# Algebra Comp Solutions

Jeffrey Ayers

March 13, 2022

## Contents

# 1 676 Final 2019 Solutions Rewritten

## 1.1 1

To do this we can use Fundamental Theorem of Finite Abelian Groups. Assume that $\mathbb{Q}$ is both free and finitely generated, then as a $\mathbb{Z}$-module we have the decomposition

$$\mathbb{Q} \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

If $\mathbb{Q}$ has a torsion part, then there exists $x \in \mathbb{Z}$ such that $xn = 0$ for $n \in \mathbb{Q}$, which cannot be true, $\mathbb{Q}$ has no nonzero zero divisors. Thus the torsion part is 0, and so $\mathbb{Q}$ is not finitely generated. So,

$$\mathbb{Q} \cong \mathbb{Z}^r$$

If $r \geq 2$ then we can find at least two linearly independent rationals $x_1, x_2$ over $\mathbb{Z}$. So there are $n, m \in \mathbb{Z}$ such that $nx_1 + mx_2 = 0$ implies $n = m = 0$. But if $x_1 = a/b, x_2 = p/q$ then $(pb)(a/b) - (qa)(p/q) = 0$, which is a contradiction.

Hence $\mathbb{Q} \cong \mathbb{Z}$, so the rational are cyclic as a $\mathbb{Z}$-module, and so generated by an element $a/b \in \mathbb{Q}$. But the element $\frac{1}{b+1}$ can never be written as $k\frac{a}{b}$ for $k \in \mathbb{Z}$. Therefore $\mathbb{Q}$ is neither free nor finitely generated as a $\mathbb{Z}$-module.

More explicitly for the finitely generated part: If $\mathbb{Q}$ is finitely generated there is a collection of rationals $\{\frac{a_1}{b_1}, ..., \frac{a_n}{b_n}\}$ at generate the rationals. Let $m = lcm(b_1, ..., b_n)$, then $\mathbb{Q} \subset \langle \frac{1}{m} \rangle$, as for any generator $a_i/b_i$ can be written as $a_i(b_1 \cdots b_{i-1}b_{i+1} \cdots b_n)\frac{1}{c} = a_i/b_i$

As $\frac{1}{2m} \in \mathbb{Q}$ we get $\frac{1}{2m} = \frac{k}{m}$ for some $k \in \mathbb{Z}$. But this means that $2mk = m \implies 2k = 1$ for some integer $k$, which is not possible.

## 1.2 Question 3

### a

First a lemma: If $H$ is a normal subgroup of $G$ of index $p$ then for all $K \leq G$, either $K \leq H$ or $G = HK$ and $|K : K \cap H| = p$. If $K \nleq H$ then as $H$ is normal, the set $HK$ is a subgroup of $G$.

From this lemma we easily arrive at the result: $A_G \trianglelefteq S_G$ of index 2, thus $\pi(G)$ has an odd permutation, so $\pi(G) \notin A_G$ hence the second part applies so $|\pi(G) : \pi(G) \cap A_G| = 2$. As the permutation representation is injective we know that

### b

Let $g \in G$ be an element of order $n$, $|G| = mn$. Consider the permutation representation $\pi : G \to S_{mn}$, then $\pi(g)$ is a permutation. By definition the permutation is left mulitplication by $x$, so $\pi(x) = (g, xg, ..., x^{n-1}g)$. As $g$ has order $n$ the order of this permutation has order dividing $n$, so in particular all the cycles have order dividing $n$. If some cycle has order less than $n$, say $\sigma$ then for $a \in \sigma$

$$\pi(x^k)(a) = x^k \cdot a = a$$

Where the first equality is by definition, and the second is because $\pi(x^k)$ acts trivially on any element $a \in \sigma$, as $\sigma$ is assumed to be a $k$-cycle. But the last equality means that $x^k = 1$ which is a contradiction. Thus $\pi(x)$ consists of only $n$-cycles. As $|G| = mn$, the action of $x$ splits $G$ into $m$ $n$-cycles as these cycles are the orbits of $G$ which partition the group.

### c

If $|G| = 2k$ for $k$ odd then by Cauchy's theorem there is an element $g$ of order 2. By part b there is a permutation $\pi(g)$ is a product of $k$ 2-cycles, meaning that it's an odd permutation. Thus by part a $G$ has a subgroup of index 2.

### d

Subgroups of index 2 are normal: the number of left and right cosets is 2, and as $hH = H = Hh$ if $g \notin H$ then the number of left and right cosets is 2, so $gH = G - H = Hg \implies gH = Hg$. So by part c, $G$ is not simple.

## 1.3 Question 4

### a)

As $M^4 = M^2$ we have $M$ satisfies $x^4 - x^2 = x^2(x-1)(x+1)$ so there are two possibilities for the minimal polynomial: the above polynomial or $x(x-1)(x+1)$. In the former case we know that $x^2$ appears in the charactersitic and minimal polynomial so the largest Jordan block of 0 is $2 \times 2$ and there is 1 such Jordan block. We can permute where the block lives in the Jordan form: there are 3 possibilities, and each of these 3 possibilities yields 2 more choices for where 1, -1 live, yielding 6 conjugacy classes.

If the minimal polynomial is $x(x-1)(x+1)$ we get a diagonal matrix with

## 1.4 8

### a)

If $x$ exists then $a|x \implies x \in (a)$ and $x|b \implies x \in (b)$ so $(x) \subseteq (a) \cap (b)$. To show it's the unique largest ideal by property 2 we have if $a|x', b|x'$ then $(x') \subseteq (a) \cap (b)$, but $x|x' \implies (x') \subseteq (x)$ and thus $(x)$ is the largest principal ideal in the intersection

### b)

If $R$ is a Euclidean domain, then $R$ is a PID, so every ideal is principal, in particular $(a) \cap (b)$ is principal. By part a the ideal generated by the lcm is the unique largest principal ideal in the intersection, which means it is the intersection.

### c)

If $R$ is Euclidean, then $(a) \cap (b) = (x)$, where $x = lcm(a, b)$. If $d = \gcd(a, b)$ then $a = da_1, b = db_1$, so $ab/d = da_1b_1 = ab_1 \implies a|ab/d$, similarly $b|ab/d$. If $x$ is the lcm, then $ar = x \implies abr = bx$, so $ab/x$ divides $b$, simiarly $ab/x$ divides $a$. So $ab/x$ divides $d$, and therefore $ab/d$ divides $x$, thus is equal to $x$.

## 1.5 9

### 1.5.1 a

False (non-degenerate alternating forms exist only on even dimensional spaces)

### 1.5.2 b

True ($\mathbb{C}^5 = \mathbb{R}^{10}$)

### 1.5.3 c

True (complex spectral theorem)

### 1.5.4 d

False (Not symmetric, fails spectral theorem)

### 1.5.5 e

False (-2 ¡0)

# 2 677 Spring 2020 Final Exam Rewrites

## 2.1 Question 4

### 2.1.1 a

To show $T \in \mathrm{Hom}_G(V, V)$ we need that $g \cdot Tv = Tgv$, but this is just

$$T(gv) = z(gv) = gzv = g \cdot Tv$$

### 2.1.2 b

Now, since $T : V \to V$ is a homomorphism of G reps by Schur's lemma $T$ is a scalar times the identity. Specifically it must be a root of unity times the identity because $z$ has an order in $G$, say n, so

$$\rho(z)^n = \rho(z^n)\rho(1) = 1$$

So $\rho(z)$ satisfies $x^n - 1$, meaning that the eigenvalues are roots of unity. In particular $T = \rho(z)$ being a multiple of the identity with an eigenvalue a root of unity, it must mean that $\rho(z) = \epsilon I$

### 2.1.3 c

As $\rho(z) = \epsilon I$ the character is the trace of this representation, which is a sum of $\epsilon$, the dimension of $V$ times, aka $\epsilon\chi(1)$

# 3 Question 5

Let $W = \mathbb{C}^3$ be the permutation rep of $S_3$. The character of this is just the number of fixed points of the standard basis elements under permutations of $S_3$: 1 has 3 fixed points, (12) has 1 fixed point, (123) has none.

The multiplicities are gotten via taking the inner product of the irreducible reps with $W \otimes W \otimes U'$. The character of this tensor product is the product of the respective values of the characters. So for 1 we get 9, for (12) we get -1, and (123) yields 0. Thus we check for the trivial rep $U$, and standard rep $V$:

$$(\chi_U, \chi_{W\otimes W\otimes U'}) = \frac{1}{6}(1(9)(1) + 3(-1)(1)) + 0 = 1$$

$$(\chi_{U'}, \chi_{W\otimes W\otimes U'}) = \frac{1}{6}(1(9)(1) + 3(-1)(-1)) + 0 = 2$$

$$(\chi_V, \chi_{W\otimes W\otimes U'}) = \frac{1}{6}(1(9)(2) + 3(1)(0)) + 0 = 3$$

So we have the following decomposition:

$$W \otimes W \otimes U' \cong U \oplus 2U' \oplus 3V$$

## 3.1 Question 7

## 3.2 Question 8

### 3.2.1 a

Check

### 3.2.2 b

Let $K$ be a splitting field of $f$ over $F_3$, and let $\alpha$ be a root fo $f$ in $K$. Then the Frobenius morphism sends $\alpha \mapsto \alpha^3$, so

$$(\alpha^3)^3 - \alpha^3 + 2 = (\alpha^3 - \alpha + 2)^3 = 0$$
$$(\alpha^9)^3 - \alpha^9 + 2 = (\alpha^3 - \alpha + 2)^9 = 0$$

Since in $F_3$ we have $x^3 = x$, so both $\alpha^3$ and $\alpha^9$ are roots.

