Algebra Sample Pre-lim Problems

El Tigre

Contents

1 Fall 2018

1. Prove that $\mathbb{Z}$ is a Principal Ideal Domain.

Let $I \subset \mathbb{Z}$ be an ideal. Pick an element $a \neq 0 \in I$ with minimal absolute value. Since $\mathbb{Z}$ is a Euclidean Domain, we can use the Division Algorithm. For any $b \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ such that

$$b = qa + r,$$

where $0 \leq r < |a|$. Since $r = b - qa$, $r \in I$, and since $r < |a|$, r must be 0 by the minimality of $|a|$. This implies that $a|b$, so $b \in (a)$. b is an arbitrary element of I, so $I = (a)$.

2. Let $\mathbb{H}$ be the real quaternions. Then $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$ is isomorphic to which of the following rings? Prove your answer:

(a) $\mathbb{C} \times \mathbb{C}$

(b) $\mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$

(c) $\mathbb{M}_2(\mathbb{C})$

(d) $\mathbb{M}_2(\mathbb{R})$

(e) $\mathbb{M}_2(\mathbb{H})$

(f) $\mathbb{M}_2(\mathbb{R}) \times \mathbb{M}_2(R)$

(c) is the correct answer.

Short answer:

The real quaternions form a non-commutative ring, and tensoring with $\mathbb{C}$ gives another non-commutative ring, since

$$(1 \otimes i)(1 \otimes j) = 1 \otimes k;$$
$$(1 \otimes j)(1 \otimes i) = 1 \otimes -k.$$

So, the answer is neither (a) nor (b).

We can think of the remaining choices as $\mathbb{R}$-algebras, with obvious scalar multiplication. We can see that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$ is 8-dimensional, spanned by $\{1, i\} \otimes \{1, i, j, k\}$. $\mathbb{M}_2(\mathbb{C})$ is also an 8-dimension $\mathbb{R}$-algebra, while $\mathbb{M}_2(\mathbb{R})$ is 4-dimensional, and both $\mathbb{M}_2(\mathbb{H})$ and $\mathbb{M}_2(\mathbb{R}) \times \mathbb{M}_2(\mathbb{R})$ are 16-dimensional. So, the answer must be (c).

Long answer:

Recall that

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\},$$

where $\{1, i, j, k\}$ form a group given by the following table:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

We claim that this is isomorphic to the group generated by the 2×2 matrices

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \leftrightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k \leftrightarrow \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

under multiplication. Indeed, all of the nonidentity matrices here have square -1, and matrix multiplication will show that they satisfy the same relations as the quaternions.

Let $z \in \mathbb{C}, \mathbf{h} = a1 + bi + cj + dk \in \mathbb{H}$, where $1, i, j, k$ denote the matrices given above. Define a map

$$\mathbb{C} \times \mathbb{H} \to \mathbb{M}_2(\mathbb{C}$$

$$(z, \mathbf{h}) \mapsto z\mathbf{h},$$

where the product on the right denotes scalar multiplication. It's easy to see that this is $\mathbb{R}$-balanced, so by the Univsersal Property of Tensor Products, this induces a homomorphism $\Phi : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \to \mathbb{M}_2(\mathbb{C})$ where

$$z \otimes \mathbf{h} \mapsto z\mathbf{h}.$$

Using the correspondence above, we can write

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \frac{i}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \leftrightarrow 1/2 \otimes 1 - i/2 \otimes i$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{i}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \leftrightarrow 1/2 \otimes 1 + i/2 \otimes i$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} - \frac{i}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \leftrightarrow 1/2 \otimes j - i/2 \otimes k$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} - \frac{i}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \leftrightarrow 1/2 \otimes j - i/2 \otimes k$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \frac{-1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} - \frac{i}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \leftrightarrow -1/2 \otimes j - i/2 \otimes k$$

To get the complex versions of the matrices on the left, just scale everything by i. So, given a matrix

$$\begin{pmatrix} a_{11}+ib_{11} & a_{12}+ib_{12} \\ a_{21}+ib_{21} & a_{22}+ib_{22} \end{pmatrix},$$

send it to the tensor

$$\begin{aligned}
&\Big((a_{11}+ib_{11})/2\otimes 1 - i(a_{11}+ib_{11})/2\otimes i\Big) + \Big((a_{22}+ib_{22})/2\otimes 1 + i(a_{22}+ib_{22})/2\otimes i\Big)\\
&+\Big((a_{12}+ib_{12})/2\otimes j - i(a_{12}+ib_{12})/2\otimes k\Big) + \Big(-(a_{21}+ib_{21})/2\otimes j - i(a_{21}+ib_{21})/2\otimes k\Big)\\
&= \Big((a_{11}+ib_{11})/2 + (a_{22}+ib_{22})/2\Big)\otimes 1 + \Big(-i(a_{11}+ib_{11})/2 + i(a_{22}+ib_{22})/2\Big)\otimes i \quad (1)\\
&+\Big((a_{12}+ib_{12})/2 - (a_{21}+ib_{21})/2\Big)\otimes j + \Big(-i(a_{12}+ib_{12})/2 - i(a_{21}+ib_{21})/2\Big)\otimes k.
\end{aligned}$$

Call this homomorphism Ψ. We'll show that Φ and Ψ are inverses. Let $z_j = a_j + ib_j$, and consider the element $\mathbf{x} = z_1\otimes 1 + z_2\otimes i + z_3\otimes j + z_4\otimes k \in \mathbb{C}\otimes_{\mathbb{R}}\otimes\mathbb{H}$. Then,

$$\begin{aligned}
\Psi(\Phi(\mathbf{x})) &= \Psi\begin{pmatrix} a_1-b_2+i(b_1+a_2) & a_3-b_4+i(b_3+a_4) \\ -a_3-b_4+i(a_4-b_3) & a_1+b_2+i(b_1-a_2) \end{pmatrix}\\
&= w_1\otimes 1 + w_2\otimes i + w_3\otimes j + w_4\otimes k,
\end{aligned}$$

where the w_l's are complex numbers. When we apply Ψ to this matrix, we use the formula above to get

$$w_1 = \frac{a_1-b_2+i(b_1+a_2)}{2} + \frac{a_1+b_2+i(b_1-a_2)}{2} = a_1+ib_1 = z_1;$$

$$w_2 = \frac{-i(a_1-b_2+i(b_1+a_2)}{2} + \frac{i(a_1+b_2+i(b_1-a_2))}{2} = a_2+ib_2 = z_2;$$

$$w_3 = \frac{a_3-b_4+i(b_3+a_4)}{2} - \frac{-a_3-b_4+i(a_4-b_3)}{2} = a_3+ib_3 = z_3;$$

$$w_4 = \frac{-i(a_3-b_4+i(b_3+a_4))}{2} - \frac{i(-a_3-b_4+i(a_4-b_3))}{2} = a_4+ib_4 = z_4.$$

So, $\Psi(\Phi(\mathbf{x})) = \mathbf{x}$.

In the other direction, let $A = (c_{ij}) \in \mathbb{M}_2(\mathbb{C})$ with $c_{ij} = a_{ij} + ib_{ij}$, with $a_{ij}, b_{ij} \in \mathbb{R}$.

Then, $\Psi(A)$ is the same as equation (1). Applying Φ to (1) gives us the matrix $B = (d_ij) \in \mathbb{M}_2(\mathbb{C})$ with

$$d_{11} = (a_{11} + ib_{11})/2 + (a_{22} + ib_{22})/2 + i\bigg(- i(a_{11} + ib_{11})/2 + i(a_{22} + ib_{22})/2\bigg) = a_{11} + ib_{11};$$

$$d_{12} = (a_{12} + ib_{12})/2 - (a_{21} + ib_{21})/2 + i\bigg(- i(a_{12} + ib_{12})/2 - i(a_{21} + ib_{21})/2\bigg) = a_{12} + ib_{12};$$

$$d_{21} = -\bigg((a_{12}+ib_{12})/2-(a_{21}+ib_{21})/2\bigg)+i\bigg(-i(a_{12}+ib_{12})/2-i(a_{21}+ib_{21})/2\bigg) = a_{21}+ib_{12};$$

$$d_{22} = (a_{11} + ib_{11})/2 + (a_{22} + ib_{22})/2 - i\bigg(- i(a_{11} + ib_{11})/2 + i(a_{22} + ib_{22})/2\bigg) = a_{22} + ib_{22}.$$

So,

$$\Phi(\Psi(A)) = A.$$

This implies that Ψ and Φ are inverses, which means $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathbb{M}_2(\mathbb{C})$. So, (c) is the correct answer.

4. Solve the following:

(a) Prove that $R/I \otimes_R R/J \cong R/(I + J)$ for R a commutative ring and $I, J \subset R$ ideals.

(b) Find the dimension of $\mathbb{Q}[x, y]/(x^2 + y^2) \otimes_{\mathbb{Q}[x,y]} \mathbb{Q}[x, y]/(x + y^3)$ as a vector space over $\mathbb{Q}$, or explain why it's infinite.

(a)

For a commutative ring R, a quotient R/I has a natural R-bimodule structure

$$r \cdot \overline{s} = \overline{rs} = \overline{sr} = \overline{s} \cdot r.$$

Define a map

$$\varphi : R/I \times R/J \to R/(I+J),$$
$$(\overline{r}, \overline{s}) \mapsto \overline{rs}).$$

First, we show that this is well defined: suppose that $\overline{r} = \overline{r'}, \overline{s} = \overline{s'}$. Then,

$$rs - r's' = rs - r's + r's - r's' = (r - r')s + r'(s - s') \in I + J.$$

So, $\varphi(\overline{r}, \overline{s}) = \varphi(\overline{r'}, \overline{s'})$, and so φ is well-defined. It is also R-balanced since

$$\varphi(\overline{rr'}, \overline{s}) = \overline{rr's} = \varphi(\overline{r}, \overline{r's}).$$

So, by the Universal Property of tensor products, we get a homomorphism $\Phi : R/I \otimes R/J \to R/(I+j)$ such that $\Phi(\overline{r} \otimes \overline{s}) = \overline{rs}$.

Now, consider the homomorphism

$$\Psi : R/(I+J) \to R/I \otimes R/J,$$

$$\overline{r} \mapsto \overline{r} \otimes \overline{1}.$$

We claim that Φ and Ψ are inverse to each other. Indeed,

$$\Psi\Phi(\overline{r} \otimes \overline{s}) = \Psi(\overline{rs}) = \overline{rs} \otimes \overline{1} = \overline{r} \cdot s \otimes \overline{1} = \overline{r} \otimes s \cdot \overline{1} = \overline{r} \otimes \overline{s},$$

$$\Phi\Psi(\overline{r}) = \Phi(\overline{r} \otimes \overline{1}) = \overline{r}.$$

So, $R/I \otimes R/J \cong R/(I+J)$.

(b) By part (a), we have

$$\mathbb{Q}[x,y]/(x^2+y^2) \otimes_{\mathbb{Q}[x,y]} \mathbb{Q}[x,y]/(x+y^3) \cong \mathbb{Q}[x,y]/((x^2+y^2)+(x+y^3)).$$

This gives us the relations

$$x^2 = -y^2, x^4 = y^4 = -xy.$$

By the first relation, the only non-constant monomials that occur in this quotient are $x^n y^\epsilon$, where $\epsilon \in \{0,1\}$. We can write

5. Solve the following questions:

(a) If F is a field, prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible over F.

(b) Show that $f(x) = x^2 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$, and find the inverse of $1 + x$ in $\mathbb{Q}[x]/(f(x))$.

(a) We want to show that the maximal ideals of $F[x]$ are of the form $(f(x))$, where $f(x)$ is irreducible over F. Recall that $F[x]$ is a PID when F is a field.

Consider an arbitrary ideal $I = (f(x))$ in $F[x]$. If $f(x)$ is reducible, then we can write $f(x) = p(x)q(x)$ for nonconstant polynomials p and q. This implies that $(f(x)) \subsetneq (q(x))$, and since $q(x)$ is nonconstant, it is not all of $F[x]$. So, I is not maixmal.

If $(f(x))$ is not maximal, then it is properly contained in some ideal J. Since $F[x]$ is a PID, there's some polynomial $g(x)$ such that $f(x) = g(x)h(x)$ and $\deg h \geq 1$, which implies that $f(x)$ is reducible.

So, $I = (f(x))$ is maximal if and only if f is irreducible. Since $F[x]/(f(x))$ is a field if and only if $(f(x))$ is maximal, this implies that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

(b) We have $x^2 = -2x - 2$ in $\mathbb{Q}[x]/(f(x))$, so

$$-(1+x)^2 = -x^2 - 2x - 1 = 2x + 2 - 2x - 1 = 1,$$

so the inverse of $1 + x$ is $-1 - x$.

6. Let V be the subspace of $\mathbb{C}^3$ spanned by $v_1 = (1, -1, 0), v_2 = (0, 1, -1)$, which is an invariant subspace under the permutation action of S_3, and so gives a two-dimension representation $\rho : S_3 \to GL(V)$.

(a) Write down the matrices of $\rho(\sigma)$ in this basis.

(a)

S_3 acts on a triple $\mathbf{v} = (v_1, v_2, v_3)$ by defining $\sigma \cdot \mathbf{v}$ to be the triple with v_i in the $\sigma(i)$th entry.

$\rho(1)$ is of course the identity matrix.

$$(12)\cdot(1,-1,0)=(-1,1,0)=-v_1,\quad (12)\cdot(0,1,-1)=(1,0,-1)=v_1+v_2,$$

$$\Rightarrow \rho(12)=\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$(13)\cdot(1,-1,0)=(0,-1,1)=-v_2, (13)\cdot(0,1,-1)=(-1,1,0)=-v_1,$$

$$\Rightarrow \rho(13)=\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

$$(23)\cdot(1,-1,0)=(1,0,-1)=v_1+v_2, (23)\cdot(0,1,-1)=(0,-1,1)=-v_2,$$

$$\Rightarrow \rho(23)=\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

$$(123)\cdot(1,-1,0)=(0,1,-1)=v_2, (123)\cdot(0,1,-1)=(-1,0,1)=-v_1-v_2,$$

$$\Rightarrow \rho(123)=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$(132)\cdot(1,-1,0)=(-1,0,1)=-v_1-v_2, (132)\cdot(0,1,-1)=(1,-1,0)=v_1,$$

$$\Rightarrow \rho(132)=\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

2 Spring 2018

1. What is the splitting field of $f(x) = x^3 + x + 1 \in \mathbb{F}_5[x]$?

Since this polynomial is just degree 3, we can show that it is irreducible by just checking for roots:

$$f(\overline{0}) = \overline{1}, f(\overline{1}) = \overline{3}, f(\overline{2}) = \overline{1}, f(\overline{3}) = \overline{1}, f(\overline{-1}) = \overline{-1}.$$

So, $f(x)$ is irreducible over $\mathbb{F}_5$.

Consider the field $\mathbb{F}_{5^3}$, which is the splitting field of the polynomial $x^{5^3} - x$ over $\mathbb{F}_5$. We know that this polynomial is the product of all distinct irreducible polynomials in $\mathbb{F}_5[x]$ with degree dividing 3. $f(x)$ is such a polynomial, so its roots lie in $\mathbb{F}_{5^3}$. We know that $[\mathbb{F}_{5^3}, \mathbb{F}_5] = 3$. Since $[L, k] = [L, E][E, k]$ for fields $L \supset E \supset k$, we know that there are no intermediary fields between $\mathbb{F}_{5^3}$ and $\mathbb{F}_5$, so $\mathbb{F}_{5^3}$ is indeed the splitting field of $f(x)$.

2. Prove that if G is a nontrivial nilpotent group, then its center $Z(G)$ is also nontrivial.

If G is nilpotent then the lower central series of G terminates for some n:

$$G \supset G^1 \supset G^2 \supset \ldots \supset G^n = 1,$$

where $G^1 = [G, G]$, the commutator of G, and $G^i = [G, G^{i-1}]$. Suppose n is such that $G^n = 1$ and $G^{n-1} \neq 1$. then, we have

$$1 = G^n = [G, G^{n-1}] = \{xyx^{-1}y^{-1} : x \in G, y \in G^{n-1}\}.$$

Since $G^{n-1} \neq 1$, there exists some non-identity element $y \in G^{n-1}$, and since $G^n = 1$, we have $xyx^{-1}y^{-1} = 1$ for all $x \in G$, but by rearranging this gives us $xy = yx$, so $y \in Z(G)$.

3. Let G be a group of order 50, and let n be the number of elements of order 5 in G. Find all possible values of n, and prove that this list is correct.

Since $50 = 2 \cdot 5^2$, the Sylow-5 subgroups of 50 are of order 25. If n_5 is the number of Sylow-5 subgroups in G, then by the third Sylow-theorem, we have

$$n_5 \equiv 1 \mod 5, n_5 | 2.$$

This implies that there is only one Sylow-5 subgroup P of G.

By the second Sylow theorem, all p-groups are contained in a Sylow-p group. Since all elements of order 5 generated a subgroup of order 5, all element of order 5 lie in P.

Since $|P| = 5^2$ and 5 is prime, P must be Abelian, and by the Fundamental Theorem of Finitely Generated Abelian Groups, $P \cong \mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5$. In the first case, $n = 4$, (these elements are $\overline{5}, \overline{10}, \overline{15}, \overline{20}$), and in the second case, all nonidentity elements have order 5, so $n = 24$.

4. Consider the algebra $A = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Give a basis for A as a vector space over $\mathbb{R}$, and write out the product of every pair of basis vectors.

A simple tensor in A looks like $(x + iy) \otimes (u + iv)$, where $x, y, u, v \in \mathbb{R}$. We can re-write this tensor as

$$(x + iy) \otimes (u + iv) = x \otimes u + x \otimes iv + iy \otimes u + iy \otimes iv$$

$$= xu(1 \otimes 1) + xv(1 \otimes i) + vu(i \otimes 1) + yv(i \otimes i).$$

So a basis for V as a vector space over $\mathbb{R}$ is

$$\{1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i\}.$$

The products of each pair of these vectors are

$$(1 \otimes 1)^2 = 1, (1 \otimes 1)(1 \otimes i) = 1 \otimes i, (1 \otimes 1)(i \otimes 1) = i \otimes 1, (1 \otimes 1)(i \otimes i) = i \otimes i,$$

$$(1 \otimes i)^2 = -(1 \otimes 1), (1 \otimes i)(i \otimes 1) = i \otimes i, (1 \otimes i)(i \otimes i) = -i \otimes 1,$$

$$(i \otimes 1)^2 = -(1 \otimes 1), (i \otimes 1)(i \otimes i) = -(1 \otimes i),$$

$$(i \otimes i)^2 = 1 \otimes 1.$$

5. Give an example of a field F and a polynomial $f(x) \in F[x]$ that is irreducible but not separable.

Let $F = \mathbb{F}_2[t]$, and let $f(x) = x^2 - t = (x - \sqrt{t})^2$. It's not separable since it has a double root $\sqrt{t}$, which doesn't lie in $\mathbb{F}_2[t]$, which implies that $f(x)$ is irreducible over $\mathbb{F}_2[t]$.

6. Calculate the character table of the dihedral group D_4, by definition the group of order 8 with generators x, y and relations

$$x^4 = y^2 = 1, yxyx = 1.$$

The conjugacy classes of D_4 are

$$\{1\}, \{r, r^3\}, \{r^2\}, \{s, sr^2\}, \{sr, sr^3\}.$$

D_4 is not abelian, and $D_4/\langle r^2 \rangle$ is abelian, so $D_4' = \langle r^2 \rangle$. This quotient group is isomorphic to V the Klein-4 group, since it is made up of the element $\{\overline{1}, \overline{r}, \overline{s}, \overline{sr}\}$, each of which has order 2. Since this group has order 4, D_4 has four degree-1 representations. Since D_4 has five conjugacy classes and the sum of the squares of the degrees of the irreducible representations is 8, we must have that there is only one more irreducible representation, and that it is degree 2.

Since $a^2 = 1$ for all $a \in V$, the representations must send each element of V to (± 1). This gives us four distinct one-dimensional characters.

Each element of D_4 is a rotation or reflection in $\mathbb{R}^2$, so we can map each element to its corresponding rotation/reflection matrix in $\mathbb{R}^2$. r rotates by 90 degrees, and s reflects about the line $y = x$, so we get

$$r \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By calculating the traces of each character we get the following character table:

	1	r^2	s	r	sr
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

3 Fall 2017

1. Let $F \subset K$ be an inclusion of fields and let $\alpha, \beta \in K$ be two elements which are algebraic over F. Show that $\alpha + \beta$ is also algebraic over F.

Since α and β are algebraic, $[F(\alpha, \beta) : F]$ is finite. Since $F(\alpha, \beta)$, is a field, it contains γ, where $\gamma = \alpha + \beta, \alpha\beta, or \alpha/\beta$ (assuming $\beta \neq 0$). In any of these three cases, we have $F \subset F(\gamma) \subset F(\alpha, \beta)$, so

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\gamma)][F(\gamma) : F].$$

Since $F(\alpha, \beta)$ is a finite extension, and by this equation, we must have $F(\gamma)$ is a finite extension, hence γ is algebraic over F.

2. Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of $1 + \sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$, and let K be the splitting field of f. What is $[K : \mathbb{Q}]$ and what is Gal$(K/\mathbb{Q})$?

$1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$, and so $\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) \subset \mathbb{Q}(\sqrt[3]{2})$. Then,

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4})][\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) : \mathbb{Q}],$$

so $[\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) : \mathbb{Q}]|3$. Since

3. Let $M_n(\mathbb{R})$ denote the ring of $n \times n$ matrices over $\mathbb{R}$, and consider a (possibly non-unital) ring homomorphism $f : M_{n+1}(\mathbb{R}) \to M_n(\mathbb{R})$. Can f be non-zero?

The kernel of f is a two-sided ideal of $M_{n+1}(\mathbb{R})$. The only two-sided ideals of a matrix ring are the ring itself and 0. If f is nonzero, then $\ker f$ must be injective. We can think of these matrix rings as vector spaces over $\mathbb{R}$ of dimension $(n+1)^2$ and n^2. If $\ker f = 0$, then by the Rank theorem, $\dim \operatorname{ran} f = (n+1)^2$. However, the range of f is a subspace of $M_n(\mathbb{R})$, and thus must have dimension at most n, so this is a contradiction. Hence, f must be nonzero.

