generated by a, b respectively. Then if $A \cap B = \{1\}$, then $|AB| = |A| \cdot |B| = 16$, which is a contradiction. Therefore there is an element of order 2 in $A \cap B$, which we denote -1, which satisfies $a^2 = b^2 = -1$. Then we can write all the elements of $G : \{1, -1, a, -a, b, -b, ab, ba\}$, and in fact $ba = -ab$. We see that $G \cong Q$, the quaternion group.

Suppose now that there is no element of order 4 that does not commute with a. Then there must exist an element of order 2 that does not commute with a, which we also call b. Then since $A \cap B = \{1\}$, $|AB| = |A| \cdot |B| = 8$, so we can write all the elements of G again: $\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$, which we see is isomorphic to D_8, the dihedral group of the square. These are the only two nonabelian groups of order 8, and they are not isomorphic since Q contains more elements of order 4 than does D_8.

Recall that there is an irreducible complex representation of a group G for each of its conjugacy classes, and further the sum of the squares of the dimensions of the representations must equal the order of the group. The only way to sum squares to 8 is $1+1+1+1+1+1+1+1$, $1+1+1+1+4$, or $4+4$. The first case corresponds to 8 conjugacy classes of G, which could imply G is abelian, a contradiction. Therefore G must contain an irreducible representation of dimension 2, so that $2^2 = 4$ is part of this sum. □

Problem 3.
For a positive integer n, let $\Phi_n(X)$ be the nth cyclotomic polynomial. If a is an integer and p a prime not dividing n, such that p divides $\Phi_n(a)$, show that the order of $a \mod p$ is n. Using this prove that there are infinitely many primes p such that p is 1 modulo n.

Solution.
If $p \mid \Phi_n(a)$, then $\Phi_n(a) = 0$ in $\mathbb{F}_p$. As such a is an nth root of unity modulo p, so it is a root of $X^n - 1 = 0$. We need to show that it is a primitive nth root of unity, so that the order of a modulo p is 1. We know that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Suppose that a were a dth root of unity modulo p. Then $\Phi_d(a) = \Phi_n(a) = 0$, which would make a a multiple root of $X^n - 1$. However since $p \nmid n$, the polynomial $X^n - 1$ is separable, so it cannot have a multiple root. Therefore a is a primitive nth root of unity.

Since $a^n = 1 \mod p$, we know that in $\mathbb{F}_p^\times$ we have $a^n = 1$, so $n \mid p - 1$, which is to say that $p \equiv 1 \mod n$. Therefore we need to show that there are infinitely many primes that divide the set of values $\Phi_n(a)$ for $a \in \mathbb{Z}$. First, since $\Phi_n(a) \to \infty$ as $a \to \infty$, there is some prime $p \nmid n$ dividing some value of $\Phi_n(a)$. But this is (or at least should be) clear, so we are done. □

Problem 4.
Given a field K of characteristic p, when is an α that is algebraic over K said to be separable? Show that if α is algebraic over K, then α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.

Solution.
An algebraic element α is separable over K if its minimal polynomial $m_\alpha \in K[X]$ is separable, that is, its formal polynomial derivative is nonzero.

First, consider the extension $K(\alpha^{p^n}) \subset K(\alpha)$. Then since α is a root of the polynomial $X^{p^n} - \alpha^{p^n}$, we have $m_\alpha \mid X^{p^n} - \alpha^{p^n}$ over $K(\alpha^{p^n})[X]$. But since we are working in characteristic p, $X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$ in $K(\alpha)$, m_α is not a separable polynomial. In fact, this extension is purely inseparable.

Suppose that α is separable. Then the subextension $K(\alpha^{p^n}) \subset K(\alpha)$ is also separable, so since it is also purely inseparable, it is trivial. Hence $K(\alpha) = K(\alpha^{p^n})$. Conversely, if α is not separable, then the minimal polynomial of α is of the form $f(X^{p^k})$ where $f(X)$ is a separable polynomial and $k \geq 1$. But then α^p is a root of the polynomial $f(X^{p^{k-1}})$, so the extension $K(\alpha^p)$ is strictly of lower degree than $K(\alpha)$. Therefore $K(\alpha) \supsetneq K(\alpha^p)$.

Now suppose that we are in this case and $K(\alpha) = K(\alpha^{p^n})$. Then since $K(\alpha^p) \supset K(\alpha^{p^n})$, this is a contradiction that $K(\alpha)$ is strictly larger. This completes the proof.

□

Problem 5.
Let G be a finite group which has the property that for any element $g \in G$ of order n, and an integer r prime to n, the elements g and g^r lie in the same conjugacy class. Then show that the character of every representation of G takes values in the rational numbers $\mathbb{Q}$ (in fact even the integers $\mathbb{Z}$). (Hint: Use Galois theory.)

Solution.
Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation. Consider an element $\rho(g)$. Then since this is a complex representation, we may represent $\rho(g)$ by a diagonal matrix $\mathrm{diag}(\lambda_1, \ldots, \lambda_m)$. Since $\rho(g)^n = \rho(g^n) = I_m$, we must have λ_i is an nth root of unity for each i, so we write $\rho(g) = \mathrm{diag}(\zeta_n^{a_1}, \ldots, \zeta_n^{a_m})$.

If χ is a character of ρ, then $\chi(\rho(g)) = \sum_{i=1}^m \zeta_n^{a_i} \in \mathbb{Q}(\zeta_n) \subset \mathbb{C}$. Consider $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. This group consists precisely of the automorphisms $\sigma(\zeta_n) = \zeta_n^r$ for some $(r, n) = 1$. We claim that $\chi(\rho(g))$ is fixed by every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If this is so, then $\chi(\rho(g))$ lies in the fixed field of the Galois group, which is $\mathbb{Q}$, so we would be done.

To prove the claim, we have

$$\sigma(\chi(\rho(g))) = \sigma\left(\sum_{i=1}^m \zeta_n^{a_i}\right) = \sum_{i=1}^m \zeta_n^{a_i \cdot r} = \mathrm{tr}\left(\mathrm{diag}(\zeta_n^{a_1}, \ldots, \zeta_n^{a_m})\right)^r = \chi(\rho(g^r)).$$

But since χ is a class function and g, g^r lie in the same conjugacy class, we have $\sigma(\chi(\rho(g))) = \chi(\rho(g))$. This proves the claim. □

Problem 6.
Let I be an ideal of a commutative ring and $a \in R$. Suppose the ideals $I + Ra$ and $(I : a) := \{x \in R : ax \in I\}$ are finitely generated. Prove that I is also finitely generated.

Solution.
We have $I + Ra/Ra = I/I \cap Ra = I/a(I : a)$ by their definitions. Therefore if $I + Ra$ is finitely generated, its quotient is also finitely generated. We have an exact sequence

$$0 \to a(I : a) \to I \to I/a(I : a) \to 0.$$

Since $(I : a)$ is finitely generated, $a(I : a)$ is also finitely generated. We further have surjections

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{R}^m & \longrightarrow & \mathbb{R}^{m+n} & \longrightarrow & \mathbb{R}^n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & a(I:a) & \longrightarrow & I & \longrightarrow & I/a(I:a) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the middle surjection follows from the Five Lemma. Hence I is finitely generated as well. □

Problem 7.
Give an example of a 10×10 matrix over $\mathbb{R}$ with minimal polynomial $(X+1)^2(X^4+1)$ which is not similar to a matrix with rational coefficients.

Solution.
In $\mathbb{R}$, we may factor $(X^4+1) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$. Therefore choose any matrix in $M_{10}(\mathbb{R})$ with invariant factors $\{X^2+\sqrt{2}X+1, X^2+\sqrt{2}X+1, (X+1)^2(X^4+1)\}$, which we know exists by appealing to any canonical form. Suppose that there was a matrix α with rational coefficients with these invariant factors. Then in particular, the determinant of the matrix $X \cdot I_{10} - \alpha$ would be the product of the invariant factors, a polynomial in $\mathbb{R}[X]$ but not in $\mathbb{Q}[X]$. But since α has only rational entries, and the determinant is a function on the entries of the matrix, we must have $\det(X \cdot I_{10} - \alpha) \in \mathbb{Q}[X]$, and this is preserved under similarity. Therefore α cannot have these invariant factors, so we are done. □

Problem 8.
Suppose that E/F is an algebraic extension of fields such that every nonconstant polynomial in $F[X]$ has at least one root in E. Show that E is algebraically closed.

Solution.
We need to show that every nonconstant polynomial in $E[X]$ has at least one root in E. If this is true, then let α be a root of $f(X) \in E[X]$. Then $f(X) = (X-\alpha)g(X)$. Then g has a root in E, and by induction on the degree of the polynomial, f splits over E. Therefore every polynomial over $E[X]$ splits in E, so E is algebraically closed.

Let α be an algebraic element over E. Since E/F is algebraic, α is algebraic over F, so let m_α be its minimal polynomial over F. Let m_α split in some K/F. If m_α is separable, then $K = F(\beta)$ for some element β. Since $m_\alpha(\gamma) = 0$ for some $\gamma \in E$, we can embed K into E by $\beta \mapsto \gamma$, so that m_α also splits in E. In particular, E is perfect.

However, suppose F is not perfect. Let $\operatorname{char} F = p$. Now take the perfect closure of F in E, i.e. $F_{\text{perf}} = \{a \in E : a^{p^n} \in F \text{ for some } n > 0\}$. By construction, F_{perf} is a perfect field. We claim that every irreducible (hence separable) polynomial over F_{perf} has a root in E, which would complete the proof. But every $f \in F_{\text{perf}}[X]$ has $f^{p^k} \in F[X]$ for a large enough $k > 0$, and f and f^{p^k} have the same roots. Therefore f has a root in E, which completes the proof. □

Problem 9.
Prove that if $ab = 1$ in a semisimple ring, then $ba = 1$.

Solution.
A semisimple ring is artinian and noetherian. Let $\ell_a : R \to R$ be left multiplication by a. This map is surjective because $abc = c$ for any c. We claim that it is also injective. Let R denote our ring and let $N_i = \ker \ell_a^i$ be a chain of ideals of R. We have $N_1 \subset N_2 \subset \ldots$, since $ax = 0 \implies a^2x = 0$. Therefore this is an ascending chain, and since R is Noetherian, it stabilises at some term n, so that $\ker \ell_a^n = \ker \ell_a^{n+m}$ for all $m \in \mathbb{N}$. Suppose that $x \in \ker \ell_a$. Since ℓ_a is surjective, there exists $y \in R$ so that $\ell_a^n(y) = a^n y = x$. Therefore $y \in N_{n+1}$. But since $N_{n+1} = N_n$, we have $a^n y = 0$, hence $x = 0$. Therefore $\ker \ell_a = 0$, so the map is injective.

Take $\ell_a(ba-1)$. We have $aba = a$ so $a(ba-1) = aba - a = a - a = 0$, so by injectivity this implies that $ba - 1 = 0$, so $ba = 1$ as required. □

Problem 10.
Let A be the functor from the category of groups to the category of (unital) rings taking a group G to the group ring $\mathbb{Z}[G]$ of all finite formal sums $\sum_{g\in G} a_g g$ with $a_g \in \mathbb{Z}$. Prove that A has a right adjoint functor.

Solution.
A right adjoint functor to A would be a functor B from **Ring** to **Group** such that, for a group G and ring R,

$$\mathrm{Hom}_{\mathbf{Ring}}(A(G), R) \cong \mathrm{Hom}_{\mathbf{Group}}(G, B(R)).$$

For a ring homomorphism $\varphi : \mathbb{Z}[G] \to R$, every coefficient a_g must be mapped to $\underbrace{1_R + \ldots + 1_R}_{a_g \text{ times}}$.
Therefore this ring homomorphism is completely determined by $\varphi(g)$ for each $g \in G$. However, since we we have $\varphi(g)\varphi(g^{-1}) = 1_R$, we must have $\varphi(g) \in R^\times$. This is only restriction, however, so we claim that the functor B is $B(R) = R^\times$. We have shown how every map in the left set yields a map in the right set. Conversely, given a map $\psi : G \to R^\times$, this yields a map $\hat{\psi} : \mathbb{Z}[G] \to R$ by

$$\hat{\psi}\left(\sum_{g\in G} a_g\, g\right) = \sum_{g\in g}\left(\underbrace{1_R + \ldots + 1_R}_{a_g \text{ times}}\right)\cdot \psi(g).$$

Therefore B is indeed a right adjoint to A. □

3 Spring 2013

Problem 1.
Let G be a free abelian group of rank r, so $G \cong \mathbb{Z}^r$ as groups. Show that G has only finitely many subgroups of a given finite index n.

Solution.
Let $H \subset G$ be a subgroup of index n. Then G acts on G/H by left multiplication, which induces a group homomorphism $\varphi : G \to S_n$. We know that H is the stabiliser of the coset $H \in G/H$. Labelling this coset 1 (where we view the symmetric group as the permutations of $\{1, \ldots, n\}$), the stabiliser is all those elements whose presentation does not contain (1). This is a subgroup $H' \subset S_n$ which satisfies $\varphi^{-1}(H') = H$.

The above shows that that any subgroup of index n determines a unique morphism $\varphi : G \to S_n$, as the original subgroup is recovered by the action. Since G is free abelian of rank r, we know that any morphism $G \to S_n$ comes (uniquely) from a set map $\{1, \ldots, r\} \to S_n$, of which there are only $r \cdot n!$. Therefore there are only finitely many maps $G \to S_n$, so there are only finitely many subgroups of index n. □

Problem 2.
Assume that L is a Galois extension of the field of rational numbers $\mathbb{Q}$ and that $K \subset L$ is the subfield generated by all roots of unity in L. Suppose that $L = \mathbb{Q}[a]$, where $a^n \in \mathbb{Q}$ for some positive integer n. Show that the Galois group $\mathrm{Gal}(L/K)$ is cyclic.

Solution.
We may assume that n is the minimal such n. Since L normal, it is a splitting field of $X^n - a^n$ over $\mathbb{Q}$ since one root of this polynomial lies in L. We see that $\zeta_n \in L$ for all nth roots of unity, so $\mu_n \subset K$. An element $\sigma \in \mathrm{Gal}(L/K)$ can only send $a \mapsto \zeta_n^r a$, since these are the only roots of $X^n - a^n$ over K. Since $L = K[a]$ and $\sigma(\zeta_n) = \zeta_n$ since $\zeta_n \in K$, see that $\mathrm{Gal}(L/K) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, so it is cyclic. □

Problem 3.
Let $K \subset L$ be an algebraic extension of fields. An element $a \in L$ is called *abelian* if $K[a]$ is a Galois extension of K with abelian Galois group $\mathrm{Gal}(K[a]/K)$. Show that the set of abelian elements L is a subfield of L containing K.

Solution.
Let $\hat{L}$ denote the set of abelian elements of L. Since for any $a \in K$, $\mathrm{Gal}(K[a]/K) = 0$, the trivial abelian group, $K \subset \hat{L}$. Suppose that $a, b \in \hat{L}$ are arbitrary elements. Then since $K[-a] = K[a^{-1}]$, we know that these elements are also abelian. Therefore we need only show that $a + b, ab$ are abelian elements.

Note that any subfield of an abelian extension is an abelian extension. If $K[a]/K$ is abelian and $K \subset E \subset K[a]$, then E corresponds to a subgroup $H \subset \mathrm{Gal}(K[a]/K)$. Since H is a normal subgroup of $\mathrm{Gal}(K[a]/K)$, E/K is a Galois extension with $\mathrm{Gal}(E/K) = G/H$, which is still abelian.

Now suppose $a, b \in \hat{L}$. Then by a theorem of Galois theory (e.g. Lang VI, Theorem 1.14), $\mathrm{Gal}(K[a]K[b]/K) \hookrightarrow \mathrm{Gal}(K[a]/K) \times \mathrm{Gal}(K[b]/K)$. Since the direct product of abelian groups if an abelian group, $K[a]K[b]$ is an abelian extension of K. Since $a+b, ab \in K[a]K[b]$, they generate abelian subextensions of $K[a]K[b]$, and by the above reasoning $a + b, ab \in \hat{L}$. This completes the proof. □

Problem 4.
Let $\mathbb{F}_2$ be the field with 2 elements and let $R = \mathbb{F}_2[X]$. List, up to isomorphism, all R-modules with 8 elements.

Solution.
We use the classification theorem of modules over a PID. Since R is a finite module, it is in particular an $\mathbb{F}_2$ vector space. We can write

$$M \cong R/n_1R \oplus R/n_2\mathbb{R} \oplus \cdots \oplus R/n_rR$$

for polynomials $n_1 \mid n_2 \mid \cdots \mid n_r$. In our case, we have $\sum_{i=1}^{r} \deg n_i = 3$, so we have three options: $r = 1, \deg n_1 = 3$, $r = 2, \deg n_2 = 2$, and $r = 3, \deg n_3 = 1$. The first case yields 8 options. For the second case, we need n_2 to be reducible, so we have $X(X+1), X^2, (X+1)^2$ as choices. The first choice yields 2 decompositions, and the latter choices yield 1 decomposition

each, for a total of 4. For the linear case, we need the same linear term repeated thrice, which is 2 choices. Therefore there are 14 in all, listed by invariant factors below:

$$\{X^3 + (0/1)X^2 + (0/1)X + (0/1)\}$$
$$\{X^2, X\}, \{X^2 + X, X + (0/1)\}, \{X^2 + 1, X + 1\}$$
$$\{X, X, X\}, \{X + 1, X + 1, X + 1\}.$$

□

Problem 5.
Let R be a commutative local ring, so R has a unique maximal ideal $\mathfrak{m}$.