### 3.2.3 c

$[K : F_3] = 9$ since $K$ is the splitting field of a degree 3 polynomial over $F_3$, we also know that $[F_3(\alpha) : F_3] = 9$ as $\alpha$ is a root of an irreducible degree 3 polynomial and $F_3(\alpha) \cong F_3[x]/(f)$, as there is exactly one finite field of order $3^2$ we get $K = F_3(\alpha)$

### 3.2.4 d

If $g(x) \in F_3[x]$ is a polynomial of degree 3 over $K$ and it's reducible there's nothing to show. Assume that $g(x)$ is irreducible, then as the field $K$ has order 9, the polynomial $x^9 - x$ splits completely over $K$, and $g(x) \mid x^9 - x$, so $g(x)$ splits in $K$.

## 3.3 Question 9

### 3.3.1 a

Choose the polynomial $\phi_n(x) = \prod_{\zeta \text{primative}}(x - \zeta)$, this is of degree $\varphi(n)$. By definition this is a separable polynomial whose roots are the primative nth roots of unity. Thus $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a splitting field of a separable polynomial, thus Galois.

### 3.3.2 b

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, then

$$\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$$

So $\sigma(\zeta)$ has order precisely n as $\zeta$ has order n.

# 4 January 2021

## 4.1 Question 1

If $R$ is commutative with 1 and $P$ is any prime ideal, then recall that we have a bijection between $R[t]/P[t]$ and $(R/P)[t]$. Thus $R/P$ is an integral domain, and therefore $(R/P)[t]$ is an integral domain, which means so is $R[t]/P[t]$, thus $P[t]$ is a prime ideal, as $R[t]$ is commutative.

To elaborate more we have a map $\varphi : R[t] \to (R/P)[t]$ gotten by reducing coefficients of polynomials in $R[t]$ mod $P$. The kernel of this map are those polynomials which have coefficients in $P$, i.e. the ring $P[t]$, thus by the first isomorphism theorem

$$R[t]/P[t] \cong (R/P)[t]$$

## 4.2 Question 2

Let $R$ be commutative with 1. $M$ an module over $R$ and $N$ a submodule. Let $\text{Ann}(M)$ be the annihilator of $M$ and be a maximal ideal of $R$. Then $R/\text{Ann}(M)$ is a field, and we can turn $M$ into an $R/\text{Ann}(M)$ module via the action

$$(r + \text{Ann}(M)) \cdot m = rm + \text{Ann}(M)$$

Note that this is well-defined because any element in the annihilator kills any $m \in M$. From this we have that $M$ is a module over a field, hence it's a vector space, and by the Fundamental Theorem of Finitely Generated Modules over a PID we know it has a decomposition

$$M \cong R/\text{Ann}(M)^k \oplus (R/\text{Ann}(M))/(a_1) \oplus \cdots \oplus (R/\text{Ann}(M))/(a_n)$$

But $M$ be a vector space over a field, it has no torsion part, so it's a free module hence

$$M \cong (R/\text{Ann}(M))^k$$

As such every submodule (vector subspace) of $M$ is a direct sum of copies of $R/\text{Ann}(M)$, hence if $N \cong (R/\text{Ann}(M))^l$, then we know

$$M \cong N \oplus (R/\text{Ann}(M))^{k-l}$$

And $(R/\text{Ann}(M))^{k-l} = K$ the other desired submodule (subspace).

**Note**: Every vector space is a free module, remember free modules are those with bases!

## 4.3 Question 3

### a)

Let $P$ a be a Sylow $p$-subgroup. If $P$ is characteristic, then for all $\phi \in \text{Aut}(G)$, $\phi(P) = P$, in particular for the inner automorphism given by conjugation we have $gPg^{-1} = P$, so $P$ is normal.

Now let $P$ be normal, so by Sylow's theorems it's the unique Sylow $p$-subgroup. To show it's characteristic, we need that $\phi(P) = P$ for any automorphism, but remember that for such an automorphism to exist we need that $|\phi(P)| = |P|$, i.e. that $\phi(P)$ is a Sylow $p$-subgroup. This is true because for any $g \in P$, $g^{p^k} = 1$, and so $\phi(g)^{p^k} = \phi(g^{p^k}) = 1$ hence $\phi(P)$ is a $p$-subgroup, as every element has order dividing a power of a prime, thus Sylow's theorem says that $\phi(P)$ is conjugate to the Sylow $p$-subgroup $P$, which is normal thus is equal to $P$. But $\phi(P)$ needs to have order equal to $P$, hence $\phi(P) = P$

### b)

No, for example take the quaternion group $Q_8$. It has normal subgroup $\mathbb{Z}/2\mathbb{Z}$ consisting of $\pm 1$. Left multiplication by any group element is an automorphism, but $i \cdot 1 = i \notin \mathbb{Z}/2\mathbb{Z}$, and $i \cdot -1 = -i \notin \mathbb{Z}/2\mathbb{Z}$, so this is not a characteristic subgroup.

## 4.4 Question 4

TO DO

## 4.5 Question 5

Let $G$ be a group with $p^n$ elements, the fact that any $p$-group has nontrivial center follows easily from the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{n} |C_i| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|$$

Where $C_i$ is the ith conjugacy class of size greater than 1. As $|G| = p^n$, then $|G : C_G(g_i)| = p^k$ for some $1 \leq k \leq n$. So $p$ divides the LHS of the class equation and $\sum_{i=1}^{n} |G : C_G(g_i)|$, so it must divide $|Z(G)|$, thus it's of nontrivial size.

Now from this we can see that any $p$-group is solvable, which can be shown via induction on $n$ and using the center: The base case $p^1$ is clear, as an group of size $p$ is cyclic, hence $G/Z(G)$ is abelian. Assume now that this holds for $k \leq n$ and we'll show it holds for $n + 1$. Now as $Z(G)$ is a normal subgroup of $G$, and abelian, so it's solvable, and nontrivial. Now look at $G/Z(G)$. This

is either trivial, in which case $G = Z(G)$ and so solvable, or it's of order less than $p^n$, thus by the inductive step, it's solvable.

The number of inequivalent 1-dimensional representations is equal to the size of the abelianization of $G$, and as $G/[G,G]$ is nontrivial as $G$ is solvable (so it has a derived series) we get that there are at least $p$ inequivalent 1-dimensional representation.

## 4.6 Question 6

First assume $g$ is conjugate to $g^{-1}$, then there exists $h \in G$ such that $hgh^{-1} = g^{-1}$, then we have that

$$\chi(hgh^{-1}) = \chi(g^{-1})$$

But as characters are class functions, they're constant on conjugacy classes, hence

$$\chi(hgh^{-1}) = \chi(g) = \chi(g^{-1})$$

As $\chi(g) = \chi(g^{-1})$, and $\chi(g^{-1}) = \overline{\chi(g)}$, due to the fact that every element of a finite group has finite order, so the eigenvalues are nth roots of unity, for $n$, the order of $g$.

Next assume that $\chi(g) \in \mathbb{R}$ for every $g \in G$ and irreducible character $\chi$. As such we know that $\chi(g) = \overline{\chi(g)}$, and so via column orthogonality

$$\sum_{\chi} \chi(g^{-1})\overline{\chi(g)} = \begin{cases} |G|/C(g) & g \sim g^{-1} \\ 0 & \text{else} \end{cases}$$

But as $\chi(g) \in \mathbb{R}$ we have

$$\sum_{\chi} \chi(g^{-1})\overline{\chi(g)} = \sum_{\chi} \chi(g^{-1})\chi(g^{-1}) = \sum_{\chi} \chi(g^{-1})^2 > 0$$

Due to the trivial representation yielding character 1, so $g \sim g^{-1}$

**Note** REMEMBER THE ORTHOGONALITY RELATIONS:
Column orthogonality:

$$\sum_{\chi} \chi(g)\overline{\chi(h)} = \begin{cases} |G|/C(g) & g \sim h \\ 0 & \text{else} \end{cases}$$

Where $C(g)$ is the size of the conjugacy class of $g$

Row orthogonality: $(\chi_i, \chi_j) = \delta_{ij}$

## 4.7 Question 7

Let $A, B$ be two commuting $n \times n$ matrices over $\mathbb{C}$, with $A$ diagonizable. We need to show they're simultaneously block diagonalizable. Both matricies live over an algebraically closed field, so by JCF theorem, they both have a JCF. Moreover, $A$ is diagonlizable so it's Jordan form is diagonal. This is similar to the proof that commuting matricies are simulatenously diagonlizable.