4. Find all maximal ideals of the ring $\mathbb{F}_7[x]/(x^2+1)$ and the ring $\mathbb{F}_7[x]/(x^3+1)$.

By the fourth isomorphism of rings, and because $\mathbb{F}_7[x]$ is a PID (since $\mathbb{F}_7$) is a field, the maximal ideals of the quotient rings $\mathbb{F}_7[x]/(x^2+1)$ and $\mathbb{F}_7[x]/(x^3+1)$ correspond to the irreducible polynomials that divide x^2+1 and x^3+1, respectively.

First, for x^2+1, it is easy to check via direct calculation that x^2+1 has no roots in $\mathbb{F}_7$, and, being of dimension ≤ 3, this tells us that it is irreducible, so $\mathbb{F}_7[x]/(x^2+1)$ has no maximal ideals.

Second, for x^3+1, we can see that it has roots 3, 5, and -1, so

$$x^3 + 1 = (x-3)(x+5)(x+1),$$

and these are obviously irreducible, so this ring has three maximal ideals.

5. Let F be a field and $p, q \in F[x]$. Show that

$$F[x]/(p) \otimes_{F[x]} F[x]/(q) \cong F[x]/(\mathbf{gcd}(p,q)).$$

Define a map

$$\varphi : F[x]/(p) \times F[x]/(q) \to F[x]/(\gcd(p,q)),$$
$$(f,g) \mapsto fg.$$

First, we claim that φ is well-defined. Indeed, if $f \equiv f' \mod (p)$ and $g \equiv g' \mod (q)$, then $f = f' + h_1 p$ and $g = g' + h_2 q$ for some polynomials h_1, h_2. then,

$$fg = (f' + h_1 p)(g' + h_2 q) = f'g' + f'h_2 q + g'h_1 p + h_1 h_2 p \equiv f'g' \mod (\gcd(p,q)).$$

So, φ is well-defined. Next, we claim that it is $F[x]$ balanced. Indeed, if $f, g, h \in F[x]$, then

$$\varphi(fh, g) = fhg \mod (\gcd(p,q)) = f(hg) \mod (\gcd(p,q)) = \varphi(f, hg),$$

and

$$\varphi(f+h, g) = (f+h)g \mod (\gcd(p,q)) = fg + hg \mod (\gcd(p,q)) = \varphi(f,g) + \varphi(h,g),$$

and by the same argument, φ is linear in the second term. So, by the Universal Property of Tensor Products, φ induces a homomorphism

$$\Phi : F[x]/(p) \otimes_{F[x]} F[x]/(q) \to F[x]/(\gcd(p,q))$$

such that $\Phi(f \otimes g) = fg \mod (\gcd(p,q))$.

Now, define

$$\Psi : F[x]/(\gcd(p,q)) \to F[x]/(p) \otimes_{F[x]} F[x]/(q),$$
$$f \mapsto f \otimes 1.$$

The fact that Ψ is a homomorphism is obvious. We claim that Ψ is well-defined. Indeed, if $f \equiv g \mod (\gcd(p,q))$, then $f - g = hd$, where h is some polynomial and $d = \gcd(p,q)$. By definition of the gcd, there exist polynomials m, n such that $d = mp + nq$. Then,

$$\Psi(f-g) = hd \otimes 1 = h(mp+nq) \otimes 1 = (hmp + hnq) \otimes 1 = (hm)p \otimes 1 + (hn)q \otimes 1 = 0 + hn \otimes q = 0.$$

Thus, $\Psi(f) = \Psi(g)$, and so Ψ is well-defined. Finally, we have

$$\Psi(\Phi(f \otimes g)) = \Psi(fg) = fg \otimes 1 = f \otimes g,$$

$$\Phi(\Psi(f)) = \Phi(f \otimes 1) = f.$$

So, Φ and Ψ are inverses, which implies that Φ is an isomorphism.

6. Prove that if p is a prime number, then every group G with p^2 elements is abelian.

By Lagrange, either $|Z(G)| = 1, p, p^2$. By the Class Equation, $|Z| \neq 1$. If $|Z(G)| = p$, then $G/Z(G)$ is cyclic, so $G/Z(G) = \langle xZ(G) \rangle$. Then, if $g, h \in G$, there exist $n, m \geq 0$ and $z_1, z_2 \in Z(G)$ so that

$$gh = x^n z_1 x^m z_2 = x^m z_2 x^n z_1 = hg,$$

implying G is abelian, which is a contradiction. Hence, $|Z(G)| = p^2$, so $Z(G) = G$.

4 Spring 2017

1. Let G be a finite group and $H \leq G$ a subgroup such that $[G : H] = p$, where p is the smallest prime dividing $|G|$. Show that $H \trianglelefteq G$.

Let X denote the set of left cosets of H, so $|X| = p$, and let G act on X by left multiplication, and let $K = \ker \pi$. If $x \in \ker \pi$, then $xH = H$, so $x \in H$, which implies $K \leq H$. Let $[H : K] = k$, so that $[G : K] = pk$. This implies that the image of G in $S_X = S_p$ has order pk, and being a subgroup of S_p, it divides $p!$, so k divides $(p-1)!$. This forces $k = 1$, for otherwise k would be divisible by some prime strictly smaller than p, which is a contradiction. So, $H = K$, and since K is normal, H is normal.

2. Let k be a field, and let $f \in k[x]$ be of degree $n \geq 1$. Let K be the splitting field of f. Prove that $[K : k] \leq n!$.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f, so that $K = F(\alpha_1, \ldots, \alpha_n)$. Then,

$$[K : k] = [k(\alpha_1, \ldots, \alpha_n) : k(\alpha_1, \ldots, \alpha_{n-1})][k(\alpha_1, \ldots, \alpha_{n-1}), k(\alpha_1, \ldots, \alpha_{n-2})] \cdots [k(\alpha_1) : k].$$

Since α_1 satisfies a degree n polynomial, we have $[k(\alpha_1) : k] \leq n$. We know that, over $k(\alpha_1)$, α_2 satisfies the polynomial $f/(x - \alpha_1)$, so that $[k(\alpha_1, \alpha_2) : k(\alpha_1)] \leq n - 1$. Continuing in this way, we get

$$[k(\alpha_1, \ldots, \alpha_i) : k(\alpha_1, \ldots, \alpha_{i-1})] \leq n - i + 1,$$

which implies

$$[K : k] \leq 1 \cdot 2 \cdot \ldots \cdot n - 1 \cdot n = n!.$$

3. Not on syllabus

4. Give an example of a projective R-module that is not free for $R = \mathbb{R}[x]/(x^4 + x^2)$.

$x^4+x^2 = x^2(x^2+1)$. The ideals (x^2) and (x^2+1) are clearly comaximal, since $-x^2+x^2+1 = 1$. So, by the Chinese Remainder Theorem

$$R \cong \mathbb{R}[x]/(x^2) \oplus \mathbb{R}[x]/(x^2+1).$$

R is free over itself, and since $\mathbb{R}[x]/(x^2)$ is a direct summand of R, it is a projective R-module.

If $\mathbb{R}[x]/(x^2)$ were a free R-module, then it would be isomorphic to some direct some of copies of R, so as a real vector space, $\mathbb{R}[x]/(x^2)$ would have dimension at least 4, however, it only has dimension 2, so this is impossible, hence $\mathbb{R}[x]/(x^2)$ is not a free R-module.

5. Let G be the nonabelian group of order 57.

(a) How many 1-dimensional characters does G have?

The number of 1-dimensional characters of G is $|G/G'|$, where G' is the commutator subgroup of G. $57 = 19 \cdot 3$, So the proper subgroups of G are of size 19 and 3, which are prime, so there exist subgroups of both orders by the Sylow Theorems. Since 3 is the smallest prime dividing 57, the Sylow-19 subgroup is normal. Another way to see this is that

$$n_{19} \equiv 1 \mod 19. \quad n_{19}|3,$$

so $n_{19} = 1$. The Sylow-3 subgroups cannot be normal, for otherwise we'd have $G \cong \mathbb{Z}_{19} \times \mathbb{Z}_3$, which would then imply that G is abelian. Since $G'\text{char}G$, this implies that $|G'| = 19$, so $|G/G'| = 3$, and so there are three 1-dimensional characters of G.

(b) What are the dimensions (aka degrees) of the other irreducible characters of G?

We know that

$$57 = r_1^2 + \ldots + r_k^2$$

where r_i is the degree of each distinct irreducible character, and k is the number of conjugacy classes of G. It is also a known result that the degrees of the irreducible representations of G must divide the order of G. Since $19^2 > 54$ this implies that all the remaining irreducible representations must be of degree 3.

6. Let $\mathbb{F}$ be a finite field.

(a) Show that $|\mathbb{F}| = p^r$ for some prime p.

Since $\mathbb{F}$ is finite, it has characteristic p for some prime p. Let F denote the prime subfield of $\mathbb{F}$, which is isomorphic to $\mathbb{F}_p$. We can consider the extension $\mathbb{F}/F$, which is finite of degree r, since $\mathbb{F}$ is finite. So, we can write $\mathbb{F}$ as

$$a_1 x_1 + \ldots + a_r x_r,$$

where $a_i \in F$ for all i. Since $F = \mathbb{F}_p$, there are p choices for each a_i, hence p^r total choices, so p^r total elements of $\mathbb{F}$.

Alternate proof: Since $\mathbb{F}$ is finite, it has characteristic p for some prime p, i.e. 1 has order p in $(\mathbb{F}, +)$. Then for any $a \in \mathbb{F}$, $pa = p(a \cdot 1) = pa \cdot p1 = 0$, so the additive order of a divides p and hence equals p for all $a \neq 0$. But then Cauchy's theorem says that if q is any prime dividing the order of an arbitrary group G then there exists a $g \in G$ of order q. Hence p is the only prime that divides the order of $\mathbb{F}$ so $|\mathbb{F}| = p^r$ for some $r \in \mathbb{N}$.

(b) Show that the multiplicative group $\mathbb{F} \setminus \{0\}$ is a cyclic group.

If $x, y \in \mathbb{F}^\times$ with relatively prime orders a and b respectively, consider the element xy. Since $(xy)^{ab} = 1$, the order of xy is $\leq ab$. $(xy)^a = y^a$, which has order b. Since $(a, b) = 1$, there's not smaller number c such that ac is a multiple of b, for if $b|c$, then $b|c$, so $c = bq$, and the smallest such c is b itself. Similarly, $(xy)^b = x^b$ has order a. So, ab divides the order of xy, which implies that the order of xy is ab.

If $d|a$. Then $x^{a/d}$ must have order d, since any smaller number c will give a number smaller than a.

If x, y have arbitrary orders, then factor these orders into primes:

$$|x| = p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$
$$|y| = p_1^{\beta_1} \cdots p_n^{\beta_n},$$

where $\alpha_i, \beta_i \geq 0$. The lcm is

$$p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_n^{\max\{\alpha_n, \beta_n\}}.$$

For each i, we shoed above that we can find elements with orders $p_i^{\alpha_i}$ and $p_i^{\beta_i}$. Pick the element with the larger order, call it z_i. Then, the z_i's have relatively prime orders, so their product will give us an element with the desired order.

Now, suppose that $x \in \mathbb{F}^\times$ with largest order a. We claim that the order of each element in $\mathbb{F}^\times$ divides r. Indeed, if this were false, then there'd be an element y with order $b \not| a$,

and so $\text{lcm}(a,b) > a$, and by our work above, there'd be an element with that order, which contradicts the maximality of a. So, $g^a = 1$ for all $g \in \mathbb{F}^\times$.

Now, let r be the largest order in $\mathbb{F}^\times$, and consider the polynomial $x^r - 1$. By our work above, we know that every element in $\mathbb{F}^\times$ is a root of this polynomial, so the order of the group is at most r, but since $r||\mathbb{F}^\times|$ by Lagrange's Theorem, we have the reverse inequality, and so the two values are equal, and so $\mathbb{F}^\times$ is cyclic.

Alternate Proof: Let $|\mathbb{F}^\times| = n$ and let $d|n$. Then any element $a \in \mathbb{F}^\times$ whose order divides d is a root of the polynomial $p(x) = x^d - 1$. Since $\mathbb{F}$ is a field $p(x)$ has at most d roots in $\mathbb{F}$, so $\mathbb{F}^\times$ has at most d elements whose order divides d for all $d|n$.

Recall the Fundamental Theorem of Finite Abelian groups states that every finite abelian group is the internal direct sum of cyclic groups whose orders are prime powers.

$$\mathbb{F}^\times \cong \bigotimes_{i=1}^{k} \mathbb{Z}_{p_i^{m_i}}$$

where the p_i's are not necessarily distinct primes dividing n. Let $r = lcm(p_1^{m_1}, \ldots, p_k^{m_k})$. Observe that $r|n$ and that for all $a \in \mathbb{F}^\times$, $a^r = 1$, so the order of a divides r. Since $|\mathbb{F}^\times| = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$, the property in the above paragraph and the fact that $r \leq p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ implies that $r = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$. Hence the p_i's are distinct primes and so $\mathbb{F}^\times$ is a direct product cyclic groups of relatively prime orders, which implies that $\mathbb{F}^\times$ itself is cyclic.

5 Fall, 2016

1. Let F_n be the free group on n generators with $n \geq 2$. Prove that the center $Z(F)$ is trivial.

Let $G = \langle g_1, \ldots, g_n \rangle$ and suppose $h \in Z(F)$. h can be written as a reduced word $h = h_1 \cdots h_k$, where each $h_i = g_j^{m_j}$ where m_j is an integer. Since $h \in Z(G)$, $hh_1^{-1} = h_1^{-1}h$, which implies that

$$h_2 \ldots h_k = h_1 \cdots h_k h_1^{-1}.$$

However, $h_1 \neq h_2$ since $n \geq 2$. Also, $h_1^{-1} = g_j^{m_j}$ for some j, so the most cancellation that can occur on the right hand side is if h_k is a power of g_j, but since $n \geq 2$, h_{k-1} is not a power of g_j and so no further cancellation can occur, which means the left hand side remains undisturbed. In particular, if $n = 2$, we have $g_1^{m_1} g_2^{m_2}$, then we have $g_2^{m_2} = g_1^{m_1} g_2^{m_2} g_1^{-m_1}$, which is impossible.

2. Let G be a finite group that acts transitively on a set X of cardinality ≥ 2. Show that there exists an element G which acts on X without any fixed points. Is the same true if G is infinite?

By Burnside's Counting Lemma,

$$|G| \cdot |X/G| = \sum_{\alpha \in G} |\text{fix}(\alpha)|$$

where $|X/G|$ is the number of orbits. If G acts transitively, this value is 1. Since $|X| \geq 2$, $|\text{fix}(e)| \geq 2$, where e is the identity of G. Then, if $|\text{fix}(\alpha)| \geq 1$ for all $\alpha \neq e$, we have

$$\sum_{\alpha \in G} |\text{fix}(\alpha)| \geq |G| + 1,$$

which is a contradiction. Hence, at least one element cannot have a fixed point.

Now, let $G = S_{\mathbb{Z}}$, and let $H \geq G$ be the subgroup of elements that permute only finitely many members of $\mathbb{Z}$. This group is transitive, since $(m, n) \in \mathbb{Z}$ for all $m, n \in \mathbb{Z}$. Also, since every $\sigma \in H$ permutes finitely many elements, there must be an $n \in \mathbb{Z}$ such that $\sigma(n) = n$, i.e. every $\sigma \in H$ has a fixed point.

3. Show that every linear transformation $A : \mathbb{R}^3 \to \mathbb{R}^3$ has both a 1-dimensional invariant subspace and a 2-dimensional invariant subspace.

The characteristic polynomial of A is degree 3, hence it must have a real root λ of multiplicity 1. If λ has multiplicity 3, then A is similar to a diagonal matrix and then we're done. Otherwise, we have $\dim E_\lambda = 1$ (see Friedberg, pg 264). Let v_λ be the corresponding eigenvector. Then, E_λ is a 1-dimensional invariant subspace of A, and its direct-sum complement is a two-dimensional invariant subspace of A (pretty much done, but check the end).

4. Let $I, J \subset R$ be ideals in a PID. Prove that $I + J = R$ if and only if $IJ = I \cap J$.

Suppose $I + J = R$. We get $IJ \subset I \cap J$ for free. Suppose $x \in I \cap J$. Let $(a) = I, (b) = J$. Since $I + J = R$, there exist $m, n \in R$ such that $am + bn = 1$, so that $x = (am + bn)x = m(ax) + n(xb) \in IJ$, so $IJ = I \cap J$.

If $IJ = I \cap J$, then $I \cap J = (ab)$. Since R is a PID, it is also a UFD, a and b decompose uniquely into primes:

$$a = u_1 p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$
$$b = u_2 q_1^{\beta_1} \cdots q_l^{\beta_l},$$

where u_1, u_2 are units. Suppose a and b have a common prime p. However, that would imply that there exists an element $d \in I \cap J$ that divides ab but isn't associate to ab, hence $d \notin (ab)$, which is a contradiction. So, they don't have any primes in common, which implies $\gcd(a, b) = 1$, so $I + J = R$.

5. Let F be a finite field and let L be the subfield of F generated by elements of the form x^3 for all $x \in F$. Prove that if $L \neq F$, then F has exactly 4 elements.

F has order p^k for some prime p and integer $k \geq 1$, and so $F^\times$ has order $p^k - 1$. The multiplicative group $L^\times$ is a subgroup of $F^\times$. If $p^k - 1$ is relatively prime to 3, then x^3 will generate all of $F^\times$ for a generator x of $F^\times$. If 3 does divide $p^k - 1$, then x^3 will not generate $F^\times$, and each element of $L^\times$ will have order equal to one-third of their original order, i.e. $|x^3| = |x|/3$. So, the order of $L^\times$ is $\frac{1}{3}(p^k - 1)$. L is also a subfield, and therefore additive subgroup, of F, so $|L| = p^l$ for some $0 < l < k$, and therefore $|L^\times| = p^l - 1$, so we have the equation

$$p^l - 1 = \frac{1}{3}(p^k - 1),$$

which can be re-arranged to get

$$(3 - p^{k-l})p^l = 2.$$

Since $l > 0$, we must have $p = 2$ and $l = 1$, which implies $k = 2$, and therefore $|F| = 4$.

6. Show that the $\mathbb{R}$-modules $L = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $M = \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ are not isomorphic.

Short answer: $M \cong \mathbb{C}$ and $L \cong \mathbb{C}^2$.

We can write every element of M as $z \otimes 1$ where $z \in \mathbb{C}$, since if $\sum(z_i \otimes w_i) \in \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$, then we can write it as

$$\sum(z_i \otimes w_i) = \sum(z_i w_i \otimes 1) = \left(\sum z_i w_i\right) \otimes 1,$$

which gives a clear $\mathbb{R}$-vector space isomorphism with $\mathbb{C}$.

Over $\mathbb{R}$, L has basis $\{1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i\}$, so it has dimension 4 over $\mathbb{R}$.

6 Spring 2016

1. Let k be a field and let $R = Mat_{n,n}(k)$ be the ring of $n \times n$ matrices with entries from k. Let $f : R \to S$ be any ring homomorphism. Show that f is either injective or zero.

$K = \ker f$ is an ideal of R. Let I be the set of terms of elements of K, which is a subset of k. We claim that this is an ideal of k. Indeed, if $a, b \in I$, then there are matrices $A, B \in K$ such that a is the i, jth entry of A and b is the s, tth entry of B. Apply elementary matrices that moves b to the i, jth entry, and call this matrix $\tilde{B}$, which is in K since K is an ideal. Then, $a + b$ is the i, jth entry of $A + \tilde{B}$, so that I is an abelian group.

If $r \in k$ and $a \in I$, apply elementary matrices that send a to the $1, 1$-entry of A, and call this matrix $\tilde{A}$, which is in K since K is an ideal. Then, $rI\tilde{A}$, which is in K since K is an ideal, has ra in its $1, 1$-entry. So, I is an ideal of k. Since k is a field, $I = k$ or 0.

If $I = 0$, then clearly $K = 0$, which implies that f is injective.

If $I = k$, we claim that $K = R$. Indeed, since K is an ideal, we can apply matrices that move terms and delete rows and columns, so if $a \in k$, the matrix with a in the i, j column is an element of K, and since K is an abelian group, we can add these matrices to get any matrix in R. So, $K = R$, which implies that $f \equiv 0$.

2. Let R be a ring with identity, consisting of p^2 elements. Show that R is commutative.

Let $x \in R \setminus \{0\}$. Then, $Z(x)$ is a subring of R, and in particular is a subgroup of R. By Lagrange, $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, then we're done. Otherwise, if $|Z(G)|$, then $R/|Z(G)| = \langle \alpha \rangle$ is a cyclic group. Let $r, s \in R \setminus Z(G)$. So, there exist $z_1, z_2 \in Z(G)$ and $n, m \in \mathbb{Z}$ such that $r = z_1 + n\alpha$ and $s = z_2 m\alpha$. Then,

$$rs = (z_1+n\alpha)(z_2+m\alpha) = z_1z_2+z_1m\alpha+n\alpha z_2+mn\alpha^2 = z_2z_1+z_2n\alpha+m\alpha z_1+nm\alpha^2 = (z_2+m\alpha)(z_1+n\alpha).$$

This implies that $r, s \in Z(x)$, which is a contradiction. Hence, $|Z(x)| = R$, and since x is arbitrary, R is commutative.

3. Let G be a group generated by elements a, b each of which has order 2. Prove that G has a subgroup of index 2.

Let $H = \langle ab \rangle = \langle ba \rangle$. We claim that $[G : H] = 2$, with the cosets being H and aH. Indeed, since $a^2 = b^2 = 1$, the elements of G are strings of a's and b's, such as $abababa$. The power of each a and b cannot exceed 1 since a and b have order 2. So, there are four types of strings:

1. start and end with a,
2. start with a and end with b,
3. start with b and end with a,
4. start and end with b.

In the first case, we have an element of the form $abababa \dots baba = a(ba)^n$ for some n, which is an element of aH.

In the second case, we have $abab \dots abab = (ab)^n$ for some n, so it's an element of H.

In the third case, we have $babab \dots aba = (ba)^n$ for some n, so it's an element of H

In the final case, we have $babab \dots abab = b(ab)^n$ for some n. Since $a(ab) = b$, this is an element of aH.

Thus, $[G : H] = 2$.

4. Prove that every finite group G of order > 2 has a nontrivial automorphism.

If G is nonabelian, then there's some $g \in G$ such that $ghg^{-1} \neq h$ for at least on $h \in H$. Thus, the inner automorphism of conjugation by g is a nontrivial automorphism.