(a) Show that if $x \in \mathfrak{m}$ then $1 - x$ is invertible.

(b) Show that if R is Noetherian and if $\mathfrak{a}$ is an ideal such that $\mathfrak{a}^2 = \mathfrak{a}$ then $\mathfrak{a} = 0$.

Solution.

(a) If $1 - x$ is not invertible, then it is contained in some maximal ideal $\mathfrak{m}' \subset R$. But R is a local ring, so we must have $1 - x \in \mathfrak{m}$. But then $1 - x + x \in \mathfrak{m} \implies \mathfrak{m} = R$, a contradiction. Hence $1 - x$ is not contained in any maximal ideal, so $1 - x$ is invertible.

(b) Viewing $\mathfrak{a}$ as an R-module, since R is Noetherian, $\mathfrak{a}$ is finitely generated. Since R is local, $\mathfrak{m}$ is its Jacobson radical. Applying Nakayama's lemma, since $\mathfrak{a} \cdot \mathfrak{a} = \mathfrak{a}$, there is some element $r \in R$ so that $r = 1 \mod \mathfrak{a}$ such that $r\mathfrak{a} = 0$. Since $r = 1 \mod \mathfrak{a}$, we have $1 - r \in \mathfrak{a} \subset \mathfrak{m}$. As such $1 - (1 - r) = r \in R^\times$. Then $M = r^{-1}rM = 0$.

□

Problem 6.
Let D be a division ring of characteristic 0. Assume that D has dimension 2 as a $\mathbb{Q}$-vector space. Show that D is commutative.

Solution.
We know that $0 \neq 1 \in D$, and since D has characteristic 0, $\mathbb{Z} \subset D$. Indeed, $\mathbb{Q} \subset D$ since D is a division ring. Therefore we realise D as a division algebra of dimension 2 over $\mathbb{Q}$. As such, $\mathbb{Q} \subset Z(D)$, and in particular $qX = Xq$ for any $q \in \mathbb{Q}$. Therefore take a basis $\{1, X\}$ for D over $\mathbb{Q}$. Then every element in D is of the form $a + bX$. As such, we have

$$(a+bX)(c+dX) = ac+bXc+adX+bXdX = ca+cbX+dXa+dXbX = (c+dX)(a+bX).$$

Therefore D is commutative. □

Problem 7.
Let $F = \mathbb{F}_2$ be the field with 2 elements. Show that there is a ring homomorphism $F[\mathrm{GL}_2(F)] \to M_2(F)$ that sends the element g in the group ring to the matrix $g \in M_2(F)$. Show that this homomorphism is surjective. Let K be the kernel; since it is a left ideal, it is a (left) $\mathrm{GL}_2(F)$-module. Is this module indecomposable? (Reminder: a module is indecomposable if it is not the direct sum of two proper submodules.) Describe the simple modules in its composition series.

Solution.
We can see that $1 \cdot \mathrm{GL}_2(F)$ injects into $\mathrm{GL}_2(F) \subset M_2(F)$. It is also easy to verify that the map is surjective by direct computation.

Calculating out the rest of this is nasty, but it is easily done. I may update this section at a later time. □

Problem 8.
Let $\mathcal{C}$ and $\mathcal{D}$ be additive categories, and let $\Phi : \mathcal{C} \to \mathcal{D}$ be a functor. Show that if Φ has a right adjoint, then Φ commutes with direct sums and for any two objects x and y in $\mathcal{C}$, the map $\Phi_{x,y} : \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(x), \Phi(y))$ is a homomorphism.

Solution.
Let $\Psi : \mathcal{D} \to \mathcal{C}$ be the right adjoint, so that for $a \in \mathcal{C}$ and $b \in \mathcal{D}$, we have

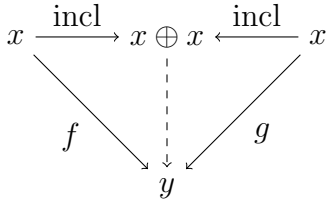
$$\mathrm{Hom}_{\mathcal{D}}(\Phi(a), b) \cong \mathrm{Hom}_{\mathcal{C}}(a, \Psi(b)).$$

Suppose that $x = \coprod_{i \in I} x_i$ is a direct product in $\mathcal{C}$. Then for any $y \in \mathcal{D}$,

$$\begin{aligned}\mathrm{Hom}_{\mathcal{D}}(\Phi(x), y) \cong \mathrm{Hom}_{\mathcal{C}}\left(\coprod x_i, \Psi(y)\right) &\cong \prod \mathrm{Hom}_{\mathcal{C}}(x_i, \Psi(y)) \\ &\cong \prod \mathrm{Hom}_{\mathcal{D}}(\Phi(x_i), y) \cong \mathrm{Hom}_{\mathcal{D}}\left(\coprod \Phi(x_i), y\right).\end{aligned}$$

Therefore in $\mathcal{D}$ both $\coprod \Phi(x_i)$ and $\Phi(\coprod x_i)$ satisfy the universal property of the coproduct, so they must be equal. Hence Φ commutes with direct sums.

We write $+$ for the abelian group action on Hom sets. Then for $f, g \in \mathrm{Hom}_{\mathcal{C}}(x, y)$, we see that



where the middle arrow induced by the direct sum is $f + g$. Therefore applying Φ to this diagram, we see that $\Phi(f + g)$ must be $\Phi(f) + \Phi(g)$ since Φ commutes with the direct sum. □

Problem 9.
Let D be an associative ring without zero divisors, and assume the centre of D is a field over D which is a finite-dimensional vector space. Prove that D is a division algebra.

Solution.
Let $0 \neq \alpha \in D$. Then we claim the vector space endomorphism $\ell_\alpha : D \to D$ where $\beta \mapsto \alpha\beta$ is injective. Indeed, since D has no zero divisors, $\alpha\beta = 0$ implies $\beta = 0$. Therefore since D is a finite dimensional vector space, ℓ_α is surjective as well by counting dimensions. Hence there exists a unique $\gamma \in D$ so that $\alpha\gamma = 1$, so $\alpha \in D^\times$. Therefore $D^\times = D \setminus \{0\}$, so D is a division algebra. □

Problem 10.
Let G be a finite group of order n and $\rho : G \to \mathrm{GL}(V)$ be a complex representation of G of dimension n. Show that ρ cannot be irreducible.

Solution.
By general representation theory, we have the sum of the squares of the dimensions of the irreducible representations that comprise ρ must equal the order of the group. Suppose that ρ is irreducible. Then $(\dim \rho)^2 = n^2 \neq n$ unless G is the trivial group. Hence ρ cannot be irreducible. □

4 Fall 2012

Problem 1.
Let p be a prime integer and let G be a (finite) p-group. Write C for the subgroup of central elements $x \in G$ satisfying $x^p = 1$. Let N be a normal subgroup of G such that $N \cap C = \{1\}$. Prove that $N = \{1\}$.

Solution.
Assume that N is nontrivial. First, we claim that any nontrivial normal subgroup N of a p-group intersects its centre nontrivially. To see this, consider the action of G on N by conjugation. Since G is a p-group, we have $|N| \equiv |N^G| \mod p$, where $N^G = \{n \in N : g \cdot n = n \text{ for all } g \in G\}$, which is a consequence of the orbit-stabiliser theorem. Since $|N| \equiv 0 \mod p$, then $p \mid |N^G|$. Since $1 \in N^G$, $|N^G| \geq 1$, hence N^G is a nontrivial subgroup of N which intersects $Z(G)$ nontrivially.

Since N_G is a subgroup of a p-group, it too is a p-group, so it contains an element of order p. Hence that element $x \in N \cap C$, a contradiction. Therefore N must be a trivial normal subgroup. □

Problem 2.
Let A be an $n \times n$ matrix over F having only one invariant factor. Prove that every $n \times n$ matrix over F that commutes with A is a polynomial in A with coefficients in F.

Solution.
Consider A acting on $V = F^n$. Since A has only one invariant factor, there exists a vector $v \in V$ so that $\{Av, \ldots, A^n v\}$ is a basis for V. Then we can write $B(Av) = \sum_{i=1}^{n} a_i A^i v$ using the given basis. But we also have $B(Av) = A(Bv)$, i.e.

$$\sum_{i=1}^{n} a_i A^i v = A(Bv) \implies Bv = \sum_{i=i}^{n} a_i A^{i-1} v.$$

Let $C = \sum_{i=i}^{n} a_i A^{i-1}$. We claim that $B = C$ on all of V. Since any vector in $w \in V$ may be written as $p(A)v$ for some $p \in F[X]$ of degree $n-1$ (using the basis $\{v, A, \ldots, A^{n-1}v\}$ now), we have

$$Bw = Bp(A)v = p(A)Bv = p(A)Cv = Cp(A)v = Cw.$$

Therefore B is a polynomial in A. □

Problem 3.
Let F be a field and let n be a positive integer such that F has no nontrivial field extensions of degree less than n. Let $L = F(x)$ be a field extension with $x^n \in F$. Prove that every element in L is a product of elements of the form $ax + b$ with $a, b \in F$.

Solution.
Since x satisfies $X^n - x^n = 0$, we know $[L : F] \leq n$. If $[L : F] < n$, then $L = F$ by assumption, so any element $b \in F$ is expressible in the form $0 \cdot x + b$, and we are done. Therefore suppose $[L : F] = n$.

Consider $y \in L$. Then $y = \sum_{i=0}^{m} a_i x^i$ for some $a_i \in F$, where $m < n$. Consider the corresponding polynomial $f(X) = \sum_{i=0}^{m} a_i X^i$. Then we claim f splits over F. Suppose not. Then let α be a root of f. then $[F(\alpha) : F] \leq \deg f = m < n$, so $F(\alpha) = F$, i.e. $\alpha \in F$. Hence we can write $f(X) = (X - \alpha)g(X)$. By induction, this shows that f splits. Therefore we obtain a factorisation of $f(X)$ into linear factors:

$$f(X) = \prod_{i=i}^{m} (c_i X + d_i).$$

This corresponds with a factorisation

$$\beta = \prod_{i=1}^{m} (c_i x + d_i)$$

as claimed. □

Problem 4.
Let F be the functor from the category of rings to the category of sets taking a ring R to the set $\{x^2 : x \in R\}$. Determine whether F is representable.

Solution.
Suppose it were representable. Then let $F = \mathrm{Hom}(R, -)$. Then in particular, $\mathrm{Hom}(R, R)$ must be in bijection with R^2. Let $x \in R^2$ be the element corresponding to the identity $1_R \in \mathrm{Hom}(R, R)$, and let $x = y^2$. Then for a map $g : R \to S$, we have the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(R,R) & \xrightarrow{g\circ -} & \mathrm{Hom}(R,S) \\ {\scriptstyle\sim}\downarrow{\scriptstyle \alpha_R} & & {\scriptstyle\sim}\downarrow{\scriptstyle \alpha_S} \\ F(R) & \xrightarrow{F(g)} & F(S) \end{array}$$

1_R has the unique property that $g \circ 1_R = g$, so we see what this means for the bottom row. $x \in F(R)$ has the unique property that for every $b^2 \in F(R)$, there is a unique $g : R \to S$ so that $F(g)(x) = b^2$, i.e. $g(x) = b^2$.

But this is evidently not the case. Consider $S = \mathbb{Z}[X]$. Then there should be a unique group homomorphism $g : R \to S$ such that $g(x) = X^2$, so evidently $g(y) = \pm X$. But since there is an automorphism φ of S interchanging X and $-X$, we see that $(\varphi \circ g)(x) = g(x) = X^2$, so this homomorphism is not unique. Therefore F is not representable. □

Problem 5.
Let G and H be finite groups and let V and W be irreducible (over $\mathbb{C}$) G- and H-modules respectively. Prove that the $G \times H$-module $V \otimes W$ is also irreducible.

Solution.
We use the theory of characters. If the character of $V \otimes W$ is 1, then $V \otimes W$ is irreducible. Since $\operatorname{tr}(V \otimes W) = \operatorname{tr} V \cdot \operatorname{tr} W$, if ρ_G, ρ_H are characters on G and H, then the character θ on $G \times H$ is given by $\theta(g,h) = \rho_G(g)\rho_H(h)$. Then

$$|\theta|^2 = \langle \theta, \theta \rangle = \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \theta(g,h)\overline{\theta(g,h)}.$$

Rearranging this to suit our case,

$$\begin{aligned}
|\theta|^2 &= \frac{1}{|G|} \sum_{g \in G} \left(\rho_G(g)\overline{\rho_G(g)} \left(\frac{1}{|H|} \sum_{h \in H} \rho_H(h)\overline{\rho_H(h)} \right) \right) \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\rho_G(g)\overline{\rho_G(g)}|\rho_H|^2 \right) = |\rho_H|^2 \left(\frac{1}{|G|} \sum_{g \in G} \rho_G(g)\overline{\rho_G(g)} \right) \\
&= |\rho_G|^2|\rho_H|^2 = 1
\end{aligned}$$

since ρ_G and ρ_H were irreducible characters on G and H. Therefore $|\theta|^2 = 1$, so θ is an irreducible character, and $V \otimes W$ is irreducible as desired. □

Problem 6.
Let D_n be a dihedral group of order $2n > 4$; so, it contains a cyclic subgroup C of order n on which $\sigma \in D_n$ outside C acts as $\sigma c \sigma^{-1} = c^{-1}$ for all $c \in C$. When is the cyclic subgroup C with the above property unique? Determine all n for which D_n has a unique cyclic subgroup C and justify your answer.

Solution.
Let r denote the rotation and s the reflection in D_n. We claim that all elements of order n are of the form r^k. Indeed, we have $(sr^k)^2 = (sr^k)(r^{-k}s) = 1$ for any $k \in \{0, \ldots, n-1\}$. Therefore the only elements of order n are the usual r^k with $(k,n) = 1$. Therefore in every case, the cyclic subgroup C is $\langle r \rangle$. □

Problem 7.
Let D be a central simple division algebra of dimension 4 over a field F. If a quadratic extension K/F can be isomorphically embedded into D as F-algebras, prove that $D \otimes_F K$ is isomorphic to $M_2(K)$ as K-algebras.

Solution.
Assume $\operatorname{char} F \neq 2$. Let $K = F(\sqrt{\alpha})$. Recall that for quaternion algebras, the cases of division algebra and matrix algebra and mutually exclusive and collectively exhaustive. Since D is central and simple, $D \otimes_F K$ is a central simple algebra over K of dimension 4,

so it suffices to prove that it is not division. Indeed, since K may be embedded into D, we have $K \otimes_F K \subset D \otimes_F K$ as a subalgebra. We claim that

$$\sqrt{\alpha} \otimes 1 - 1 \otimes \sqrt{\alpha}$$

is a zero divisor. Indeed,

$$\begin{aligned}(\sqrt{\alpha} \otimes 1 + 1 \otimes \sqrt{\alpha})(\sqrt{\alpha} \otimes 1 - 1 \otimes \sqrt{\alpha}) &= \alpha \otimes 1 - \sqrt{\alpha} \otimes \sqrt{\alpha} + \sqrt{\alpha} \otimes \sqrt{\alpha} - 1 \otimes \alpha \\ &= \alpha \otimes 1 - 1 \otimes \alpha = (\alpha - \alpha) \otimes 1 = 0\end{aligned}$$

since in the last step, we may move α over the tensor product. Hence $D \otimes_F K$ is not division, so it is isomorphic to $M_2(K)$.

If the characteristic of F is 2 and the extension is separable, the above argument holds with (roughly) $\beta \otimes 1 + 1 \otimes \gamma$, where β, γ are the roots of the quadratic polynomial of which K is the splitting field. □

Problem 8.
How many monic irreducible polynomials over $\mathbb{F}_p$ of prime degree l are there? Justify your answer.

Solution.
We claim that the product of all irreducible polynomials of degree $d \mid n$ equals $f(X) = X^{p^n} - X$. Given any $\alpha \in \mathbb{F}_{p^n}$, $f(\alpha) = 0$. Hence the irreducible polynomial of α divides f, and the degree of α divides the degree of the extension n. Conversely, for any monic irreducible polynomial g of degree $d \mid n$, g has roots $\mathbb{F}_{p^d}$. Since $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$, all the roots of α lie in $\mathbb{F}_{p^n}$, so $g \mid f$. Hence

$$X^{p^n} - X = \prod_{\deg g = d \mid n} g(X).$$

Now, since l is prime, the only divisors of l are 1 and l. There are evidently p irreducible polynomials of degree 1, and so the degree of the product of the polynomials of degree l is $p^l - p$. Since each of those polynomials has degree l itself, their number is $\frac{p^l - p}{l}$. □

Problem 9.
Consider a covariant functor $F : R \mapsto R^\times$ from the category of commutative rings with identity to the category of sets. Let $G = \mathrm{Aut}_{\mathrm{functors}}(F)$ be made up of natural transformations $I : F \to F$ having an inverse $J : F \to F \in G$ such that $I \circ J = J \circ I$ is the identity natural transformation. Prove that F is representable, that G is a finite group, and find the order of the group G with justification.

Solution.
First, F is representable by $\mathbb{Z}[X, X^{-1}]$, the polynomial ring. Let $\varphi \in \mathrm{Hom}(\mathbb{Z}[X, X^{-1}], R)$ be a homomorphism. Then $\varphi(1) = 1_R$, and by extension $\varphi(n) = n \cdot 1_R$ for any $n \in \mathbb{Z}$. Further, X may be sent to any invertible element in R, and this determines the image of X^{-1} as well. Further, these are the only homomorphisms $\mathbb{Z}[X, X^{-1}] \to R$. Hence F is represented by $\mathbb{Z}[X, X^{-1}]$.