First a lemma

**Lemma.** *Commuting matricies preserve each others eigenspaces*

*Proof.* $AB = BA$, so if $v$ is an eigenvector of $A$ with eigenvalue $\lambda$, $ABv = BAv = B\lambda v = \lambda Bv$, so $Bv$ is in the eigenspace corresponding to eigenvalue $\lambda$. Said another way, every eigenvector $v$ of $A$, when hit with $B$ yields another eigenvector with the same eigenvalue as $v$. □

By the lemma, every eigenspace $V_{A,\lambda}$ of $A$ is invariant under $B$. $A$ is diagonlizable, so there exists a basis of eigenvectors, in particular for $V_{A,\lambda_1}, ..., V_{A,\lambda_n}$ eigenspaces of $A$,

$$\mathbb{C}^n = V_{A,\lambda_1} \oplus \cdots \oplus V_{A,\lambda_n}$$

Writing $B$ in the basis of eigenvectors thus yields a block diagonal matrix. So in the change of basis matrix $P$ corresponding to the basis of eigenvectors of $A$ we have that $PAP^{-1} = D$ for a diagonal $D$, as $A$ is diagonlizable, and $PBP^{-1}$ is a block diagonal matrix. Each block is in the basis corresponding to the eigenvalue $\lambda_i$ of $A$, which is also an eigenvalue of $Bv$ for each eigenvector $v$. (Unclear about this step) Therefore $PBP^{-1} = J$ the Jordan Canonical Form of $B$.

## 4.8 Question 8

Over $\mathbb{C}$ this polynomial factors as $(x-1)(x+1)(x-1)(x^2+x+1) = (x-1)^2(x+1)(x-\zeta)(x-\zeta^2)$ where $\zeta$ is a primative 3rd root of unity. There are only 2 possibilities of minimal polynomials for this: $(x-1)^2(x+1)(x-\zeta)(x-\zeta^2)$ or $(x-1)(x+1)(x-\zeta)(x-\zeta^2)$. From here the possible RCFs are clear.

## 4.9 Question 9

## 4.10 Question 10

### a)

Clearly $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension: it's the splitting field of the separable polynomial $x^2 - 2$, and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$

The extension $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - \sqrt{2}$. $\alpha$ is a 4th root of 2, and hence $\alpha^2 - \sqrt{2} = \sqrt{2} - \sqrt{2} = 0$. The root of this polynomial are $\pm\alpha$, which both are in $\mathbb{Q}(\alpha)$ and this polynomial is separable, hence $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2})$ is Galois. Furthermore this also has Galois group $\mathbb{Z}/2\mathbb{Z}$ as the 2 roots are mapped either to each other or themselves (the trivial automorphism or the order 2 automorphism)

**b)**

To show $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois we need that it's not a splitting field or that the polynomial it splits is not separable. $\alpha$ is a root of the polynomial $x^4 - 2$, which has roots $\alpha, \alpha\zeta^k$ for $1 \leq k \leq 3$, the field $\mathbb{Q}(\alpha)$ is real, and so it cannot contain any complex roots of unity, thus the field extension over $\mathbb{Q}$ is not Galois.

# 5 August 2020

## 5.1 Question 1

Let $T$ be a linear operator on an $n$-dimensional complex vector space such that $\ker(T) = \text{im}(T)$. The hint says to note that it may not be true that there exists such a $T$ for all dimensions, so let's investigate. If $\ker(T) = \text{im}(T)$ then by rank-nullity

$$\dim V = \dim \ker(T) + \dim \text{im}(T) = 2 \dim \ker(T)$$

So as the dimension of $V$ is a multiple of 2 we know that $V$ is an even-dimensional space.

Furthermore we know that for all $v \in V$, $Tv \in \text{im}(T)$ this is also in $\ker(T)$, so $T(Tv) = 0$, which means that $T^2 v = 0$ for all $v \in V$, thus $T$ is nilpotent. This means that the polynomial $x^2$ kills $T$, and therefore the minimal polynomial must divide $x^2 \implies$ it's either $x$ or $x^2$. Hence the Jordan blocks are either (0) or $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. If the minimal polynomial is $x$, then this means that the operator is the zero operator (if $x$ kills $T$ then $T = 0$). Hence the minimal polynomial is $x^2$, and the characteristic polynomial must be $x^{\dim V} = x^n$.

Now we know the characteristic and minimal polynomial we can find the JCF. The multiplicity of the minimal polynomial is the size of the largest Jordan block of the corresponding eigenvalue, in our case all eigenvalues are 0, as this is a nilpotent operator. For this one, the size of the largest Jordan block is 2, and the multiplicity of the characteristic polynomial is the sum of the sizes of the Jordan blocks of 0. The dimension of $V$ is even, so it's $2k$, and the sum of the sizes of the Jordan blocks is therefore $2k$, with the largest being of size 2, meaning that we have the following JCF

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

## 5.2 Question 2

Use Cayley Hamilton

## 5.3 Question 5

### 5.3.1 b

Use 4th isomorphism theorem? The ideals in $\mathbb{F}_q[x,y]/I$ are ideals $J/I$ which are in bijection with ideals $I \subset J$. Ideals $J$ are such that they divide $I = (x,y)^2$, so there are 2? $(x,y)$ and the whole ring.

## 5.4 Question 6

Let $P$ be a normal Sylow $p$-subgroup of finite group $G$. As $G$ is finite, every element has an order, so $g \in G$ there is a nonnegative integer $n$ such that $g^n = 1$. For any element $g \in P$, if $|P| = p^k$, then $g^{p^k} = 1$. For any homomorphism $f : G \to G$ we know

$$1 = f(g^{p^k}) = (f(g))^{p^k}$$

So the element $f(g)$ has order dividing $p^k$, meaning that every element is prime order, so it's a $p$-group. By Sylow's theorem every $p$-group is conjugate to a Sylow-$p$ subgroup, so $f(P) \leq hPh^{-1}$, but as $P$ is normal we have that $hPh^{-1} = P$, so $f(P) \leq P$

## 5.5 Question 7

Irreducible reps are given by the number of conjugacy classes, there are 6 conjugacy classes in $S_5$, and 5 in $C_5$, yielding 30 in total, thus 30 irreducible reps. The number of 1 dimensional reps is given by the order of the abelianization, which is

$$S_5 \times C_5/[S_5 \times C_5, S_5 \times C_5] = S_5/[S_5, S_5] \times C_5/[C_5, C_5] \cong S_5/A_5 \times C_5/1 \cong \mathbb{Z}/2\mathbb{Z} \times C_5$$

For a total of 10 1-dimensional irreducible reps

## 5.6 Question 8

Let $X = \{(i,j) : 1 \leq i \leq 3, 1 \leq j \leq 3, i \neq j\}$. The character of the representation $\mathbb{C}[X]$ is given by the number of fixed points of the action on the coordinates. The number of elements in $X$ is 6: (12), (21), (13), (31), (23), (32). Using elements $(1), (12), (123)$ as our representatives of the conjugacy classes we have

$$\chi_{\mathbb{C}[X]}(1) = 6$$
$$\chi_{\mathbb{C}[X]}(12) = 0$$
$$\chi_{\mathbb{C}[X]}(123) = 0$$

Clearly sending $1 \mapsto 1$ yields all 6 fixed points, sending $1 \mapsto 2, 2 \mapsto 1$ will result in no fixed points, as each element of $X$ has a 1 or a 2 in the transpositions, and the 3 cycle also clearly has no fixed

points. Hence we now compute the inner product of $\chi_{\mathbb{C}[X]}$ with each of the 3 irreducible characters of $S_3$:

$$(\chi_{\mathbb{C}[X]}, \chi_{triv}) = \frac{1}{6}(1 \cdot 1 \cdot 6 + 3 \cdot 1 \cdot 0 + 2 \cdot 1 \cdot 0) = 1$$

$$(\chi_{\mathbb{C}[X]}, \chi_{sign}) = \frac{1}{6}(1 \cdot 1 \cdot 6 + 3 \cdot -1 \cdot 0 + 2 \cdot 1 \cdot 0) = 1$$

$$(\chi_{\mathbb{C}[X]}, \chi_{standard}) = \frac{1}{6}(1 \cdot 2 \cdot 6 + 3 \cdot 0 \cdot 0 + 2 \cdot -1 \cdot 0) = 2$$

Where for each inner product we divide by the order of $S_3$, the sum up the number of elements in the conjugacy class times the evaluation of the characters of a representative of the conjugacy class. All in all we have the following decomposition:

$$\mathbb{C}[X] = U \oplus V \oplus 2W$$

Where $U$ is the trivial rep, $V$ is the sign rep, and $W$ is the standard rep with multiplicity 2.