If G is abelian, then $G \cong \mathbb{Z}_{n_1^{p_1}} \times \ldots \times \mathbb{Z}_{n_k^{p_k}}$ by the Fundamental Theorem. The automorphism group of $\mathbb{Z}_{n_1{}^{p_1}}$ is nontrivial, so pick some automorphism of $\mathbb{Z}_{n_1{}^{p_1}}$ and fix the other components of the direct product to get a nontrivial automorphism. However, if every

$n_i = 2$ and $p_i = 1$, we can permute the elements of the direct product to get a nontrivial automorphism.

5. Find all possible Jordan canonical forms for a matrix $A = T((123))$ if T is a two-dimensional complex linear representation of the symmetric group S_3.

There is only one two dimensional complex linear representation of S_3, and that is the standard representation.

$$T((123)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

This matrix has eigenvalues $\frac{-1\pm\sqrt{3}i}{2}$, and so the Jordan canonical form is

$$\begin{pmatrix} \frac{-1+\sqrt{3}i}{2} & 0 \\ 0 & \frac{-1-\sqrt{3}i}{2} \end{pmatrix}$$

6. Find the smallest nonnegative integer $c \geq 0$ for which $R_c = \mathbb{Z}[x]/(c, x^2 - 2)$ is a (a) Domain

We claim that R_0 is a domain. Indeed, Suppose that $p(x), q(x) \in \mathbb{Z}[x]$ such that $\overline{p(x)q(x)} = 0$ in R_0. This implies that $p(x)q(x) \in (x^2-2)$, which implies that x^2-2. x^2-2 is irreducible (by Eisenstein for $p = 2$) and $\mathbb{Z}[x]$ is a UFD (since it is a Euclidean Domain), which implies that $x^2 - 2$ is prime. So, $x^2 - 2$ divides either $p(x)$ or $q(x)$. In either case, this implies that $\overline{p(x)} = 0$ or $\overline{q(x)} = 0$. So, R_0 is an integral domain.

(b) Field

This is equivalent to find the smallest c such that $(c, x^2 - 2)$ is maximal. If $c = 1$, then $(1, x^2 - 2) = \mathbb{Z}[x]$, and so it cannot be maximal. If $c = 2$, then $x^2 = x \cdot x = 0$, so R_2 is not even a domain.

If $c = 3$, we claim that R_3 is a field. Indeed, R_3 consists of the elements $a_0 + a_1 x$ for $0 \leq a_0, a_1 \leq 2$, and here is the table of elements along with their inverses:

elements	inverses
0	N/A
x	2x
2x	x
1	1
1+x	2+x
1+2x	2+2x
2	2
2+x	1+x
2+2x	1+2x

The inverse rely on the fact that $2x(x) = 2x^2 = 2(2) = 4 = 1$.

7 Fall 2015

1. Let G be a finite group such that all Sylow subgroups of G are normal and abelian. Show that G is abelian.

Let $P_1, \ldots, P_n$ be the Sylow subgroups of G. Since they're all normal, they all correspond to different primes, and since they're all normal, it's true that $G \cong P_1 \times \ldots \times P_n$, and since all of these Sylow subgroups are assumed to be abelian, this implies that G is also abelian.

2. For a finite group G, define the subset $G^2 = \{g^2 : g \in G\} \subset G$. Is it true that G^2 is always a subgroup?

Let $G = A_4$. The element $(123) = (132)^2$ and $(234) = (243)^2$, and their product is $(12)(34)$, but this element is $(1324)^2$, but 4-cycles are odd, hence $(12)(34) \notin A_4^2$, and so A_4^2 is not a group.

3. What is the smallest possible n for which there is an n by n real matrix M

which has both

i. the rank of M^2 smaller than the rank of M,

ii. M leaves infinitely many length one vectors fixed.

If M fixes infinitely many unit vectors, then M must have an invariant subspace of dimension at least 2, since there are only two unit vectors in $\mathbb{R}$. This forces $n \geq 4$, since if M has a 2-dimensional invariant subspace, then so will M^2, so $\text{rank}M^2 \geq 2$. This implies that if $n = 3$ and $\text{rank}M = 2$ or 3, then so will $\text{rank}M^2$. So, let $n = 4$ and

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

The elements e_1, e_2, e_4 are in the range of M, and e_3 is in the kernel of M, so $\text{rank}M = 3$ and $\dim \ker M = 1$. Also,

$$M^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

This matrix has rank$= 2$ and $\dim \ker = 2$, and so this fixes the unit circle in $\mathbb{R}^2$ and satisfies condition 1.

4. Let I denote the ideal in the ring $\mathbb{Z}[x]$ generated by 5 and $x^3 + x + 1$. Is I a prime ideal?

My guess is yes since 5 is prime.

Suppose that $\overline{p(x)q(x)} = 0$, so that $p(x)q(x) \in (5, x^3 + x + 1)$, so

$$p(x)q(x) = r(x)(x^3 + x + 1) + 5h(x).$$

Reduce the coefficients of $p(x)$ and $q(x)$ mod 5 and suppose then that $p(x)q(x) \neq 0$. If $p(x)q(x)$ is still 0 in $\mathbb{Z}[x]/I$, then $x^3 + x + 1 | p(x)q(x)$. $x^3 + x + 1$ is irreducible (rational roots theorem) and is therefore prime, since $\mathbb{Z}[x]$ is a UFD. So, $x^3 + x + 1$ divides $p(x)$ or $q(x)$. So, WLOG, $p(x) = g(x)(x^3 + x + 1) + 5k(x)$ so $p(x) = 0$ in $\mathbb{Z}[x]/I$.

If $p(x)q(x) \equiv 0 \bmod 5$, then look at the terms of each polynomial:

$$p(x) = a_0 + a_1x + a_2x^2, \quad q(x) = b_0 + b_1x + b_2x^2,$$

$$p(x)q(x) = a_0b_0 + (a_0b_1 + b_0a_1)x + (a_0b_2 + a_1b_1 + b_0a_2)x^2 + (a_1b_2 + a_2b_1)x^3 + a_2b_2x^4.$$

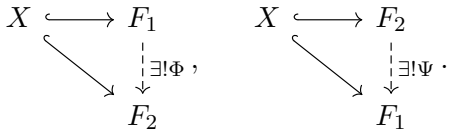
At least one of a_0, b_0 must be a multiple of 5, since 5 is prime. WLOG, assume a_0 is.

If b_0 is not, then looking at the coefficient of x, a_1 must be a multiple of 5. If b_0 is, then the coefficient shows that one of b_1, a_1 must be a multiple of 5. WLOG, assume a_1 is.

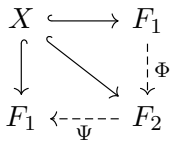
If b_1 is not, then the coefficient of x^3 show that a_2 must be a multiple of 5. If b_1 is, then the coefficient of x^4 shows that at least one of a_2 or b_2 must be a multiple of 5. So, 5 must divide at least one of $p(x)$ or $q(x)$, so $p(x) = 0$ or $q(x) = 0$. Thus, $\mathbb{Z}[x]/I$ is a domain, so I is prime.

5. Show that two free groups are isomorphic if and only if they have equal rank.

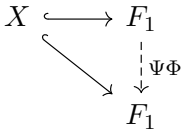
If F_1 and F_2 are equal rank, then they have, up to bijection, the same basis X. So, we have inclusion maps $X \hookrightarrow F_1$ and $X \hookrightarrow F_2$. Then, we have commutative diagrams



This gives us the commutative diagram



Which simplifies to



However, the identity also satisfies this diagram, and by uniqueness, $\Psi\Phi$ is the identity on F_1. By the same argument, $\Phi\Psi$ is the identity on F_2. So, $F_1 \cong F_2$.

Now, suppose that $F_1 \cong F_2$, and let X_1, X_2 be bases for F_1 and F_2, respectively. We claim that the homomorphisms from a free group F with basis X to $\mathbb{Z}_2$ are in bijection with functions $\gamma : X \to \mathbb{Z}_2$. Indeed, by definition of a free group, for every function $\gamma : X \to \mathbb{Z}_2$, we get a unique homomorphism $\phi : F \to \mathbb{Z}_2$, and if $\phi : F \to \mathbb{Z}_2$ is a homomorphism, then the restriction of ϕ to the basis of F gives a map $\gamma : X \to \mathbb{Z}_2$.

Since $F_1 \cong F_2$, $\mathrm{Hom}(F_1, \mathbb{Z}_2) = \mathrm{Hom}(F_2, \mathbb{Z}_2)$, so the cardinalities are the same. We claim that $|\mathrm{Hom}(F_1, \mathbb{Z}_2)| = 2^{|X_1|}$. Indeed, for each $x \in X_1$, we have 2 choices for where to send x, hence there are $2^{|X_1|}$ total functions. This implies that $2^{|X_1|} = 2^{|X_2|}$, which implies that $|X_1| = |X_2|$.

6. Find the $\mathbb{Q}$-dimension of the splitting field over $\mathbb{Q}$ of $x^5 - 3$.

The roots of this polynomial are $\sqrt[5]{3}\zeta_5^n$ for $0 \leq n \leq 4$. So, the degree of this extension is

$$[\mathbb{Q}(\sqrt[5]{3}, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{3}, \zeta_n) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{3}, \zeta_n) : \mathbb{Q}(\sqrt[5]{3})][\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}].$$

Since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$, the degree of this extension is divisible by 20. Also, $\sqrt[5]{3}$ satisfies a polynomial of degree 5 over the field $\mathbb{Q}(\zeta_5)$ so $[\mathbb{Q}(\sqrt[5]{3}, \zeta_n) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is at most 20, hence it is 20.

8 Spring 2015

1. Show that if M is a nondiagonalizable complex matrix and M^n is diagonalizable, then $\det(M) = 0$.

Since M is a complex matrix, we can put it into Jordan canonical form. Since M^n is diagonal, then each Jordan block raised to the nth power is diagonal. However, a Jordan block can only eventually become diagonal if λ, the eigenvalue, is 0, since

$$J^n = \lambda^n I + \sum_{i=1}^{m-1} \binom{n}{i} \lambda^{n-i} L^i$$

where J is an $m \times m$ Jordan block. So, $\lambda = 0$, which implies that $\det(M) = 0$.

2. Find the degree of $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ over $\mathbb{Q}$.

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

We claim that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. Indeed, if it were, then there would be $a, b \in \mathbb{Q}$ such that

$$\sqrt[3]{2} = a + b\sqrt{2} \Rightarrow 2 = (a + b\sqrt{2})^3 = a^3 + 3a^2b\sqrt{2} + 6ab^2 + 2b^3\sqrt{2},$$

$$\Rightarrow b(3a^2 + 2b^2) = 0 \Rightarrow b = 0,$$

which implies $\sqrt[3]{2}$ is rational, which it is not. So, $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$, so $x^3 - 2$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and so it's the minimal polynomial, so

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}), \mathbb{Q}(\sqrt{2})] = 3,$$

and we know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so the entire degree is 6.

3. Show that if G is an infinite simple group then every proper subgroup has infinitely many conjugates. Use this to conclude that G has infinitely many automorphisms.

Suppose there exists a proper subgroup $H \leq G$ with only finitely many congugates

$$H, g_1Hg_1^{-1}, \ldots, g_nHg_n^{-1}.$$

Let G act on H via conjugation, and consider the permutation representation $\pi : G \to S_{n+1}$. By the First Isomorphism Theorem,

$$G/\ker\pi \cong \mathrm{im}\pi.$$

The image is finite, hence $G/\ker\pi$ needs to be finite. G is simple, so its only normal subgroups are G and $\{e\}$, and G is infinite, hence $\ker\pi = G$, which implies $gHg^{-1} = H$ for all $g \in G$. So, H is a normal subgroup of G, which contradicts its simplicity. Thus, every proper subgroup has infinitely many conjugates. Because of this, the subgroup $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ has to be infinite, for otherwise each subgroup would not have infinitely many conjugates. This in turn implies that $\mathrm{Aut}(G)$ is infinite as well.

4. Find a quotient ring of $\mathbb{Z}[x]$ which is a PID but not a field.

Let $I = (x)$, so that $\mathbb{Z}[x]/I \cong \mathbb{Z}$, which is a PID but not a field.

5. Let $R = \mathbb{Q}[x]/(x^3 - 2)$.

(a) Is R a field? Why or why not?

$\mathbb{Q}[x]$ is a PID and $x^3 - 2$ is irreducible over $\mathbb{Q}$, hence it's maximal, which implies that $\mathbb{Q}[x]/(x^3 - 2)$ is a field.

(b) Run the extended Euclidean algorithm on $x^3 - 2$ and $x^2 - x + 1$ to find polynomials $A(x)$ and $B(x)$ with

$$A(x)(x^3 - 2) + B(x)(x^2 - x + 1) = \mathbf{gcd}(x^3 - 2, x^2 - x + 1).$$

Both of these polynomials are irreducible, so their gcd is 1. Now, to run the algorithm. By doing polynomial long division, we get

$$x^3 - 2 = (x + 1)(x^2 - x + 1) + 1 \Rightarrow 1 = x^3 - 2 - (x + 1)(x^2 - x + 1),$$

so $A(x) = 1$ and $B(x) = -(x + 1)$.

(c) Does $x^2 - x + 1$ have a multiplicative inverse in R? If yes, find it.

By (b) $(x + 1)(x^2 - x + 1) + 1 = 0$ in R, so $-(x + 1)(x^2 - x + 1) = 1$, so the multiplicative inverse of $x^2 - x + 1$ in R is $-(x + 1)$.

6. Let G be a finite group and $\rho : G \to GL_n(\mathbb{C})$ a representation.

(a) Show $\delta : G \to \mathbb{C}, g \mapsto \det(\rho(g))$ is a linear character of G (i.e. a group homomorphism to the multiplicative group)

Let $g, g' \in G$. ρ is a homomorphism, so $\rho(gg') = \rho(g)\rho(g')$. Then,

$$\det(\rho(gg')) = \det(\rho(g)\rho(g')) = \det(\rho(g))\det(\rho(g')) = \delta(g)\delta(g').$$

So, δ is a linear character.

(b) Show that if $\delta = -1$ for some $g \in G$, then G has a normal subgroup of index 2.

9 Fall 2014

1. Let G_1, G_2 be finite index subgroups of a group G. Show that the intersection $G_1 \cap G_2$ has finite index in G.

Let G_1 act on the set of left cosets of G_2, which is a finite set. The stabilizer of G_2 is $G_1 \cap G_2$, so by the orbit-stabilizer theorem, the size of the orbit containing G_2 (which is finite) is $[G_1 : G_1 \cap G_2]$, so

$$[G : G_1 \cap G_2] = [G : G_1][G_1 : G_1 \cap G_2].$$

Both of the factors on the right are finite, so the product on the left is as well.

2. Let G be a finite group and $N \subset G$ a subgroup of index p, where p is the smallest prime dividing $|G|$. Prove N is a normal subgroup of G.

Let G act on the set $X = \{H, g_1H, \ldots, g_{p-1}H\}$ of left cosets of H by multiplication. If x is in the kernel K of the action, then in particular $xH = H$, so that $K \leq H$, and so

$$[G : K] = [G : H][H : K] = pk.$$

If π is the permutation representation, then by the first isomorphism theorem G/K is isomorphic to a subgroup of S_p, and so $pk|p!$, so $k|(p-1)!$. If $k \neq 1$, then this would imply that k is divisible by a prime smaller than p, which contradicts our assumption, hence $k = 1$, so $H = K$. Since K is normal, so is H.

3. Does the additive group $\mathbb{Q}$ admit an epimorphism to a nontrivial finite group. Justify your answer.

If $\varphi : \mathbb{Q} \to G$ is a homomorphism, with G finite, then for any $q \in \mathbb{Q}$,

$$\varphi(q) = |G|\varphi(q/|G|) = e,$$

since $g^{|G|} = e$ for all $g \in G$ by Lagrange. Thus, φ is trivial, so no such epimorphism exists.

4. List all ideals of $\mathbb{F}_p[x]/(x^2 + x - 6)$ when

(a) $p = 7$,

By the 4th isomorphism theorem, the ideals of $\mathbb{F}_p[x]/(x^2 + x - 6)$ correspond to the ideals of $\mathbb{F}_p[x]$ that contain $x^2 + x - 6$, and since $\mathbb{F}_7[x]$ is a PID, these are the ideals of the form $(p(x))$, where $p(x)|x^2 + 6 - 6$, which are $x - 2$ and $x - 4$. So the ideals of $\mathbb{F}_p[x]/(x^2 + x - 6)$ are $(x - 2)/(x^2 + x - 6)$ and $(x - 4)/(x^2 + x - 6)$.

(b) $p = 5$**.**

Same argument, but in this case, the only ideal is $(x - 2)/(x^2 + x - 1)$.

5. Let ρ be a representation of a finite group G on a vector space V and let $v \in V$.

(a) Show that averaging $\rho_g(v)$ over G gives a vector $\overline{v} \in V$ which is fixed by G.

$$\rho_{g'}(\overline{v}) = \rho_{g'}\left(\frac{1}{|G|}\sum_{g\in G}\rho_g(v)\right) = \frac{1}{|G|}\sum_{g\in G}\rho_{g'}\rho_g(v) = \frac{1}{|G|}\sum_{h\in G}\rho_h(v) - = \overline{v}.$$

(b) What can you say about this vector when ρ is an irreducible representation?

Since $\overline{v}$ is G-invariant, then $Span\{\overline{v}\}$ is a G-invariant subspace of V. If ρ is irreducible, V has no non-trivial invariant subspaces. So either V is one-dimensional and ρ is trivial, or $\overline{v} = 0$.

6. If R is a commutative ring with identity, and S is a multiplicative subset of R, then every ideal J of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R. Is I uniquely determined by J? Why or why not?

Let $R = \mathbb{Z}$ and $S^{-1} = \mathbb{Z} - \{0\}$, so $S^{-1}R$ is the field of fractions of $\mathbb{Z}$. Then, clearly $S^{-1}R = S^{-1}\mathbb{Z}$. However, we claim that $S^{-1}R = S^{-1}2\mathbb{Z}$ as well. Indeed, $2/2 = 1$, so $1 \in S^{-1}2\mathbb{Z}$, which implies that $S^{-1}2\mathbb{Z}$ contains the entire ring. Thus, we have two different ideals in R that determine the same ideal in $S^{-1}R$, so I is not uniquely determined by J.

10 Spring 2014

1. Find the smallest order of a group which is not cyclic and not isomorphic to a symmetric group on five objects.

The orders 1, 2, 3, 5, 7 are out. For 4, the Klein 4 group is just isomorphic to a subgroup generated by two disjoint 2-cycles. The nonabelian group of order 6 is D_3 which is a subgroup of S_3 which can be embedded as a subgroup of S_5. Same with D_4. However, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian and generated by three elements of order 2. The elements of order 2 in S_5 are two-cycles and the pairs of 2-cycles, but since we're in S_5, it's impossible to find three such elements that commute with each other.

2. Consider the four dimensional real vector space

$$V = \{f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{R}\}$$

with the $\mathbb{R}[x]$-module structure given by shifting so that $(xf)(r) = f(r+1)$. Find a direct sum decomposition into irreducible $\mathbb{R}[x]$-modules.

We just need to find the rational canonical form. A basis for V is $\{e_i\}$ for $1 \leq i \leq 4$, where $e_i(j) = \delta_{ij}$. x defines a linear transformation on V, where $xe_i = e_{i-1}$, so $e_1 \mapsto e_4$. This gives us a matrix

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

which is the transpose of the companion matrix $x^4 - 1$. So, $V \cong \mathbb{R}[x]/(x^4 - 1)$. We can decompose this into irreducible $\mathbb{R}[x]$ modules, which are the maximal ideals of $\mathbb{R}[x]/(x^4-1)$, so

$$V \cong (x-1)/(x^4-1) \oplus (x+1)/(x^4-1) \oplus (x^2+1)/(x^4-1).$$

3. Let p, q be prime numbers with $p < q$ such that p is not a divisor of $q - 1$. Let G be a group of order qp. Which of the following is true: (a) G is always simple. (b) G is never simple. (c) G could be simple or non-simple.

Let n_p and n_q denote the number of Sylow p and q-subgroup of G, respectively. By the Sylow Theorems,

$$n_p \equiv 1 \mod p, \;\; n_p | q,$$
$$n_q \equiv 1 \mod q, \;\; n_q | p.$$

Since q is prime, $n_p = 1$ or q. Suppose $n_p = q$. Since $n_p \equiv 1 \mod p$, there's an s such that $n_p = sp + 1$, which implies that

$$sp + 1 = q \Rightarrow sp = q - 1 \Rightarrow p | q - 1$$

which is a contradiction. So, $n_p = 1$, which implies that there is exactly one Sylow p-subgroup of G, and that it's normal. So, G is never simple.

4. Give an example of a ring R and an R-module M which is projective but not free.

Let $R = \mathbb{Z}_6$ and $M = \{\overline{0}, \overline{2}, \overline{4}\} \cong \mathbb{Z}_3$. $\mathbb{Z}_6$ is free over itself, and isomorphic to the direct sum $\mathbb{Z}_3 \oplus \mathbb{Z}_2$. This implies that $\mathbb{Z}_3$ is projective, being a direct summand of a free module. However, if $\mathbb{Z}_3$, were a free $\mathbb{Z}_6$-module, then it would be a direct sum of copies of $\mathbb{Z}_6$,

implying that it would have order ≥ 6, but this is impossible. Hence, $\mathbb{Z}_3$ is not free as a $\mathbb{Z}_6$-module.

6. Let $\mathbb{C}(x)$ be the field of complex rational functions, i.e., the fraction field of the polynomial ring $\mathbb{C}[x]$. Let $\mathbb{C}(y)$ be another copy of the same field in the variable y. This field is an algebra over $\mathbb{C}$, hence $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ is another algebra over $\mathbb{C}$. Is it also a field?

Thanks to Wencin Poh for providing this solution.

Let R denote $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$. We will show that element $z = 1 \otimes 1 + \dfrac{1}{x} \otimes y \in R$ is a nonzero element that is not a unit.

Define the map

$$\varphi : \mathbb{C}(x) \times \mathbb{C}(y) \to \mathrm{Frac}(\mathbb{C}[x, y])$$

by linear extension of

$$\left(\frac{f(x)}{g(x)}, \frac{p(y)}{q(y)}\right) \mapsto \frac{f(x)p(y)}{g(x)q(y)},$$

where $f, g \in \mathbb{C}[x]$ and $p, q \in \mathbb{C}[y]$ with g and q being nonzero. Note that φ is linear in both components and is $\mathbb{C}$-balanced. Thus, by the universal property of tensor product, we have a unique nonzero $\mathbb{C}$-module homomorphism

$$\tilde{\varphi} : \mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y) \to \mathrm{Frac}(\mathbb{C}[x, y])$$

extending φ.