We claim that $\mathrm{Aut}_{\mathrm{functors}}\, F \cong \mathrm{Aut}_{\mathbf{Rings}}\, \mathbb{Z}[X, X^{-1}]$. Assuming this, the only nontrivial ring automorphism of $\mathbb{Z}[X, X^{-1}]$ sends $X \mapsto X^{-1}$, and we have $\mathrm{Aut}_{\mathrm{rings}}\, \mathbb{Z}[X, X^{-1}] \cong \mathbb{Z}/2\mathbb{Z}$. Indeed, by Yoneda's lemma we have

$$\mathrm{Hom}_{\mathrm{functors}}(F) \cong \mathrm{Hom}_{\mathrm{functors}}(h^{\mathbb{Z}[X,X^{-1}]}, F) \cong F(\mathbb{Z}[X, X^{-1}]) = \{\pm 1, X^{\pm 1}\}.$$

However, the homomorphisms corresponding to $X \mapsto \{\pm 1\}$ are not invertible homomorphisms, so we are left with the automorphisms $X \mapsto \{X^{\pm 1}\}$. This completes the proof. □

Problem 10.
For a finite field of order q, consider the polynomial ring $R = \mathbb{F}[X]$, and let L be a free R-module of rank 2. Give the number of R-submodules of M such that $XL \subsetneq M \subsetneq L$ and justify your answer.

Solution.
First, we simplify the problem by quotienting out by XL, so obtain the chain

$$0 \subsetneq N \subsetneq L/XL \cong \mathbb{F} \times \mathbb{F}.$$

where N is a submodule. Therefore we need to find all dimension 1 subspaces of $\mathbb{F}^2$. These are entirely determined by nonzero vectors of $\mathbb{F}^2$, of which there are $q^2 - 1$, but divided by the nonzero spans of each vector space, which yields

$$\frac{q^2 - 1}{q - 1} = q + 1.$$

□

5 Spring 2012

Problem 1.
Let V be a finite dimensional space over $\mathbb{Q}$ and $G \subset \mathrm{GL}(V)$ a finite subgroup. Prove that the $\mathbb{Q}$-subalgebra of $\mathrm{End}(V)$ generated by G is semisimple.

Solution.
By Maschke's theorem, the group algebra of a finite group by a field of characteristic zero is semisimple. In particular [1]:

Assume $\mathrm{char}\, \mathbb{F} \nmid |G|$. Let V be a finite dimensional $\mathbb{F}[G]$-module, and let $W \subset V$ be a submodule. Choose an idempotent element $e \in \mathrm{End}_{\mathbb{F}}(V)$ so that $eV = W$. Let

$$\bar{e} := \frac{1}{|G|} \sum_{g \in G} geg^{-1},$$

where we view $g \in \mathrm{End}_{\mathbb{F}}(V)$. Then

$$h\bar{e} = \frac{1}{|G|} \sum_{g \in g} hgeg^{-1} = \frac{1}{|G|} \sum_{g \in G} (hg)e(hg)^{-1}h = \bar{e}h.$$

for all $h \in G$, and thus $\bar{e} \in \mathrm{End}_{\mathbb{F}[G]}(V)$. Since $W \subset V$ is a submodule, $\bar{e}$ satisfies $\bar{e}V \subset W$ and $\bar{e}|_W = \mathrm{id}_W$. Hence $\bar{e}$ is an idempotent satisfying $\bar{e}V = W$, so we have $V = W \oplus (1-\bar{e})V$. Repeating this process, we can reduce V into a direct sum of irreducible submodules, so every $\mathbb{F}[G]$-module is semisimple. □

Problem 2.
Let V be the vector space of all $a \in \mathbb{R}^n$ such that $a_1 + \ldots + a_n = 0$. The symmetric group S_n acts naturally on V. Prove that the S_n-module V is simple.

Solution.
Note that the vectors $B = \{e_1 - e_i : i \in \{2, \ldots, n\}\}$ form a basis for V. V is an $(n-1)$-dimensional vector space since it is precisely the orthogonal complement to $e_1 + \ldots + e_n$ under the usual inner product, and the $n-1$ vectors B are linearly independent and in V.

Therefore let W be a submodule of V, and let $v = (v_1, \ldots, v_n) \in W$ be a nonzero vector. Then two entries $v_i \neq v_j$ are both nonzero, since only one nonzero entry contradicts $\sum v_i = 0$. Therefore applying an appropriate permutation, we may assume $v_1 \neq v_2$ are nonzero. Then applying the transposition $\tau = (1\,2)$, we have

$$\tau v - v = (v_1 - v_2, v_2 - v_1, 0, \ldots, 0) \in W.$$

Multiplying by $(v_1 - v_2)^{-1}$, we have $e_1 - e_2 \in W$. Then applying the transpositions $(2\,i)$ for $i \in \{3, \ldots, n\}$, we see that $B \subset W$. Therefore $W = V$, so V is simple. □

Problem 3.
Let R be a commutative local ring, and P a finitely generated projective R-module. Show that P is a free module.

Solution.
This is a consequence of Nakayama's lemma. Let $P = Rm_1 + \ldots + Rm_k$ be an expression of P with the minimal number of elements. Then we have an exact sequence

$$0 \to N = \ker \varphi \to R^k \xrightarrow{\varphi} P \to 0,$$

and since P is projective, we have $R^k \cong P \oplus N$. Therefore we need to prove that $N = 0$. Let $\mathfrak{m}$ be the unique maximal ideal in R. Applying the functor $- \otimes R/\mathfrak{m}$, we have

$$(R/\mathfrak{m})^k \cong P/\mathfrak{m}P \oplus N/\mathfrak{m}N.$$

We claim that $\dim_{R/\mathfrak{m}}(R/\mathfrak{m})^k = \dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = k$. If $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) < k$, then by Nakayama's lemma P can be generated by fewer than k elements, which is a contradiction. Thus we have $N/\mathfrak{m}N = 0$. By Nakayama's lemma, since $J(R) = \mathfrak{m}$, $\mathfrak{m}N = N$ implies $N = 0$. Hence $R^k \cong P$, so P is free. □

Problem 4.
Let R be the subring of $M_3(\mathbb{R})$ consisting of all matrices (a_{ij}) with $a_{31} = a_{32} = 0$. Determine the Jacobson radical of R.

Solution.
We use that $x \in J(R)$ if and only if $xy - 1 \in R^\times$ for all $y \in R$. We use the general formula

$$\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ \delta & \varepsilon & \eta \\ 0 & 0 & \zeta \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a\alpha + b\delta - 1 & a\beta + b\varepsilon & a\gamma + b\eta + c\zeta \\ d\alpha + e\delta & d\beta + e\varepsilon - 1 & d\gamma + e\eta + f\zeta \\ 0 & 0 & g\zeta - 1 \end{pmatrix}.$$

If $g \neq 0$, then $\zeta = 1/g$ creates a zero row on the bottom, so the matrix cannot be invertible. Playing around with this more, you will see that $J(R) = \{\alpha \in R : a = b = d = e = g = 0\}$. □

Problem 5.
Let G be a finite group, K a normal subgroup, and P a Sylow p-subgroup of G. Prove that $P \cap K$ is a Sylow p-subgroup of K.

Solution.
Let $C = P \cap K$. Since $C \subset P$, C is a p-subgroup of K, so it sits inside some Sylow p-subgroup D of K. Likewise D sits inside some Sylow p-subgroup Q of G. Since Q is conjugate to P (as all Sylow p-subgroups are), write $gQg^{-1} = P$. We have $|C| \leq |D| = |Q \cap K|$. Further, $|C| = |P \cap K| = |Q \cap K|$. To see this, suppose $q \in P \cap K$. Then $gqg^{-1} \in g(P \cap K)g^{-1} = gPg^{-1} \cap K = Q \cap K$, so the elements are in bijective correspondence. Hence $|C| = |D|$, so C is a Sylow p-subgroup. □

Problem 6.
Determine the Galois group of the polynomial $X^8 + 16$ over $\mathbb{Q}$.

Solution.
Let f be this polynomial. Beginning with one root, we see $\zeta_{16}\sqrt{2}$ is a root of f, where ζ_{16} is a primitive 16th root of unity. Therefore we construct the Galois group in two steps:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_{16}) \subset K, \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset K$$

where K is the splitting field of $X^8 + 16$. Evidently $\mathbb{Q}(\zeta_{16})$ and $\mathbb{Q}(\sqrt{2})$ are both Galois over $\mathbb{Q}$, but their intersection is not $\mathbb{Q}$. In particular, we have

$$\zeta_{16}^2 = \zeta_8 = e^{i\pi/4} = \cos(\pi/4) + i\sin(\pi/4) = \frac{\sqrt{2} + i\sqrt{2}}{2}.$$

So that $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2})$. Therefore we see that $K = \mathbb{Q}(\zeta_{16})$, and it is easy to verify that for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have $\sigma(\sqrt{2}) = \sqrt{2}$. Hence the Galois group of this polynomial is $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. □

Problem 7.
Let F be a finite field with p^n elements. Find the number of elements of F that can be written in the form $a^p - a$ for some $a \in F$.

Solution.
Let $f = X^p - X \in \mathbb{F}_p[X]$, which is a vector space endomorphism of F. Its kernel is simply roots of the polynomial $X^p - X$, of which there are p. Therefore $|\operatorname{im} f| = |F|/|\ker f|$, we have $|\operatorname{im} f| = p^{n-1}$. Therefore p^{n-1} elements of F can be written in this form. □

Problem 8.
Let R be a reduced (no nonzero nilpotent elements) commutative ring that has a unique proper prime ideal. Show that R is a field.

Solution.
If the prime ideal in question is the zero ideal, then R is a field, since its unique proper prime ideal is in particular maximal, so that $R/0 \cong R$ is a field.

Since R is reduced, it has a zero nilradical. But the nilradical is precisely the intersection of all prime ideals, of which there is only one. Therefore the only prime must be zero, so we are done. □

Problem 9.
Let R be a flat commutative $\mathbb{Z}$-algebra, and $\mathbf{Mod}_R$ the category of R-modules. Suppose that I is an injective R-module. Show that the underlying abelian group of I is divisible.

Solution.
Suppose that I is indivisible as an abelian group. Therefore there exists $n \in \mathbb{N}$ and $x \in I$ so that $x \neq n \cdot y$ for any $y \in I$. Consider the map $f : \mathbb{Z} \to \mathbb{Z}$ given by $1 \mapsto n$, and the map $g : \mathbb{Z} \to I$ given by $1 \mapsto x$. Then if I were injective, there exists a unique lifting $h : \mathbb{Z} \to I$ so that $h \circ f = g$. In particular,

$$x = g(1) = h(f(1)) = h(n) = n \cdot h(1),$$

which is a contradiction since x is not divisible by n. Therefore as a $\mathbb{Z}$-module, I is not injective. Suppose that I is injective as an R-module. Then tensoring over $\mathbb{Z}$ by R, exact sequences are preserved by flatness, so we have $f : R \to R$, $g : R \to I$, and a unique lift $h : R \to I$ so that $g = h \circ f$. Then we have $x = g(1) = n \cdot h(1)$ as before. Since nothing here depends on the R-module structure, this map descends back down to $\mathbb{Z}$, which is a contradiction. Therefore I cannot be an injective R-module, and we are done. □

Problem 10.
Determine the automorphism group of the symmetric group S_3 up to isomorphism.

Solution.
Recall that $\operatorname{Aut} S_3$ is comprised of inner automorphisms and outer automorphisms, and that for a general group G, the inner automorphisms of G is isomorphic to $G/Z(G)$. In our case, $Z(S_3) \cong 1$, so $\operatorname{Inn} S_3 \cong S_3$.

We claim that every automorphism of S_3 is inner. By the above, we have a map $S_3 \to \operatorname{Aut} S_3$ by $\sigma \mapsto \varphi_\sigma$, where $\varphi_\sigma(\rho) = \sigma\rho\sigma^{-1}$. For any automorphism φ, the set of transpositions in S_3 is preserved, which induces a group homomorphism from $\operatorname{Aut} S_3$ to the symmetric group of set of transpositions, i.e. $\operatorname{Aut} S_3 \to S_3$. This map is injective since the set of transpositions generates S_3, so two different automorphisms cannot permute the transpositions in the same way. Therefore $|\operatorname{Aut} S_3| \leq |S_3|$, so our original injective map $S_3 \to \operatorname{Aut} S_3$ must be surjective as well. Hence $S_3 \cong \operatorname{Aut} S_3$. □

6 Fall 2011

Problem 1.
For a finite field $\mathbb{F}$, prove that the order of the group $\mathrm{SL}_2(\mathbb{F})$ is divisible by 6.

Solution.
Let $\mathbb{F} = q$. Consider the determinant map $\det : \mathrm{GL}_2(\mathbb{F}) \to \mathbb{F}^\times$, which is a group homomorphism since $\det(ab) = (\det a)(\det b)$. Then $\mathrm{SL}_2(\mathbb{F}) \cong \ker \det$. Additionally, det is clearly a surjective map. By the first isomorphism theorem,

$$|\mathrm{GL}_2(\mathbb{F})/\mathrm{SL}_2(\mathbb{F})| = |\mathbb{F}^\times|.$$

Since all groups are finite, we may rewrite this

$$|\mathrm{SL}_2(\mathbb{F})| = |\mathrm{GL}_2(\mathbb{F})|/|\mathbb{F}^\times|.$$

$|\mathbb{F}^\times| = q - 1$, since only $0 \in \mathbb{F} \setminus \mathbb{F}^\times$. Now we calculate $|\mathrm{GL}_2(\mathbb{F})|$. Recall that a nonsingular matrix is equivalent to choosing two linearly independent vectors in $\mathbb{F}^2$. For the first vector, choose any $v \neq (0,0) \in \mathbb{F}^2$. For the second, we cannot select any vector in the span of v, of which there are q. Hence

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

Given any three consecutive integers, one of them is divisible by 3, and one of them is divisible by 2. Hence their product is divisible by 6. □

Problem 2.
Let G be a non-trivial finite group and p a prime. If every subgroup $H \neq G$ has index divisible by p, prove that the centre of G has order divisible by p.

Solution.
Let G act on itself by conjugation. Then the orbits of this map are precisely the conjugacy classes of G. We have, letting x run over representatives of conjugacy classes,

$$G = \bigcup_{x \in G} Gx = Z(G) \cup \bigcup_{x \in G, |Gx| > 1} Gx.$$

By the orbit-stabiliser theorem,

$$|G| = |Z(G)| + \sum_{x \in G, |Gx|>1} |Gx| = |Z(G)| + \sum_{x \in G, |Gx|>1} |G : G_x|,$$

where G_x is the stabiliser of x in G under this action. Since each G_x is a subgroup, by assumption it has index divisible by p. Since $|G : \{e\}| = |G|$ is also divisible by p, we must have $p \mid |Z(G)|$ as well. This completes the proof. □

Problem 3.
Let R be a local UFD of Krull dimension 2. Let $\pi \in R$ be neither zero nor a unit. Prove that $R[1/\pi]$ is a PID.

Solution.
Since prime ideals in $R[1/\pi]$ correspond precisely to prime ideals in R not containing π, we see that $R[1/\pi]$ has dimension at most 1, since the unique maximal ideal $\mathfrak{m} \subset R$ is no longer a prime ideal in the localisation. If $R[1/\pi]$ has dimension 0, then it is a field, so a fortiori a PID.

Now $R[1/\pi]$ is a dimension 1 UFD, so we claim that every prime ideal is principal. Let $\mathfrak{p}$ be a prime ideal. Then we may find $a \in \mathfrak{p}$ which is an irreducible element by repeatedly reducing any element. Since we are in a UFD, (a) is a prime ideal, so we have a chain $0 \subsetneq (a) \subset \mathfrak{p}$. Since $R[1/\pi]$ has dimension 1, we must have $(a) = \mathfrak{p}$, so every prime ideal is principal.

We claim that this is sufficient to prove that every ideal of $R[1/\pi]$ is principal. Otherwise, consider the set S of nonprincipal ideals in $R[1/\pi]$. For some ascending (by inclusion) chain $\{\mathfrak{a}_i\} \in S$, the ideal $\mathfrak{a} = \bigcup \mathfrak{a}_i$ is an upper bound of this chain. If $\mathfrak{a} \notin S$, then $\mathfrak{a}$ is principal. Let $\mathfrak{a} = (x)$. Then $x \in \mathfrak{a}_i$ for some i, and hence $\mathfrak{a} = (x) = \mathfrak{a}_i \subset \mathfrak{a}$. But this implies that a principal ideal is in S, which is not possible. Therefore $\mathfrak{a}$ is not principal, so applying Zorn's lemma we let $\mathfrak{b}$ be a maximal element of S.