## 5.7 Question 9

Let $K \subset F$ be a field extension with $u \in F$. If $[K(u) : K]$ is odd, then we need that $K(u) = K(u^2)$. First it's clear that $K(u^2) \subset K(u)$ given that all powers of $u$ appear in $K(u)$. To show the reverse we need that $[K(u) : K(u^2)] = 1$. We have that

$$[K(u) : K] = [K(u) : K(u^2)][K(u^2) : K]$$

$u$ is a root of the polynomial $x^2 - u^2 \in K[u^2]$. This polynomial is either reducible or irreducible. If it's irreducible, then this means that $K(u^2)$ is the splitting field of $x^2 - u^2$, and therefore $[K(u) : K(u^2)] = 2$ as $x^2 - u^2$ is a degree 2 irreducible polynomial, but this means that $[K(u) : K]$ is not odd, which is a contradiction. Thus $x^2 - u^2$ is reducible, and hence $[K(u) : K(u^2)] = 1$, so $K(u) = K(u^2)$

## 5.8 Question 10

One can check that in this field, 7 is a root of $x^3 - 2$, so $x^3 - 2 = (x - 7)p(x)$. Using the Euclidean algorithm we can divide $x^3 - 2$ by $x - 7$ to get that

$$x^3 - 2 = (x - 7)(x^2 + 7x + 5)$$

Now $x^2 + 7x + 5$ is irreducible in $\mathbb{Z}_{11}$, and so for an irreducible polynomial of degree $d$ over a finite field $\mathbb{F}_p$, with root $\alpha$, the other roots are $\alpha^p, \alpha^{p^2}, ..., \alpha^{p^{d-1}}$. For this polynomial, with root $\alpha$, such that $\alpha^2 + 7\alpha + 5 = 0$, it has another root $\alpha^{11}$. This is a degree 2 irreducible polynomial over a finite field, and therefore it's Galois group is generated by the Frobenius automorphism, $\alpha \mapsto \alpha^{11}$.

Now, we have that the field automorphisms fix elements of $\mathbb{Z}_{11}$, so $7 \mapsto 7$, and thus we have an order 2 automorphism given by the Frobenius map, hence the Galois group is $\mathbb{Z}_2$.

# 6 January 2020

## 6.1 Question 1

Show that a group of order 56 is not simple.

**Solution** $56 = 2^3 \cdot 7$, by Sylow's theorems this means that $n_7 \equiv 1 \mod 7$ and $n_7 | 8$, so $n_7 = 1$ or 8. If $n_7 = 1$ we're done, so assume that $n_7 = 8$. In this case we count the number of elements of order 7: $8(7-1) = 8 \cdot 6 = 48$. We have $56 - 48 = 8$ elements unaccounted for, and as the Sylow 2-subgroup has 8 elements, these are all the elements in the group. Hence there is exactly one Sylow 2-subgroup, thus as group of order 56 is not simple.

## 6.2 Question 2

If a group of order 35 actions on a set of order 18, show the action has a fixed point.

## 6.3 Question 5

Let $I_1, ..., I_m$ be ideals in an integral domain. If $I_1 \cap \cdots \cap I_m = \{0\}$ then show that at least one of the $I_j$ is the zero ideal.

**Solution** Assume none of the ideals is the zero ideal, so there exists at least one $a_j \in I_j$ which is nonzero. Let $a_1, .., a_m$ be the elements of the respective ideals which are nonzero, then the element $a_1 \cdots a_m \in I_1 \cap \cdots \cap I_m$. This means that $a_1 \cdots a_m = 0$, but we assumed none of these elements are zero, which is impossible as we are in an integral domain. Hence one of the ideals must be zero.

## 6.4 Question 7

# 7 August 2019

## 7.1 Question 1

How many elements of order 7 are there in a simple group of order 168?

**Solution** $168 = 2^3 \cdot 3 \cdot 7$, by Sylow's theorems we know that $n_7 \equiv 1 \mod 7$ and divides 24. Thus $n_7 = 1$ or 8, but as the group is simple it must be 8. Counting the number of elements of order 8 is the product of the number of Sylow 7-subgroups and 1 minus the size of one of the Sylow 7-subgroups, which is 7. Thus there are $8(7-1) = 48$ elements of order 48.

## 7.2 Question 2

**Solution part a** Consider the permutation representation on cosets of $H$:

$$\pi_H : G \to \text{Perm}(C_H) \cong S_{[G:H]} = S_n$$

The kernel of this map, call it $K$, is the largest normal subgroup of $G$ contained in $H$, and if we look at

$$\varphi : G/K \to S_n$$

Given by $\varphi(g+K) = \pi_H(g)$ we get that this is injective from the First Isomorphism theorem. As such we have

$$[G:K] = |G/K| \leq |S_n| = n!$$

**Solution part b** Assume for contradiction that $G$ is a subgroup of $A_7$. Then the index of $G$ is 5, $7!/504 = 5$. Thus by part $a$ we know that there is a normal subgroup $K$ of $G$ such that $K \leq A_7$ and $[A_7 : K] \leq 5!$. But this means that $A_7$ has a normal subgroup which is impossible as it's a simple group.

## 7.3 Question 3

**Solution** Let $R$ be a finite commutative ring with unit, and $P$ be a prime ideal. We know that $R/P$ is then an integral domain, and moreover is finite as $R$ is. But finite integral domains are fields, and hence $R/P$ is a field, which occurs if and only if $P$ is maximal.

## 7.4 Question 4

**Solution** The indices of inertia are the number of positive, negative and zero eigenvalues of the matrix. From the basis element we can write the matrix by reading off the coefficients:

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 8 \end{pmatrix}$$

The minimal polynomial is $x(x^2 - 11x + 21)$ by checking. As such the roots are $x = 0, x = \frac{11 \pm \sqrt{37}}{2}$, so we have 2 positive indices of inertia and 0 negative indices of inertia.

## 7.5 Question 6

**Solution part a** Find the minimal polynomial, then find the RCF. The minimal polynomial of this matrix is $x^2 - x - x$ so the RCF is

$$\begin{pmatrix} 0 & 6 \\ 1 & 1 \end{pmatrix}$$

**Solution part b** The annihilator of the module defined by $A$ is defined as all the polynomials such that when you evaluate on $A$ you get the 0 matrix. Well this is just the ideal generated by the minimal polynomial, so the annihilator is $(x^2 - x - 6)$

## 7.6 Question 7

**Solution part a** Can show that $x^3 + x + 1$ is irreducible via the rational roots test. In a field we know that irreducible elements are the same as prime elements, so $x^3 + x + 1$ is prime and thus the ideal generated by the polynomial is prime. The ideal $(x^3 + x + 1)$ is nonzero and in a field a nonzero prime ideal is the same as a maximal ideal, hence $\mathbb{Q}[x]/(x^3 + x + 1)$ is a field.

**Solution part b** To find the multiplicative inverse of $\alpha + 1$ we need to find the GCD of $1 + x$ and $x^3 + x + 1$. We use polynomial long division to find that

$$x^3 + x + 1 = (1 + x)(x^2 - x + 2) + 1$$

Thus

$$1 = (1 + x)(x^2 - x + 2) - (x^3 + x + 1)$$

So the inverse of $1 + \alpha$ is $\alpha^2 - \alpha + 2$.

## 7.7 Question 8

**Solution** To find the splitting field of $x^p - 2$ over $\mathbb{Q}$ we need the roots of this polynomial over $\mathbb{Q}$. Note that this is an irreducible polynomial by Eisenstein. Clearly one such root is $\sqrt[p]{2}$, but we also have $\sqrt[p]{2}\omega$ where $\omega$ is a primitive $p^{th}$ root of unity, as well as all powers of $\omega$ from 1 to $p - 1$. This comprises all the roots so the splitting field is $\mathbb{Q}(\sqrt[p]{2}, \omega)$.

To find the degree we compute

$$[\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$$

We know that

$$[\mathbb{Q}(\omega) : \mathbb{Q}]$$

has degree $p-1$ as this is the degree of the cyclotomic polynomial, which is the minimal polynomial of $\omega$ over $\mathbb{Q}$.

The degree of $[\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}(\omega)]$ is the minimal polynomial of $\mathbb{Q}(\sqrt[p]{2}, \omega)$ over $\mathbb{Q}(\omega)$, which is $x^p - 2$. So in total we have

$$[\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}] = p(p-1)$$

## 7.8 Question 9

$x^3 - 2$ is irreducible over $F_7$ as a check shows. If $\alpha$ is a root of $x^3 - 2$ then other roots are gotten by taking 7th powers: $\alpha, \alpha^7, \alpha^{7^2}$, and $\alpha^{7^3} = \alpha$ in $F_7(\alpha)$. Now as $\alpha^3 - 2 = 0 \implies \alpha^3 = 2$, so $\alpha^7 = (\alpha^3)^3\alpha = 4\alpha$, and $\alpha^4 9 = 2\alpha$. Our Galois group is cyclic since $|\mathrm{Gal}(\mathbb{F}_7(\alpha)/\mathbb{F}_7)| = [\mathbb{F}_7(\alpha) : \mathbb{F}_7] = 3$ and there is only one group of order 3 up to isomorphism.