We note that $\tilde{\varphi}$ is also a $\mathbb{C}$-algebra homomorphism since $\tilde{\varphi}(1 \otimes 1) = 1$ and $\tilde{\varphi}$ is multiplicative as it is multiplicative on simple tensors.

Therefore $\tilde{\varphi}(z) = \dfrac{y}{x}$ is nonzero in $\mathrm{Frac}(\mathbb{C}[x, y])$, so z is nonzero in R.

Now, assume for the sake of a contradiction that there is $r \in R$ with $r \left(1 \otimes 1 + \dfrac{1}{x} \otimes y\right) = 1 \otimes 1$.

Without loss of generality (after taking least common multiple of denominators if necessary), let

$$r = \sum_{k \geq 0,\, l \geq 0} c_{kl} \frac{x^{k+1}}{xp(x)} \otimes \frac{y^l}{q(y)},$$

for some $c_{kl} \in \mathbb{C}$, $p \in \mathbb{C}[x]$ and $q \in \mathbb{C}[y]$, where the sum is over finitely many k's and l's.

Now, expansion of rz again yields terms of the form $c_{kl}\dfrac{x^{k+1}}{xp(x)} \otimes \dfrac{y^l}{q(y)}$ or $c_{kl}\dfrac{x^k}{xp(x)} \otimes \dfrac{y^{l+1}}{q(y)}$. If we choose a nonzero term in r such that y^l appears with the highest degree, say $c_{mn}\dfrac{x^{m+1}}{xp(x)} \otimes \dfrac{y^n}{q(y)}$, then by choice of the term, the expansion of rz would contain a nonzero term $c_{mn}\dfrac{x^m}{xp(x)} \otimes \dfrac{y^{n+1}}{q(y)}$. On the other hand, this expansion must equal $1 \otimes 1$, so in particular, the coefficient of $\dfrac{x^m}{xp(x)} \otimes \dfrac{y^{n+1}}{q(y)}$ must be zero - a contradiction.

Therefore, our initial assumption was false and we conclude that R cannot be a field as we have a nonzero nonunit element in R.

11 Fall2013

1. Let $G \subset \mathbb{M}_n(\mathbb{C})$ be a group of complex $n \times n$ matrices. Let V be the linear span of V and $V^\times$ the set of invertible elements of V. Show that $V^\times$ is also a group.

$I \subset G$, so $I \subset V^\times$. Now, if $A \in V^\times$, then we want to show that A^{-1} is as well. Suppose we can write $A = z_1A_1 + z_2A_2$ for $A_1, A_2 \in V$. We can write this as $\frac{1}{z_2}A_2^{-1}(A_1A_2 + I)$.

2. Consider an attempt to make an $\mathbb{R}$-linear map

$$f : \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \quad \textbf{or} \quad \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C},$$

in either direction given by the formula

$$f(x \otimes y) = x \otimes y.$$

In which direction is this map well-defined? Is it then surjective? Is it injective?

The map in the $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ direction is not well-defined. Consider the element $1 \otimes i = i \otimes 1 \in \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$. In $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, these two elements are not equal, which would imply $1 \otimes i$ maps to two elements, so f is not well-defined in this case.

For the other direction, define

$$\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C},$$

$$(z, w) \mapsto z \otimes w.$$

This map is $\mathbb{R}$-bilinear:

$$\varphi(z_1 + rz_2, w) = (z_1 + rz_2) \otimes w = z_1 \otimes w + r(z_2 \otimes w),$$

$$\varphi(z, w_1 + rw_2) = z \otimes (w_1 + rw_2) = z \otimes w_1 + z \otimes (rw_2) = z \otimes w_1 + (rz) \otimes w_2 = z \otimes w_1 + r(z \otimes w_2).$$

So, this induces a homomorphism $f : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ such that $f(x \otimes y) = x \otimes y$. This map is clearly surjective, for if $x \otimes y \in \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$, then $x \otimes y \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ maps to $x \otimes y \in \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$. However, $f(1 \otimes i) = f(i \otimes 1)$, but these elements are not equal in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, so f is not injective.

4. Let G be a group with an odd number of elements that has a normal subgroup N with 17 elements. Show that N lies in the center of G.

Since N is normal, we can have G act on the elements of N by conjugation. This gives a homomorphism

$$\pi : G \to \mathrm{Aut}(N) \cong (\mathbb{Z}/17\mathbb{Z})^{\times} \cong \mathbb{Z}/16\mathbb{Z},$$

which only has subgroups of even order, other than the trivial group. This implies that $\ker \pi = G$, so that $gng^{-1} = n$ for all $n \in N$, so $N \subset Z(G)$.

6. Compute $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ and find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

We'll show that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Indeed, suppose that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so that

$$\sqrt{3} = a + b\sqrt{2},$$

$$\Rightarrow 3 = a^2 + 2b^2 + 2ab\sqrt{2}.$$

So, either $a = 0$ or $b = 0$. Either case is impossible since 3 is irrational, so $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, so $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. The elements of this field are sums and products of elements of the form $a + b\sqrt{2}$ and $c + d\sqrt{3}$, so $\mathbb{Q}$-basis for this is

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}.$$

This is $\mathbb{Q}$-linearly independent and has four elements, so it must be a basis, since the vector space has dimension 4.

12 Spring 2013

1. Let A be a Boolean ring, i.e. $a^2 = a$ for all $a \in A$. Prove that A is commutative.

Note that

$$2a = (2a)^2 = 4a^2 = 4a \Rightarrow 2a = 0.$$

Now, for $a, b \in R$,

$$(a + b)^2 = a^2 + ab + ba + b^2 = a + b \Rightarrow ab + ba = 2ab = 0 \Rightarrow ba = ab.$$

2. Let R be a commutative ring with $1_R \neq 0$. Let $I \subset R$ be an ideal so that R/I is a division ring. Prove that I is maximal in R.

R is commutative, so R/I is commutative, and since R/I is a division ring, that implies that R/I is a field, which implies that I is maximal.

3. Let n and m be natural numbers. Show that the free group of rank n is isomorphic to the free group of rank m if and only if $m = n$.

Suppose that $m = n$. Let F_1 and F_2 be free groups with generating sets X_1, X_2 respectively. Since $m = n$, there's a bijection $\gamma : X_1 \to X_2$. By the Universal property of free groups, there's are unique homomorphisms $\Phi : F_1 \to F_2, \Psi : F_2 \to F_1$ making the following diagrams commute:

$$\begin{array}{ccc} X_1 & \hookrightarrow & F_1 \\ & \searrow^{\gamma} & \downarrow{\scriptstyle \Phi} \\ & & F_2 \end{array}, \qquad \begin{array}{ccc} X_2 & \hookrightarrow & F_2 \\ & \searrow^{\gamma^{-1}} & \downarrow{\scriptstyle \Psi} \\ & & F_1 \end{array}.$$

Putting these diagrams together gives

$$\begin{array}{ccc} X_1 & \hookrightarrow & F_1 \\ \downarrow{\scriptstyle \gamma} & \searrow^{\gamma} & \downarrow{\scriptstyle \Phi} \\ X_2 & \hookrightarrow & F_2 \\ & \searrow^{\gamma^{-1}} & \downarrow{\scriptstyle \Psi} \\ & & F_1 \end{array},$$

which reduces to

$$\begin{array}{ccc} X_1 & \hookrightarrow & F_1 \\ & \searrow^{id} & \downarrow{\scriptstyle \Psi\circ\Phi} \\ & & F_1 \end{array}.$$

Since the identity also makes this last diagram commute, we have $\Psi \circ \Phi = id_{F_1}$, so Φ is an isomorphism.

If F_1 and F_2 are isomorphic, then

$$\mathrm{Hom}(X_1, \mathbb{Z}_2) = \mathrm{Hom}(F_1, \mathbb{Z}_2) \cong \mathrm{Hom}(F_2, \mathbb{Z}_2) = \mathrm{Hom}(X_2, \mathbb{Z}_2),$$

and $\mathrm{Hom}(X_i, \mathbb{Z}_2) = 2^{|X_i|}$, and so $2^{|X_1|} = 2^{|X_2|}$, which implies that $|X_1| = |X_2|$.

4. Let E/K be a field extension of degree 2^k, $k \geq 1$. Let $f \in K[x]$ be a polynomial of degree 3 with a root in E. Must f have a root in K?

Let α denote the root of f in E. Suppose that f does not have a root in K. Since $\deg f \leq 3$, this implies that f is irreducible, so that f is the minimal polynomial of α, so $[K(\alpha) : K] = 3$, which implies that

$$2^k = [E : K] = [E : K(\alpha)][K(\alpha) : K] = 3q,$$

which is a contradiction. So, f must have a root in K.

5. Consider the multiplicative group $\mathbb{F}_{13}^{\times}$ of the field $\mathbb{F}_{13}$. Which elements generate the group, and which elements are squares in $\mathbb{F}_{13}^{\times}$?

Here, we're going to use the fact that if $a \not| p$ and for every prime divisor q of $p-1$ we have $a^{\frac{p-1}{q}} \not\equiv 1 \mod p$, then a is a primitive root of $\mathbb{F}_{13}^{\times}$.

The prime divisors of 12 are 2 and 3, so we need to check a^4 and a^6 for every element of $\mathbb{F}_{13}^{\times}$. Since these are both even powers, we just need to check 1-6, since 7-12 are just -6 - -12. Checking these elements individually, we get

$$2^4 = 3, \quad 2^6 = -1,$$
$$3^4 = 3, \quad 3^6 = 1,$$
$$4^4 = -4, \quad 4^6 = 1,$$
$$5^4 = 1,$$
$$6^4 = -4, \quad 6^6 = -1.$$

This tells us that $\pm 2, \pm 6$ are primitive roots of $\mathbb{F}_{13}^{\times}$. This agrees with the fact that there are $\varphi(\varphi(13)) = 4$ primitive roots of $\mathbb{F}_{13}^{\times}$, where φ is the Euler totient function. If we square the elements, we get

$$2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 3, \quad 5^2 = 1, \quad 6^2 = 10,$$

so the squares are 1, 3, 4, 9, 10.

6. Let G be a group. Prove or disprove the following statements.

(a) If G is abelian, then every finite dimensional irreducible complex representation of G is one-dimensional.

For finite groups, yes. We know that $\mathbb{C}G$ is a commutative ring, and $\mathbb{C}G$ is isomorphic to a direct product of matrix rings, where the size of each matrix is the dimension of each irreducible complex representation of G. Since matrix rings are commutative only when the matrices are 1×1, we must have that all of the irreducible complex representation are one-dimensional.

(b) If every irreducible complex representation of G is one-dimensional, then G is abelian.

13 Fall 2012

1. Can a vector space over an infinite field be a finite union

$$V = \bigcup_{i=1}^{k} V_i,$$

where for each i, $V_i \neq V$?

Suppose that $V = \bigcup_{i=1}^{k} V_i$ over an infinite field F, where $V_i \subsetneq V$. Pick some $x \in V_1$ and $y \in V - V_1$, and consider the set

$$\{x + cy : c \in F - \{0\}\}.$$

Since $y \notin V_1$, no elements of this set are in V_1. Since k is infinite and there are finitely many V_i's, there must be some V_i, $i \neq 1$ such that infinitely many of these elements are in V_i (though we really just need two). Pick any two such elements $x + c_1 y, x + c_2 y \in V_i$. Then,

$$\frac{1}{c_1 - c_2}\Big((x + c_1 y) - (x + c_2 y)\Big) = \frac{1}{c_1 - c_2}\Big((c_1 - c_2)y\Big) = y \in V_i.$$

This further implies that $x \in V_i$. x was an arbitrary element of V_1, so we get that $V_1 \subset \bigcup_{i=1}^{k} V_i$. If we repeat this process, we get that $V_1, V_2, \ldots, V_{k-1} \subset V_k$, and so $V_k = V$, but this contradicts the assumption that $V_k \subsetneq V$, so this cannot happen.

(b) Can the group $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ be a union of finitely many proper subgroups?

Let $(x, y) \in \mathbb{Z}^2$. There are three cases which can occur: x is even, y is even, or both x and y are odd.

If x is even, then (x, y) belongs in the subgroup $\{(2a, b) : a, b \in \mathbb{Z}\}$. If y is even, then (x, y) belongs in the subgroup $\{(a, 2b) : a, b \in \mathbb{Z}\}$. If both x and y are odd, then there exist integers n, m such that $x = 2n + 1, y = 2m + 1$. Then, $x + y = 2(m + n + 1)$. Let $a = m + n + 1$ and $b = n - m$. Then,

$$a + b = 2n + 1 = x,$$

$$a - b = 2m + 1 = y.$$

This implies that $(x, y) \in \{(a + b, a - b) : a, b \in \mathbb{Z}\}$. Thus, these three subgroups cover $\mathbb{Z}^2$.

2. Let G be an abelian group with n generators. Show that every subgroup $H \subset G$ has a generating sets consisting of at most n generators.

If $n = 1$, then G is cyclic and we're done. So, suppose this is true for $n = k-1$, and suppose G is generated by k elements $a_1, \ldots, a_k$. Consider the quotient group $G/\langle a_n \rangle$. Since the natural projection maps elements of G thusly:

$$m_1 a_1 + \ldots + m_n a_n \mapsto m_2 \overline{a}_2 + \ldots + m_n \overline{a}_n,$$

G is generated by at most $n-1$ elements, so by the inductive hypothesis, all subgroups $\overline{H}$ of G are generated by at most $n-1$ elements. By the fourth isomorphism theorem, subgroups $\overline{H}$ of $G/\langle a_1 \rangle$ correspond to subgroups H of G that contain $\langle a_1 \rangle$, and $H/\langle a_1 \rangle = \overline{H}$. This implies that H is generated by at most n elements. If we do the same thing for the remaining a_i, we'll cover every subgroup, so every subgroup of G has at most n generators.

3. Let F be a field and let $P \subset F$ be the intersection of all subfields in F. Show that if F has characteristic 0, then $P \cong \mathbb{Q}$, and if F has characteristic $p > 1$, then $P \cong \mathbb{F}_p$.

Every subfield of F contains 1, so every subfield contains the subfield generated by 1, so this must be the smallest subfield of F. If F has characteristic 0, then P consists of all elements $n \cdot 1$ for $n \in \mathbb{Z}$, as well as their multiplicative inverses $\frac{1}{n}$ for $n \neq 0$, and since P is a field we can multiply these elements to get p/q for $p, q \in \mathbb{Z}$ and $q \neq 0$. So, P is isomorphic to $\mathbb{Q}$.

If F has characteristic p, then P consists of the elements

$$1, 2 \cdot 1, \ldots (p-1) \cdot 1,$$

and these correspond to elements of $\mathbb{F}_p$, so this list contains all of the multiplicative inverses as well, so $P \cong \mathbb{F}_p$.

4. Let R be a commutative ring and I an ideal of R. Prove or disprove: The set $\sqrt{I} = \{a \in R : \exists n > 0, a^n \in I\}$ is an ideal.

$0 \in I$, so $\sqrt{I}$ is nonempty. If $a, b \in \sqrt{I}$, then there exist $n, m > 0$ such that $a^n, b^m \in I$. Since R is commutative, we can use the binomial theorem, so

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}.$$

For the first n terms of this, $m + n - k \geq m$, so $b^{m+n-k} \in I$, and for the remaining terms, $k \geq n$, so $a^k \in I$. Since I is an ideal, this implies that $(a+b)^{m+n} \in I$, so $\sqrt{I}$ is an abelian group.

If $r \in R$, and $a \in \sqrt{I}$, then $(ra)^n = r^n a^n \in I$. So, $\sqrt{I}$ is an ideal of R.

5. Find the number of field homomorphisms $\phi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$.

If ϕ is a field homomorphism $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, and θ is a root of $x^3 - 2$, then $\phi(\theta^3 - 2) = 0$, which implies that $\phi(\theta)$ is also a root of this polynomial. So, $\sqrt[3]{2}$ can map to $\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2}, e^{4\pi i/3}\sqrt[3]{2}$, and so there are three such field homomorphisms.

6. Consider the dihedral group D_4 of order 8.

(a) Find the conjugacy classes of D_4.

Here are the conjugacy classes, found by brute force:

$$\{1\}, \{r, r^3\}, \{r^2\}, \{s, sr^2\}, \{sr, sr^3\}.$$

(b) Find the character table of D_4.

D_4 is not abelian, and $D_4/\langle r^2 \rangle$ is abelian, so $D_4' = \langle r^2 \rangle$. This quotient group is isomorphic to V the Klein-4 group, since it is made up of the element $\{\overline{1}, \overline{r}, \overline{s}, \overline{sr}\}$, each of which has order 2. Since this group has order 4, D_4 has four degree-1 representations. Since D_4 has five conjugacy classes and the sum of the squares of the degrees of the irreducible

representations is 8, we must have that there is only one more irreducible representation, and that it is degree 2.

Since $a^2 = 1$ for all $a \in V$, the representations must send each element of V to (± 1). This gives us four distinct one-dimensional characters.

Each element of D_4 is a rotation or reflection in $\mathbb{R}^2$, so we can map each element to its corresponding rotation/reflection matrix in $\mathbb{R}^2$. r rotates by 90 degrees, and s reflects about the line $y = x$, so we get

$$r \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By calculating the traces of each character we get the following character table:

	1	r^2	s	r	sr
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

14 Spring 2012

1. Let A be a real upper triangular matrix so that A and A^T commute. Show that A is diagonal.

Since A is upper triangular,

$$(A^T A)_{11} = a_{11}^2 = (AA^T)_{11} = a_{11}^2 + a_{12}^2 + a_{13}^2 + \ldots + a_{1n}^2,$$
$$\Rightarrow a_{12}^2 + a_{13}^2 + \ldots + a_{1n}^2 = 0 \Rightarrow a_{1i} = 0, i \in \{2, \ldots, n\}.$$

$$\Rightarrow (A^T A)_{22} = a_{22}^2 = (AA^T)_{22} = a_{22}^2 + a_{23}^2 + \ldots + a_{2n}^2,$$
$$\Rightarrow a_{23}^2 + \ldots + a_{2n}^2 = 0 \Rightarrow a_{2i} = 0, i \in \{3, 4, \ldots, n\}$$
$$\vdots$$

$$\Rightarrow (A^TA)_{ii} = a_{ii}^2 = (AA^T)_{ii} = a_{ii}^2 + a_{ii+1}^2 + \ldots + a_{in}^2,$$
$$\Rightarrow a_{ii+1}^2 + \ldots + a_{in}^2 = 0 \Rightarrow a_{ij} = 0, j \in \{i+1, \ldots, n\}.$$

This implies that the only nonzero entries are the diagonal ones, so A is diagonal.

2. Suppose that G is a group which contains no index 2 subgroups. Show that every index 3 subgroup in G is normal.

Let H be a subgroup of G of index 3. Let G act on the set X of cosets of H, which is a set of order 3, and let K denote the kernel of the action, which is a normal subgroup of G. Since $kH = H$ for all $k \in K$, $K \leq H$. Then,

$$[G : K] = [G : H][H : K] = 3k.$$

The image of G under the permutation representation of this action therefore has order $3k$, which divides 3!. So, $k = 1$ or $k = 2$. If $k = 2$, then $G \cong S_3$, which has a subgroup of index 2 ($\langle(123)\rangle$) and so $k = 1$, which implies that $K = H$, so $H \trianglelefteq G$.

3. Let F be a field and $F^\times$ be the multiplicative group of nonzero elements of F. Show that every finite subgroup of $F^\times$ is cyclic.

If $x, y \in \mathbb{F}^\times$ with relatively prime orders a and b respectively, consider the element xy. Since $(xy)^{ab} = 1$, the order of xy is $\leq ab$. $(xy)^a = y^a$, which has order b. Since $(a, b) = 1$, there's not smaller number c such that ac is a multiple of b, for if $b|c$, then $b|c$, so $c = bq$, and the smallest such c is b itself. Similarly, $(xy)^b = x^b$ has order a. So, ab divides the order of xy, which implies that the order of xy is ab.

If $d|a$. Then $x^{a/d}$ must have order d, since any smaller number c will give a number smaller than a.

If x, y have arbitrary orders, then factor these orders into primes:

$$|x| = p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$
$$|y| = p_1^{\beta_1} \cdots p_n^{\beta_n},$$

where $\alpha_i, \beta_i \geq 0$. The lcm is

$$p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_n^{\max\{\alpha_n,\beta_n\}}.$$

For each i, we shoed above that we can find elements with orders $p_i^{\alpha_i}$ and $p_i^{\beta_i}$. Pick the element with the larger order, call it z_i. Then, the z_i's have relatively prime orders, so their product will give us an element with the desired order.

Now, suppose that $x \in \mathbb{F}^\times$ with largest order a. We claim that the order of each element in $\mathbb{F}^\times$ divides r. Indeed, if this were false, then there'd be an element y with order $b \not| a$, and so $\text{lcm}(a, b) > a$, and by our work above, there'd be an element with that order, which contradicts the maximality of a. So, $g^a = 1$ for all $g \in \mathbb{F}^\times$.

Now, let r be the largest order in $\mathbb{F}^\times$, and consider the polynomial $x^r - 1$. By our work above, we know that every element in $\mathbb{F}^\times$ is a root of this polynomial, so the order of the group is at most r, but since $r||\mathbb{F}^\times|$ by Lagrange's Theorem, we have the reverse inequality, and so the two values are equal, and so $\mathbb{F}^\times$ is cyclic.

4. Prove that $\mathbb{R}[x]/(x^2 - 1) \cong \mathbb{R} \oplus \mathbb{R}$, but $\mathbb{R}[x]/((x^2 - 1)^2) \ncong \mathbb{R} \oplus \mathbb{R}$.

I'm not sure what isomorphism type this is, but I'm going to guess as $\mathbb{R}$-modules, or $\mathbb{R}$-vector spaces, but this is easy, since

$$\mathbb{R}[x]/(x^2 - 1) = \{a_0 + a_1 x : a_i \in \mathbb{R}\}$$

is a two-dimensional real vector space, as is $\mathbb{R} \oplus \mathbb{R}$, while

$$\mathbb{R}[x]/((x^2 - 1)^2) = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 : a_i \in \mathbb{R}\}$$

is a four-dimensional real vector space.