Since $\mathfrak{b}$ is not principal, in particular it is not prime. Therefore there exists $a, b \notin \mathfrak{b}$ so that $ab \in \mathfrak{b}$. Let $\mathfrak{b}_a = \mathfrak{b} + (a)$ and $\mathfrak{b}_b = \mathfrak{b} + (b)$. Since $\mathfrak{b} \subsetneq \mathfrak{b}_a, \mathfrak{b}_b$, these ideals are not in S, so they are principal. Let $\mathfrak{b}_a = (\alpha)$. Examine the quotient ideal

$$\mathfrak{k} = (\mathfrak{b} : \mathfrak{b}_a) := \{x \in R[1/\pi] : x\mathfrak{b}_a \subset \mathfrak{b}\}.$$

We claim that $\mathfrak{b} = \mathfrak{b}_a\mathfrak{k}$. Clearly we have $\mathfrak{b}_a\mathfrak{k} \subset \mathfrak{b}$. Conversely, suppose that $x \in \mathfrak{b}$. Then we can write $x = y\alpha$. But then $(x) = (y\alpha) = y\mathfrak{b}_a \subset \mathfrak{b}$, so $y \in \mathfrak{k}$, so $x \in \mathfrak{b}_a\mathfrak{k}$.

Now we finally note that $\mathfrak{k} \subset \mathfrak{b}_b$. If $x \in (a), y \in (b)$, then for $z, z' \in \mathfrak{b}$ we have

$$(z + x)(z' + y) = zz' + zx + z'y + xy \in \mathfrak{b}.$$

Therefore $\mathfrak{k} \notin S$, so $\mathfrak{k} = (\beta)$ for some β. Hence $\mathfrak{b} = (\alpha)(\beta) = (\alpha\beta)$, a contradiction. Therefore S must be empty, so $R[1/\pi]$ is a PID. □

Problem 4.
Let p be a prime. Prove that the nilradical of the ring $\mathbb{F}_p[X] \otimes_{\mathbb{F}_p[X^p]} \mathbb{F}_p[X]$ is a principal ideal.

Solution.
We claim that the nilradical is generated by $X \otimes 1 - 1 \otimes X$. Let $\mathfrak{n} = (X \otimes 1 - 1 \otimes X)$. Then first, we see

$$(X \otimes 1 - 1 \otimes X)^p = X^p \otimes 1 - 1 \otimes X^p = 0$$

since the lower degree terms are zero in characteristic p and we may move X^p over the tensor product, so $\mathfrak{n}$ is contained in the nilradical N.

Now we use the property that R/N has no nontrivial nilpotents. We examine $R/\mathfrak{n}$. Since we are modding out by the relation $X \otimes 1 = 1 \otimes X$, we may move X across the tensor product freely. That is,

$$R/\mathfrak{n} \cong \mathbb{F}_p[X] \otimes_{\mathbb{F}_p[X]} \mathbb{F}_p[X].$$

But this is isomorphic to $\mathbb{F}_p[X]$ alone, which is a domain, so has no nontrivial nilpotents. Hence $\mathfrak{n} = N$, so N is principal. □

Problem 5.
Let $\mathbb{F}$ be a finite field and let $\bar{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$. Let K be a subfield of $\bar{\mathbb{F}}$ generated by all roots of unity over $\mathbb{F}$. Show that any simple K-algebra of finite dimension over K is isomorphic to the matrix algebra $M_n(K)$ for a positive integer n.

Solution.
By the Artin-Wedderburn theorem, a simple K-algebra of finite dimension of isomorphic to some matrix algebra $M_n(D)$ for a division algebra D/K of finite dimension. Therefore it suffices to show that $D = K$.

We claim that, in fact, $K = \bar{\mathbb{F}}$. Let $\bar{\mathbb{F}}/L/\mathbb{F}$ be an algebraic extension. Then fine $\mathbb{F}/\mathbb{F}_p$ is a finite extension over its prime field, we have $L/\mathbb{F}_p$ is an algebraic extension, so $L \cong \mathbb{F}_{p^n}$ for some $n \in \mathbb{N}$. Then every element of L satisfies the equation $X^{p^n} - X = 0$, and all nonzero elements satisfy $X^{p^n-1} = 1$. Therefore the elements of L are $p^n - 1$th roots of unity, so $L \subset K$. Therefore K contains all algebraic extensions of $\mathbb{F}_p$, so it contains all algebraic extensions of $\mathbb{F}$, and therefore $K = \bar{\mathbb{F}}$. Therefore there does not exist a nontrivial division algebra over $K = \bar{\mathbb{F}}$, so every simple K-algebra must be isomorphic to $M_n(K)$ for some $n > 0$. □

Problem 6.
Let R be a commutative ring and let M be a finitely generated R-module. Let $f : M \to M$ be R-linear such that $f \otimes \mathrm{id} : M \otimes_R R[T] \to M \otimes_R R[T]$ is surjective. Prove that f is an isomorphism.

Solution.
We have an exact sequence

$$0 \to \ker f \to M \xrightarrow{f} \operatorname{im} f \to 0.$$

Applying the tensor $- \otimes_R R[T]$ is right exact, so we have an exact sequence

$$M \otimes_R R[T] \xrightarrow{f \otimes \mathrm{id}} \operatorname{im} f \otimes_R R[T] \to 0$$

Therefore f is surjective. We need to prove that f is also injective. We claim that any surjective map $f : M \to M$ for a finitely generated module is also injective.

Let $A = \operatorname{End}_R M$, the endomorphism ring over which M is also a module, and consider the left ideal $\mathfrak{a} = (f) \subset A$. Then $\mathfrak{a}M = M$ since f is surjective. Then by Nakayama's lemma, there exists $g \in A$ so that $gM = 0$ and $g \equiv 1_M \mod \mathfrak{a}$. Therefore

$$g(m) = 0 \implies m + f(m) \cdot h(m) = 0$$

for some $h \in A$. Suppose that $f(m) = 0$. Then we must have $m = 0$ as well, so f is injective. Therefore f is an isomorphism. □

Problem 7.
Let $\mathcal{C}$ be the category of semi-symplectic topological quantum paramonoids of Rice-Paddy type, satisfying the Mussolini-Rostropovich equations at infinity. Let X, Y be objects of $\mathcal{C}$ such that the functors $\mathrm{Mor}_{\mathcal{C}}(X, -), \mathrm{Mor}_{\mathcal{C}}(Y, -)$ are isomorphic as covariant functors from $\mathcal{C}$ to **Sets**. Show that X and Y are isomorphic in $\mathcal{C}$.

Solution.
We know by Yoneda's lemma that the natural transformations between F and h^A, the covariant functor represented by A, is isomorphic to $F(A)$. In our case, we have a natural transformation $\alpha : h^X \xrightarrow{\sim} h^Y$, so there is a corresponding natural map in $f \in h^Y(X) = \mathrm{Mor}_{\mathcal{C}}(Y, X)$. We claim that this map is the desired isomorphism.

Let $\alpha^{-1} : h^Y \xrightarrow{\sim} h^X$ be the inverse of α. This corresponds to a map $g : X \to Y$, and we claim $f \circ g = \mathrm{id}_X$. But since $\alpha^{-1} \circ \alpha = \mathrm{id}_{h^X}$, and id_{h^X} must correspond to the identity map 1_X, we are done. □

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

Solution.
First, by Eisenstein's criterion, this polynomial $f(X)$ is irreducible. For a root α of $f(X)$, we know $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, so $5 \mid |\Gamma|$. Therefore Γ contains an element of order 5, which must be a 5-cycle since $\Gamma \subset S_5$.

Now we claim Γ contains a transposition. If so, by the well-known fact that S_p is generated by a p-cycle and any transposition, $\Gamma = S_5$. To prove the claim, first note that $f(X)$ has one real root. We claim that it has exactly three real roots. We see $f'(X) = 5X^4 - 9$, which has real roots at $\pm\sqrt[4]{9/5}$ only. Therefore the graph of $f(X)$ crosses the X-axis at most thrice, and indeed by the intermediate value theorem we can check that it crosses the X-axis precisely three times. Therefore a valid permutation of the roots is complex conjugation, which is a transposition in Γ because there are only two complex roots. This completes the proof. □

Problem 9.
(a) Is there a group G with $\mathbb{C}[G]$ isomorphic to $\mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$?

(b) Is there a group G with $\mathbb{Q}[G]$ isomorphic to $\mathbb{Q} \times \mathbb{Q} \times M_3(\mathbb{Q})$?

Solution.
We use throughout the Artin-Wedderburn theorem since group algebras of finite groups by fields of characteristic zero are semisimple. Further, we know that $\dim \mathbb{C}[G] = |G|$, and the number of factors is equal to the number of conjugacy classes.

(a) Since $\dim \mathbb{C}[G] = 6$, we need a group of order 6 with three conjugacy classes. The group $G \cong D_6 = S_3$ works, because the three conjugacy classes are the three cycle types.

(b) Since $\dim \mathbb{Q}[G] = 11$, we must have $G = \mathbb{Z}/11\mathbb{Z}$. But this group has 11 conjugacy classes, so we cannot have a decomposition as above. Therefore no such group exists.

□

Problem 10.
Let K/k be an extension of finite fields. Show that the norm $N_{K/k} : K \to k$ is surjective.

Solution.
Let $\operatorname{char} K = p$. Recall that

$$N_{K/k}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha).$$

Let $[K : k] = n$. Then in particular, $\mathrm{Gal}(K/k) \cong \mathbb{Z}/n\mathbb{Z}$, and it is generated by the Frobenius map $\varphi(a) = a^q$, where $q = |k|$. Therefore in general,

$$N_{K/k}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha) = \alpha \cdot \varphi(\alpha) \cdots \varphi^{n-1}(\alpha) = \alpha^{1+q+\cdots+q^{n-1}}$$

Let β be a generator of $K^\times$. Then we claim that $N_{K/k}(\beta)$ generates $k^\times$. We see that

$$N_{K/k}(\beta)^{q-1} = (\beta^{1+q+\cdots+q^{n-1}})^{q-1} = \beta^{q^n-1} = 1.$$

In words, since β has order $q^n - 1$, $\beta^{1+q+\cdots+q^{n-1}}$ has order $q^n - 1/(1 + q + \cdots + q^{n-1}) = q - 1$. Therefore this element generates $k^\times$, so in particular the norm map is surjective. □

7 Spring 2011

Problem 1.
Let G be a group of order n. Show that there are two subgroups H_1 and H_2 of the symmetric group S_n, both isomorphic to G such that $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$.

Solution.
Consider the action on G on itself by left multiplication. Since this action is faithful, we have an injection of G into S_n, so we may identify $G \cong H_1 \subset S_n$. Similarly, the action of G on itself by right multiplication, which must be given by $g \cdot x = xg^{-1}$, is also faithful and yields an embedding onto $H_2 \subset S_n$. We claim that these subgroups of S_n commute.

Indeed, given $x \in G$, we have $h_1h_2 \cdot g = h_2h_1 \cdot g$, since (if we identity group elements in G with group elements in S_n) we have $h_1(gh_2^{-1}) = (h_1g)h_2^{-1}$ by associativity of group multiplication. Therefore these elements commute in S_n, so we are done. □

Problem 2.
Let G be a finitely generated group. Show that G contains only finitely many subgroups of any fixed finite index.

Solution.
Let $G = \langle g_1, \ldots, g_n \rangle$, and let $m > 0$ be a positive integer. Let H be a subgroup of index m. Then G acts on the set of cosets G/H by left multiplication, which induces a group homomorphism $\varphi : G \to S_m$. We can realise H as the set $\{g \in G : \varphi(g) \cdot H = H\}$. Therefore any choice of H produces a unique $\varphi : G \to S_m$. Since G is generated by n elements, there are at most $n \cdot |S_m|$ homomorphisms $G \to S_m$. Therefore there are at most $n \cdot |S_m| < \infty$ subgroups of index m. □

Problem 3.
Let R be a Noetherian domain. Show that every nonzero nonunit in R is a product of irreducible elements and that R is a UFD if and only if every nonzero nonunit in R is a product of prime elements, where an element is prime if it generates a nonzero prime ideal.

Solution.
Let $S \subset R$ be the family of the principal ideals of elements without an irreducible factorisation. If this family is nonempty, then since R is Noetherian it contains a maximal element (a). Since a does not have an irreducible factorisation, it itself is not irreducible, so we may write $a = bc$ for some $b, c \in R \setminus R^\times$. As such, $(a) \subsetneq (b)$. Therefore $(b) \notin S$, so b has a factorisation into irreducible elements $p_1 \cdots p_n$. Similarly, $(a) \subsetneq (c)$, so $c = q_1 \cdots q_m$. Therefore $a = bc = p_1 \cdots p_n \cdot q_1 \cdots q_m$ is a factorisation of a into irreducible elements, hence S is empty.

Suppose that R is a UFD, so that this factorisation is unique. Then we claim that, in fact, every irreducible element is prime. Indeed, let x be an irreducible element, and let $\mathfrak{p} = (x)$. Then suppose that $\bar{y}, \bar{z} \in R/\mathfrak{p}$, where $y, z \in R$, satisfy $\bar{y}\bar{z} = 0$. Then $yz \in (x)$, which implies that $yz = xa$ for some $a \in R$. Therefore the unique irreducible factorisation (up to association) of yz contains x, so the unique irreducible factorisation of either y or z contains x, which implies that y or z is an element in (x). Hence $\bar{y}$ or $\bar{z} = 0$, so $R/\mathfrak{p}$ is a domain. Therefore (x) is prime, so x is a prime element. As such, since every element of R has a factorisation into irreducible elements, and each of these elements is prime, then every element of R has a factorisation into prime elements.

Conversely, let $x = p_1 \cdots p_n$ be a factorisation of x into prime elements, and let $x = q_1 \cdots q_m$ be a factorisation into irreducible elements. Then since $p_1 \mid q_1 \cdots q_m$, we have $p_1 \mid q_i$ for some i, and with reordering we may assume $i = 1$. Therefore write $q_1 = p_1 a_1$. Since q_1 was irreducible, we must have $a_1 \in R^\times$. Since we are in a domain, we may cancel the term p_1 from both sides to obtain

$$p_2 \cdots p_n = q_2 \cdots q_m \cdot a_1.$$

Continuing this process, we obtain

$$1 = q_{m-n} \cdots q_n \cdot a_1 \cdots a_n.$$

Hence we must have $m = n$. Therefore the two factorisations above were the same up to rearrangement and association, which implies that R is a UFD. □

Problem 4.
Prove that every prime ideal in $\mathbb{Z}[t]$ can be generated by two elements.

Solution.
Let $\mathfrak{p} \in \mathbb{Z}[t]$ be a prime ideal. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, since $(\mathbb{Z}[t]/\mathfrak{p}) \cap \mathbb{Z} = \mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$. Therefore $\mathfrak{p} \cap \mathbb{Z}$ is a principal ideal, either 0 or $p\mathbb{Z}$ for p a prime element.

Suppose that $\mathfrak{p} \cap \mathbb{Z} = 0$. Then we claim that $\mathfrak{p}$ is principal in $\mathbb{Z}[t]$. Let $f \in \mathfrak{p}$ be a polynomial of minimal degree in $\mathfrak{p}$, which by assumption has $\deg f > 0$ since $\mathfrak{p}$ contains no constant terms. Write $f = c(f)f'$, where f' is a primitive polynomial. Then since $\mathfrak{p}$ is prime, either $c(f) \in \mathfrak{p}$ or $f' \in \mathfrak{p}$, but $c(f) \notin \mathfrak{p}$ since $c(f) \in \mathbb{Z}$. Hence f' is a primitive polynomial in $\mathfrak{p}$ of minimal degree. We claim that $\mathfrak{p} = (f')$. Let $g \in \mathfrak{p}$. Suppose that $f' \nmid g$. Then

the greatest common divisor of f' and g would have degree less than that of f' (since f' is primitive). By the Euclidean algorithm we may realise $\gcd(f', g)$ as a linear combination of f' and g, so $\gcd(f', g) \in \mathfrak{p}$, which contradicts the minimality of f'. Hence $f' \mid g$, so $(f') = \mathfrak{p}$.

Now suppose that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Consider the image of $\mathfrak{p}$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Then $\overline{\mathfrak{p}}$ is a principal ideal, so write $\overline{\mathfrak{p}} = \bar{f} \cdot \mathbb{Z}/p\mathbb{Z}[X]$. If we let f be a polynomial lying over $\bar{f}$ in $\mathfrak{p}$, then we have $f = \bar{f} + g(X)$, for $g(X) \in p\mathbb{Z}[X]$. But since $p \in \mathfrak{p}$, $g(X) \in \mathfrak{p}$, so in fact the same $\bar{f}$ lies in $\mathfrak{p}$, which we rename f' to avoid confusion.

We claim that $\mathfrak{p} = (p, f')$. Certainly $(p, f') \subset \mathfrak{p}$. Let $g \in \mathfrak{p}$, and examine $\bar{g}$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Since $\bar{g} \in \overline{\mathfrak{p}}$, we have $\bar{g} = \bar{h} \cdot f'$, where $\bar{h}$ is a polynomial in $\mathbb{Z}/p\mathbb{Z}[X]$. Then moving back to preimages, let $h = \bar{h} + h'$ and $g = \bar{g} + g'$ for $g', h' \in p\mathbb{Z}[X]$. Then we have

$$g = (\bar{h} + h')f' + g' \in (f') + (p) = (p, f')$$

which proves our claim. □

Problem 5.
Let F be a field having no nontrivial field extensions of odd degree and K/F a finite field extension. Show if K has no field extensions of degree two, then F is perfect and K is algebraically closed.

Solution.
Suppose that F is not perfect, and let E/F be an extension. Then in particular, let $\alpha \in E$ be an inseparable element so that $F(\alpha)/F$ is a purely inseparable extension. Then $[F(\alpha) : F] = p^n$ for some $n \geq 0$. Suppose p is odd. Then we must have $[F(\alpha) : F] = 1$ since every extension of odd degree is trivial. Therefore $\alpha \in F$. Since this is true for any α, E/F is a separable extension, so F is perfect.