## 7.9 Question 10

Let $V$, $W$ be complex finite dimensional representations of finite $G$, $f : V \to W$ a surjective homomorphism of $G$-reps. If there is a nonzero vector $w \in W$ such that $gw = w$ for all $g \in G$, then I claim that $\tilde{v} = \frac{1}{|G|}\sum_{g\in G} gv$ is such a vector in $V$, where $f(v) = w$.

First as $f$ is surjective there exists such a $v \in V$ that $f(v) = w$. So we need $h\tilde{v} = \tilde{v}$ for all $h \in G$:

$$\begin{aligned} g\tilde{v} &= h\frac{1}{|G|}\sum_{g\in G} gv \\ &= \frac{1}{|G|}\sum_{g\in G} hgv \\ &= \frac{1}{|G|}\sum_{k\in G} kv \qquad \text{Where hg= k, and we reorder the sum} \\ &= \tilde{v} \end{aligned}$$

As desired.

Next we need to actually see that $f(\tilde{v}) = w$:

$$\begin{aligned}
f(\tilde{v}) &= f\left(\frac{1}{|G|}\sum_{g\in G} gv\right) \\
&= \frac{1}{|G|}\sum_{g\in G}(fgv) \\
&= \frac{1}{|G|}\sum_{g\in G} gf(v) \qquad \text{Since f is a hom of G-reps} \\
&= \frac{1}{|G|}\sum_{g\in G} gw \\
&= \frac{1}{|G|}\sum_{g\in G} w \\
&= w\frac{1}{|G|}\sum_{g\in G} \\
&= w
\end{aligned}$$

# 8 August 2018

## 8.1 Question 1

### a)

We need that $V_0 \cap V_1 = \{0\}$ and that $V_0 + V_1 = V$.

First let $v \in V_0 \cap V_1$, then $Pv = 0v$ and $Pv = 1v$, but the only way for this to hold is if $v$ is the zero vector, as you cannot have two eigenvalues for one eigenvector.

Next we need $V = V_0 + V_1$, let $v \in V$, then we can represent $v$ as the sum $v - Pv + Pv$. $Pv \in V_1$ as $P(Pv) = P^2v = 1 \cdot Pv$, and $v - Pv \in V_0$ as $P(v - Pv) = Pv - P^2v = Pv - Pv = 0$. Thus the $V$ is the desired direct sum.

### b)

First as $(,)$ is an inner product we always have $0 \leq (v, w)$. To show that $(Pv, v) \leq (v, v)$ we'll first use that $v = u + w$ for $u \in V_0, w \in V_1$.

$$\begin{aligned}
(Pv, v) &= (P(u + w), u + w) \\
&= (Pu + Pw, u + w) \\
&= (w, u + w) \\
&= (u, w) + (w, w) \\
&= (w, w) \quad \text{because } u, w \text{ are orthogonal} \\
&\leq (u, u) + (w, w) \\
&= (u, u) + (u, w) + (w, u) + (w, w) \\
&= (v, v)
\end{aligned}$$

## 8.2 Question 2

Let $M = \begin{pmatrix} 4 & 9 \\ -1 & 2 \end{pmatrix}$ Then using Jordan form we can find an invertible matrix $A$ such that $M = AJA^{-1}$, then computing powers of the matrix $M$ is much easier as we can just compute powers of the Jordan matrix.

First we need the characteristic polynomial: $(x - 1)^2$, and as the polynomial $x - 1$ does not kill $M$ we know this is also the minimal polynomial. So the Jordan form of $M$ is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Next we need to find the matrix $A$, and to do this we need the eigenvectors of $M$, computing yields that we have a single eigenvector $\begin{pmatrix} -3 \\ 1 \end{pmatrix}$. The columns of $A$ will consist of the eigenvectors of $M$, but as we only have 1 we need another vector.....

## 8.3 Question 3

## 8.4 Question 4

**a)**

Let $G$ be a group of order $45 = 3^2 \cdot 5$, via Sylow's theorems we know that there is a unique Sylow 5 subgroup and a unique Sylow 3 subgroup, call these $P, Q$ respectively. As these are unique, both are normal, and hence the set $PQ$ is a subgroup of $G$. The subgroup $P \cap Q$ is contained in both $P$ and $Q$ so by Lagrange, it has order 1, and so $PQ \cong P \times Q$. $P$ is a prime order group, hence is cyclic, thus abelian, and $Q$ is a prime squared order group, thus abelian. As $P, Q$ is abelian we know $P \times Q$ is. Since $P, Q$ are both subgroups of $PQ$ the order of this subgroup is divisible by 5 and 9, hence is divisible by 45. But this means that $G = PQ \cong P \times Q$, which is a direct product of abelian groups, so $G$ is abelian.

**b**

By the Fundamental Theorem of Finite Abelian Groups we know that $G$ is isomorphic to a direct sum of cyclic groups:

$$G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3^{n_1}\mathbb{Z} \times \mathbb{Z}/3^{n_2}\mathbb{Z}$$

Where $n_1 + n_2 = 2$, so either both are 1 or one is 2 and the other is 0. All in all we have 2 possible groups of order 45:

$$G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

## 8.5 Question 5

Let $A \in M_2(\mathbb{Q})$ be such that $A^6 = I$. As $A$ is a $2 \times 2$ matrix we know that the characteristic polynomial is of degree 2, and hence the minimal polynomial is of degree 1 or 2. If $A^6 = I$, then $A$ satisfies the polynomial $x^6 - 1$, if we factor this over $\mathbb{Q}$ we get

$$x^6 - 1 = (x-1)(x^2 + x + 1)(x+1)(x^2 - x + 1)$$

In order for $A^6 = I$, it is possible, as the problem does not specify what the order of $A$ must be, that $A$ could have order less than 6. Thus the possible list of invariant factor, keeping in mind that

the minimal polynomial has degree less than 2 is as follows:

$$(x-1),(x-1)$$

$$(x+1),(x+1)$$

$$(x-1)(x+1)$$

$$x^2+x+1$$

$$x^2-x+1$$

Thus the possible RCFs given these invariant factors are

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

Checking, one can see that every matrix in this list, when raised to a power less than order equal to 6 yields the identity matrix.

## 8.6 Question 6

In the $x_1, x_2, x_3$ basis the quadratic form has matrix representative

$$\begin{pmatrix}2&-1&-1\\-1&1&-1\\-1&-1&\lambda\end{pmatrix}$$

Note: We halve the nondiagonal entries unless both $x_ix_j$ and $x_jx_i$ appear as we need a symmetric matrix. The quadratic form is positive definite when the matrix is positive definite, i.e. when the determinants of the subminors are all positive.

First we have that $2>0$, clearly. Next look at $\begin{pmatrix}2&-1\\-1&1\end{pmatrix}$ this has positive determinant as well. Finally we look at the determinant of the whole matrix which is $\lambda-5>0$, hence we need $\lambda>5$.

## 8.7 Question 7

We can write the relations as a matrix:

$$\begin{pmatrix}8&4&0\\2&4&12\\6&4&4\end{pmatrix}$$

Then using elementary row and column operations one can reduce this matrix to Smith Normal Form, and simply read off the coefficients:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

This the direct product of the cyclic groups

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}$$

## 8.8 Question 8

### a)

Let $G$ be a finite group with complex finite dimensional representation $V$. Let $g \in G$, then there is a positive integer $n$ such that $g^n = 1$. As such we have

$$\rho(g)^n = \rho(g^n) = \rho(1) = 1$$

So the $\rho(g)$ satisfies $x^n - 1$, hence the eigenvalues of are $n^{th}$ roots of unity. The character of $g$ is therefore a sum of roots of unity, as it's the trace of $\rho(g)$ which is a sum of eigenvalues.

### b)

$\chi(g) \in \mathbb{R}$, if and only if $\chi(g) = \overline{\chi(g)}$. As $\chi(g)$ is a sum of roots of unity, and the inverse of roots of unity are the complex conjugates, we know that

$$\overline{\chi(g)} = \sum \overline{\lambda_i} = \sum \lambda_i^{-1} = \chi(g^{-1})$$

So $\chi(g) = \chi(g^{-1})$

## 8.9 Question 9

Let $F$ be the field with $q$ elements, and $f(x)$ is an irreducible polynomial in $F[x]$ of degree $n$ with root $\alpha$ in a splitting field over $F$. Then $[F(\alpha) : F] = n$, and so $\alpha \in F_{q^n}$, hence $\alpha^{q^n} = \alpha$, thus $\alpha$ is a root of $x^{q^n} - x$.

## 8.10 Question 10

# 9 August 2017

## 9.1 Question 1

### a)

If the norm of an element in $\mathbb{Z}[i]$ is prime, it's irreducible. This is because $N(a+bi) = a^2 + b^2$, and $p$ factors as a product of irreducible if and only if $p = a^2 + b^2$ is the sum of two integer squares. For this it can be done explicitly but using the fact that the norm of the Gaussian integers is the product of the element with it's complex conjugate.