5. Show that 9 and $6 + 3\sqrt{-5}$ do not have a greatest common divisor in $\mathbb{Z}[\sqrt{-5}]$.

If an element of this domain divides both of these numbers, then it must have norm dividing 81, which is the norm of both of these numbers. Such are elements are

$$\pm 1 \pm 4\sqrt{-5} (\text{norm} = 81), \quad \pm 3, \pm 2 \pm \sqrt{-5} (\text{norm} = 9).$$

The first element is not a divisor since it is not 9 or $6 + \sqrt{-5}$ up to a unit. By doing some division, we see that the common divisors are $\pm(2 + \sqrt{-5})$ and ± 3:

$$\frac{9}{2+\sqrt{-5}} = \frac{9(2-\sqrt{-5})}{(2+\sqrt{-5})(2-\sqrt{-5})} = \frac{18-9\sqrt{-5}}{9} = 2-\sqrt{-5},$$

$$\frac{6+3\sqrt{-5}}{2+\sqrt{-5}} = \frac{(6+3\sqrt{-5})(2-\sqrt{-5})}{9} = 27/9 = 3,$$

$$\frac{6+3\sqrt{-5}}{3} = 2+\sqrt{-5}.$$

However, 3 clearly does not divide $2+\sqrt{-5}$, and

$$\frac{3}{2+\sqrt{-5}} = \frac{6-3\sqrt{-5}}{9} \notin \mathbb{Z}[\sqrt{-5}],$$

so neither can be a gcd, hence 9 and $6+3\sqrt{-5}$ have no gcd.

6. Let F be a field, x and indeterminate, and let $F[[x]]$ denote the ring of formal power series with coefficients in F, where multiplication is defined as it is for polynomials. Prove that an element $s = \sum_{n=0}^{\infty} a_n x^n$ is a unit in $F[[x]]$ if and only if $a_0 \neq 0$. Show that every ideal of $F[[x]]$ is of the form $x^n F[[x]]$ for some $n \geq 0$.

Suppose that $a = \sum_{n=0}^{\infty} a_n x^n$ is a unit with inverse $a^{-1} = \sum_{n=0}^{\infty} b_n x^n$. Then,

$$1 = aa^{-1} = a_0 b_0 + (a_0 b_1 + b_0 a_1)x + \ldots \Rightarrow a_0 b_0 = 1 \Rightarrow a_0 \neq 0.$$

Suppose $a = \sum_{n=0}^{\infty} a_n x^n$ is an element of $F[[x]]$ with $a_0 \neq 0$. Then, we can construct an inverse $\sum_{n=0}^{\infty} b_n x^n$:

$$1 = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \ldots + \left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n + \ldots,$$

$$a_0 b_0 = 1, \sum_{k=0}^{n} a_k b_{n-k} = 0.$$

Let $b_0 = a_0^{-1}$. Suppose b_{n-1} is defined. Then,

$$a_0 b_n + a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0 = 0,$$

$$\Rightarrow b_n^{-1} = -a_0^{-1}(a_1 b_{n-1} + \ldots + a_n b_0).$$

So, by induction, we can find every b_n, and so a has an inverse.

Let I be an ideal, and let $a = \sum_{n=0}^{\infty} a_n x^n \in I$ be such that a has the smallest "trailing degree" n, so $a = x^n \sum_{k=n}^{\infty} a_k x^{k-n}$. We claim that $I = (x_n)$. Indeed, $\sum_{k=n}^{\infty} a_k x^{k-n}$ is invertible, so $x_n \in I$. If $b \in I$, then we can write

$$b = x^m \sum_{k=m}^{\infty} b_k x^{k-m}$$

where $m \geq n$, so

$$b = x^n x^{m-n} \sum_{k=m}^{\infty} b_k x^{k-m} \in (x_n).$$

Thus, $I = (x^n)$.

15 Fall 2011

1. Show that there is no commutative ring with the identity whose additive group is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

If such an R existed, then 1_R would be identified with some element of $\mathbb{Q}/\mathbb{Z}$. Every element of this group has finite order, so R would have some finite characteristic n. However, pick any $m > n$. Then, $\frac{k}{m} \notin \mathbb{Z}$ for any $0 < k \leq n$, so $\frac{n}{m} \neq 0$, but this is a contradiction.

2. Let $p \neq 2$ be prime and let $\mathbb{F}_p$ be the field of p elements.

(a) How many elements have square roots in $\mathbb{F}_p$?

We can write the elements of $\mathbb{F}_p$ as

$$1, 2, 3, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}, \ldots, -3, -2, -2,$$

so we only need to check the first $\frac{p-1}{2}$ elements. We claim that each of these gives a unique square root. Indeed, if $a^2 \equiv b^2 \mod p$ and both a and b are positive, then

$$p|a^2 - b^2 = (a-b)(a+b)$$

and since p is prime, either $p|a-b$ or $p|a+b$. In either case, we have $a \equiv b \mod p$. So, we have $\frac{p-1}{2}$ square roots.

(b) How many have cube roots in $\mathbb{F}_p$?

Consider the map $x \mapsto x^3$. Recall, $\mathbb{F}_p^\times$ is cyclic, and so if $3 \not| p-1$, then if x is a generator for this group, then x^3 is as well, so every element is a cube root.

If $3|p-1$, then $\langle x^{\frac{p-1}{3}} \rangle$ is of order $\frac{p-1}{3}$, and so we have that many cube roots.

Finally if $p = 2$ then 1 is the only cube root, and if $p = 3$, then both 1 and 2 are cube roots since $2^3 = 8 = 2$.

3. Prove that every finite group is isomorphic to a certain group of permutations (a subgroup of S_n for some n).

List the elements of G:

$$G = \{g_1, \ldots, g_n\}.$$

Let G act on itself by left multiplication. So, for each $g_i \in G$, there's a $g_j (= g^{-1}g_i)$ such that $gg_i = g_j$. So, for each $g \in G$, we get a permutation $\sigma_g \in S_n$ where $\sigma_g(i) = j$. So, we get an injective homomorphism $\Phi : G \to S_n$ where $g \mapsto \sigma_g$. This is injective because if $g \neq g'$, then $ge = g \neq g'e = g'$, so they define different permutations. By the First Isomorphism Theorem, we get that $G \cong \Phi(G) \leq S_n$.

5. Prove or disprove: If the group G of order 55 acts on a set X of 39 elements, then there is a fixed point.

If $x \in X$, then by the Orbit-Stabilizer Theorem, $|\mathcal{O}_x| = \frac{|G|}{|S_x|}$. By Lagrange, $|S_x| = 1, 5, 11, 55$. Clearly, it cannot be 1, and assume that the orbits are of sizes only 11 and 5. Then, this would imply that

$$5n + 11m = 39$$

for some $0 \leq n \leq 7, 0 \leq m \leq 3$. This implies that $5n$ ends in a 0 or 5, while $11m$ ends in a 0, 1, 2, or 3. In any case, $5n + 39m$ must end in 0, 1, 2, 3, 5, 6, 7, 8, so it is impossible for $5n + 11m = 39$, so there must be a fixed point.

6. Prove or disprove: $(\mathbb{Z}_{35})^\times \cong (\mathbb{Z}_{39})^\times \cong (\mathbb{Z}_{45})^\times \cong (\mathbb{Z}_{70})^\times \cong (\mathbb{Z}_{78})^\times \cong (\mathbb{Z}_{90})^\times$.

If $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, then

$$\left(\mathbb{Z}_n\right)^\times \cong \left(\mathbb{Z}_{p_1^{\alpha_1}}\right)^\times \times \ldots \times \left(\mathbb{Z}_{p_n}^{\alpha_n}\right)^\times.$$

So, $(\mathbb{Z}_{35})^\times (\mathbb{Z}_7)^\times \times (\mathbb{Z}_5)^\times \cong \mathbb{Z}_6 \times \mathbb{Z}_4$, while $(\mathbb{Z}_{39})^\times \cong (\mathbb{Z}_3)^\times \times (\mathbb{Z}_{13})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{12}$, which are not isomorphic, since the first group has 4 subgroups of order 12, while the second has 8.

16 Fall 2010

1. Let G be a group which admits a finite set of generators. Show that G is countable

$G = \langle x_1, \ldots, x_n \rangle$ for some finite set $x_1, \ldots, x_n \in G$. So, G consists of strings of the form

$$x_{i_1}^{\epsilon_1} \cdots x_{i_k}^{\epsilon_k}$$

where $x_{i_j} \in \{x_1, \ldots, x_n\}$ (and not necessarily distint), and $k \geq 0$ and $\epsilon_j \in \{\pm 1\}$. So, we can write

$$G = \bigcup_{i=1}^{\infty} G_i,$$

where G_i is the set of such strings of length i. Since there are $2n$ choices per position, $|G_i| = (2n)^i$. So, we have a countable number of finite sets, so G must be countable.

2. Let G be a finite group. Show that G embeds in $GL(n, \mathbb{Z})$ for some n.

Since G is finite, say of size n, we can order the elements into a list:

$$\{g_1, g_2, \ldots, g_n\}.$$

G acts on itself by multiplication, so given a $g \in G$, we get a new list

$$\{gg_1, gg_2, \ldots, gg_n\}.$$

So, we can associate to each g a matrix. If g maps g_j to g_i for some $1 \leq i \leq n$, then put a 1 in the ith row and jth column, and 0's in the rest of the entries in this row and column. For example, the matrix for $(1,0) \in (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ with the ordering $\{(0,0),(1,0),(0,1),(1,1)\}$ would be

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

These matrices are invertible since they're just elementary matrices, which have determinant 1, hence are invertible.

3. Not on syllabus

4. Consider the ring $R = \mathbb{Z}[x]$. Give an example, with a proof, of an ideal that is not principle, and of an ideal that is not prime.

Let $I = (2, x)$, which we claim is not principle. Indeed, if $(2, x) = (p(x))$ for some $p(x) \in \mathbb{Z}[x]$, then $2 = p(x)q(x)$ for some $q(x)$. Since x and 2 are not invertible, we must have both p and q constant with $p = 1$ or 2. Since $I \neq R$, $p = 2$, however, that would imply that $x = 2g(x)$ for some polynomial $g(x)$, but 2 is not invertible, so this is impossible. Hence, I is not principle.

Let $J = ((1-x)^2)$. J is not prime because R/J is not an integral domain. The polynomial $\overline{x-1} \in R/J$ is nonzero, but $\overline{(x-1)^2} = 0$, and hence is a zero divisor.

5. Let R be a ring with identity. Recall that $x \in R$ is called *nilpotent* if $x^n = 0$ for some n. Prove that if x is nilpotent, then $1 + x$ is invertible.

$$(1+x)(1-x+x^2-x^3+x^4-\ldots+(-1)^{n-1}x^{n-1})$$
$$x-x^2+x^3-x^4+x^5+\ldots+(-1)^{n-2}x^{n-1}+(-1)^{n-1}x^n$$
$$+1-x+x^2-x^3+x^4-x^5+\ldots+(-1)^{n-2}x^{n-2}+(-1)^{n-1}x^{n-1}$$
$$=1+(-1)^{n-1}x^n=1.$$

6. Let F be a nontrivial finite extension field of $\mathbb{R}$. Prove that F is isomorphic to $\mathbb{C}$. You may use the fundamental theorem of algebra.

Let $\alpha \in F \setminus \mathbb{R}$ be a root of an irreducible polynomial $p(x) \in \mathbb{R}[x]$. If $p(x)$ is irreducible over $\mathbb{R}$, then we claim it must be of degree at most 2. Indeed, by the Fundamental Theorem of Algebra, $p(x)$ splits over $\mathbb{C}$, and if z is a root, then so is $\overline{z}$, and $(x-z)(x-\overline{z}) \in \mathbb{R}[x]$. So, $p(x)$ can be reduced to linear and quadratic factors. So, if we have a finite extension of $\mathbb{R}$, then it must be of degree 2. We can embed $F = \mathbb{R}(\alpha)$ in the algebraic closure $\overline{R} = \mathbb{C}$ of $\mathbb{R}$, and then

$$2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : F][F : \mathbb{R}] = 2[\mathbb{C} : F],$$

and so $[\mathbb{C} : F] = 1$ which implies that the fields are equal.

17 Spring 2010

1. Let R be a commutative ring with identity. An ideal I of R is said to be *radical* if for every $x \in R$ such that $x^n \in I$ for some n, we have $x \in I$. Prove that I is radical if and only if it is equal to the intersection of all prime ideals containing I.

"$\Leftarrow$" If J is a prime ideal, then $x^n \in J$ implies $x \in J$, for prime implies x or x^{n-1} is in J, if $x \in J$, then we're done. If $x^{n-1} \in J$, then by induction we're done.

So, if $x^n \in I$, then x^n is in every prime ideal containing I, which implies that x is in every prime ideal containing I, so by hypothesis $x \in I$, so I is radical.

"$\Rightarrow$" Suppose $x \notin I$. Let J denote the largest ideal such that no power of x is in J, which exists by Zorn's Lemma. Now, consider the quotient ring R/J. By the Correspondence

Theorem, the ideals of R/J are the ideals of R containing J. By hypothesis, these ideals must contain some power of x. In particular, if $r \notin J$, then $\overline{x}^i \in (\overline{r})$ for some i.

If $rs \in J$, then $\overline{rs} = \overline{0}$ in R/J. If neither r nor s is in J, then there exist i, j such that $\overline{x}^i \in (\overline{r}), \overline{x}^j \in (\overline{s})$, which implies $\overline{x}^{i+j} \in (\overline{rs}) = (\overline{0})$, but this implies $x^{i+j} \in J$, which is a contradiction, so one of r or s must be in J. Thus, J is prime.

5. Prove that if R is an integral domain with a finite group of units $R^\times$, then the group of units is cyclic.

If R is an integral domain, then R is commutative, so $R^\times$ is a field. So, we just need to prove the equivalent proposition that the group of a units of a finite field is cyclic:

If $x, y \in \mathbb{F}^\times$ with relatively prime orders a and b respectively, consider the element xy. Since $(xy)^{ab} = 1$, the order of xy is $\leq ab$. $(xy)^a = y^a$, which has order b. Since $(a, b) = 1$, there's not smaller number c such that ac is a multiple of b, for if $b|c$, then $b|c$, so $c = bq$, and the smallest such c is b itself. Similarly, $(xy)^b = x^b$ has order a. So, ab divides the order of xy, which implies that the order of xy is ab.

If $d|a$. Then $x^{a/d}$ must have order d, since any smaller number c will give a number smaller than a.

If x, y have arbitrary orders, then factor these orders into primes:

$$|x| = p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$
$$|y| = p_1^{\beta_1} \cdots p_n^{\beta_n},$$

where $\alpha_i, \beta_i \geq 0$. The lcm is

$$p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}.$$

For each i, we shoed above that we can find elements with orders $p_i^{\alpha_i}$ and $p_i^{\beta_i}$. Pick the element with the larger order, call it z_i. Then, the z_i's have relatively prime orders, so their product will give us an element with the desired order.

Now, suppose that $x \in \mathbb{F}^\times$ with largest order a. We claim that the order of each element in $\mathbb{F}^\times$ divides r. Indeed, if this were false, then there'd be an element y with order $b \not| a$, and so $\text{lcm}(a, b) > a$, and by our work above, there'd be an element with that order, which contradicts the maximality of a. So, $g^a = 1$ for all $g \in \mathbb{F}^\times$.

Now, let r be the largest order in $\mathbb{F}^\times$, and consider the polynomial $x^r - 1$. By our work above, we know that every element in $\mathbb{F}^\times$ is a root of this polynomial, so the order of the

group is at most r, but since $r||\mathbb{F}^\times|$ by Lagrange's Theorem, we have the reverse inequality, and so the two values are equal, and so $\mathbb{F}^\times$ is cyclic.

6. Give an example of an irreducible polynomial of degree n (for some n) over $\mathbb{Q}$ whose Galois group does not have $n!$ elements.

Let $p(x) = x^3 + 1$, which has roots

$$\frac{1}{2} + \frac{\sqrt{-3}}{2}, -\frac{1}{2} + \frac{\sqrt{-3}}{2}, \frac{1}{2} - \frac{\sqrt{-3}}{2},$$

all of which are complex numbers, so $p(x)$ is irreducible over $\mathbb{Q}$. We can see that, if ζ is a third root of unity, $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\sqrt{-3})$. We also have the reverse inclusion:

$$\sqrt{-3} = \frac{1}{2} + \frac{\sqrt{-3}}{2} - \frac{1}{2} + \frac{\sqrt{-3}}{2} = \zeta + \zeta^2.$$

So, $\mathbb{Q}(\sqrt{-3})$ is the splitting field of x^3+1, and is of degree 2, since the minimal polynomial of $\sqrt{-3}$ is $x^2 + 3$.

18 Fall 2009

1. Recall that an integral domain R is said to be a *unique factorization domain* if every element $x \in R$ can be written as a product of irreducible elements $\prod_{i=1}^m p_i$, and if the p_i's are uniquely determined up to reordering and multiplication by units. Show that if R is a UFD then every irreducible element generates a prime ideal.

Let p be irreducible, and consider the ideal (p), and suppose that $rs \in (p)$. Since R is a UFD, there's a unique (modulo reordering and unit multiplication) factorization for both r and s:

$$r = p_1 \cdots p_n, \quad s = q_1 \cdots q_m,$$

and there exists an $x \in R$ such that $rs = xp$. By uniqueness of factorization, since p is irreducible, it must be, without loss of generality, equal to up_i for some $1 \leq i \leq n$ and some unit u (there is no difference if p is equal to one of the q_i's). This implies that $r \in (p)$ (or $q \in (p)$), hence (p) is a prime ideal.

2. The field extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ (really? just call it $\sqrt[4]{2}$) are both Galois (you do not need to prove this). Show that $\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q}$ is not Galois. For concreteness, assume the square roots are positive.

$x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein and contains $\sqrt[4]{2}$ as a root, hence it is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$, and therefore the extension $\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q}$ is degree four. This polynomial has roots $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. Since only the former two elements are in $\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q}$ and because elements of $\mathrm{Aut}(\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q})$ send roots to roots, a nontrivial automorphism of this field extension can only send $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. Since this is the only generator of $\mathbb{Q}(\sqrt{\sqrt{2}})$ over $\mathbb{Q}$, this completely determines the elements of the automorphism group, i.e. there are only two elements of $\mathrm{Aut}(\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q})$, one that sends $\sqrt[4]{2}$ to itself, and one that sends $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. Hence, $|\mathrm{Aut}(\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q})| = 2$, which is strictly less than the degree of the extension, and so the extension is not Galois.

3. Let A and B be linear transformations on a finite dimensional vector space V. Prove that the dimension of $\ker(AB)$ is less than or equal to $\dim\ker(A) + \dim\ker(B)$.

We claim that $\ker(AB)$ is made up of two subspaces, one of which is a subspace of $\ker(B)$, and the other of which has dimension $\leq \dim\ker(A)$.

If $x \in \ker(AB)$, then $ABx = 0$. Either $Bx = 0$, or $Bx \neq 0$ and $A(Bx) = 0$, so either $x \in \ker(B)$ or $Bx \in \ker(A)$. If we denote $\tilde{B}$ to be the restriction of B to $\ker(AB)$, then by the rank theorem, we can write

$$\dim\ker(AB) = \dim\ker(\tilde{B}) + \dim\mathrm{ran}(\tilde{B}).$$

Clearly, $\dim\ker(\tilde{B}) \leq \dim\ker(B)$. Since $A(Bx) = 0$ for all $x \in \ker(AB)$, the range of $\tilde{B}$ lies in $\ker(A)$, so the range of $\tilde{B}$ is a subspace of $\ker(A)$, so $\dim\mathrm{ran}(\tilde{B}) \leq \dim\ker(A)$. So,

$$\dim\ker(AB) = \dim\ker(\tilde{B}) + \dim\mathrm{ran}(\tilde{B}) \leq \dim\ker(B) + \dim\ker(A).$$

4. Let G be a group and H and K subgroups such that H has finite index in G. Prove that $H \cap K$ has finite index in K.

Let K act on the cosets of H by left multiplication, which by assumption is a finite set. By the Orbit-Stabilizer Theorem, the size of the orbit containing H is $|K : H \cap K|$, since the elements of K that stabilize H are those that are also in H. So $|K : H \cap K| < \infty$.

5. Prove that the algebra $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to the algebra $\mathbb{C} \oplus \mathbb{C}$.

6. If V is a finite dimensional linear representation of a group G, then by definition the character function $\chi(g)$ is the trace of the action of g. This is usually studied when V is a complex vector space, but is well-defined over any field. Find an example of a nontrivial representation of a group G over some field F, such that $\chi(g) = 0$ for all g.

Let V be the two dimensional vector space over $\mathbb{F}_2$ with basis $\{u_1, u_2\}$, and let $G = \mathbb{Z}_2$. Define an action of G on V by having $\overline{1}(u_1) = u_2, \overline{1}(u_2) = u_1$. Then, $2 \cdot \overline{1}(u_i) = u_i$, so this is a linear representation of G. The matrices corresponding to this representation are

$$\overline{0} \mapsto \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \quad \overline{1} \mapsto \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix},$$

both of which have trace 0.

19 Winter 2009

1(a)

Note that this is an upper triangular matrices, so the diagonal terms of M^2 are the squares of the diagonal terms of M, so we have

$$\begin{pmatrix} 1 & x & y \\ 0 & 2 & z \\ 0 & 0 & 3 \end{pmatrix}.$$

From here, we can see that

$$3x = 3, \quad 4y + z = 3, \quad 5z = 5,$$

so $x = 1, y = -1, z = 1$.

(b) Note that $-M$ is another solution. How many such matrices are there?

There are eight such matrices. The $(1,1)$-entry must be ± 1, the $(2,2)$-entry ± 2, the $(3,3)$-entry ± 3. We can form eight ordered triples from this, and using the same method as in part (a), we see that for each ordered triple, there is one matrix satisfying our matrix equation.

2. Show that there are at least two nonisomorphic, non-abelian groups of each of the orders 24 and 30.

Both S_4 and D_{12} are non-abelian and have order 24, but D_{12} has an element of order 24, while the maximum order of an element in S_4 is 4.

Both D_{15} and $\mathbb{Z}/5\mathbb{Z} \times S_3$ have order 30 and are nonabelian. However, the second group has only three elements of order 2:

$$(0,(12)),(0,(13)),(0,(23)),$$

while $\langle sr^k \rangle$ for $0 \leq r \leq 11$ are all groups of order 2 in D_{15}, so these two groups are not isomorphic.