If $p = 2$, then the case is somewhat different. We claim that K is a perfect field. Let L/K be a finite extension, and let $\alpha \in L$ be an inseparable element not in K. Then $[K(\alpha) : K] = 2^n$ for some $n > 0$, where the minimal polynomial of α is $X^{2^n} - \alpha^{2^n}$. Hence the degree of $\alpha^{2^{n-1}}$ is 2, so $\alpha^{2^{n-1}} \in K$, which is a contradiction. Hence L/K is separable, so K is perfect.

We claim that any finite subextension of a perfect field is perfect. We prove this in general. Let K/F be a finite extension, where K is perfect and $\operatorname{char} K = p$. Then let $\alpha \in K$ be an inseparable element. Choose n minimal so that $\alpha^{p^n} \in F$, so $[F(\alpha) : F] = p^n$, and assume $n > 1$. Since K is perfect, $K^p = K$, so let $\beta \in K$ so that $\beta^p = \alpha$. Hence $\beta^{p^{n+1}} \in F$, so $[F(\beta) : F] = p^{n+1}$. Continuing this process, we can create arbitrarily large subextensions of K over F, so K/F is infinite, a contradiction. Hence we must have $\alpha \in F$, so K/F is a separable extension. Suppose now that L/F is a finite field extension. Then if $K/L/F$, we have L/F is separable since K/F is separable. If $L/K/F$, we have L/K is separable since K is perfect, so L/F must be separable since each subextension is separable. Therefore F is perfect.

Therefore let E/K be a finite field extension and L be its normal closure over F. Then L/F is Galois. Let G be the Galois group of L/F, and write $|G| = 2^n m$, where m is odd. By Galois correspondence, there exists a field of degree m over F, which by assumption must be trivial. Hence $m = 1$, so G is a 2-group. By the general theory of p-groups, the subgroups of G are nested with orders consecutive powers of 2. In particular, let $H \subset G$ be the subgroup

corresponding to K/F. Then there is a subgroup $H' \supset H$ corresponding to a field M/K of degree 2. But K has no field extensions of degree 2, so no such H' can exist, which implies that $G = H$. Hence this collapses $L = K$, so in particular $E = K$. Hence K has no finite extensions, therefore it has no algebraic extensions, so it is algebraically closed. □

Problem 6.
Prove that over a finite field there are irreducible polynomials of any positive degree.

Solution.
Let $\mathbb{F}_q$ be a finite field, where $q = p^n$. Then for any positive integer m there is a finite field of order $q^m = p^{nm}$, and $\mathbb{F}_p \subset \mathbb{F}_q \subset \mathbb{F}_{q^m}$ is a tower of field extensions. Therefore $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$. Further, since $(\mathbb{F}_{q^m})^\times$ is cyclic with some generator α, we have $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Therefore we have $m = [\mathbb{F}_{q^m} : \mathbb{F}_q] = \deg m_\alpha$, the minimal (irreducible) polynomial of α. Therefore there is an irreducible polynomial of degree m for any $m > 0$. □

Problem 7.
Let $T : V \to V$ be a linear operator on a finite dimensional vector space. Prove that the characteristic polynomial p_T is irreducible if and only if T has no nontrivial invariant subspaces.

Solution.
Suppose that p_T is irreducible. Then p_T is also the minimal polynomial of T, so we have

$$V \cong F[X]/(p_T).$$

Since (p_T) is a prime ideal in a PID, it is also a maximal ideal, so V is actually a field. Since an invariant subspace of T corresponds to a ideal of V, no nontrivial example exists.

Conversely, suppose that T has no nontrivial invariant subspaces. Then there must be only one invariant factor. Otherwise, the Jordan normal form would have multiple blocks, which correspond to invariant subspaces. In particular, the characteristic polynomial is the minimal polynomial of T. Now, if the minimal polynomial of T were reducible, then there would be an invariant subspace corresponding to an irreducible factor of it, which by assumption does not exist. Hence p_T is irreducible as well. □

Problem 8.
Let V be a finite dimensional vector space over a field F. Prove that every right ideal in $\mathrm{End}_F(V)$ is of the form $\{T : \mathrm{im}\, T \subset W\}$ for a unique subspace W of V.

Solution.
Let $\mathfrak{a} \subset \mathrm{End}_F(V)$ be a right ideal. Let $T \in \mathfrak{a}$ be an endomorphism of maximal rank. Then we claim that for all $S \in \mathfrak{a}$, $\mathrm{im}\, S \subset \mathrm{im}\, T$. Let $V = \ker T \oplus U$ be an orthogonal decomposition. Then $T : U \to \mathrm{im}\, T$ is an isomorphism. Therefore we can invert T on $\mathrm{im}\, T$ via $Q \in \mathrm{End}_F(V)$ so that $Q(v) = T^{-1}(v)$ if $v \in \mathrm{im}\, T$ and $Q(v) = 0$ if $v \in \ker T$ and linear extension to the rest of V. Since $\mathfrak{a}$ is a right ideal, $T \circ Q \in \mathfrak{a}$, and this is an isomorphism from $\mathrm{im}\, T$ to itself.

Let $S \in \mathfrak{a}$ and suppose that $S(v) = w \notin \operatorname{im} T$ for some $v \in V$. Let $R \in \operatorname{End}_F(V)$ so that $R(u) = v$ for some $v \in \ker T$ and $R \equiv 0$ outside of the span of u. Then $S \circ R \in \mathfrak{a}$, so the map $T \circ Q + S \circ R \in \mathfrak{a}$. Then

$$(T \circ Q + S \circ R)(u) = 0 + S(v) = w.$$

Further, since $S \circ R \equiv 0$ on $\operatorname{im} T$ and $T \circ Q : \operatorname{im} T \xrightarrow{\sim} \operatorname{im} T$ is an isomorphism, the rank of $T \circ Q + S \circ R$ is strictly larger than the rank of T. But this is a contradiction. Therefore $\operatorname{im} S \subset \operatorname{im} T$.

Let $W = \operatorname{im} T$. Then we claim that $\mathfrak{a} = \{S \in \operatorname{End}_F(V) : \operatorname{im} S \subset W\}$. The inclusion $\subset$ is proven above. Now, let $S \in \operatorname{End}_F(V)$ so that $\operatorname{im} S \subset W$. Let $T_S \in \operatorname{End}_F(V)$ so that $T_S(v) = T^{-1}(S(v))$, which is sensible since $S(v) \in \operatorname{im} T$. Then $T \circ T_S = S$, and since $T \circ T_S \in \mathfrak{a}$, we have $S \in \mathfrak{a}$. This completes the proof.

□

Problem 9.
Let G be a finite group of invertible linear operators on a finite dimensional vector space V over the field of complex numbers. Prove that if $(\dim V)^2 > |G|$, then there is a proper nonzero subspace $W \subset V$ such that $g(w) \in W$ for every $g \in G$ and every $w \in W$.

Solution.
By the Artin-Wedderburn theorem, we know that $\mathbb{C}[G] = \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C})$, where $\sum_{i=1}^{r} n_i^2 = |G|$. We would like to show that every vector space V as above cannot be irreducible, that is, cannot be a simple $\mathbb{C}[G]$-module. Indeed, simple $\mathbb{C}[G]$-modules correspond precisely to simple modules over one of the matrix algebras in the direct sum decomposition of $\mathbb{C}[G]$, and these are only $\mathbb{C}^{n_i}$. Therefore suppose $\dim V = n$. If it is simple, it must be a simple module over the matrix algebra $M_n(\mathbb{C})$. But then $n^2 > |G|$, which contradicts the above equality from Artin-Wedderburn. Hence no such V is irreducible, so it has a subspace as above, and we are done. □

Problem 10.
Show that there is a (covariant) functor from the category of groups to the category of sets taking a group G to the set of all subgroups of G. Determine whether this functor is representable.

Solution.
Let F : **Groups** $\to$ **Sets** be that functor. We need to examine how F acts on group homomorphisms $f : G \to H$. We let $F(f) : F(G) \to F(H)$ send the set of subgroups $\{G_1, \ldots, G_n\}$ to $\{f(G_1), \ldots, f(G_n)\}$, where we delete any repeated elements. Since the image of a subgroup is a subgroup, this set of images of subgroups of G is a subset of the subgroups of H.

Let 1_G be the identity map on G. Then $\{G_1, \ldots, G_n\}$ is mapped to itself under 1_G, so $F(1_G) = 1_{F(G)}$. Further, if $f : G \to H$ and $g : H \to K$ are two homomorphisms, we have

$$\{G_1, \ldots, G_n\} \overset{F(f)}{\mapsto} \{f(G_1), \ldots, f(G_n)\} \overset{F(g)}{\mapsto} \{g(f(G_1)), \ldots, g(f(G_n)\}$$
$$\overset{F(g \circ f)}{\mapsto} \{(g \circ f)(G_1), \ldots, (g \circ f)(G_n)\}.$$

Since these sets are the same (up to deleting repeats), we have $F(g \circ f) = F(g) \circ F(f)$. Therefore F is a functor.

However F is not representable. Suppose that $F = \mathrm{Hom}(X, -)$ for a group X. Then in particular,

$$2 = |F(\mathbb{Z}/3\mathbb{Z})| = |\mathrm{Hom}(X, \mathbb{Z}/3\mathbb{Z})|.$$

Let $\varphi \in \mathrm{Hom}(X, \mathbb{Z}/3\mathbb{Z})$ be the nontrivial homomorphism. Let $\psi \in \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ be the nontrivial automorphism $1 \mapsto 2$. Then $\psi \circ \varphi$ is another nontrivial homomorphism in $\mathrm{Hom}(X, \mathbb{Z}/3\mathbb{Z})$, so $|\mathrm{Hom}(X, \mathbb{Z}/3\mathbb{Z})| > 2$, which is a contradiction. Therefore F is not representable. □

8 Fall 2010

Problem 1.
Let **Group** be the category of groups and **Ab** be the category of abelian groups. If F : **Ab** $\to$ **Group** is the inclusion of categories, then find a left adjoint to F and prove that it is a left adjoint.

Solution.
We claim that the left adjoint to F is G : **Group** $\to$ **Ab** so that $G(X) = X/[X, X]$, the abelianisation of the group X. G would need to satisfy, for all groups X and abelian groups Y,

$$\mathrm{Hom}_{\mathbf{Ab}}(G(X), Y) = \mathrm{Hom}_{\mathbf{Group}}(X, F(Y)).$$

Since both sets are group homomorphisms, we will suppress the subscript on Hom. First, we look at any homomorphism φ from an arbitrary group X into an abelian group Y. Then

$$\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = e_Y$$

for every element $ghg^{-1}h^{-1} \in [X, X]$. Therefore φ factors through $[X, X]$, so it descends to a homomorphism $\bar{\varphi} : X/[X, X] \to Y$. Conversely, given a homomorphism $\psi : X/[X, X[\to Y$, we can define a homomorphism $\hat{\psi} : X \to Y$ by $\hat{\psi}(g) = \psi(g[X, X])$. This is well defined since

$$\psi(g \cdot hkh^{-1}k^{-1}) = \psi(g)\psi(h)\psi(k)\psi(h)^{-1}\psi(k)^{-1} = \psi(g \cdot 1),$$

so $\hat{\psi}$ does not depend on the choice of coset representative. Therefore these Hom-sets are equal, so G is the left adjoint to F. □

Problem 2.
Let $F : \mathcal{C} \to$ **Sets** be a covariant functor on a category $\mathcal{C}$. Assume that F is representable by an object $C_F \in \mathrm{Obj}(\mathcal{C})$. Identity which of the following statements are necessarily correct, proving your answers in each case.

(a) If $C \in \mathrm{Obj}(\mathcal{C})$ and $F(C) \neq \emptyset$, then there is an element $f \in \mathrm{Mor}_{\mathcal{C}}(C_F, C)$;

(b) If G is a left adjoint of F, then G is representable;

(c) If $C, D \in \mathrm{Obj}(\mathcal{C})$, and there is a map of sets $f : F(C) \to F(D)$, then there exists a $g \in \mathrm{Mor}_{\mathcal{C}}(C, D)$;

(d) If $C, D \in \mathrm{Obj}(\mathcal{C})$, and there exists a map $g \in \mathrm{Mor}_{\mathcal{C}}(C, D)$, then there exists a map of sets $f : F(C) \to F(D)$ (note that we are not guaranteed in advance that $F(D) \neq \emptyset$);

(e) If $h \in \mathrm{Mor}_{\mathcal{C}}(D, C_F)$, then for any $C \in \mathrm{Obj}(\mathcal{C})$, there is a map of sets $F(C) \to \mathrm{Mor}_{\mathcal{C}}(D, C)$.

Solution.
Throughout, we suppress $\mathcal{C}$ when it is obvious.

(a) We know that $\mathrm{Mor}_{\mathcal{C}}(C_F, C) = F(C)$, and since $F(C) \neq \emptyset$, there is an f corresponding to some element in $F(C)$.

(b) If G is left adjoint of F, then $G : \mathbf{Sets} \to \mathcal{C}$. Therefore if $\mathcal{C} \not\subset \mathbf{Sets}$, it makes no sense to talk about representing the functor G. Hence G is not necessarily representable.

(c) This is not necessarily true. Let $\mathcal{C}$ be the category of unital rings. Then consider the rings $\mathbb{R}$ and $\mathbb{Q}$. Suppose $\varphi : \mathbb{R} \to \mathbb{Q}$ is a ring homomorphism. Then we must have $\varphi(\sqrt{2})^2 = 2$, but there is no square root of 2 in $\mathbb{Q}$. Therefore there are no ring homomorphisms from $\mathbb{R}$ to $\mathbb{Q}$. Now consider the functor $F : \mathbf{Ring} \to \mathbf{Sets}$ that sends a ring to its set of units. This functor is representable by $\mathbb{Z}[X, X^{-1}]$. Since $F(\mathbb{R}), F(\mathbb{Q}) \neq \emptyset$, there is a map $F(\mathbb{R}) \to F(\mathbb{Q})$. But there is no corresponding map in **Ring** to this map.

(d) This is false if and only if we can construct this situation so that $F(C) \neq \emptyset$ and $F(D) = \emptyset$, since there is always a map into any nonempty set and from the empty set. Therefore suppose that $F(C) \neq \emptyset$. Then there exists a map $f \in \mathrm{Mor}(C_F, C)$. Then $g \circ f \in \mathrm{Mor}(C_F, D)$, and there exists an element in $F(D)$, so the situation never occurs. Therefore there is always a map $F(C) \to F(D)$.

(e) If we identify $F(C) = \mathrm{Mor}(C_F, C)$ we are looking for a set map from $\mathrm{Mor}(C_F, C) \to \mathrm{Mor}(D, C)$. If $f : C_F \to C$, then $f \circ h : D \to C$. so we indeed have a set map via $- \circ h$. We can construct the actual map $F(C) \to \mathrm{Mor}(D, C)$ via the natural isomorphism.

□

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

Solution.
Let G be a simple group of order 120. Examine the Sylow 5-subgroups of G. We have $n_5 \equiv 1 \mod 5$ and $n_5 \mid 24$. By assumption, $n_5 \neq 1$ so we see $n_5 = 6$. Let G act on its set of Sylow 5-subgroups by conjugation. This induces a homomorphism $\varphi : G \to S_6$. Since G is simple, we know that $\ker \varphi$ is either $\{e\}$ or G itself. Clearly $\ker \varphi \neq G$ since the Sylow subgroups are conjugate. Therefore $\varphi : G \hookrightarrow S_6$.

Suppose that $G \subset A_6$. Then there is an action of A_6 on A_6/G, which is a three element set. Since A_6 is also simple, the induced action $\psi : A_6 \to S_3$ is injective, which is a contradiction since $|A_6| > |S_3|$. Therefore if G is not a subset of A_6, then consider $G \cap A_6$. This intersection is nontrivial since the product of any two odd permutations is even, so lands inside A_6. Therefore since $A_6 \triangleleft S_6$, $A_6 \cap G \triangleleft G$. But this implies that G is not simple. Therefore no such group exists. □

Problem 4.

(a) Show from first principles (i.e. without using the classification theorem) that a subgroup of a finitely generated abelian group is finitely generated.

(b) Let $M \subset \mathbb{Z}^3$ be the subgroup generated by the elements $(13, 9, 2), (29, 21, 5)$, and $(2, 2, 2)$. Determine the isomorphism class of the quotient group $\mathbb{Z}^3/M$.

Solution.

(a) See Fall 2009, Problem 3. I did that one before this one, and the result there is stronger anyway.

(b) This question is equivalent to reducing the matrix

$$\begin{pmatrix} 13 & 9 & 2 \\ 29 & 21 & 5 \\ 2 & 2 & 2 \end{pmatrix}$$

via row and column operations. Painstakingly, one can verify that we obtain

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 16 \end{pmatrix}.$$

This corresponds to the quotient $\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \cong \mathbb{Z}/16\mathbb{Z}$.

□

Problem 5.

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

Solution.