### b)

We'll prove the more general result that for any nonzero ideal $I \subset \mathbb{Z}[i]$ the quotient $\mathbb{Z}[i]/I$ is finite. Let $a + bi \in \mathbb{Z}[i]$, then consider $a + bi + I$ where $I = (\alpha)$ for some element $\alpha \in \mathbb{Z}[i]$. This holds as the Gaussian integers are a Euclidean Domain, hence a PID. Via the division algorithm we have

$$a + bi = q\alpha + r$$

where $N(r) < N(\alpha)$, therefore there are only finitely many choices for $N(r)$ as $N(\alpha) = c^2 + d^2$ for $\alpha = c + di$. Thus reducing mod $I$ yields

$$a + bi + I = r + I$$

so finitely many elements for $\mathbb{Z}[i]/I$. The fact that $\mathbb{Z}[i]/(2+i)$ is a field comes from the fact that irreducible elements are the same as primes in a Euclidean Domain, and nonzero prime ideals are maximal, thus a finite field.

## 9.2 Question 2

Assume $M/N$ is torsion. Finitely generated torsion modules over an integral domain have nonzero annihilator, as $M \cong R^2$ and $N = Rn$ the quotient is finitely generated.

# 10 August 2016

## 10.1 Question 1

## 10.2 Question 3

### a)

Let $v$ be an eigenvector of $S$, then

$$TSv = T(Sv) = T\lambda v = \lambda Tv = STv$$

So $Tv$ is also an eigenvector of $S$ with the same eigenvalue as $v$, but as $S$ has $n$ distinct roots (eigenvalues) the dimensions of the eigenspaces are 1. Therefore $Tv$ is a scalar multiple of $v$, and therefore $Tv = \mu v$, hence $v$ is an eigenvector for $T$.

**b)**

To show that $T = 0$ for $T$ nilpotent we show that for any vector $w \in V$, $Tw = 0$. As the eigenvectors for $S$ form a basis of $V$ then this can be done by showing that $T$ is zero on every eigenvector. Let $v$ be an eigenvector of $S$, then $T^k = 0 \implies T^k v = 0$, so

$$T^k v = (\mu v)^k = \mu^k v = 0$$

As the eigenvectors of $S$ are eigenvectors of $T$. Now eigenvectors are nonzero by definition, so $\mu^k = 0 \implies \mu = 0$. Thus $Tv = 0$ for every eigenvector of $S$ and so they form a basis of $V$ yielding that $T \equiv 0$

## 10.3 Question 4

$b \implies a$, obviously. To see the other direction we need polarization.

## 10.4 Question 5

Let $|G| = n$ and $|G : H| = m$. As $H \leq N_G(H)$ we get

$$|G : N_G(H)| < |G : H|$$

Let $G$ act by conjugation, then the stabilizer is exactly $N_G(H)$, which by Orbit-Stabilizer means that the number of all conjugate subgroups (the orbit under conjugation) is $|G : N_G(H)|$. Each of these conjugate subgroups contains the identity element and has order equal to $H$: $|xHx^{-1}| = H$, and so each one has at most

$$1 + |G : N_G(H)|(|H| - 1)$$

elements. The 1 for the identity, $|G : N_G(H)|$ for the number of conjugate subgroups, and $(|H| - 1)$ for the number of elements in each of them, minus 1 to avoid double counting. So we have

$$1 + |G : N_G(H)|(|H| - 1) \leq 1 + |G : H|(|H| - 1) \leq 1 + |G| - |G : H| < |G|$$

## 10.5 Question 6

Let $|G| = 65 = 5 \cdot 13$. By Sylow's theorem there exists unique Sylow subgroups $P, Q$ of orders 5 and 13, respectively. First we show that $G = PQ$. The set $PQ$ is a subgroup because both of these being unique Sylow subgroups means that $P$ and $Q$ are normal (only need 1 of them to be normal

though), thus $PQ$ is a subgroup. $|PQ| = \frac{|P||Q|}{|P \cap Q|}$, but as $|P \cap Q|$ must be divisible by 5 and 13, it's cardinality is 1. Thus $5||PQ|$ and $13||PQ|$ so $65||PQ|$ and therefore $G = PQ$. Both of these are prime order, hence they're cyclic, which means $P = \langle x \rangle, Q = \langle y \rangle$. We'll show $G$ is generated by $xy$.

As $P$ is normal we know $yxy^{-1} \in P$ so $yxy^{-1}x^{-1} \in P$, similarly $yxy^{-1}x^{-1} \in Q$ as $xy^{-1}x^{-1} \in Q$ thus $yxy^{-1}x^{-1} \in P \cap Q$ so $xy = yx$. Therefore we know $(xy)^n = x^n y^n$. Moreover as $x$ has order 5 and $y$ has order 13, the order of $xy$ has order divisible by 5 and 13, so the order of $xy$ must have order divisible by 65. But the order of $G$ is 65 which means that as a consequence of Langrange, the order of $xy$ is 65 hence $xy$ generates $G$

## 10.6 Question 7

If $E/K$ is an algebraic extension, then for every nonzero element $e$ in $E$ there is an irreducible polynomial $p(x)$ in $K[x]$ such that $p(e) = 0$. As $R \subset E$ for any nonzero element in $r \in R$, $r \in E$. So there is an irreducible polynomial $p(x) \in K[x]$ such that $p(r) = 0$. Explicitly write out what $p(x)$ is,

$$0 = p(r) = \sum_{i=0}^{n} a_i r^i$$

then

$$-a_0 = \sum_{i=1}^{n} a_i r^i$$

so

$$1 = r\left(\frac{-1}{a_0}\sum_{i=1}^{n} a_i r^{i-1}\right)$$

and then divide by the nonzero constant term and factor out $r$.

## 10.7 Question 8

The roots of $f(x)$ are $\pm\sqrt{6}, \pm\sqrt{10}$, so the splitting field is $\mathbb{Q}(\sqrt{6}, \sqrt{10})$. The degree is 4, doing the usual degree computation.

The automorphisms will send roots of $x^2 - 6$ to its own roots, and likewise with $x^2 - 10$. So the automorphisms will send

$$\sqrt{6} \mapsto \pm\sqrt{6}$$
$$\sqrt{10} \mapsto \pm\sqrt{10}$$

These are two degree 2 automorphisms so the Galois group is $\mathbb{Z}/2 \times \mathbb{Z}/2$

**Note:** $\mathbb{Q}(\sqrt{6}, \sqrt{10})$ is the splitting field of a separable polynomial, this is why it's Galois.

## 10.8 Question 9

To find the number of irreducible representations we need to find the number of conjugacy classes of $S_5$. Counting we see there are 7:

$$(1), (12), (123), (1234), (12345), (12)(34), (123)(45)$$

So there are 7 irreducible representations of $S_5$.
As for the number of 1 dimensional representations we know that this is the same as the number of 1 dimensional representations of the abelianization.

$$S_5/[S_5, S_5] \cong S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$$

So there are 2 1-dimensional representations.

**Note:** we can say that $A_5$ is the abelianization of $S_5$ because it's the smallest subgroup for which the quotient group is abelian. Remember to say this.

## 10.9 Question 10

**a)**

$T^{p-1} = I$ means that $T$ satisfies the polynomial $x^{p-1} - 1 = 0$, which over $\mathbb{F}_p$ splits as

$$x^{p-1} - 1 = \prod_{\alpha \in \mathbb{F}_p^\times} (x - \alpha)$$

So every nonzero element of the finite field appears as a root, and these are distinct. Since $T$ is killed by $f(x) = x^{p-1} - 1$, by definition of the minimal polynomial, it must divide $f(x)$. As $T \in GL_2(\mathbb{F}_p)$, the minimal polymomial should have degree 1 or 2. In either case it's either linear or degree 2 with 2 distinct roots. In either case an operator with minimal polynomial a product of distinct roots is diagonalizable.

**b)**

The matrix

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

Does the trick: Can show via induction that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

But the matrix is not diagonalizable as the minimal polynomial is $(x-1)^2$

# 11 January 2016

## 11.1 Question 1

## 11.2 Question 2

## 11.3 Question 3

Clearly $W \subset W^{\perp\perp}$. Showing the reverse we assume that $v \in W^{\perp\perp}$. Then we can write $V = W \oplus W^{\perp}$, so $v = w + u$, thus $v - w = u \in W^{\perp}$. Now by the first inclusion we get that $v - w \in W^{\perp\perp}$, so $v - w \in W^{\perp} \cap W^{\perp\perp}$, hence $v - w$ is orthogonal to itself, meaning that $v - w = 0$, so $v \in W$

## 11.4 Question 4

**a)**

**b)**

If $T$ is nilpotent and self-adjoint, by the Spectral Theorem there exists an orthonormal basis of (real) eigenvectors. Then $Tv_i = T^*v_i = \lambda_i v_i$, raising to the nth power yields zero, so $Tv_i = 0$ for all eigenvectors, thus $T = 0$.

## 11.5 Question 5

If $-1$ is a square, then in the field $\mathbb{F}_q$ the polynomial $x^2 + 1$ has a root $\alpha$. If $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ is a field extension, then we must have that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = 1$ or 2. So we have $p$ odd and either $n$ is 1 or 2.