5. Let A be the group of rational numbers under addition, and let M be the group of positive rational numbers under multiplication. Determine all homomorphisms from A to M.

Suppose $\varphi : A \to M$ is a homomorphism. We know that $\varphi(0) = 1$, and now let's find what $\varphi(1)$ can possibly be. Note that $\varphi(p/q) = \varphi(1/q)^p$. In particular, $\varphi(1) = \varphi(1/n)^n$ for all $n \geq 1$, so for each $n \geq 1$, there exist relatively prime positive integers p_n, q_n such that $\varphi(1) = \frac{p_n^n}{q_n^n}$. So, if $\varphi(1) = x/y$, then

$$x = \frac{p_n^n}{q_n^n} y,$$

which implies q_n^n divides $p_n^n y$, but p_n and q_n are relatively prime, so q_n divides y. This implies that there are only finitely many such q_n's. Similarly, since

$$y = \frac{q_n^n}{p_n^n} x,$$

there are only finitely many distinct p_n's. This implies that there must exist $m_1 > m_2 \geq 1$ such that $p = p_{m_1} = p_{m_2}$ and $q = q_{m_1} = q_{m_2}$, and

$$\left(\frac{p}{q}\right)^{m_1} = \left(\frac{p}{q}\right)^{m_2}$$

$$\Rightarrow (p/q)^{m_1-m_2} = 1 \Rightarrow p/q = 1.$$

Thus, $\varphi(1)$ must be 1, so the only homomorphism is $A \to M$ is the trivial homomorphism.

20 Fall 2008

1(a) Show that if $f(x) \in \mathbb{Q}[x]$ is an irreducible (nonconstant) polynomial then $\mathbb{Q}[x,y]/f(x)$ is a principal ideal domain.

If $f(x)$ is irreducible, then $(f(x))$ is a maximal ideal, which implies that $\mathbb{Q}[x]/(f(x))$ is a field.

$$\mathbb{Q}[x.y]/(f(x)) = (\mathbb{Q}[x])[y]/(f(x))$$

$$= \{\overline{p_n(x)}y^n + \overline{p_{n-1}(x)}y^{n-1} + \ldots + \overline{p_1(x)}y + \overline{p_0(x)} : n \geq 0 : \overline{p_i(x)} \in \mathbb{Q}[x]/(f(x))\} = \Big(\mathbb{Q}[x]/(f(x))\Big)[y].$$

Polynomial rings over fields are PIDs, which implies that $\mathbb{Q}[x,y]/(f(x))$ is a PID.

(b) Find a generator for the ideal (x,y).

In $\mathbb{Q}[x,y]/(f(x))$,

$$\overline{(x,y)} = \overline{p(x,y)}\overline{x} + \overline{q(x,y)}y$$

If we let $\overline{p(x,y)} = \overline{x}^{-1}$, we get that $\overline{(x,y)} = (\overline{1})$.

Show that $x^2 - y^3 \in \mathbb{Q}[x,y]$ is irreducible and $(x,y) \subset \mathbb{Q}[x,y]/(f(x))$ is not principal.

Think of $\mathbb{Q}[x,y]$ as $\mathbb{Q}[y][x]$ If $x^2 - y^3$ has a root $\alpha \in \mathbb{Q}[y]$, then $\alpha = \pm y^{3/2} \notin \mathbb{Q}[y]$, which implies that $f(x,y)$ is irreducible. Since $x^2 = y^3$, we get that

$$\mathbb{Q}[x,y]/(f(x,y)) = p_2(x)y^2 + p_1(x)y + p_0(x).$$

x, y, y^2 are not invertible, so we can't get a $p(x,y)$ such that $x = q_1 p$ and $y = q_2 p$.

2. Assume that p is prime, D and P are subgroups of a finite group F with $D \trianglelefteq F$ and having index $[F : D]$ relatively prime to p and P a p-group. Show that $P \leq D$.

Since F is finite, $[F : D] = \frac{|F|}{|D|}$. We can write $|F| = p^\alpha m$ with $p \not| m$. Since $[F : D]$ is relatively prime to p, p must divide $|D|$, and in particular, p^α must divide $|D|$, so we can write $|D| = p^\alpha k$ for some $k \not| p$. Since $|P|$ is a p-group, $|P| = p^\alpha$, and because $D \trianglelefteq F$, DP is a subgroup, with order

$$|DP| = \frac{|D||P|}{|P \cap D|} = \frac{p^{2\alpha}k}{|P \cap D|}.$$

Since α is the largest number such that p^α divides $|F|$, we must have $p^\alpha | D \cap P|$, and since $D \cap P \leq P$, $|D \cap P| = p^\alpha$, so $P = D \cap P$, which implies that $P \subset D$.

3. Let M be a 3×3 matrix of complex numbers with characteristic polynomial $x^3 + 5x^2 + 3x + (9 - i)$.

If we look at an $n \times n$ companion matrix, we can see that the determinant is $(-1)^n$ times the constant term of the corresponding polynomial, so here $\det M = -9 + i$, so $\det M^2 = (\det M)^2 = (9 - i)^2$.

Looking again at the companion matrix, we see that the trace is the negative of the x^{n-1} coefficient, so here $\mathrm{tr}M = -5$.

4. Assume that R is an integral domain and J is a nonzero ideal of R viewed as an R-module. Is J always, sometimes, or never a direct sum of two nontrivial R-submodules?

Suppose $J = I_1 \oplus I_2$, where I_1 and I_2 are R-submodules. WLOG assume I_1 is nontrivial Let $x \in I_1,$, $y \in I_2$, with $x \neq 0$, and consider their product $xy = yx$. Since I_1 and I_2 are R-submodules, we have $xy \in I_1 \cap I_2 = \{0\}$, which implies $y = 0$. This implies $I_2 = 0$, so J is ***never*** a direct sume of two nontrivial R-submodules.

5. If H is a subgroup of a group G, then a subgroup $K \subset G$ is called a *complement* of H if K has exactly one element in each left coset of H.

(a) Show that if H is normal, then all complements of H are isomorphic to each other.

Suppose K_1 and K_2 are two complements of H. Define a map $\phi : K_1 \to K_2$ that sends each element x_1 of K_1 to the element x_2 of K_2 that belongs in the same coset as x_1. ϕ is well-defined by how complements are defined, and it is clearly a bijection. It remains to show that it is a homomorphism.

Since H is normal, G/H is a group. So, if $x, y \in K_1$, then xy is in the same coset at $\phi(x)\phi(y)$, and since this coset contains only one element of K_2, we must have $\phi(xy) = \phi(x)\phi(y)$.

(b) Show that the inclusion of symmetric groups $S_3 \subset S_4$ has two complements which are not isomorphic.

$$S_4/S_3 = \{e, (14)S_3, (24)S_3, (34)S_3\};$$

$$\Rightarrow K_1 = \langle (1234) \rangle = \{e, (14)(13)(12), (24)(13), (34)(13)(23)\} \cong \mathbb{Z}/4\mathbb{Z};$$

$$K_2 = \{e, (14)(23), (24)(13), (34)(12)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

21 Winter 2008

1. Suppose that G is a finitely-generated group and $n \in \mathbb{N}$. Show that G contains finitely many subgroups of index $\leq n$.

We can solve the equivalent problem of showing that G contains finitely many subgroups of index n for each n.

Let $\{H_\alpha\}_{\alpha \in I}$ be the collections of subgroups of index n, and suppose that G is generated by k elements. Since the H_α's are of the same index, if $H_{\alpha_1} \subset H_{\alpha_2}$, then $H_{\alpha_1} = H_{\alpha_2}$.

Suppose that there are infinitely many such H_α's.

2. Let A be an $n \times n$ complex matrix. Prove or disprove:

(a) A is similar to its transpose.

Consider an $n \times n$ Jordan block

$$\begin{pmatrix} 1 & \lambda & 0 & \dots & 0 \\ 0 & 1 & \lambda & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \lambda \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

To get the transpose of this block, simply swap the kth row with the $n-k+1$-colum, and then swap the kth row with the $n-k+1$ row. So, switch the 1st row/colum with the nth row/column, the 2nd row/column with the $n-1$ row/column, etc. This can be done by multiplying on the left and right of this block by the elementary matrix

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

with 1's on the antidiagonal and 0's elsewhere. Thus, a Jordan block is similar to its transpose, and so a direct sum of Jordan blocks is similar to its transpose. Since every complex matrix is similar to a unique direct sum of Jordan blocks, this implies that a complex matrix is indeed similar to its transpose.

(b) If the sum of the elements of each column of A is 1, then 1 is an eigenvalue of A.

$\mathbb{C}$ is algebraically closed, so we can put A into Jordan canonical form J, so there exists an invertible matrix A such that $J = PAP^{-1}$. A Jordan block is similar to its transpose, so there exists an invertible matrix Q such that $J^T = QJQ^{-1}$, and there's an invertible S such that $A^T = SJ^TS^{-1}$, so

$$A^T = SQPAP^{-1}Q^{-1}S^{-1},$$

so A is similar to A^T.

If the sum of the elements of each column of A is 1, then the sum of the elements of each row of A^T is 1, so

$$A^T x = x,$$

where x is the vector with 1's in each coordinate. By (a), we have invertible P such that

$$PAP^{-1}x = x \Rightarrow A(P^{-1}x) = P^{-1}x,$$

so 1 is an eigenvalue with eigenvector $P^{-1}x$.

3. Recall that if R is a ring, an R-module M is projective means if $f : A \to B$ is an R-module homomorphism between two other R-modules, and if $g : M \to B$ is a homomorphism, then there is always a solution $h : M \to A$ to the equation $g = fh$. Prove that among $\mathbb{Z}$-modules, the only cyclic module $\mathbb{Z}/N$ which is projective is $\mathbb{Z}/0 = \mathbb{Z}$.

$\mathbb{Z}$ is a projective $\mathbb{Z}$-module because it is free over itself, and free $\Rightarrow$ projective.

Let $A = \mathbb{Z}, B = \mathbb{Z}_n$, and $M = \mathbb{Z}_n$. We'll show that $\mathbb{Z}_n$ is not projective. Let $f : A \to B$ to the natural projection map $\pi : \mathbb{Z} \to \mathbb{Z}_n$, and let $g : \mathbb{Z}_n \to \mathbb{Z}_n$ be the identity map. If $\mathbb{Z}_n$ were projective, then there would be an $h : \mathbb{Z}_n \to A$ such that $\mathrm{id}_{\mathbb{Z}_n} = \pi \circ h$. However, every element of $\mathbb{Z}_n$ has finite order, and the only $\mathbb{Z}$-linear map (i.e. abelian group homomorphism) from $\mathbb{Z}_n \to \mathbb{Z}$ is the 0 map. So, $\mathbb{Z}_n$ is not projective.

4. Prove that $M_n(\mathbb{C})$, the algebra of $n \times n$ complex matrices, has non notrivial two-sided ideals.

Since we're considering complex matrices, we can just consider Jordan blocks.

If J_λ is the $n \times n$ Jordan block corresponding to the eigenvalue λ, then $J_\lambda J_{-\lambda} = I$. So, given any complex matrix, we can multiply by matrices to get to its Jordan canonical form, and from there we can easily get to the identity matrix. So, if I is a two-sided ideal containing a nonzero matrix, then it must contain the idenity matrix, and is therefore the whole algebra.

5. Let A and B be maps with 25 elements. There is more than one possibility

of A up to isomorphism, and likewise for B. Since all abelian groups are $\mathbb{Z}$ modules, we may tensor $A \otimes B$ as $\mathbb{Z}$-modules. What are the possibilities for the number of elements of $A \otimes B$?

By the FTFGAG, the two possibilities for A and B are $\mathbb{Z}_{25}$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$, so the three nonisomorphic possibilities for $A \otimes B$ are

$$\mathbb{Z}_{25} \otimes \mathbb{Z}_{25}, \quad \mathbb{Z}_5 \times \mathbb{Z}_5 \otimes \mathbb{Z}_5 \times \mathbb{Z}_5, \quad \mathbb{Z}_{25} \otimes \mathbb{Z}_5 \times \mathbb{Z}_5.$$

By using the Universal property on the $\mathbb{Z}$-bilinear map

$$\mathbb{Z}_{25} \times \mathbb{Z}_{25} \to \mathbb{Z}_{25},$$
$$(\overline{a}, \overline{b}) \mapsto \overline{ab},$$

we get that $\mathbb{Z}_{25} \otimes \mathbb{Z}_{25} \cong \mathbb{Z}_{25}$.

We can see that $\mathbb{Z}_5 \times \mathbb{Z}_5 \otimes \mathbb{Z}_5 \times \mathbb{Z}_5$ is generated by 4 elements:

$$(a,b) \otimes (c,d) = (a,0) \otimes (c,d) + (0,b) \otimes (c,d) = (1,0) \otimes (ac, ad) + (0,1) \otimes (bc, bd)$$
$$= (1,0) \otimes (ac, 0) + (1,0) \otimes (0, cd) + (0,1) \otimes (bc, 0) + (0,1) \otimes (0, bd)$$
$$= ac[(1,0) \otimes (1,0)] + ad[(1,0) \otimes (0,1)] + bc[(0,1) \otimes (1,0)] + bc[(0,1) \otimes (0,1)].$$

We're going to show that this tensor product is isomorphism to $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Define a map

$$(\mathbb{Z}_5 \times \mathbb{Z}_5) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \to \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5,$$
$$\Big((a,b),(c,d)\Big) \mapsto (ac, ad, bc, bd).$$

This map is $\mathbb{Z}$-bilinear:

$$\Big(n(a_1,b_1) + m(a_2,b_2), (c,d)\Big) = \Big((na_1 + ma_2, nb_1 + mb_2), cd\Big)$$
$$\mapsto \Big((na_1 + ma_2)c, (na_1 + ma_2)d, (nb_1 + mb_2)c, (nb_1 + mb_2)d\Big)$$
$$= (na_1c + ma_2c, na_1d + ma_2d, nb_1c + mb_2c, nb_1d + mb_2d)$$
$$= n(a_1c, a_1d, b_1c, b_1d) + m(a_2c, a_2d, b_2c, b_2d),$$

so by the Universal Property, induces a group homomorphism $\Phi : (\mathbb{Z}_5 \times \mathbb{Z}_5) \otimes (\mathbb{Z}_5 \times \mathbb{Z}_5) \to \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Define

$$\Psi : \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \to (\mathbb{Z}_5 \times \mathbb{Z}_5) \otimes (\mathbb{Z}_5 \times \mathbb{Z}_5),$$

$$(a,b,c,d) \mapsto (1,0)\otimes(a,b)+(0,1)\otimes(c,d).$$

We'll show that these are inverses:

$$\Phi(\Psi(a,b,c,d)) = \Phi((1,0)\otimes(a,b)+(0,1)\otimes(c,d)) = (a,b,0,0)+(0,0,c,d) = (a,b,c,d),$$

$$\begin{aligned}\Psi(\Phi((a,b)\otimes(c,d))) &= \Psi(ac,ad,bc,bd) = (1,0)\otimes(ac,ad)+(0,1)\otimes(bc,bd)\\ &= (a,0)\otimes(c,d)+(0,b)\otimes(c,d) = (a,b)\otimes(c,d).\end{aligned}$$

Thus, Φ is an isomorphism, which implies that this tensor product has 5^4 elements.

Finally, we have $\mathbb{Z}_{25}\otimes(\mathbb{Z}_5\times\mathbb{Z}_5)$. We claim that this is isomorphic to $\mathbb{Z}_5\times\mathbb{Z}_5$. Define a map

$$\begin{aligned}\varphi : \mathbb{Z}_{25}\times(\mathbb{Z}_5\times\mathbb{Z}_5) &\to \mathbb{Z}_5\times\mathbb{Z}_5,\\ (a,(b,c)) &\mapsto (ab,ac).\end{aligned}$$

This is well defined because if $a_1 \equiv a_2 \mod 25$, then they are congruent mod 5, and it's easy to see that this is bilinear, so it induces a homomorphism $\Phi : \mathbb{Z}_{25}\otimes(\mathbb{Z}_5\times\mathbb{Z}_5) \to \mathbb{Z}_5\times\mathbb{Z}_5$. Define

$$\begin{aligned}\Psi : \mathbb{Z}_5\times\mathbb{Z}_5 &\to \mathbb{Z}_{25}\otimes(\mathbb{Z}_5\times\mathbb{Z}_5),\\ (a,b) &\mapsto 1\otimes(a,b).\end{aligned}$$

Then,

$$\Phi(\Psi(a,b)) = \Phi(1\otimes(a,b)) = (a,b),$$
$$\Psi(\Phi(a\otimes(b,c))) = \Psi(ab,ac) = 1\otimes(ab,ac) = a\otimes(b,c).$$

Thus, Φ is an isomorphism, so this tensor product has 25 elements.

22 Fall 2007

2. Consider the ring $\mathbb{R}[[x]]$ of formal power series in x with real coefficients. What are the units in this ring? What are the ideals?

We claim that the invertible elements are those whose constant term is nonzero. Indeed, suppose that $\mathbf{a} = \sum_{n=0}^{\infty} a_n x^n$ has an inverse $\mathbf{b} = \sum_{n=0}^{\infty} b_n x^n$. Then,

$$1 = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots \Rightarrow a_0b_0 = 1 \Rightarrow a_0 \neq 0.$$

Now, suppose that $\mathbf{a} = \sum_{n=0}^{\infty} a_n x^n$ is such that $a_0 \neq 0$. We want to construct an inverse $\mathbf{b} = \sum_{n=0}^{\infty} b_n x^n$ such that

$$1 = a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots + \left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n + \ldots,$$

and we will do so inductively. Looking at this equation, we want $a_0b_0 = 1$ and all the other terms to be 0. So, let $b_0 = a_0^{-1}$, and $b_1 = -a_0^{-2}a_1$. Now, suppose that $b_0, \ldots, b_{n-1}$ have been defined. We can then define b_n, since

$$0 = \sum_{k=0}^{\infty} a_k b_{n-k} = a_0b_n + a_1b_{n-1} + \ldots + a_{n-1}b_1 + a_nb_0,$$

$$\Rightarrow b_n = -a_0^{-1}(a_1b_{n-1} + \ldots + a_nb_0).$$

So, we have a formula to define b_n, and so by induction, we can define $\mathbf{b} = \mathbf{a}^{-1}$.

Now, let I be an ideal of $\mathbb{R}[[x]]$. Define the degree of an element $a(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{R}[[x]]$ to be the smallest nonnegative integer k such that the coefficient of x^k is nonzero. Among the elements of I, pick one of minimal degree k, and call it $a(x) = a_kx^k + \ldots = x^k \sum_{n=k}^{\infty} a_n x^{n-k} = x^k\tilde{a}(x)$. By our work above, $\tilde{a}(x)$ is invertible, so $x^k \in I$. Let $b(x) = \sum_{n=0}^{\infty} b_n x^n$ be another element of I, with degree $m \geq k$, so we can write

$$b(x) = x^m \sum_{n=m}^{\infty} b_n x^{n-m} = x^k x^{m-k} \sum_{n=m}^{\infty} b_n x^{n-m}.$$

This implies that $b(x) \in (x^k)$, and so $I = (x^k)$, so the ideals of $\mathbb{R}[[x]]$ are the principal ideals of the form (x^k), where $k \geq 0$.

5. Show that the group $\mathbb{Q}$ of rational numbers with respect to addition is not finitely generated.

Suppose that $\mathbb{Q}$ is generated by $p_1/q_1, \ldots, p_k/q_k$, where we can assume that $(p_i, q_i) = 1$ for each i. Since there are finitely many q_i's and infinitely many primes, we can pick a prime p such that $p \not| q_i$ for each i. Then, suppose that we can write

$$\frac{1}{p} = a_1\frac{p_1}{q_1} + \ldots + a_k\frac{p_k}{q_k}, \quad a_i \in \mathbb{Z}$$

$$= \frac{\left(\prod_{i\neq 1} q_i\right)a_1p_1 + \ldots + \left(\prod_{i\neq k} q_k\right)a_kp_k}{q_1\cdots q_k},$$

$$\Rightarrow q_1\cdots q_k = p\left(\left(\prod_{i\neq 1} q_i\right)a_1p_1 + \ldots + \left(\prod_{i\neq k} q_k\right)a_kp_k\right)$$

This implies that $p|q_1\cdots q_k$. p is prime, so p must divide one of the q_i's but we picked p such that this isn't the case, so we have a contradiction. So, $\mathbb{Q}$ is not finitely generated.

6. Show that $\det(\exp(A)) = e^{\mathrm{tr}(A)}$ for every complex matrix A, where $\exp(A)$ is defined as $\exp(A) = I + A + A^2/2 + \ldots + A^k/k! + \ldots$.

Since A is a complex matrix, we can put A into Jordan canonical form, so that A is "pretty much diagonal," i.e. other than the diagonal, the only non-zero terms are possibly 1's located on the off-diagonal above the diagonal. This simplifies matrix multiplication, as well as taking determinants, for now the determinant is just the product of the diagonal terms, and if the diagonal entries of A are $\lambda_1\ldots,\lambda_n$, then the diagonal entries of A^k are $\lambda_1^k,\ldots,\lambda_n^k$. So, the determinant of e^A is just the product

$$\det(e^A) = \left(\sum_{k=0}^{\infty}\frac{\lambda_1^k}{k!}\right)\cdots\left(\sum_{k=0}^{\infty}\frac{\lambda_n^k}{k!}\right) = e^{\lambda_1}\cdots e^{\lambda_n} = e^{\lambda_1+\ldots+\lambda_n} = e^{\mathrm{tr}(A)}.$$

23 Winter 2007

1. Let R be a ring with identity, and let I be an ideal of R. Under what conditions on I is R/I a field? An integral domain? A commutative ring with identity?

R/I is a field if and only if I is maximal, and R/I is an integral domain if and only if I is a prime ideal.

2. Let V be a vector space, and let A and B be a pair of commuting operators on V. Show that if W is an invariant subspace for A, then so are the spaces BW and $B^{-1}W = \{v \in V : Bv \in W\}$.

Let $Bw \in BW$. Since A and B commute, then

$$A(Bw) = (AB)w = (BA)w = B(Aw) \in BW$$

since W is A-invariant. This implies that $A(BW) \subset BW$, so BW is A-invariant.