Consider the set X in $G \times S$ where $(g, s) \in X$ if $g(s) = s$. Then we see

$$|X| = \sum_{g \in G} |\{s \in S : g(s) = s\}| = \sum_{s \in S} |\{g \in G : g(s) = s\}|.$$

The first sum is the quantity with which we are concerned. The second quantity is the stabiliser of s, denoted G_s, so we have

$$|X| = \sum_{s \in S} |G_s| = \sum_{s \in S} \frac{|G|}{|Gs|}$$

where Gs is the orbit of s by the orbit-stabiliser theorem. Since this action is transitive, we have $|Gs| = |S|$. Hence

$$\sum_{g \in G} |\{s \in S : g(s) = s\}| = \sum_{s \in S} \frac{|G|}{|S|} = |G|.$$

Let the sets on the left be denoted X_g. We know that $|X_e| \geq 2$ since $e(s) = s$ for all $s \in S$. Therefore if $|X_g| > 0$ for all $g \in G$, we have

$$\sum_{g \in G} |\{s \in S : g(s) = s\}| \geq 1 + |G| > |G|,$$

a contradiction. Hence some $g \in G$ has $X_g = \emptyset$, as required. □

Problem 6.
Let R be the 5-dimensional tautological representation of S_5. Show that R is isomorphic to the direct sum of the trivial representation and an irreducible 4-dimensional representation.

Solution.
First, let R take e_1, e_2, e_3, e_4, e_5 as a basis, where S_5 acts on R by permuting these basis elements. We see that the subspace spanned by $e_1 + e_2 + e_3 + e_4 + e_5$ is S_5-invariant (since its generator is), so it is corresponds to a 1-dimensional representation of S_5, which must be isomorphic to the trivial representation.

Let W denote this subrepresentation of R, generated by the vector $w = e_1+e_2+e_3+e_4+e_5$. Then consider $R = W \oplus W^\perp$. We claim that $W^\perp$ is also irreducible. To see this, let $v = (v_i) \in W^\perp$ be a nonzero vector. Then since $\langle v, w \rangle = 0$, we have $\sum_{i=1}^5 v_i = 0$. Since $v_i \neq 0$ for some i, we must have $v_i > 0$ and $v_j < 0$ for some $i \neq 0$. Then we have

$$(1\,i)(2\,j) \cdot v \in W^\perp \implies (1\,2)(1\,i)(2\,j) \cdot v - (1\,i)(2\,j) \cdot v = (v_i - v_j, v_j - v_i, 0, 0, 0) \in W^\perp.$$

Normalising, we see that $e_1 - e_2 \in W^\perp$. Applying to this the transpositions $(2\,j)$ for $j = 3, 4, 5$, we see that there are four linearly independent vectors in $W^\perp$, so that $W^\perp$ is generated by any nonzero element, so it is irreducible. This completes the proof. □

Problem 7.
Let k be a field and let f be an irreducible element of the polynomial ring $k[X, Y]$.

(a) Describe the localisation $k[X, Y]_{\mathfrak{p}}$, where $\mathfrak{p} = (f)$. Prove that it is a subring of the rational functions $k(X, Y)$.

(b) For any $r \in k(X, Y)$, prove that

$$r \in \mathrm{im}(k[X, Y]_{\mathfrak{p}} \to k(X, Y))$$

for all but finitely many choices of f.

Solution.

(a) This localisation is, formally, inverting every element not in $\mathfrak{p}$. This means that

$$k[X,Y]_{\mathfrak{p}} = \left\{ \frac{g}{h} : g, h \in k[X,Y], h \notin (f) \text{ i.e. } f \nmid h \right\}.$$

This is clearly contained in $k(X,Y)$. To see that it is a subring, we have

$$\frac{g_1}{h_1} + \frac{g_2}{h_2} = \frac{g_1 h_2 + g_2 h_1}{h_1 h_2}, \ \frac{g_1}{h_1} \cdot \frac{g_2}{h_2} = \frac{g_1 g_2}{h_1 h_2}.$$

The numerator satisfies the conditions above, but $h_1 h_2 \notin (f)$ is not true for general f. However, since f is irreducible and $k[X,Y]$ is a UFD, (f) is a prime ideal, so $h_1 h_2 \in (f)$ if and only if $h_1 \in (f)$ or $h_2 \in (f)$. But since $h_1, h_2 \notin (f)$, we have $h_1 h_2 \notin (f)$, so $k[X,Y]_{\mathfrak{p}}$ is closed under addition and multiplication. Further, $0 \in k[X,Y]_{\mathfrak{p}}$ is represented by $0/1$ and 1 is represented by $1/1$. Hence it is a subring.

(b) We can write r in terms of an irreducible factorisation of its numerator and denominator:

$$r = \frac{g_1 \cdots g_m}{h_1 \cdots h_n}, \ g_i, h_i \in k[X,Y] \text{ irreducible},$$

If r is in the image of this inclusion map, then we must have $h_1 \cdots h_n \notin (f)$. But since (f) is a prime ideal, $h_1 \cdots h_n \notin (f)$ if and only if $h_i \notin (f)$ for all i. But since h_i is an irreducible polynomial, if we have that $h_i = f \cdot p$ implies that $(h_i) = (f)$. Therefore r is in the image of this inclusion if and only if $h_i \not\sim f$ for any i, and since we may move any offending element of $k[X,Y]^\times$ to the numerator of the polynomial, this is equivalent to $h_i \neq f$ for any i. Therefore only finitely many choices of f exclude r from the image of the inclusion map.

□

Problem 8.
Let k be an algebraically closed field, $R = k[X_1, \ldots, X_n]$, and $f : R \to R^d$ be given by $f(p) = (pf_1, \ldots, pf_d)$ with all $f_i \in R$. Let $\mathfrak{m}$ be the ideal generated by $X_1 - a_1, \ldots, X_n - a_n$, where $a_i \in k$ for all i. Consider for an integer $r \geq 1$, the map

$$f_{\mathfrak{m}^r} : R \otimes_R (R/\mathfrak{m}^r) \to R^d \otimes_R (R/\mathfrak{m}^r)$$

induced by f. Prove that $\ker f_{\mathfrak{m}^r} \neq 0$ if and only if $f_j(a_1, \ldots, a_n) = 0$ for all j.

Solution.
We can condense these tensor products to obtain the actual map

$$f_{\mathfrak{m}^r} : R/\mathfrak{m}^r \to (R/\mathfrak{m}^r)^d$$

which sends $\bar{p} \to \bar{p} \cdot f := (\bar{p}f_1, \ldots, \bar{p}f_d)$. If $\bar{p}$ is in the kernel, then $\bar{p} \cdot f_i \in \mathfrak{m}^r$ for each i. If we assume $\bar{p}$ is nonzero, i.e. $\bar{p} \notin \mathfrak{m}^r$, then we must have $f_i \in \mathfrak{m}^s$ for some $s \geq 1$. But this means that $f_i(a_1, \ldots, a_n) = 0$ by definition. Conversely if $\ker f_{\mathfrak{m}^r} = 0$, then we cannot have $f_i \in \mathfrak{m}$ for every i, so $f_i(a_1, \ldots, a_n) \neq 0$ for some i. This completes the proof. □

Problem 9.
Let R be a unital ring. Show that the only two-sided ideals of $M_n(R)$ are of the form $M_n(I)$ for some two-sided ideal in R.

Solution.
First, suppose that $I \subset R$ is a two-sided ideal. Then given two matrices $a \in M_n(I)$ and $b \in M_n(R)$, we have

$$(ab)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Since $a_{ik} \in I$, we know that $a_{ik} b_{kj} \in I$ for all k. Therefore the sum of these elements is also in I, so $ab \in M_n(I)$. An identical argument holds for ba since I is a two-sided ideal. Hence every $M_n(I)$ is a two-sided ideal of $M_n(R)$.

Conversely, let $\mathfrak{a} \subset M_n(R)$ be a two-sided ideal. Let $I \subset R$ be the two-sided ideal generated by the elements of the matrices in $\mathfrak{a}$. Then $\mathfrak{a} \subset M_n(I)$ clearly. Notice that, since $\mathfrak{a}$ is a two-sided ideal, we have for any matrix $a \in \mathfrak{a}$

$$e^{1i} \cdot a \cdot e^{j1} = b \in \mathfrak{a}$$

where e^{kl} is the matrix with 1_R at (k, l) and 0 everywhere else. In particular this matrix b satisfies $b_{11} = a_{ij}$ and $b_{kl} = 0$ everywhere else. By repeating this again, we can find a matrix $c \in \mathfrak{a}$ so that $c_{ij} \in I$ for any element of I and $c_{kl} = 0$ everywhere else. Therefore given any matrix in $M_n(I)$, we can sum up n^2 matrices constructed in this fashion for each of its elements, and since $\mathfrak{a}$ is a two-sided ideal, it will be an element of $\mathfrak{a}$. Therefore $\mathfrak{a} = M_n(I)$, so we are done. □

Problem 10.
Let G be a group and $\mathbb{Z}[G]$ the integral group ring. Multiplication $f \cdot h$ of two elements $f = \sum_i n_i(g_i)$ and $h = \sum_j m_j(g_j)$ is

$$f \cdot h = \sum_{i,j} n_i m_j (g_i g_j).$$

Let I be the two-sided ideal

$$I = \left\{ \sum_i n_i(g_i) : \sum_i n_i = 0 \right\}.$$

Construct a natural map $F : I/I^2 \to G/[G, G]$ and prove that this map is an isomorphism of $\mathbb{Z}$-modules.

Solution.
We construct a map $F : I \to G/[G, G]$ to begin such that

$$F\left(\sum_i n_i(g_i) \right) = \prod_i g_i^{n_i},$$

where we suppress the coset notation for convenience. We see that this is an abelian group homomorphism since

$$F\left(\sum_i n_i(g_i) + \sum_j m_j(g_j)\right) = \prod_i g_i^{n_i} \prod_j g_j^{m_j} = \prod_k g_k^{\ell_k} = F\left(\sum_k \ell_k(g_k)\right)$$

where k parametrises the group elements and $\ell_k = n_k + m_k$. We claim that F is surjective. Consider an element $g \in G$. Then modulo the commutator, we can always represent the coset $g[G,G]$ by

$$g \cdot hk \cdot h^{-1} \cdot k^{-1}.$$

We can construct a preimage of this element, namely $1(g)+1(hk)-1(h)-1(k)$. This element satisfies $\sum_i n_i = 0$, so it is indeed an element of $I \subset \mathbb{Z}[G]$. Hence F is surjective. Note that I is generated by $g-1$ where g ranges over G. Then I^2 is generated by $(1(g)-1(e))(1(h)-1(e))$ for $g, h \in G$. Hence

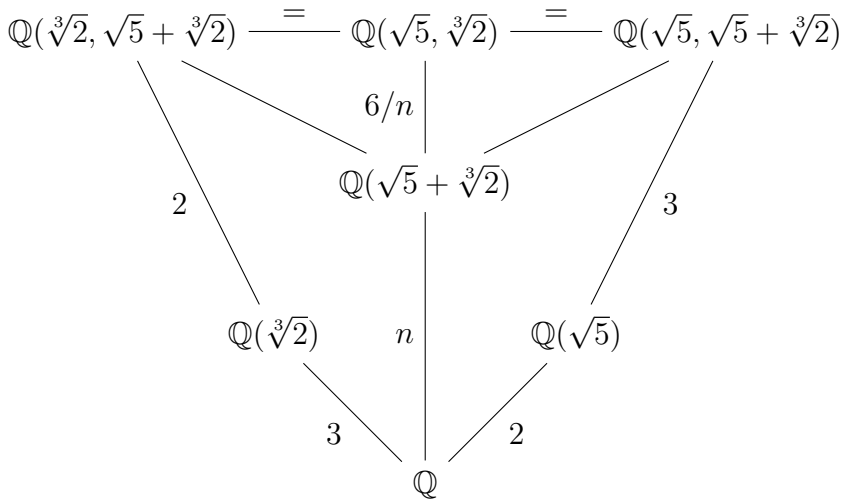
$$F((1(g)-1(e))(1(h)-1(e))) = ghg^{-1}h^{-1} \in [G,G],$$

so F factors through I^2. Then we let $F^{-1} : G \to I/I^2$ by $g \mapsto 1(g) - 1(e)$. We see that F^{-1} is surjective since $1(g) - 1(e)$ generates I and it factors through $[G,G]$ naturally. Therefore since F is invertible, it is an isomorphism.

□

Problem 11.
Show that the extension of $\mathbb{Q}$ generated by $\sqrt{5} + \sqrt[3]{2}$ is equal to $\mathbb{Q}(\sqrt{5}, \sqrt[3]{2})$.

Solution.
We construct the following tower of fields:



We know that $n = 1, 2, 3, 6$. $n = 1$ is impossible since this element is not in $\mathbb{Q}$. If we had $n = 2$, that would imply $\mathbb{Q}(\sqrt{5}, \sqrt{5} + \sqrt[3]{2})/\mathbb{Q}(\sqrt{5})$ has degree 3. But from the picture we know that it has degree at most 2. Similarly, if $n = 3$, then $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5} + \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ has degree 2, but it must have degree dividing 3 from the picture. Therefore $n = 6$, so the top extension has degree 1, i.e. the fields are the same. □

Problem 12.
Show that the multiplicative group of a finite field is cyclic and use this result to prove that the polynomial $X^4 + 1$ is never irreducible over any finite field.

Solution.
Let F be a finite field and let $F^\times$ be its multiplicative group. This is a finite abelian group, so we may write it in terms of its invariant factors

$$F^\times \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

$F^\times$ is cyclic if and only if $r = 1$. Suppose $r > 1$. Then since $n_1 \mid n_2$, there is a subgroup of $F^\times$ of the form $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$. Each of the n_1^2 elements in this subgroup satisfies $\alpha^{n_1} = 1$. This implies that there are n_1^2 roots of the polynomial $X^{n_1} - 1$. But since there are at most n_1 roots of this polynomial, this implies that $n_1^2 = n_1$, which is a contradiction since $n_1 > 1$ else $F^\times$ is infinite. Therefore we must have $r = 1$ so $F^\times$ is cyclic.

Now let $|F| = q$. If $\operatorname{char} F = 2$, then $X^4 + 1 = (X + 1)^4$, so the polynomial is reducible. Now since q is an odd number, we have $q \equiv 1, 3, 5, 7 \mod 8$. In any case, $q^2 \equiv 1 \mod 8$. Consider a quadratic extension K/F. Then

$$|K^\times| = q^2 - 1 \equiv 0 \mod 8.$$

Let $q^2-1 = 8n$. Therefore since $K^\times = \langle\alpha\rangle$, we have $(\alpha^n)^8 = 1$ is a primitive 8th root of unity. Therefore the polynomial X^8-1 splits over K. In particular, since $X^8-1 = (X^4-1)(X^4+1)$, X^4+1 splits in K. If X^4+1 were irreducible over F, then one of its roots would have degree 4, so could not lie in K, a contradiction. Therefore X^4+1 is never irreducible over any finite field. □

9 Spring 2010

Problem 1.
Show that the functor from (unitary) rings to groups sending a ring A to its group of units $A^\times$ is representable by a ring R.

Solution.
We claim that the ring $R = \mathbb{Z}[X, X^{-1}]$, where X is a variable over $\mathbb{Z}$, represents this functor F. Consider a homomorphism $\varphi : R \to A$. Since A is unital, we must have $\varphi(1) = 1_A$, so there is no choice of the image of $\mathbb{Z} \subset R$ by linear extension. Consider $\varphi(X)$. Since we have $\varphi(X)\varphi(X^{-1}) = 1_A$, we must have $\varphi(X) \in A^\times$. Further, there are no other restrictions since all sums and powers of X are independent of $\mathbb{Z}$. Hence there is a unique φ for each $a \in A^\times$. As sets, this means

$$F(A) = A^\times \cong \operatorname{Hom}_{\mathbf{Ring}}(R, A)$$

for all unital rings A. This precisely means that R represents F. □

Problem 2.
(a) Define what it means for two categories to be equivalent.

(b) A groupoid $\mathcal{G}$ is a category such that all morphism are isomorphisms. $\mathcal{G}$ is called connected if for any two objects x and y, $\mathrm{Hom}_{\mathcal{G}}(x, y)$ is nonempty. Show that any nonempty connected groupoid is equivalent to a group, that is, a groupoid with one object.

Solution.

(a) Two categories $\mathcal{C}$ and $\mathcal{D}$ are equivalent if there exists a functor $F : \mathcal{C} \to \mathcal{D}$ such that F is fully faithful and essentially surjective. F is fully faithful if $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cong \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ as sets for every objects X, Y of $\mathcal{C}$. F is essentially surjective if for every object Z of $\mathcal{D}$, there is an object X of $\mathcal{C}$ so that $F(X) \cong Z$ as objects of $\mathcal{D}$.

(b) Let $\mathcal{G}$ be a nonempty connected groupoid and let G be a group. Let $F : \mathcal{G} \to G$ by $F(X) = g$, the sole element of of G for every X in $\mathcal{G}$. Then this functor is clearly essentially surjective (indeed, it is surjective), since there exists an object in $\mathcal{G}$. Now take X, Y in $\mathcal{G}$. Notice that we have not defined the morphism set of G yet, but we do so now. We claim that the choice $\mathrm{Hom}_G(g, g) = \mathrm{Hom}_{\mathcal{G}}(Z, Z)$, for some fixed object Z in $\mathcal{G}$ makes the functor F fully faithful as well.

We claim that $\mathrm{Hom}_G(g, g) = \mathrm{Hom}_{\mathcal{G}}(X, Y)$ for every X, Y in $\mathcal{G}$. First, the right hand set is nonempty since $\mathcal{G}$ is connected, so let φ be some element. Additionally, there exist isomorphisms $f : Z \to X$ and $g : Y \to X$ by assumption. Therefore we get an isomorphism $g \circ \varphi \circ f : Z \to Z$ which corresponds uniquely to φ. But since $\mathrm{Hom}_{\mathcal{G}}(Z, Z)$ corresponds uniquely with $\mathrm{Hom}_G(g, g)$ by definition, this proves our claim. Hence $F : \mathcal{G} \to G$ is an equivalent of categories.