## 11.6 Question 6

## 11.7 Question 7

## 11.8 Question 8

## 11.9 Question 9

**a)**

We use the hint. If $x^{14} + x^7 + 1 = 0$, then taking $y = x^7$ we see that $y$ satisfies $y^2 + y + 1$, so this has roots $y = \frac{-1 \pm \sqrt{3}i}{2}$, both are 3rd roots of unity. Thus the solutions to $f(x)$ are $\alpha^7 = \frac{-1 \pm \sqrt{3}i}{2}$. Let $\zeta$ be a primative 7th root of unity, then as $\frac{-1 \pm \sqrt{3}i}{2}$ are roots of $y^2 + y + 1$, the zeros of $f(x)$ are $\alpha\zeta^k$ for $1 \leq k \leq 6$

### b)

Let $K$ be the splitting field of this polynomial, then $K = \mathbb{Q}(\alpha, \zeta)$. We know that as 7 is prime, $[\mathbb{Q}(\zeta), \mathbb{Q}] = 6$, and $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 2$, so

$$[K : \mathbb{Q}] \leq 12$$

## 11.10 Question 10

### a)

Choose the trivial rep

### b)

Choose the trivial rep and the regular rep... I'm not sure what more they want.

# 12 January 2015

## 12.1 Question 1

Let's look at the units of this ring $R$. If $\frac{a}{b} \in R$ is a unit, then $\frac{b}{a} \in R$ is it's inverse. For units to exist in $R$ both $a, b$ must be odd. Look at the set of elements for which the numerator is even $I = \{x : x = \frac{2a}{b}\}$. Then none of the elements in $I$ are a unit, since they cannot have an inverse in $R$. This is precisely the ideal (2). To see this is maximal note that if $(2) \subset J \subset R$, then if $x \in J - (2)$ we must have that $x$ is a unit, so $J = R$. Hence this ideal is maximal.

## 12.2 Question 2

## 12.3 Question 3

## 12.4 Question 4

## 12.5 Question 5

## 12.6 Question 6

If a finite group $G$ has exactly two conjugacy classes then the class equation of $G$ looks like

$$|G| = |Z(G)| + |G : C_G(x)|$$

Where one is the conjugacy class of the identity, and the other is a conjugacy class of size greater than 1. As $|Z(G)|$ is the number of conjugacy classes of size 1, having only the identity means that we get

$$|G| = 1 + |G : C_G(x)|$$

Hence,

$$|G| - 1 \mid |G|$$

Which can only be true if $|G| = 2$, hence $G \cong \mathbb{Z}_2$

## 12.7 Question 7

For

## 12.8 Question 8

$x^6 - 4 = (x^3 + 2)(x^3 - 2)$ over $\mathbb{Q}$. The roots of $x^3 - 2$ are $\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2$ for $\zeta$ a primitive 3rd root of unity. The roots of $x^3 + 2$ are the negatives of the roots of $x^3 - 2$: $-\sqrt[3]{2}, -\sqrt[3]{2}\zeta, -\sqrt[3]{2}\zeta^2$ for $\zeta$,

hence the splitting field is $\mathbb{Q}(\sqrt[3]{2}, \zeta)$.

The degree is as follows:

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

$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ as the minimal polynomial is $x^2 + x + 1$. For $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\zeta)]$ the polynomial which has all the roots is $x^3 - 2$, so $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\zeta)] \leq 3$. Thus $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}] \leq 6$ and is of degree divisible by 3 and 2, (as both $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta)$ are subfields) hence is equal to 6.

## 12.9 Question 9

**a)**

As the hint suggests we consider the map $\varphi : K \to M_n(\mathbb{Q})$ via sending $\alpha \mapsto (T_\alpha)$, where $(T_\alpha)$ is the matrix representative of the linear operator $T_\alpha : K \to K$ defined as left multiplication by $\alpha$. Fixing a basis of $K$ over $\mathbb{Q}$ gives a matrix. This is a ring homomorphism as

$$\varphi(\alpha + \beta) = T_{\alpha+\beta} = T_\alpha + T_\beta = \varphi(\alpha) + \varphi(\beta)$$

Since $T_{\alpha+\beta}(v) = (\alpha + \beta)(v) = \alpha v + \beta v$, similarly $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. To see injectivity we have that if $\alpha \in \ker \varphi$, then $T_\alpha(v) = \alpha v = 0$ for all $v \in K$, but $K$ is a field, so this means that $\alpha = 0$

**b)**

A basis for $K$ is $\{1, \sqrt{2}\}$

## 12.10 Question 10

This is just Schur's Lemma. First recall that $k[G]$-modules are just $G$-representations. As $V$ is irreducible, both the kernel and image being $k[G]$-submodules (subrepresentations), are $G$-invariant subspaces, hence are either 0 or all of $V$.

Let $k$ be algebraically closed, then every $T \in \mathrm{Hom}_{k[G]}(V, V)$ has an eigenvalue, and as such the map $(T - \lambda) \cdot id : V \to V$ is a map of $G$-representations. By the above statement this is either an isomorphism or 0, however clearly the eigenvectors of $V$ are in the kernel of this map, by definition. So $(T - \lambda) \cdot id = 0$, meaning that every map $T \in \mathrm{Hom}_{k[G]}(V, V)$ is a constant in $k$, hence

$$\mathrm{Hom}_{k[G]}(V, V) \cong k$$

# 13 August 2014

## 13.1 Question 1

If $M$ is a finitely generated abelian group then

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_l}$$

By the Structure Theorem. And $N$ is a finitely generated free abelian group so

$$N \cong \mathbb{Z}^d$$

## 13.2 Question 2

## 13.3 Question 3

**a)**

Recall that $x^n - 1 = \prod_{\zeta \text{root of unity}}(x - \zeta)$, and so if $\gcd(m, n) = 1$ they cannot share any roots of unity, hence the only share the root 1, thus

$$\gcd(x^n - 1, x^m - 1) = x - 1$$

## 13.4 Question 4

## 13.5 Question 5

## 13.6 Question 6

Consider the character table of an arbitrary finite group. Let $\chi_1, ..., \chi_n$ be the characters, then consider a linear combination of the columns:

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0$$

Row orthogonality says $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ Dotting this sum with $\chi_i$ will result in $a_i = 0$ for each $i$.

As we have a square matrix with linearly independent columns, we're invertible.

## 13.7 Question 7

## 13.8 Question 8

**a)**

**b)**

If $p \equiv 1 \mod 8$, then $p = 1 + 8k$, or equivalently $p - 1 = 8k \implies 8 \mid p - 1$, so

$$x^8 - 1 \mid x^{p-1} - 1$$

$x^4 + 1 \mid x^8 - 1$, as $x^8 - 1 = (x^4 + 1)(x^4 - 1)$

so

$$x^4 + 1 \mid x^8 - 1 \mid x^{p-1} - 1 \mid x^p - x$$

And as such $\mathbb{F}_p$ being the product of roots of $x^p - x$, contains all the roots of $x^4 + 1$

## 13.9 Question 9

## 13.10 Question 10

# 14 January 2014

## 14.1 Question 1

If $\phi_i$, $i = 1, 2, 3$ are linearly independent, then extend to a basis $\{\phi_i\}_{1 \leq i \leq n}$ of $V^*$, and let $\{e_i\}_{1 \leq i \leq n}$ be the corresponding basis of $V$. I claim that

$$\bigcap_{i=1}^{3} \ker \phi_i = span\{e_4, ..., e_n\}$$

If $v \in span\{e_4, ..., e_n\}$ then as $\phi_i(e_j) = \delta_{ij}$ we get that $\phi_i(v) = 0$ for $i = 1, 2, 3$

If $x = \sum_{i=1}^{n} a_i e_i \in \bigcap_{i=1}^{3} \ker \phi_i$, then $a_i = \phi_i(x) = 0$ for $i = 1, 2, 3$, so $x \in span\{e_4, ..., e_n\}$. Thus we have the desired equality. As the span is of dimension $n - 3$ since it's linearly independent, we get the desired result.

## 14.2 Question 2

## 14.3 Question 3

## 14.4 Question 4

## 14.5 Question 5

## 14.6 Question 6

## 14.7 Question 7

## 14.8 Question 8

## 14.9 Question 9

## 14.10 Question 10

# 15 January 2012

## 15.1 Question 2

If $A$ is an $n \times n$ matrix over $k$, then as $k \subset K$, the Rational Canonical form $M$ of $A$ satisfies the necessary conditions to be the Rational Canonical form of $A$ over $K$, but the Rational Canonical form of a matrix is unique, hence the RCF of $A$ over $k$ is the same as that over $K$. Hence the invariant factors, minimal polynomial and characteristic polynomial are same.