If $v \in B^{-1}W$. We want to show that $Av \in B^{-1}W$. Indeed, $B(Av) = (BA)v = A(Bv)$. $Bv \in W$ by definition of $B^{-1}W$, and since W is A-invariant, $A(Bv) \in W$, which implies that $Av \in B^{-1}W$, so $A(B^{-1}W) \subset B^{-1}W$.

4. Suppose that the group G is generated by elements x and y that satisfy $x^5y^3 = x^8y^5 = 1$. Is G the trivial group?

$$1 = x^8y^5 = x^3(x^5y^3)y^2 = x^3y^2;$$

$$\Rightarrow 1 = x^5y^3 = x^2(x^3y^2)y = x^2y;$$

$$\Rightarrow x^2 = y^{-1};$$

$$\Rightarrow 1 = x^8y^5 = (x^2)^4y^5 = y^{-4}y^5 = y;$$

$$\Rightarrow x^2 = 1 \Rightarrow 1 = x^5y^3 = x^5 = (x^2)^2x = x.$$

$$\Rightarrow G \text{ is trivial.}$$

24 Fall 2006

1. Let G be a matrix group, and let $g \in G$ be an element with $\det(g) \neq 1$. Show that $g \notin G'$, the commutator subgroup of G.

If $g \in G'$, then $g = xyx^{-1}y^{-1}$ for some $x, y \in G$. Then,

$$\deg(g) = \det(xyx^{-1}y^{-1}) = \det(x)\det(y)\det(x^{-1})\det(y^{-1}) = \det(xx^{-1})\det(yy^{-1}) = 1.$$

2. Let $A : V \to V$ be an operator on a finite dimensional vector space V. Suppose that A has characteristic polynomial $x^2(x-1)^4$ and minimal polynomial $x(x-1)^2$. What is the dimension of V? What are the possible Jordan forms of A?

The characteristic polynomial is $\det(A - xI)$, so $\dim(V) = 6$, and the eigenvalues are 0 and 1. If the minimal polynomial is $x(x-1)^2$, then the possible invariant factors are

1.$x(x-1)^2, \quad x(x-1)^2,$

2.$x(x-1)^2, \quad x(x-1), \quad x-1.$

The give elementary divisors

1.$x, (x-1)^2, x, (x-1)^2,$

2.$x, (x-1)^2, x, x-1, x-1,$

and so the possible Jordan forms (up to ordering of factors) are

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

3. Show that $\mathbb{Z}$ is a PID.

Let $I \subset \mathbb{Z}$ be an ideal. Pick the smallest positive integer $m \in I$, and let $n \in I$. By the Division Algorithm, we have

$$n = qm + r$$

for some $q \in \mathbb{Z}$ and some $0 \leq r < m$. Since $r = n - qm$, $r \in I$. If $r \neq 0$, then we will have contradicted the minimality of m, so $r = 0$, hence $n \in (m)$, so $I = (m)$, and therefore $\mathbb{Z}$ is a PID.

25 Winter 2006

1. Let the field E be a finite extension of a field F, and let R be a subring of E that contains F. Prove that R is a field.

R is a subgroup of E, but also has multiplicative structure and contains F, which implies that R is an F-subspace of E, which is itself and F-vector space. Let $\alpha_1, \ldots \alpha_k$ be a basis for R. Then we can extend to a basis $\alpha_1, \ldots \alpha_n$ of E, so $E = F(\alpha_1, \ldots, \alpha_n)$, and $R = F(\alpha_1, \ldots, \alpha_k)$. Since E is a finite extension, each α_i satisfies an irreducible polynomial $p_i(x)$ in $F(\alpha_1, \ldots, \alpha_{i-1})[x]$, and that $F(\alpha_i) \cong F[x]/(p_i(x))$ is a field. So, we can inductively form the field $F(\alpha_1, \ldots, \alpha_k) = R$.

2. Let R be a commutative ring with a unit. Prove that the following two properties of R are equivalent:

(a) If $a, b \in R$ and $a + b$ is invertible, then either a or b is invertible.

(b) R is local, i.e. R has a unique maximal ideal.

" $\Rightarrow$ " Let I be a maximal ideal, and J any ideal not contained in I. Since $I \neq J$, we know that $I + J = R$, so there exist $x \in I, y \in J$ such that $x + y = 1$. By (a), this implies that x or y is invertible. Since we assumed that I is maximal, we have y invertible, which implies $J = R$, and I is the only maximal ideal of R.

" $\Leftarrow$ " Suppose there exist $a, b \in R$ with $a + b$ invertible but neither a nor b is invertible. Since neither a nor b are invertible, (a) and (b) are proper ideals. Since R is a commutative ring with 1, we know that (a) and (b) are each contained in maximal ideal. By assumption, they must be contained in the same maximal ideal I. However, this implies that $a + b \in I$, but $a + b$ is invertible, so we have a contradiction.

4. Show that $\mathbb{Q}$ (the additive group of rational numbers) is not finitely generated.

Suppose that $\mathbb{Q}$ is generated by $p_1/q_1, \ldots, p_k/q_k$, where we can assume that $(p_i, q_i) = 1$ for each i. Since there are finitely many q_i's and infinitely many primes, we can pick a prime p such that $p \not| q_i$ for each i. Then, suppose that we can write

$$\frac{1}{p} = a_1\frac{p_1}{q_1} + \ldots + a_k\frac{p_k}{q_k}, \qquad a_i \in \mathbb{Z}$$

$$= \frac{\left(\prod_{i\neq 1} q_i\right)a_1p_1 + \ldots + \left(\prod_{i\neq k} q_k\right)a_kp_k}{q_1 \cdots q_k},$$

$$\Rightarrow q_1 \cdots q_k = p\left(\left(\prod_{i\neq 1} q_i\right)a_1p_1 + \ldots + \left(\prod_{i\neq k} q_k\right)a_kp_k\right)$$

This implies that $p|q_1 \cdots q_k$. p is prime, so p must divide one of the q_i's but we picked p such that this isn't the case, so we have a contradiction. So, $\mathbb{Q}$ is not finitely generated.

5. Determine all finitely generated abelian groups which have a finite group of automorphisms.

Let G be a finitely generated abelian group. Then, by the Fundamental Theorem of Finitely Generated Abelain Groups, we can write G as a product of cyclic groups:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_m\mathbb{Z} \times \mathbb{Z}^l.$$

$$\mathrm{Aut}(G) \cong \mathrm{Aut}\left(\prod_{k=1}^{m} \mathbb{Z}/n_k\mathbb{Z}\right) \times \mathrm{Aut}(\mathbb{Z}^l).$$

$\prod_{k=1}^{m} \mathbb{Z}/n_k\mathbb{Z}$ is a finite group, so it only has finitely many bijections, so its automorphism group is finite. $\mathrm{Aut}(\mathbb{Z}^l)$ is just $GL_l(\mathbb{Z})$, since an automorphism of $\mathbb{Z}^l$ involves sending each basis element $e_i = (0, \ldots, 1, 0, \ldots 0)$ to some $v_i \in \mathbb{Z}^l$ with the v_i's linearly independent. This group is finite for $l \leq 1$.

6. Suppose that $H \subset G$ is a subgroup which is contained in every nontrivial subgroup of G. Show that H is contained in the center of G.

For every $x \in G, y \in H$, $y \in \langle x \rangle$, which is an Abelian group, so $xy = yx$.

26 Winter 2005

2. Prove that $f(x) = x^4 + x + 1$ is irreducible over $\mathbb{Q}$.

By the rational roots theorem, $x^4 + x + 1$ clearly has no roots. So if $f(x)$ is reducible, then is splits into quadratic factors:

$$x^4 + x + 1 = (a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2)$$

$$= a_1a_2x^2 + (a_1b_2 + a_2b_1)x^3 + (a_1c_2 + a_2c_1 + b_1b_2)x^2 + (c_1b_2 + c_2b_1)x + c_1c_2.$$

This implies that $a_1 = a_2 = \pm 1$ and $c_1 = c_2 = \pm 1$, and $a_1b_2 + a_2b_1 = 0$ implies that $b_2 = -b_1$, and $a_1c_2 + a_2c_1 + b_1b_2 = \pm 2 - b_1^2 = 0$ implies that $b_2^2 = \pm 2$, but this is impossible since $b_1 \in \mathbb{Q}$. Hence, $f(x)$ is irreducible over $\mathbb{Q}$.

4. Give definition of PID and examples (without proofs) of

(a) a commutative ring that which is a PID;

(b) a commutative ring which is not a PID.

A PID is a commutative ring such that each ideal is generated by single element, i.e. for every ideal I, there exists an $x \in I$ such that $I = (x) = \{rx : r \in R\}$.

An example of a commutative ring that is a PID is $\mathbb{Z}$. An example of a commutative ring that isn't a PID is $\mathbb{Z}[x]$.

5. Let p be a prime number and $G = \mathbb{Z}_p$ be the finite cyclic group of order p. Prove that the group of automorphisms of G is cyclic and compute its order.

$$\mathrm{Aut}G = \left\{ \{\overline{1} \mapsto \overline{n}\} : 1 \leq n \leq p-1 \right\}$$

Let m denote a primitive root of $\mathbb{Z}_p$. Then, the map $\{\overline{1} \mapsto \overline{m}\}$ generates $\mathrm{Aut}(G)$, and the order is $p-1$. (needs better explanation)

6. Find 4 different subgroups of S_4 isomorphic to S_3 and 9 isomorphic to S_2.

For S_2:

1. $\langle(1,2)\rangle$

2.$\langle(1,3)\rangle$

3. $\langle(1,4)\rangle$

4. $\langle(4,2)\rangle$

5. $\langle(3,2)\rangle$

6.$\langle(3,4)\rangle$

7. $\langle(1,2)(3,4)\rangle$

8. $\langle(1,3)(2,4)\rangle$

9. $\langle(1,4)(2,3)\rangle$.

For S_3,

1. $\langle(1,2)\rangle \cup \langle(1,3)\rangle \cup \langle(2,3)\rangle \cup \langle(1,2,3)\rangle$

2. $\langle(1,2)\rangle \cup \langle(1,4)\rangle \cup \langle(2,4)\rangle \cup \langle(1,2,4)\rangle$

3. $\langle(1,3)\rangle \cup \langle(1,4)\rangle \cup \langle(4,3)\rangle \cup \langle(1,3,4)\rangle$

4. $\langle(3,2)\rangle \cup \langle(2,4)\rangle \cup \langle(4,3)\rangle \cup \langle(2,3,4)\rangle$.

27 Fall 2004

2. Prove that an infinite simple group does not have any proper subgroups of finite index.

Suppose H is a proper subgroup of G with finite index n. Let $X = \{g_1H, \ldots, g_nH\}$ be the set of cosets of X, and consider the permutation representation $\pi : G \to S_n$. $\ker \pi \trianglelefteq G$. Since S_n is finite and G is infinite, $\ker \pi \neq 0$, and since H is proper, $|X| > 1$, so $\ker \pi \neq G$. However, G is simple, so this is a contradiction.

3. Let G be a finitely generated abelian group. Prove that there are no non-zero homomorphisms $f : \mathbb{Q} \to G$.

Suppose that there is a $q \in \mathbb{Q}$ such that $f(q) \neq 0$. However, by Lagrange's Theorem $f(q) = |G|f(q/|G|) = 0$, which is a contradiction.

4. Prove or disprove: $\mathbb{C}[x, y]$ is a PID.

Consider the ideal $I = (x, y)$. This is not all of $\mathbb{C}[x, y]$, since $1 \notin I$ (and so no constants are contained in I). If $I = (f(x, y))$, then there's some $p(x, y), q(x, y)$ such that $x = p(x, y)f(x, y), y = q(x, y)f(x, y)$, but this is only possible if $f(x, y)$ is constant, which is a contradiction. So, $\mathbb{C}[x, y]$ is not a PID.

5. Give examples of each of the following:

(a) A finite nonabelian group.

S_3

(b) an infinite nonabelian group

$GL_2(\mathbb{R})$

(c) A group that is not finitely generated

$\bigoplus \mathbb{Z}$

6(a) Construct infinitely many non-isomorphic quadratic extensions of $\mathbb{Q}$.

(c)

Just take a sequence of constant functions on $[0,1]$, say $f_n(x) = n$. Clearly, this sequence is equitcontinuous but does not converge uniformly to any continuous function on $[0,1]$.

28 Winter 2004

1. For each of the following, give an example or prove that no such example exists.

(1) A nonabelian group of order five.

5 is prime, so any group of order five is cyclic, and therefore abelian.

(2) A nonabelian group of order four.

Looking at a group table, the only possible groups of order four are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(3) An infinite group with a subgroup of order three.

Let $G = \bigoplus \mathbb{Z}_3$ and $H = \langle \overline{1}, \overline{0}, \ldots \rangle$.

(4) Two finite groups of the same order that are not isomorphic.

$\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. In $\mathbb{Z}_4$, $\overline{1}$ has order 4, while every nonzero element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2.

(5) A group G with a normal subgroup H such that the factor group G/H is not isomorphic to any subgroup of G.

Let $G = \mathbb{Z}, H = 2\mathbb{Z}$, so that $G/H \cong \mathbb{Z}_2$, but there are no nonzero elements of $\mathbb{Z}$ with finite order, so no subgroup of G is isomorphic to G/H.

(6) A group G with a subgroup of index two that is not a normal subgroup.

This is impossible. 2 is the smallest prime dividing the order of G, so a subgroup of index 2 must be normal. (more detail needed)

2. Prove or disprove: $\mathbb{C}[x, y]$ is a PID.

Consider the ideal $I = (x, y)$. This is not all of $\mathbb{C}[x, y]$, since $1 \notin I$ (and so no constants are contained in I). If $I = (f(x, y))$, then there's some $p(x, y), q(x, y)$ such that $x = p(x, y)f(x, y), y = q(x, y)f(x, y)$, but this is only possible if $f(x, y)$ is constant, which is a contradiction. So, $\mathbb{C}[x, y]$ is not a PID.

3. Let F be a field, n, m positive integers and A an $n \times n$ matrix with coefficients in F. Suppose that $A^m = 0$. Show that $A^n = 0$.

If $A^m = 0$, then the minimal polynomial $m_A(x) = x^k$ for some $k \geq 0$. Since the characteristic polynomial $c_A(x)$ is a power of x^k and because $\deg c_A(x) = \deg \det(xI - A) = n$ since F if a field, $c_A(x) = x^n = (x^k)^m$ and $c_A(A) = 0$.

29 Fall 2003

1. Let G be a group, and p a prime. Prove or give a counter example.

(a) A group of order p is commutative.

Prime order groups are cyclic, and therefore commutative.

(b) A group of order p^2 is commutative.

If $|G| = p^2$, then $|Z(G)| = 1, p, orp^2$. By the Class Equation, $|Z(G)| \neq 1$. Assume that $|Z(G)| = p$, so that $G/Z(G)$ is cyclic of order p, generated by $xZ(G)$ for some $x \in G$. Then, for $g_1, g_2 \in G$, $g_1 = x^n z_1$ and $g_2 = x^m z_2$ for $n, m \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$. Then,

$$g_1 g_2 = x^n z_1 x^m z_2 = x^n x^m z_1 z_2 = x^{n+m} z_2 z_1 = x^m x^n z_2 z_1 = x^m z_1 x^n z_1 = g_2 g_1,$$

which implies that G is abelian, which is a contradiction. Thus, $|Z(G)| = p^2$, so G must be abelian.

(c) A group of order p^3 is commutative.

Let $G = UT(3, \mathbb{F}_p)$, which is the group of 3×3 unitriangular matrices with entries in $\mathbb{Z}_p$.

2. Let F be a finite field. Show that the number of elements of F is p^r for some prime p and positive integer r.

F is a finite field, so it has characteristic p, where p is a prime. So, it contains $\mathbb{F}_p$ as a subfield, since this is the prime subfield of F. So, we can consider F as the field extension $F/\mathbb{F}_p$ over F, so it's a vector space over $\mathbb{F}_p$. Since F is finite, it is a finite-dimensional vector space, with basis $\{x_1, \ldots, x_r\}$, so we can write every $v \in F$ as

$$v = c_1 x_1 + \ldots + c_r x_r,$$

where $c_i \in \mathbb{F}_p$. Since $|\mathbb{F}_p| = p$, there are p^r total choices for elements of F, hence $|F| = p^r$.

3. A vector space V contains an n-element set with the following properties:

(i) It is not linearly independent, but contains an $(n-1)$-element linearly independent set;

(ii) It does not span V, but is contained in an $(n+1)$-element spanning set.

Prove that $\dim V = n$.

Let $X = \{x_1, \ldots, x_n\}$ be this set, and let $\{x_1, \ldots, x_{n-1}\}$ be the linearly independent subset, and let $x_{n+1} \in V$ such that $X \cup \{x_{n+1}\}$ spans V. Since a basis is the largest linearly independent set that spans V, these assumptions imply that $n - 1 \leq \dim V \leq n + 1$. Any linearly independent set of size $\dim V$ must be a basis, and since X doesn't span $V, \{x_1, \ldots, x_{n-1}\}$ is not a basis, so $\dim V > n - 1$. Similarly, a spanning set of size $\dim V$

must be a basis, but since $X \cup \{x_{n+1}\}$ is not linearly independent by assumption, we must have $\dim V < n+1$. This forces $\dim V = n$.

5. Let $I \subset \mathbb{R}[x]$ be the ideal generated by the polynomial x^2+2x+3. Prove that the quotient ring $\mathbb{R}[x]/I$ is isomorphic to the field $\mathbb{C}$ of complex numbers.

By Eisenstein ($p = 3$), $x^2 + 2x + 3$ is irreducible over $\mathbb{R}$, so I is maximal, and so $\mathbb{R}[x]/I$ is a field.

Define a function

$$\phi : \mathbb{R}[x]/I \to \mathbb{C},$$
$$1 \mapsto 1,$$
$$x \mapsto -1 + i\sqrt{2}.$$

6. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find α so that $K = \mathbb{Q}(\alpha)$, and compute the irreducible polynomial of α over $\mathbb{Q}$

We claim that $\alpha = \sqrt{2} + \sqrt{3}$. Indeed, we can write

$$\sqrt{3} = \frac{1}{4}(\sqrt{2} + \sqrt{3})^3 - \frac{5}{4}(\sqrt{2} + \sqrt{3}).$$

This implies that $\sqrt{2}$ and $\overline{\alpha} = \sqrt{2} - \sqrt{3}$ are also in $\mathbb{Q}(\alpha)$.

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, so the minimal polynomial of α should be of degree 4. When given an element such as α, it's minimal polynomial is

$$(x - \alpha)(x + \alpha)(x - \overline{\alpha})(x + \overline{\alpha}),$$

which, after computation, gives us $x^4 - 10 + 13$.

30 Winter 2003

1. Suppose that A and B are complementary subgroups in a group G, meaning that $G = AB$ and that A and B intersect trivially (but perhaps neither A nor B is normal). Show that each right coset of A intersects each left coset of B in exactly one element.

First, we'll show that each element of G can be written uniquely as a product ab, where $a \in A$ and $b \in B$. Suppose that $a_1b_1 = a_2b_2$, which implies that $a_2^{-1}a_1 = b_2b_1^{-1}$. This implies that $a_2^{-1}a_1, b_2b_1^{-1} \in A \cap B = \{e\}$, which implies that $a_1 = a_2, b_1 = b_2$.

Now, let Ag_1 be a right coset of A, and g_2B a left coset of B, we can write $g_1 = a_1b_1, g_2 = a_2b_2$, so we can actually write $Ag_1 = Ab_1, g_2B = a_2B$. If these two cosets intersect, then we have $ab_1 = a_2b$ for some $a \in A, b \in B$. By our work above, the only choice for a is a_2 and the only choice for b is b_1. Thus, $Ag_1 \cap g_2B = \{a_2b_1\}$.

2. Find all automorphisms of $\mathbb{Z}[x]$, the ring of polynomials over $\mathbb{Z}$.

$\mathbb{Z}[x] = (1, x)$, so the automorphisms are determined by where 1 and x are sent. 1 is invertible, so 1 can be mapped to only ± 1. Also, x must be sent to $\pm x$, for otherwise, if $x \mapsto p(x)$ for some polynomial of degree > 1, then it would be impossible to get a polynomial of degree $< \deg p(x)$. If x maps to a constant, then the map wouldn't be injective, and if $x \mapsto ax$ for some $a \neq \pm$, then it would be impossible to get bx for $|b| < |a|$. Thus, we must map x to $\pm x$. So, there are 4 total automorphisms.

3. Let R be a commutative ring with identity and prime characteristic p. Show that the map

$$\varphi : R \to R,$$
$$r \mapsto r^p$$

is a homomorphism of rings (called the Frobenius homomorphism).

Since R is commutative, $(rs)^p = r^p s^p$ for $r, s \in R$. Also, commutatively allows us to use the binomial theorem:

$$(r+s)^p = \sum_{k=0}^{p} \binom{p}{k} r^k s^{p-k}.$$

For $k \neq 0, p$, $\binom{p}{k}$ is an integer divisible by p, so in these cases, $\binom{p}{k} r^k s^{p-k} = 0$. So, we're left with

$$(r+s)^p = r^p + s^p.$$

So, φ is a ring homomorphism.

4. Find a subgroup of the unit quaternions Q which is a circle. Argue a corollary: The 3-sphere is a union of disjoint circles

Possibility: can write a unit quaternion as $\cos a + \mathbf{r} \sin a$ with $\mathbf{r} = xi + yj + zk$ a unit quaternion with zero real part and $\mathbf{r}^2 = -1$, and $a \in [0, \pi]$. Then, if we fix $\mathbf{r}$, we have

$$(\cos a + \mathbf{r} \sin a)(\cos b + \mathbf{r} \sin b) = \cos(a+b) + \mathbf{r} \sin(a+b).$$

5. Let G be a group and let H be subgroup of G with finite index $n > 1$.

(a) Show that the map $G \times G/H \to G/H$ defined by $(g, aH) \mapsto gaH$ gives an action of G on the space G/H of left cosets of H in G.

$$\Big(g, (h, aH)\Big) = (g, haH) = ghaH = (gh)aH = (gh, aH);$$

$$(e, aH) = eaH = aH.$$

(b) Show that if, in addition, G is finite and the order of G does not divide $n!$, then G is not simple.

Consider the permutation representation $\pi_H : G \to S_n$ of this action, and let K be the kernel. By the first isomoprhism theorem, we have G/K isomorphic to a subgroup of S_n, so $|G/K| = [G : K]|n!$. If $|K| = 1$, then $|G||n!$, but this is a contradiction, so $|K| > 1$. Since the kernel of a homomorphism is a normal subgroup, we have that G is not simple.