□

Problem 3.
Determine, using the structure theory of abelian groups or otherwise, all finitely generated abelian groups A such that the group $\mathrm{Aut}\, A$ is finite. State clearly any basic theorems that you use. Determine the order of the automorphism group of $A = \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Solution.
From the structure theorem, we know that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z} \cong \mathbb{Z}^r \times A_{\mathrm{tor}}.$$

We examine automorphisms of $\mathbb{Z}^r$, since $\mathrm{Aut}\, A \supset \mathrm{Aut}\, \mathbb{Z}^r$. If $r = 1$, then $\mathbb{Z}$ only has two automorphisms, namely $1 \mapsto \pm 1$. Now we examine $\mathbb{Z}^2$. Treating this like a free $\mathbb{Z}$-module, we see that automorphisms here correspond bijectively to $\mathrm{GL}_2(\mathbb{Z})$. Given $\alpha \in \mathrm{GL}_2(\mathbb{Z})$, we have infinitely many choices for the first column (do not chooce $(0, 0)$) and more than zero choices for the second column, $|\mathrm{GL}_2(\mathbb{Z})| = \infty$. Hence $\mathbb{Z}^r$ has infinitely many automorphisms for $r > 1$.

If $r = 1$, then we know there are $2|A_{\mathrm{tor}}|$ maps from $\mathbb{Z}$ into A which preserve the free part, corresponding to $(1, a)$ and $(-1, a)$ for every torsion a. Further, there are at most $|A_{\mathrm{tor}}|^{|A_{\mathrm{tor}}|}$ maps from A_{tor} to A since a torsion element cannot map to a non-torsion element. We

conclude that the only finitely generated abelian groups with finite automorphisms groups are of rank 1 or rank 0.

Therefore we have 8 maps from $\mathbb{Z}$ to A sending $(1,0)$ to $(\pm 1, a)$ for $A \in \mathbb{Z}/4\mathbb{Z}$, and two automorphisms of $\mathbb{Z}/4\mathbb{Z}$ sending $(0,1) \mapsto (0,1)$ or $(0,3)$. Hence there are 16 automorphisms. □

Problem 4.
Show that if $\sigma \in \operatorname{Aut} S_4$ and $\tau \in S_4$ is a transposition, then $\sigma(\tau)$ is also a transposition. By studying the action of σ on transpositions, show that every automorphism of S_4 is inner.

Solution.
We know that $\sigma(\tau)$ has order 2, so either $\sigma(\tau)$ is a transposition or $\sigma(\tau)$ is a 2-2-cycle, i.e. of the form $(1\,2)(3\,4)$ or similar. Let $V \subset S_4$ be the subgroup generated by the 2-2-cycles of order 4. Then $\sigma(V)$ is also a normal subgroup of S_4 of order 4. But there is only one such subgroup, so σ preserves V. Therefore a transposition cannot be sent to a 2-2-cycle.

Therefore consider an automorphism of S_4. We start by mapping $(1\,2)$ to a transposition. There are 6 choices. This also defines precisely the image of $(3\,4)$, since transpositions come in commuting pairs (e.g. $(1\,2)$,$(3\,4)$). There are therefore 4 choices for the image of $(1\,3)$, and the image of $(1\,4)$ is obtained uniquely by the image of $(3\,4)(1\,4)(3\,4)$. Since these generate S_4, $|\operatorname{Aut} S_4| = 24$. Further, we know that the number of inner automorphisms of S_4 is equal to $|S_4|/|Z(S_4)|$. But $Z(S_4)$ is trivial, so there are 24 inner automorphisms of S_4. Hence every automorphism is inner.

□

Problem 5.
Give the total number and the dimensions of the irreducible complex representations of the irreducible complex representations of S_4. Prove your answer.

Solution.
Using character theory, we know that the number of representations is equal to the number of conjugacy classes of S_4. Since each cycle type is a unique conjugacy class, we know that there are 5 irreducible complex representations. Further, the sum of the dimensions of these representations equals $|S_4| = 24$, and one of these representations is the trivial representation of degree 1.

Now we need the sum of four squares to equal 23. We see that no representation has dimension 4, since we cannot obtain 7 as a sum of three of $1, 4, 9$. Further, we must have at least one representation of dimension 3. So we need to sum 3 squares to 14. We see this is obtained by (and only by) $1 + 4 + 9$. Hence the 5 irreducible complex representations of S_4 have dimensions $1, 1, 2, 3, 3$. □

Problem 6.
State and prove Schur's Lemma.

Solution.
We state this in module terminology. Let V, W be simple $F[G]$-modules. Then Schur's Lemma states that if $\varphi : V \to W$ is a $F[G]$-module homomorphism, then either φ is an

isomorphism or $\varphi = 0$. The proof is straightforward. Given such a φ, then $\ker\varphi$ is a $F[G]$-submodule of V. Since V simple, then $\ker\varphi = V$ or 0. If $\ker\varphi = V$, then we are in the case $\varphi = 0$. If $\ker\varphi = 0$, then V injects into W, so $\varphi(V)$ is a $F[G]$-submodule of W. But W is also simple, so since $\varphi(V) \neq 0$, we must have $\varphi(V) = W$. Hence φ is an isomorphism. □

Problem 7.
Show that the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if n is a power of an odd prime number, twice the power of an odd prime number, or 4.

Solution.
First, by the Chinese Remainder Theorem, we may write

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{a_i}\mathbb{Z}.$$

Suppose have a unit in $\mathbb{Z}/n\mathbb{Z}$. Then it must also be a unit in each of the factors, and the converse also holds. Hence

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{k} (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times.$$

We now examine particular cases of the group of units of $\mathbb{Z}/p^a\mathbb{Z}$. Suppose $p = 2$. Then $(\mathbb{Z}/2\mathbb{Z})^\times \cong \{1\}$, and $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$, but $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To see this last fact, we note that

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\},\ 1^2 = 3^2 = 5^2 = 7^2 = 1 \pmod 8.$$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the only group of order 4 without an element of order 4, so this is clear. Now for $\mathbb{Z}/2^a\mathbb{Z}$ for $a \geq 3$, the group of units clearly contains $(\mathbb{Z}/8\mathbb{Z})^\times$ as a subgroup, which is not cyclic. Since a cyclic group has cyclic subgroups, this proves that $\mathbb{Z}/2^a\mathbb{Z}$ is cyclic if and only if $a = 1, 2$.

Now let p be an odd prime. By the general theory of cyclic groups, $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p)\mathbb{Z} = \mathbb{Z}(p-1)\mathbb{Z}$. The generalisation to higher powers is notoriously confusing, but it is found on page 96 of [2]. We have a canonical ring homomorphism

$$\mathbb{Z}/p^{r+1}\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$$

which is induced by the inclusion of ideals $p^{r+1}\mathbb{Z} \subset p^r\mathbb{Z} \subset \mathbb{Z}$. Hence we have an induced group homomorphism

$$\lambda : (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \to (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

This is a surjective group homomorphism. Further, let $\lambda(a) = 1$. Then we have

$$a \equiv 1 \mod p^r \implies a \equiv 1 + xp^r \mod p^{r+1}$$

for any $x \in \{0, \ldots, p-1\}$. Hence $|\ker\lambda| = p$, so $|(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times| = \varphi(p^{r+1}) = p^r(p-1)$. Hence by the fundamental theorem of finitely generated abelian groups, we can write

$$(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \cong A_{p^r} \times A_{p-1}.$$

We need to show that these latter two groups are cyclic. It is not hard to show that $A_{p-1} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ from the natural surjection $(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ from above. However, for the other group, we need to work with p-adics, and I'll refer the reader to [3] for more information. The proof follows after proving this. □

Problem 8.
Let F be the field with 2 elements and let $R = F[X]$. List up to isomorphism all R-modules with 8 elements that are cyclic.

Solution.
A finite $F[X]$-module is precisely a F-vector space. In particular, such an R-module V must have $\dim_F V = 3$ so that $|V| = 2^3 = 8$. This module is cyclic if and only if it has one invariant factor. Hence its invariant factor must be a cubic polynomial in $F[X]$, and there are 8 of these corresponding to $X^3 + (0/1)X^2 + (0/1)X + (0/1)1$. Therefore there are 8 such R-modules. □

Problem 9.
Let A be a left Noetherian ring. Show that every left invertible element $a \in A$ is two-sided invertible.

Solution.
Suppose that $ba = 1$. Then let $r_a \in \operatorname{End} A$ be the map given by $x \mapsto xa$. We see that r_a is surjective since $r_a(xb) = xba = x$ for any $x \in A$. We claim that r_a is also injective. Let M_i denote the kernel of r_a^i, i.e. $x \mapsto xa^i$. Then $M_1 \subset M_2 \subset \dots$ is an ascending chain, so it stabilises since A is Noetherian. Let M_n be the point at which the chain stabilises, so that $M_n = M_{n+m}$ for all $m \in \mathbb{N}$.

Let $x \in M_1$ Then since r_a is surjective, r_a^n is surjective, so there exists $y \in A$ so that $ya^n = x$. Then $y \in M_{n+1}$ since $ya^{n+1} = xa = 0$. But since $M_n = M_{n+1}$, we have $ya^n = 0 = x$. Therefore $\ker r_a = 0$, so r_a is an isomorphism.

We see that $r_a(ab - 1) = aba - a = a - a = 0$. By injectivity, this implies $ab - 1 = 0$, so $ab = 1$. Therefore every left invertible element is two-sided invertible, and in fact by the same inverse. □

Problem 10.
Let F be a field and V a finite dimensional F-vector space. Show that $R = \operatorname{End}_F(V)$ has no nontrivial two-sided ideals.

Solution.
By basic linear algebra, $R \cong M_n(F)$, where $n = \dim V$. Hence it is sufficient to prove this result for a matrix ring $M_n(F)$ of arbitrary size n. Let $0 \neq a \in M_n(F)$ be any matrix. We claim that the two-sided ideal generated by a is all of $M_n(F)$, which would prove the claim since all minimal ideals are principal. Let $\mathfrak{a}$ be this ideal. Since $a \neq 0$, there is some $(i, j) \in \{1, \dots, n\}^2$ so that $a_{ij} \neq 0$. Let E^{kl} denote the elementary matrix so that

$$E_{ij}^{kl} = \delta_k(i)\delta_l(j).$$

In words, the matrix is zero except for 1_F in the (k, l) position. We see that

$$E^{ki} \cdot a \cdot E^{jl} = a_{ij}E^{kl} \in \mathfrak{a} \implies E^{kl} \in \mathfrak{a}$$

by multiplying by a_{ij}^{-1}. Since k, l were arbitrary above, we see that every elementary matrix is in $\mathfrak{a}$. For any matrix $b \in M_n(F)$, we have

$$b = \sum_{i,j} b_{ij} E^{ij} \in \mathfrak{a}.$$

Therefore $\mathfrak{a} = M_n(F)$, so there are no proper nontrivial two-sided ideals. □

Problem 11.
Let F be a field of characteristic zero containing the pth roots of unity for p a prime. Show that the cyclic extensions of degree p of F in any algebraic closure $\overline{F}$ of F are in one to one correspondence with the subgroups of order p of $F^\times/(F^\times)^p$.

Solution.
Let $G = F^\times/(F^\times)^p$, and denote elements by squarefree coset representatives. Take an element $\alpha \in G$ of order p, so that $\langle \alpha \rangle$ has order p as well. Let K be the splitting field of $X^p - \alpha$, which is irreducible over F by assumption. Then this is a Galois extension of F, generated by $a = \sqrt[p]{\alpha}$ in $\overline{F}$, and is of order p. Therefore its Galois group must be cyclic.

Conversely, let K/F be a cyclic extension of order p. Let σ be a generator of the Galois group. Then consider the norm of the element ζ_p. We have

$$N_F^K(\zeta_p) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\zeta_p) = 1,$$

where σ acts trivially on ζ_p since it lies in the base field F. By Hilbert's Theorem 90, there exists $\alpha \in K$ so that $\zeta_p = \sigma(\alpha)/\alpha$, i.e. $\zeta_p \alpha = \sigma(\alpha)$. Indeed, we know this $\alpha \in K \setminus F$, so $K = F(\alpha)$. This is because any intermediate field would correspond to a divisor of p, of which there is none. Further,

$$\sigma(\alpha^p) = \sigma(\alpha)^p = (\zeta_p \alpha)^p = \alpha^p,$$

so $\alpha^p \in F$. Therefore $\alpha \in F^\times/(F^\times)^p$, and generates a subgroup of order p. This completes the proof. □

Problem 12.
Determine all fields F such that the multiplicative group of F is finitely generated.

Solution.
Suppose F has characteristic 0. Then view $\mathbb{Q} \subset F$ as an embedded subfield. We claim that $\mathbb{Q}^\times$ is not finitely generated as a multiplicative group. Suppose it were generated by some $\{a_i/b_i\}$ where $i \in \{1, \ldots, n\}$. Then the denominator of any product of these elements has denominator dividing some power of $\prod_{i=1}^n b_i$. Then let $\{p_j\}$ be the set of primes in $\mathbb{Z}$ diving $\prod_{i=1}^n b_i$. In particular, this list is finite. Therefore any $1/p \in \mathbb{Q}$ so that $p \neq p_j$ for any j cannot be in the subgroup generated by $\{a_i/b_i\}$. Hence $\mathbb{Q}^\times$ is infinitely generated. Since $\mathbb{Q}^\times \subset F^\times$ as a subgroup, suppose that $F^\times$ were finitely generated. Then by the classification theorem of finitely generated abelian groups, any subgroup of $F^\times$ is also finitely generated. But this is a contradiction since $\mathbb{Q}^\times$ was not finitely generated.

If F is a finite field, then its multiplicative group is finite, so must be finitely generated. If F is not finitely generated over its prime field $\mathbb{F}_p$, then certainly $F^\times$ is not finitely generated. If it were, then the set of generators of $F^\times$ would generate F, a contradiction. Therefore let $F = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ be a finitely generated extension of $\mathbb{F}_p$. If each α_i is algebraic, then F is finite, so its multiplicative group is finitely generated. If some α_1 is transcendental, then $\mathbb{F}_p(X) \subset F$ as a subfield. But since $\mathbb{F}_p[X]$ is a UFD with infinitely many primes, we are in the same situation as $\mathbb{Q}$ not being finitely generated. Hence a transcendental extension of $\mathbb{F}_p$ does not have a finitely generated multiplicative group.

We conclude that $F^\times$ is finitely generated if and only if F is finite. □

10 Fall 2009

Problem 1.
Let **Top** be the category of topological spaces. Recall that a morphism f in some category is called a monomorphism if, for any two morphisms g_1 and g_2 that can be precomposed with f, $fg_1 = fg_2$ implies $g_1 = g_2$. Dually, f is called an epimorphism if, for any g_1 and g_2 that can be postcomposed with f, $g_1 f = g_2 f$ implies $g_1 = g_2$.

(a) Show that a continuous map $f : X \to Y$ is an monomorphism in **Top** if and only if f is one-to-one.

(b) Show by example that an epimorphism in **Top** need not be onto.

Solution.
Note that we have to assume **Top** is the category of *Hausdorff* topological spaces or (b) is not true.

(a) First, suppose f is injective. Then

$$fg_1(x) = fg_2(x) \implies f(g_1(x)) = f(g_2(x)) \implies g_1(x) = g_2(x)$$

for all x in the domain of g_1, g_2. Therefore f is a monomorphism. Conversely, suppose that that f is a monomorphism but there exists $x \neq y \in X$ so that $f(x) = f(y)$. Then let $g_1 : Z \to X$ be the projection onto the point x and $g_2 : Z \to X$ be projection onto y. Then $fg_1 = fg_2$, but $g_1 \neq g_2$, which is a contradiction.

(b) Let $f : (0, 1) \to [0, 1]$ be an embedding. Then since every continuous function on $(0, 1)$ extends uniquely to its limit points $0, 1$, $g_1 f = g_2 f$ implies $g_1 = g_2$. But f is not surjective.

□

Problem 2.
Let $F : \mathbf{Ab} \to \mathbf{Sets}$ be the forgetful functor from abelian groups to sets. Show that F does not have a right adjoint.

Solution.
Suppose it did, and call that functor G. Then we would have for every abelian group A and set X

$$\mathrm{Hom}_{\mathbf{Ab}}(A, G(X)) \cong \mathrm{Hom}_{\mathbf{Sets}}(F(A), X).$$

In particular, let A be the trivial group. Then the number of maps from $F(A)$ to a set X is precisely $|X|$. However, there is only one group homomorphism from A to any abelian group. Therefore since sets with more than one element exist, no such G could exist. □

Problem 3.
Suppose A is an abelian group that is generated by n elements. Show that any subgroup of A also can be generated by n elements.

Solution.
If A is generated by n elements, then we have a surjection $\mathbb{Z}^n \to A \to 0$ which sends basis elements of $\mathbb{Z}^n$ to generators of A. This yields a short exact sequence $\mathbb{Z}^n \xrightarrow{f} A \to 0$. Let $B \subset A$ be a subgroup. Then $f^{-1}(B) \subset \mathbb{Z}^n$ is a submodule. We claim that in a PID, a submodule of a finitely generated free module is finitely generated of lesser or equal rank.

To see this, we proceed by induction on n. First, for $n = 1$, we know that submodules of $\mathbb{Z}$ correspond to ideals of $\mathbb{Z}$, which are principal, hence generated by at most 1 elements. Suppose the $n-1$ case, and let $M \subset \mathbb{Z}^n$ be a submodule $\mathbb{Z}^n$. Then let $\varphi : M \to \mathbb{Z}$ be given by

$$\varphi((x_1, \ldots, x_n)) = \sum_{i=1}^{n} x_i.$$

Then φ is a $\mathbb{Z}$-module homomorphism, so we obtain a short exact sequence

$$0 \to \ker \varphi \to M \to \operatorname{im} \varphi \to 0.$$

$\ker \varphi$ is a submodule $\mathbb{Z}^{n-1}$, so it is free of rank at most $n-1$. Also, $\operatorname{im} \varphi \subset \mathbb{Z}$ is a submodule, we have shown it is free, so in particular it is projective. Therefore the sequence is split, so we have $M = \ker \varphi \oplus \operatorname{im} \varphi$, which has rank at most n.

Applying this to the particular situation, $f^{-1}(B)$ is free of rank at most n, so the surjection $f^{-1}(B) \cong \mathbb{Z}^n \to B \to 0$ implies that B is generated by n elements. □

Problem 4.
Let $p < q$ be primes, $n \geq 0$ an integer and G a group of order pq^n. Show that G is solvable.

Solution.
The number of Sylow q-subgroups of G satisfies $n_q \mid p$ and $n_q \equiv 1 \mod q$. Since $p < q$, so $q + 1 \nmid p$, we see that $n_q = 1$. Therefore let $Q \triangleleft G$ be the normal Sylow q-subgroup of G. Since $|G/Q| = p$, we must have $G/Q \cong \mathbb{Z}/p\mathbb{Z}$, which is an abelian group, so is solvable. Additionally, we claim that Q is solvable. We proceed by induction on n. For $n = 1$, $Q \cong \mathbb{Z}/q\mathbb{Z}$, so it is abelian group, so is solvable.

For any n, any group H of order q^n has a nontrivial centre Z. Then Z is solvable, and we have $|H/Z| \leq q^{n-1}$ is a q-group of lesser order. By induction, H/Z is solvable. Since Z and H/Z are solvable, H is solvable. Hence all q-groups are solvable.

In our case, we have Q and G/Q are solvable, so G is solvable. □

Problem 5.
Let G be a finite group and $\rho : G \to \mathrm{GL}(V)$ a complex representation. Prove that (V, ρ) splits as a direct sum of irreducible representations of G.

Solution.
This is equivalent to proving Maschke's theorem. Consider V as a $\mathbb{C}[G]$-module. Let $U \subset V$ be a submodule. If this implies that $U = 0$ or $U = V$, then V is irreducible and we are done. Otherwise, take the orthogonal complement $U^\perp = X$ in the vector space V. By definition, $V = U \oplus X$ as vector spaces. We want to show that X is actually a submodule of V, and so by induction on dimension this would prove the theorem. If V happens to be infinite dimensional, then we apply Zorn's lemma to obtain the same conclusion.

Let $\varphi \in \mathrm{End}(V)$ be the orthogonal projection onto U. We would like to modify φ so that it is a $\mathbb{C}[G]$-module homomorphism as well as a vector space homomorphism. Let φ_g denote $\rho(g) \circ \varphi \circ \rho(g)^{-1}$. Since U is a $\mathbb{C}[G]$-submodule, we have

$$\rho_G(u) = \rho(g)\varphi(\rho(g^{-1})u) = \rho(gg^{-1})(u) = u.$$

Therefore consider the map $\pi : V \to U$ given by

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} \varphi_g(v).$$

Since we are working over $\mathbb{C}$, the fraction $1/|G|$ is well defined. By the above,

$$\pi(u) = \frac{1}{|G|} \sum_{g \in G} \varphi_g(u) = \frac{1}{|G|} \cdot |G| \cdot u = u.$$

Therefore we claim that $V = U \oplus \ker \pi$ as $\mathbb{C}[G]$-modules. If $x \in \ker \pi$ and $h \in G$, then we see that

$$\begin{aligned}
\pi(\rho(h)x) &= \frac{1}{|G|} \sum_{g \in G} \varphi_g(\rho(h)x) = \frac{1}{|G|} \sum_{g \in G} \rho(g)\varphi\rho(g^{-1})\rho(h)x \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(h)\rho(h^{-1}g)\varphi\rho(g^{-1}h)x \\
&= \rho(h)\frac{1}{|G|} \sum_{g \in G} \varphi_{h^{-1}g}(x) = \rho(h)\pi(x) = 0,
\end{aligned}$$

where we use that left multiplication by h^{-1} is an automorphism of G. Therefore $\ker \pi$ is a $\mathbb{C}[G]$-submodule of V, so we are done. □

Problem 6.
Let G be a finite p-group and $\rho : G \to \mathrm{GL}(V)$ a representation over $\mathbb{F}_p$.

(a) Show that V has a one-dimensional G-invariant subspace.

(b) Show by example that (V, ρ) need not split into a direct sum of irreducible representations.

Solution.

(a) It suffices to assume V is finite dimensional here by examining subrepresentations of the span of $\{\rho(g)(v) : g \in G\}$ for any $v \in V$. Then $|V| = p^n$. Consider the partition of V into one-dimensional subspaces, of which there are $(p^n - 1)/(p - 1)$ since each subspace has order $p - 1$. In particular,

$$\frac{p^n - 1}{p - 1} = \sum_{i=0}^{n-1} p^i \equiv 1 \mod p.$$

We claim the action of G on the set of linear subspaces of V has at least one fixed point, which would correspond to a one-dimensional subrepresentation of V. Let X denote the set of linear subspaces of V, and let A denote a set of unique representatives for the nontrivial orbits of G, and G_x the stabiliser of $x \in X$ in G. Further, let X^G denote the fixed points of G on X. By the orbit-stabiliser theorem we know

$$|X| = |X^G| + \sum_{\alpha \in A} |G\alpha| = |X^G| + \sum_{\alpha \in A} |G : G_\alpha|.$$

Since G is a p-group, we know that $p \mid |G : G_\alpha|$ for each α. Therefore

$$|X| = |X^G| \equiv 1 \mod p.$$

Therefore there is at least one linear subspace fixed by G, which is what we need.

(b) Let $p = 2$, $\dim V = 2$, and $G = \mathbb{Z}/2\mathbb{Z} = \{1, a\}$. Then let ρ be the map

$$\rho(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We have $\rho(a)^2 = \rho(a^2) = \rho(1) = I_2$, so this is indeed a representation. We see that $(1, 0) \in V$ is invariant under G, and so it generates a one-dimensional irreducible subrepresentation. However the other vectors $(1, 1)$ and $(1, 0)$ are interchanged by a, so neither generates a one-dimensional subrepresentation. Therefore V is not the direct sum of irreducible subrepresentations.

□

Problem 7.

Find a homomorphism $A \to B$ of commutative rings and non-zero A-modules M, N such that the canonical map

$$B \otimes_A \operatorname{Hom}_A(M, N) \to \operatorname{Hom}_B(B \otimes_A M, B \otimes_A N)$$

is the zero map. Prove that the map is an isomorphism if M is a finitely generated projective A-module.

Solution.
This canonical map is defined by

$$b \otimes f \mapsto [x \otimes m \mapsto b \cdot x \otimes f(m)].$$

For the first part, let $A = B = \mathbb{Z}$, $M = \mathbb{Z}/3\mathbb{Z}$, and $N = \mathbb{Z}/2\mathbb{Z}$. Then $\mathrm{Hom}_{\mathbb{Z}}(M, N) = 0$, since there is no nontrivial map between these two modules. Therefore the canonical map above is the zero map since $\mathbb{Z} \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(M, N) = \mathrm{Hom}_{\mathbb{Z}}(M, N) = 0$.

For the second part, we use that $\mathrm{Hom}_A(A, N) \cong N$ for any A-module N. In our case, assuming $M = A$, we have

$$\begin{aligned} B \otimes_A N &\cong B \otimes_A \mathrm{Hom}_A(A, N) \\ &\to \mathrm{Hom}_B(B \otimes_A A, B \otimes_A N) = \mathrm{Hom}_B(B, B \otimes_A N) \cong B \otimes_A N. \end{aligned}$$

Therefore the isomorphism is clear. This generalises trivially to a free module $M = A^n$. Since both tensor products and Hom_A behave well with respect to direct sums, it holds for an M such that $M \oplus M' = A^n$ as well. Therefore if M is a finitely generated projective A-module, we have the isomorphism we require. □

Problem 8.
Prove the following facts:

(a) Any subring of $\mathbb{Q}$ sharing the identity with $\mathbb{Q}$ is a PID.

(b) For a subring $A \subset \mathbb{Z}[i]$ sharing the identity with $\mathbb{Z}[i]$, if $A \neq \mathbb{Z}$ and $A \neq \mathbb{Z}[i]$, A is not a PID.

Solution.

(a) First, let $R \subset \mathbb{Q}$ be such a subring. Then $\mathbb{Z} \subset R$ since R is closed under addition. Therefore R is a domain between $\mathbb{Z}$ and its quotient field, so we may realise R as $S^{-1}\mathbb{Z}$ for some set $S \subset \mathbb{Z} \setminus \{0\}$. In particular, we see that $S = \{b : a/b \in R\}$.

Now we know that ideals in $R = S^{-1}\mathbb{Z}$ are in bijective correspondence with ideals in $\mathbb{Z}$ avoiding S. For $\mathfrak{a} \subset R$, we have $\mathfrak{b} \subset \mathbb{Z}$ so that $\mathfrak{a} = S^{-1}\mathfrak{b}$. Since $\mathfrak{b} = (b)$ for some $b \in \mathbb{Z}$, we have that $\mathfrak{a} = (b)$ in R as well. Therefore R is a PID.

(b) Since $\mathbb{Z} \subsetneq A$, we must have $ni \in A$ for some $n > 0$, and since $A \subsetneq \mathbb{Z}[i]$, we must have $n > 1$. Let n the the minimal m so that $mi \in A$. Then we claim that $A = \mathbb{Z}[ni]$. If there were some $mi \in A$ so that $n \nmid m$, then applying the Euclidean algorithm we could obtain $\gcd(n, m)i$, which contradicts the minimality of n.

We claim that the ideal $(n + 1, ni)$ is not principal. Suppose that $a + bni$ generated this ideal for $a, b \in \mathbb{Z}$. Then in particular, if we let N be the usual norm on $\mathbb{C}$ applied to A, we have

$$N(n + 1) = (n + 1)^2 = N(\alpha)(a^2 + n^2b^2),\ N(ni) = n^2 = N(\beta)(a^2 + n^2b^2).$$

Since $(a^2 + n^2b^2)$ divides both n^2 and $(n + 1)^2$, it divides their gcd. Since $n, n + 1$ are coprime, their squares are also, so their gcd is just 1. Hence $a^2 + n^2b^2 = 1$. But this is a contradiction, since this implies $b = 0$ and $a = \pm 1$, and hence $(a + bi) = A$, which $(n + 1, ni)$ is not. Therefore this ideal is not principal, and we are done.

□

Problem 9.
Prove that every two-sided ideal of the ring $M_2(\mathbb{Z})$ is principal.

Solution.
Two-sided ideals of $M_2(\mathbb{Z})$ correspond precisely with $M_2(\mathfrak{a})$, where $\mathfrak{a} \subset \mathbb{Z}$ is a two-sided ideal. Since $\mathbb{Z}$ is a PID, we have $\mathfrak{a} = n\mathbb{Z}$. Therefore we need to snow that $M_2(n\mathbb{Z})$ is principal in $M_2(\mathbb{Z})$. Indeed, it is generated by

$$a = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}.$$

If we let E_{ij} be the elementary matrix with 1 in the (i, j) spot and 0 elsewhere, we see that

$$E_{11} \cdot a \cdot E_{12} = \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix}$$

and similarly we can find $n \cdot E_{ij} \in M_2(n\mathbb{Z})$ for $1 \leq i, j \leq 2$. Repeatedly summing these elementary matrices generates the entire ideal, so it is principal. □

Problem 10.
Let B be a central simple algebra over k of dimension 4. Prove the following facts.

(a) All left ideals of B have even dimension.

(b) $B \cong M_2(k)$ if and only if B is not a division algebra.

Solution.

(a) It suffices to show that B has no left ideal of dimension 1. Suppose that $\mathfrak{a}$ were a left ideal. Then we may write $\mathfrak{a} = Ba$ for some $a \in B$. Since $BaB = B$, a must be right invertible. But since B is Noetherian, right invertible elements are two-sided invertible, hence $Ba = B$. But this is a contradiction, hence no such $\mathfrak{a}$ exists, and we are done.

(b) We use the Artin-Wedderburn theorem. From the classification of simple algebras, we know that $B \cong M_n(D)$, where $n^2 \cdot \dim D = 4$, and D is a division algebra over k. First, if $B \cong M_2(k)$, then it is not a division algebra since we see

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

has no inverse, since it has zero determinant. Conversely, if B is not a a division algebra, then by the classification theorem it must be of the form $M_n(D)$ with $n > 1$. But $n^2 = 4$, so $\dim D = 1$, i.e. $D = k$. Therefore $B \cong M_2(k)$.

□

Problem 11.
Prove that the multiplicative group of a field F is a cyclic group if and only if F is a finite field.

Solution.
See Spring 2010, Problem 12. We only proved finitely generated if and only if F is finite, but if F is finite then you can prove that its multiplicative group is cyclic. Since $F^\times$ is a finitely generated abelian group, we can write

$$F^\times \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

the invariant factor decomposition of $F^\times$. If $k = 1$, then $F^\times$ is cyclic. Suppose that $k > 1$. Then we have $n_1 \mid n_2$, there is a subgroup $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \subset \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots$. Therefore $F^\times$ has a subgroup $H \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$. Every element in H has order n_1, i.e. $a^{n_1} = 1$ for all $a \in H$. Therefore the polynomial $X^{n_1} - 1$ has $|H|$ distinct roots. But $X^{n_1} - 1$ has at most $n_1 < |H| = n_1^2$ roots over any field, so this is a contradiction. Therefore $F^\times$ is cyclic. □

Problem 12.
Let $k = \mathbb{F}_2(t, s)$ be the field of fractions of the two variable polynomial ring $\mathbb{F}_2[t, s]$. Write θ_a for a root of $T^2 + T + a$ for $a \in k$ in an algebraic closure of k.

(a) How many intermediate fields between k and $k(\theta_t, \theta_s)$?

(b) How many intermediate fields between k and $k(\sqrt{t}, \sqrt{s})$?

Solution.
(a) We notice that both θ_t and $\theta_t + 1$ are roots of $T^2 + T + t$. Specifically,

$$(\theta_t + 1)^2 + (\theta_t + 1) + t = (\theta + t^2 + \theta_t + t) + (1 + 1) = 0.$$

Therefore $T^2 + T + t$ is a separable polynomial. We can see the same is true for $T^2 + T + s$. Since k is the splitting field of $(T^2 + T + t)(T^2 + T + s)$, it is a separable normal extension, so is Galois. Therefore intermediate fields between k and $k(\theta_t, \theta_s)$ are in bijective correspondence with subgroups of the Galois group G of this extension. We see that $|G| = 4$, and in particular

$$G \cong \mathrm{Gal}(k(\theta_t)/k) \times \mathrm{Gal}(k(\theta_s)/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

There are five subgroups of G: the whole group, the trivial subgroup, the first component, the second component, and the diagonal subgroup. Therefore there are three intermediate fields.

(b) We see that $\sqrt{t}$ is not a separable element. It is a root of $T^2 - t$, which factors as $(T + \sqrt{t})^2$ in $k(\sqrt{t}, \sqrt{s})$. Therefore the extension $k(\sqrt{t}, \sqrt{s})$ is purely inseparable. We claim that it has infinitely many intermediate fields.

Let $K_f = k(\sqrt{s} + f \cdot \sqrt{t})$, where $f \in k[s, t]$ is a nonconstant polynomial. First, note that $K_f \neq k(\sqrt{s}, \sqrt{t})$, since $[K_f : k] = 2$ and $[k(\sqrt{s}, \sqrt{t}) : k] = 4$. We claim that for $f \neq g$, we have $K_f \neq K_g$. Suppose there were $f \neq g$ such that $K_f = K_g$. Call this field K. Then

$$\sqrt{s} + g \cdot \sqrt{t} - g/f \cdot (\sqrt{s} + f \cdot \sqrt{t}) = (1 - g/f)\sqrt{s} \in K.$$

Since $g \neq f$, $1 - g/f \in K^\times$, so $\sqrt{s} \in K$. Hence $\sqrt{s}, \sqrt{t} \in K$, so $K = k(\sqrt{s}, \sqrt{t})$, which is a contradiction. Therefore since there are infinitely choices for f, there are infinitely many nonisomorphic intermediate fields K_f.

□

References

[1] This proof is taken from: *The theorems of Maschke and Artin-Wedderburn.* http://www.math.uni-bielefeld.de/ sek/select/rw1.pdf.

[2] Lang, Serge. *Algebra* (Third Edition). If you don't know how to get a copy of this book, you're in trouble for the qual.

[3] Jerry Shurman's Number Theory lecture notes, found at http://people.reed.edu/ jerry/361/lectures/lec07.pdf.