(c) Can a subgroup of order $2^2 \cdot 3 \cdot 19^2$ be simple?

The smallest n such that the order of such a group divides $n!$ is $n = 19^2$, since 19 is prime, so such a group cannot be simple.

6. Let

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}.$$

Find a matrix B so that BAB^{-1} is diagonal.

$$\det(A - xI) = x^2 - 7x + 1 \Rightarrow x = \frac{7 \pm 3\sqrt{5}}{2}.$$

The eigenvector corresponding to $\frac{7+3\sqrt{5}}{2}$ is $\langle \frac{-1+\sqrt{5}}{2}, 1 \rangle$, and the eigenvector corresponding to $\frac{7-3\sqrt{5}}{2}$ is $\langle \frac{-1-\sqrt{5}}{2}, 1 \rangle$, so the matrix B is

$$B = \begin{pmatrix} \frac{-1+\sqrt{5}}{2} & \frac{-1-\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix}^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ -1 & \frac{-1+\sqrt{5}}{2} \end{pmatrix}.$$

31 Fall 2002

1(a) Let F be a field. Show that every ideal in the ring of polynomials is principal. If $F[x]$ a UFD?

Let I be an ideal of $F[x]$, and pick $p(x) \in I$ of minimal order. If $f(x) \in I$, then by the Euclidean Algorithm,

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

for some $q(x) \in F[x]$, and for some $r(x)$ such that $0 \leq \deg r(x) < \deg p(x)$. Since $r(x) = f(x) = q(x)p(x)$, $r(x) \in I$, so $r(x) = 0$ by the minimality of $\deg p(x)$. Thus, $f(x) \in r(x)$, and so $I = (r(x))$, so every ideal of $F[x]$ is principal.

Suppose we can factor $f(x)$ into two sets of irreducibles

$$f(x) = p_1 \cdots p_n = q_1 \cdots q_m.$$

This implies that $p_1 \cdots p_n \in (q_1)$. Since q_1 is irreducible, (q_1) is maximal, and therefore prime, so some $p_i \in (q_1)$, and after possible re-labelling, say $p_1 \in (q_1)$. Since p_1 is irreducible, we have $p_1 = u_1 q_1$ for some unit u_1. So,

$$u_1 p_2 \cdots p_n = q_2 \cdots q_m.$$

Continuing in this way, we get that $u_i p_i = q_i$, and we must have $m = n$, so the q_i's are just the p_i's up to units, so the factorization is unique, and therefore $F[x]$ is a UFD.

(b) Are all UFDs PIDs? Why or why not?

By the same reasoning as in (a), $\mathbb{Z}[x]$ is a UFD. However, the ideal $(2, x)$ is not principal, so it is not a PID.

(c) Let $g(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ and let $I = (g(x))$. Prove that $\mathbb{Z}_2[x]/I$ is a field and determine the multiplicative inverse of $x + 2 + 1 + I$.

The elements of $\mathbb{Z}[x]/(g(x))$ are $a_0 + a_1 x + a_2 x^2$, where $a_i \in \mathbb{Z}_2$. Just by plugging in numbers, we see that $g(x)$ is irreducible, and therefore $(g(x))$ is maximal, which implies that $\mathbb{Z}_2[x]/(g(x))$ is a field.

$$x(x^2 + 1) = x^3 + x = 1 + x + x = 1,$$

so the inverse of $x^2 + 1$ is x.

2. Let G be a finite group and $S \leq G$.

(a) Prove that $N_G(S)$ is a subgroup of G. Let K be a subgroup of G which contains S. Prove that S is normal in K if and only if $K \subset N_G(S)$.

This first part is trivial. If $S \trianglelefteq K$, then $ksk^{-1} \in S$ for all $k \in K$, which implies that $K \subset N_G(S)$. If the converse is true, then $ksk^{-1} \in S$ for all $k \in K$, and so $S \trianglelefteq K$.

(b) Prove that the number of distinct conjugate subgroups of S is equal to the index $[G : N_G(S)]$.

Define a function

$$f : \{\text{conjugates of } S\} \to \{\text{Cosets of } N_G(S)\}$$

$$gSg^{-1} \mapsto gN_G(S).$$

If $g_1Sg_1^{-1} = g_2Sg_2^{-1}$, then $S = g_1^{-1}g_2Sg_2^{-1}g_1$, and so $g_1^{-1}g_2 \in N_G(S)$, so $g_1N_G(S) = g_2N_G(S)$, so f is well defined. It's easy to see that it's surjective, and $g_1N_G(S) = g_2N_G(S)$ implies that $g_1^{-1}g_2 \in N_G(S)$, so $g_1Sg_1^{-1} = g_2Sg_2^{-1}$. So, f is injective, and therefore we have a bijection, so the number of conjugates of S is equal to the number of cosets of $N_G(S)$, which is $[G : N_G(S)]$.

(c) If $G = S_4$ and $S = \langle(1234)\rangle$, what is $N_G(S)$?

$$S = \{1, (1234), (13)(24), (1432)\}.$$

Recall that for $\tau \in S_4$, $\tau(1234)\tau^{-1} = (\tau(1)\tau(2)\tau(3)\tau(4))$, so $\tau \in N_G(S)$ if and only if $\tau(1234)\tau^{-1} = (1234)$ or (1432). If $\tau(1234)\tau^{-1} = (1432)$, then we have four possibilities:

(i) $\tau(1) = 1, \tau(2) = 4, \tau(3) = 3, \tau(4) = 2 \Rightarrow \tau = (24)$;

(ii) $\tau(1) = 2, \tau(2) = 1, \tau(3) = 4, \tau(4) = 3 \Rightarrow \tau = (12)(34)$;

(iii) $\tau(1) = 3, \tau(2) = 2, \tau(3) = 1, \tau(4) = 4 \Rightarrow \tau = (13)$;

(iv) $\tau(1) = 4, \tau(2) = 3, \tau(3) = 2, \tau(4) = 1 \Rightarrow \tau = (14)(23)$.

If $\tau(1234)\tau^{-1}$, then we have four possibilities:

(i) $\tau = 1$;

(ii) $\tau(1) = 2, \tau(2) = 3, \tau(3) = 4, \tau(4) = 1 \Rightarrow \tau = (1234)$;

(iii) $\tau(1) = 3, \tau(2) = 4, \tau(3) = 1, \tau(4) = 2 \Rightarrow \tau = (13)(24)$;

(iv) $\tau(1) = 4, \tau(2) = 1, \tau(3) = 2, \tau(4) = 3 \Rightarrow \tau = (1432)$.

So,

$$N_G(S) = \{1, (13), (24), (12)(34), (14)(23), (13)(24), (1234), (1432)\}.$$

3. Prove or disprove the following:

(b) Let R be the ring of Gaussian integers $\mathbb{Z}[i]$. If I is the ideal generated by $3+i$, then R/I is a field.

$$\overline{a+bi} = \overline{a-3b+b(3+i)} = a-3b,$$

and $\overline{4+3i} = 1$, so $R/I \cong \mathbb{Z}$, which is not a field.

c. Every integral domain is a PID.

$\mathbb{Z}[x]$ is an integral domain, but not a PID. For instance, the ideal $(2,x)$ is not principle. If it were, then there would be a polynomial $p(x)$ such that $(p(x)) = (2,x)$, which would imply that $2 = p(x)q(x)$, which would imply that $p(x)$ is constant, while $p(x)g(x) = x$, which would imply that $p(x) = 1$. But, $1 \notin (2,x)$, so $(2,x)$ cannot be principle.

d. No group of order 48 is simple.

Let $|G| = 48$. $48 = 3 \cdot 2^4$. The number of Sylow-2 subgroups is congruent to 1 mod 2 and divides 3, while the number of Sylow-3 subgroups is congruent to 1 mod 3 and divides 16.

e. Every group of order 209 is cyclic.

$209 = 19 \cdot 11$, and the group $\mathbb{Z}_{19} \times \mathbb{Z}_{11}$ is cyclic since 11 and 19 are relatively prime.

4(a) Give an example of a real $n \times n$ matrix none of whose eigenvalues are real.

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

The eigenvalues are $\pm i$.

(b) Show that there is no such example which is 3×3. The eigenvalues of a matrix A are the roots of the characteristic polynomial of A, which is $\det(A - xI)$. For a 3×3 matrix, the degree of this polynomial is real. At least one root of a degree 3 polynomial must be real since $p(z) = 0 \Rightarrow p(\overline{z}) = 0$ for any polynomial $p(z)$ and any complex number z.

32 Winter 2002

1(a) Let G be a group acting on a set S. Let $x \in S, G_x = \{g \in G; gx = x\}$ and $\overline{x} = \{gx : g \in G\}$. Prove that $|\overline{x}| = [G : G_x]$.

Let X be the set of left cosets of G_x. Define a function

$$f : \overline{x} \to X,$$

$$gx \mapsto gG_x.$$

First, we show that f is well-defined. If $g_1x = g_2x$, then $g_2^{-1}g_1x = x$, which implies that $g_2^{-1}g_1 \in G_x$. Similarly, $g_1^{-1}g_2 \in G_x$, so $f(g_1x) = g_1G_x = g_2G_x = f(g_2x)$, hence f is well-defined.

If $f(g_1x) = f(g_2x)$, then $g_1G_x = g_2G_x$, so $g_1^{-1}g_2 \in G_x$, so $g_1^{-1}g_2x = x$, which implies that $g_2x = g_1x$, hence f is injective. If gG_x is a coset of G_x, then $f(gx) = gG_x$, so f is injective. So, f is a bijection, which implies that $|\overline{x}| = [G : G_x]$.

(b) Recall that G can act on itself by conjugation $G \times G \to G$ where $(g, x) \mapsto gxg^{-1}$. From this one obtains the class equations. State and prove the class equations explaining all terms.

For a finite group G, the Class Equation is

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|,$$

where $Z(G)$ is the center of G, $C_G(g)$ is the centralizer of the element g, and the g_i's are representatives of the distinct non-central conjugacy classes of G.

$$C_G(g_i) = \{x \in G : xg_ix^{-1} = g_i\} = G_{g_i},$$

so from part (a), $|\overline{g}_i| = |G : C_G(g_i)|$. If $g \in Z(G)$, then $xgx^{-1} = g$ for all $x \in G$, so the conjugacy class containing g is just $\{g\}$, so for each element of the center, we get a conjugacy class, so the number of central conjugacy classes is just $|Z(G)|$, and so the order of G is the sum of the orders of the distinct conjugacy classes, which is exactly the class equation.

2. Let $(\mathbb{Z}, +)$ be the additive group of integers.

(a) Prove that if H is a subgroup of $\mathbb{Z}$, then $H = \{0\}$ or $H = m\mathbb{Z}$ for some positive integer m.

Let $H \leq \mathbb{Z}$, and pick the smallest positive integer $m \in H$. We claim that $H = m\mathbb{Z}$, which is equivalent to saying that every element of H is a multiple of $\mathbb{Z}$. Indeed, if $n \in H$, then by the Division Algorithm,

$$n = qm + r$$

for some $q \in \mathbb{Z}$ and some $0 \leq r < m$. Since $r = n - qm$, $r \in H$. However, since m is the smallest positive integer in H, r is forced to be 0, so $n = qm$. Thus, $H = m\mathbb{Z}$.

(b) Let R be a commutative ring. Give the definition of prime ideals and maximal ideals in R.

An ideal I defined to be prime if whenever $xy \in I$, the either $x \in I$ or $y \in I$.

An ideal I is said to be maximal if whenever there's an ideal J such that $I \subset J \subset R$, then either $J = I$ or $J = R$.

(c) $\mathbb{Z}$ also has ring structure. What are the prime and maximal ideals in $\mathbb{Z}$? Justify your answer.

Suppose that $m\mathbb{Z}$ is a prime ideal (ideals are also groups, so they must have this form), and $xy \in m\mathbb{Z}$. This implies that $xy = qm$ so $m|xy$ and either $m|x$ or $m|y$. If m were composite, then we can find $m_1, m_2 \neq 1$ such that $m = m_1 m_2$. Then, $m_1 m_2 \in m\mathbb{Z}$, but neither m_1 nor m_2 is in $m\mathbb{Z}$ since neither is a multiple of m. So, we must have that m is prime.

$m\mathbb{Z} \subset n\mathbb{Z}$ implies that every element of $m\mathbb{Z}$ is a multiple of n, i.e. every multiple of m is a multiple of n, i.e. $n|m$. If $m\mathbb{Z}$ is maximal, then there are no integers that divide m other than m itself and 1, so m is prime.

3. Let H and K be subgroups of a group G. Assume that H, K are both normal subgroups of G and that $H \cap K = 1$.

(a) Show that $hk = kh$ for all $h \in H$ and $k \in K$.

Let $h \in H, k \in K$. Since $H \trianglelefteq G$, $khk^{-1} \in H$, so $khk^{-1}h^{-1} \in H$, and since $K \trianglelefteq G$, $hk^{-1}h^{-1} \in K$, so $khk^{-1}h^{-1} \in K$, so $khk^{-1}h^{-1} \in H \cap K$, which implies that $khk^{-1}h^{-1} = 1$,

so $kh = hk$.

(b) Prove that each element in HK can be written uniquely as hk where $h \in H$ and $k \in K$.

Let $x = hk \in HK$, and suppose that $x = h'k'$, so that $hk = h'k'$. This implies that

$$h'^{-1}h = k'k^{-1},$$

so $h'^{-1}h, k'k^{-1} \in H \cap K$, so $h'^{-1}h, k'k^{-1} = 1$, which implies that $h = h'$ and $k = k'$.

(c) Prove that $HK \cong H \times K$.

Define a function

$$\varphi : HK \to H \times K,$$

$$hk \mapsto (h, k).$$

By (b), this is well-defined. If $(h_1, k_1) = (h_2, k_2)$ then $h_1 = h_2$ and $k_1 = k_2$ so $h_1k_1 = h_2k_2$, hence φ is injective. If $(h, k) \in H \times K$, then $\varphi(hk) = (h, k)$, so φ is surjective. Finally, using (a), we have

$$\varphi((h_1k_1)(h_2k_2)) = \varphi(h_1h_2k_1k_2) = (h_1h_2, k_1k_2),$$

$$\varphi(h_1k_1)\varphi(h_2k_2) = (h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2).$$

So, φ is an isomorphism.

4. Let R be a commutative ring with identity and prime characteristic p. Show that the Frobenius homomorphism

$$\varphi : R \to R$$

$$r \mapsto r^p$$

is indeed a ring homomorphism.

The multiplicative part is clear since R is commutative.

Let $a, b \in R$. Since R is commutative, we can use the Binomial Theorem:

$$(a+b)^p = \sum_{k=1}^{p} \binom{p}{k} a^k b^{p-k} = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^k b^{p-k}.$$

$\frac{p!}{k!(p-k)!}$ is an integer, p is prime, and $k!(p-k)!$ contains no factor of p, so $k!(p-k)$ divides $(p-1)!$, and so $\frac{p!}{k!(p-k)!} = pq_k$ for some integer q_k. Since R has characteristic p, this means that all of the terms of $(a+b)^p$ except for a^p and b^p are 0, so $(a+b)^p = a^p + b^p$, and therefore φ is a Ring homomorphism.

5. Let $\mathbb{F}$ be a finite field with q elements and let W be a k-dimensional vector space over $\mathbb{F}$. Show that the number of distinct bases of W is

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1}).$$

If $\{x_1, \ldots, x_k\}$ is any basis of W, then the elements of W are of the form

$$c_1 x_1 + \ldots + c_k x_k,$$

where $c_i \in \mathbb{F}$, which implies that W contains q^k elements. The number of distinct bases of W is just the number of linearly independents subsets of W of size k. To construct such a set, first pick a nonzero element x_1 of W, of which there are $q^k - 1$. To pick the second basis element x_2, it must be nonzero and not in the span of x_1. $\text{span}\{x_1\} = cx_1, c \in \mathbb{F}$, so there are q vectors that we can't choose, so there are $q^k - q$ choices for x_2. Now, suppose we have picked $x_1, \ldots, x_{i-1}$. To pick x_i, we cannot pick a vector in $\text{span}\{x_1, \ldots, x_{i-1}\}$, of which there are q^{i-1}, so there are $q^k - q^{i-1}$ choices for x_i. Thus, there are

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$$

ways to pick a basis for W.

33 2001

1. Suppose that a group G acts on a set X. Show that if $x, y \in X$ belong to the same G-orbit, then $|G_x| = |G_y|$, where $G_x = \{g \in G : gx = x\}$.

First, we'll prove the orbit-stabilizer theorem: **Let G be a group acting on a set S. Let $x \in S, G_x = \{g \in G; gx = x\}$ and $\overline{x} = \{gx : g \in G\}$. Prove that $|\overline{x}| = [G : G_x]$.**

Let X be the set of left cosets of G_x. Define a function

$$f : \overline{x} \to X,$$

$$gx \mapsto gG_x.$$

First, we show that f is well-defined. If $g_1x = g_2x$, then $g_2^{-1}g_1x = x$, which implies that $g_2^{-1}g_1 \in G_x$. Similarly, $g_1^{-1}g_2 \in G_x$, so $f(g_1x) = g_1G_x = g_2G_x = f(g_2x)$, hence f is well-defined.

If $f(g_1x) = f(g_2x)$, then $g_1G_x = g_2G_x$, so $g_1^{-1}g_2 \in G_x$, so $g_1^{-1}g_2x = x$, which implies that $g_2x = g_1x$, hence f is injective. If gG_x is a coset of G_x, then $f(gx) = gG_x$, so f is injective. So, f is a bijection, which implies that $|\overline{x}| = [G : G_x]$. (This is just 1(a) from the Winter 2002 exam)

Since x and y are in the same orbit, $\overline{x} = \overline{y}$, so $[G : G_x] = |\overline{x}| = |\overline{y}| = [G : G_y]$, which implies that $|G_x| = |G_y|$.

2. Prove or give a counter example: If $0 \to K \to G \to H \to 0$ is an exact sequence of groups with both K and H abelian, then G is abelian.

Let $K = \mathbb{Z}/3\mathbb{Z}$, $G = S_3$, and $H = \mathbb{Z}/2\mathbb{Z}$.

Define $\varphi : K \to G$ by sending $\overline{1}$ to (123) and $\psi : G \to H$ by $\sigma \mapsto \text{sgn}(\sigma)$. This gives a short exact sequence, since the image of φ is the subgroup of 3-cycles, which are exactly the kernel of ψ, since they are the even permutations of S_3. Also, both K and H are abelian, but G is not, so this proposition is not true.

3. Prove or disprove: $\mathbb{Z}[x]$ is a PID.

$(2, x)$ is an ideal of $\mathbb{Z}[x]$ that is not principal.

4. Argue that the commutator subgroup of a group G is characteristic, and so is the center.

Let $z \in G'$, the commutator, so $z = xyx^{-1}y^{-1}$, and let ϕ be an automorphism of G. Then, $\phi(z) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1}$, which is also an element of G', so every automorphism maps G' to G', and so it's a characteristic subgroup of G.

If $z \in Z(G)$, then we claim that $\phi(z) \in Z(G)$ for every automorphism of G. Indeed, if $x \in G$ and $\phi \in \text{Aut}(G)$, then there exists an $x' \in G$ such that $\phi(x') = x$. Then,

$$x\phi(z) = \phi(x')\phi(z) = \phi(x'z) = \phi(zx') = \phi(z)\phi(x') = \phi(z)x.$$

Thus, $\phi(z) \in Z(G)$, and so $Z(G)$ is characteristic.

5(a) Give an example of a finite field of order 3 and a field of order 9.

A field of order 3 is $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}$. A field of order 9 is $\mathbb{F}_{3^2}$, which we can construct by taking $\mathbb{F}_3[x]/(x^2 - x - 1)$, since $x^2 - x - 1$ can be easily seen to be irreducible by just checking for roots.

(b) Let F be a finite field. Show that the order of F is equal to p^n for some prime p and some positive integer n.

Let F' be the prime subfield of F. Since F is finite, it must have finite characteristic, which must be some prime p, and therefore $F' = \mathbb{F}_p$. We can consider F as a vector space over $\mathbb{F}_p$, which must be finite dimensional since F is finite. So, we have some basis $\{x_1, \ldots, x_n\}$ of F over F', and so the elements of F are of the form

$$a_1x_1 + \ldots + a_nx_n,$$

where $a_i \in \mathbb{F}_p$, so there are p^n total possibilities for the elements of F, hence F has order p^n.

(c) Show that the multiplicative group $F^\times$ consisting of the non-zero elements of a finite field F is a cyclic group.

If $x, y \in \mathbb{F}^\times$ with relatively prime orders a and b respectively, consider the element xy. Since $(xy)^{ab} = 1$, the order of xy is $\leq ab$. $(xy)^a = y^a$, which has order b. Since $(a, b) = 1$, there's not smaller number c such that ac is a multiple of b, for if $b|c$, then $b|c$, so $c = bq$, and the smallest such c is b itself. Similarly, $(xy)^b = x^b$ has order a. So, ab divides the order of xy, which implies that the order of xy is ab.

If $d|a$. Then $x^{a/d}$ must have order d, since any smaller number c will give a number smaller than a.

If x, y have arbitrary orders, then factor these orders into primes:

$$|x| = p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$
$$|y| = p_1^{\beta_1} \cdots p_n^{\beta_n},$$

where $\alpha_i, \beta_i \geq 0$. The lcm is

$$p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}.$$

For each i, we shoed above that we can find elements with orders $p_i^{\alpha_i}$ and $p_i^{\beta_i}$. Pick the element with the larger order, call it z_i. Then, the z_i's have relatively prime orders, so their product will give us an element with the desired order.

Now, suppose that $x \in \mathbb{F}^\times$ with largest order a. We claim that the order of each element in $\mathbb{F}^\times$ divides r. Indeed, if this were false, then there'd be an element y with order $b \not| a$, and so $\text{lcm}(a, b) > a$, and by our work above, there'd be an element with that order, which contradicts the maximality of a. So, $g^a = 1$ for all $g \in \mathbb{F}^\times$.

Now, let r be the largest order in $\mathbb{F}^\times$, and consider the polynomial $x^r - 1$. By our work above, we know that every element in $\mathbb{F}^\times$ is a root of this polynomial, so the order of the group is at most r, but since $r||\mathbb{F}^\times|$ by Lagrange's Theorem, we have the reverse inequality, and so the two values are equal, and so $\mathbb{F}^\times$ is cyclic.