Same invariant factors means same RCF means similar

# 16 August 2011

## 16.1 Question 7

Let $\mathcal{H}$ be the set of subgroups of $G$ such that $|G : H| = p$. The order of $\mathcal{H}$ will assumed to be nonempty, otherwise it's clearly true as $p|0$. As $G$ acts on $\mathcal{H}$ via conjugation we have the following equation for $\mathcal{H}$, where $H_1, .., H_k$ are the representatives of the conjugacy classes:

$$|\mathcal{H}| = \sum_{i=1}^{k} |G : C_G(H_i)| = \sum_{i=1}^{k} |\mathcal{O}_{H_i}|$$

Where $\mathcal{O}_{H_i}$ is the orbit of $H_i$. This is because the orbits partition the set $\mathcal{H}$, and the size of each conjugacy class is gotten by $|G : C_G(H_i)|$, so these are equal. The orbit stabilizer theorem says

$$\frac{|G|}{|\text{Stab}(H_i)|} = |\mathcal{O}_{H_i}|$$

We can rewrite the left hand side of the above as

$$\frac{|G|}{|C_G(H_i)|} = |\mathcal{O}_{H_i}|$$

I'm writing this to ease my own confusion about why $C_G(H_i)$ is the size of the stabilizer, and not $N_G(H_i)$. Recall that under the action of conjugation, the stabilizer of a set is the normalizer, by definition. The reason we have the centralizer here is because the set we are acting upon is $\mathcal{H}$ NOT the subgroup $H_i$, these are the elements of the set. As such the stabilizer of a single element of the set $\mathcal{H}$ is the centralizer of that element, in this case $C_G(H_i)$.

From here we note that $|H_i| \leq |C_G(H_i)| \leq |G|$, and as $|G| = p|H_i|$ we either have that $|C_G(H_i)| = |H|$ or $|G|$. In the latter case $H \trianglelefteq G$, and in the former we have that $\frac{|G|}{|C_G(H_i)|} = \frac{|G|}{|H_i|} = \frac{p|H_i|}{|H_i|} = p$. So the above equation for $|\mathcal{H}|$ will have $p$ dividing the right hand side, thus it divides the left hand side.

# 17 August 2009

## 17.1 Question 3

If $A$ is an $n \times n$ complex matrix with all entries equal to 1, then the rank, the number of linearly independent columns, is 1. Rank is similarity invariant , so the Jordan Canonical Form of $A$ also has rank 1. By rank nullity, the dimension of the kernel, i.e. the dimension of the eigenspace for 0 is $n-1$, which is the geometric multiplicity, thus the number of Jordan Blocks corresponding to 0.

The algebraic multiplicity is the multiplicity of the root 0 in the characteristic polynomial, which is greater than or equal to the geometric multiplicity, hence the algebraic multiplicity of 0 is at least $n-1$. This means that $x^{n-1}$ has to divide the characteristic polynomial. It also must be of degree $n$, so it's of the form $x^{n-1}(x-a)$, where $a$ is the other eigenvalue. The trace of the matrix is the sum of the eigenvalues, and since $A$ has only 1's down the diagonal, and 0's as the other eigenvalues the remaining eigenvalue must be $n$. So the characteristic polynomial is $x^{n-1}(x-n)$.

Next we need to find the minimal polynomial of this matrix. Since the rank of $A$ is 1, the image of $A$ is 1-dimensional, so $A$ acts as a scalar by the eigenvalue. So the minimal polynomial is $x(x-n)$.

Now we must split into two case, depending on if the characteristic of the field divides $n$. If $p \nmid n$ then the minimal polynomial is $x(x-n)$, which has distinct roots, and thus the Jordan Canonical Form is diagonal with 0's down the diagonal $n-1$ times, and a single $1 \times 1$ block for $n$ due to the geometric multiplicity of 0 being $n-1$.

If $p|n$ then $n = 0$ in the field, so the minimal polynomial becomes $x^2$. As such the size of the largest Jordan block is 2, and the geometric multiplicity being $n-1$ means there are $n-1$ blocks for 0. So there is 1 Jordan block of size 2, and $n-2$ Jordan blocks of size 1 corresponding to 0.

# 18 August 2007

# 19 January 2007

## 19.1 Question 1

### a)

Clearly by definition $IJ \subseteq I \cap J$. To show the reverse let $a \in I \cap J$, then as $I, J$ comaximal there exists $x \in I, y \in J$ such that $x + y = 1$, so

$$a = a \cdot 1 = a(x + y) = ax + ay \in IJ$$

where $ax + ay \in IJ$ since $IJ$ consists of products of elements in $I, J$.

### b)

For a counterexample consider the ring $\mathbb{Z}$ with the ideals $(2), (4)$, then $(2) \cap (4) = (4)$, but $(2)(4) = (8)$

## 19.2 Question 2

Let $H$ be a subgroup of a finite group $G$, and let $G$ act on $H$ via conjugation. The number of distinct conjugates of $H$ is precisely the number of orbits of $H$ under this action. By the Orbit-Stabilizer Theorem,

$$\frac{|G|}{|\text{Stab}(H)|} = |\mathcal{O}_H|$$

Now, $\text{Stab}(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$, the normalizer of $H$. We know that $H \leq N_G(H)$ and so $|G : \text{Stab}(H)| = |G : N_G(H)| \leq |G : H|$, in particular $|G : N_G(H)| \mid |G : H|$. Thus

$$|\mathcal{O}_H| = \frac{|G|}{|\text{Stab}(H)|} = |G : N_G(H)| \mid |G : H|$$

So the number of distinct subgroups conjugate to $H$ divides the index of $H$ in $G$.

## 19.3 Question 7

### a)

The number of lines through the origin of $\mathbb{F}_3^2$ is the span of $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$.This yields 4 elements. To show $G$ acts transitively on this we need that for any

**b)**

If we do part b separately we get that the order of $\mathrm{SL}_2(\mathbb{F}_3)$ is the order of $\mathrm{GL}_2(\mathbb{F}_3)$ divided by the order of $\mathbb{F}_3^\times$. This can be seen by looking at the kernel of the surjective map

$$det : GL_2(\mathbb{F}_3) \to \mathbb{F}_3^\times$$

Clearly this is a surjective map

## 19.4 Question 10

Let $G$ be the cyclic group of order $m$ with generator $\langle a \rangle$, define a representation

$$\rho : G \to GL(V)$$

$$a \mapsto T$$

Then since $T^m = I$, $\rho(a)$ has minimal polynomial dividing $x^m - 1$, thus is diagonalizable. By Maschke's theorem, since we're given a $T$-stable subspace $W \subset V$, and we have a representation for which the charactersitic of our field (0) doesn't divide the order of the group (m) we get that there is a $T$-stable subspace $U \subset V$ for which a direct sum decomposition exists.

# 20 January 2006

## 20.1 Question 2

It can be shown that in general

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_{\gcd(n,m)}$$

For us it's easier to just compute this group, but this can guide our answer. If $f : \mathbb{Z}_{15} \to \mathbb{Z}_{21}$, then as 1 has order 15 in the domain, the order of $f(1)$ must have order dividing 15:

$$15 \cdot f(1) = f(15) = f(0) = 0$$

So by Lagrange we need elements in $\mathbb{Z}_{21}$ which are of order 1 or 3. We can check these are just 0,7,14. Another way to see this is that we need elements that are $15a \equiv 0 \mod 21$, 5 is coprime to 21 so it's invertible, so we are looking at elements $3a \equiv 0 \mod 21$ which is just $a \equiv 0 \mod 7$, in our group this is just 0,7,14 as we've seen.

## 20.2 Question 4

Define $f(X) = tr(X^T X)$, this is a positive definite quadratic form. If $X$ is symmetric, then $f(X) = q(X)$, and if $X$ is skewsymmetric $f(X) = -q(X)$. Recall we have a direct sum decomposition:

$$M_n(\mathbb{R}) = Sym \oplus SSym$$

Into symmetric and skew-symmetric matricies. The signature is therefore $(\frac{n(n+1)}{2}, \frac{n(n-1)}{2}, 0)$. The direct sum decomposition can be shown as follows: Let $A$ be symmetric, $B$ be skewsymmetric. Then we have the inner product $\langle A, B\rangle = tr(A^T B)$, so

$$\langle A, B\rangle = tr(A^T B) = tr(AB) = tr(BA) = tr(-B^T A) = \langle -B, A\rangle = -\langle A, B\rangle$$

For any $A \in M_n(\mathbb{R})$ we have

$$A = \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T)$$

# 21 August 2005

## 21.1 Question 1

Let $A \in M_n(\mathbb{C})$ be such that the characteristic polynomial has distinct roots, then by Cayley-Hamilton, the minimal polynomial of $A$ has distinct roots, hence $A$ is diagonalizable. As such there is a basis of eigenvectors of $A$, and in particular we can decompose $\mathbb{C}^n$ as a direct sum of eigenspaces:

$$\mathbb{C}^n = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_n}$$

As $X, Y$ commute with $A$, $X, Y$ preserve the eigenspaces of $A$: If $v$ is an eigenvector of $A$, then $Xv, Yv$ are eigenvectors of $A$, and belong to the eigenspace $V_\lambda = \{v \in V : Av = \lambda v\}$. Moreover every eigenvector of $A$ is an eigenvector of $X$ and $Y$: if $v \in \mathbb{C}^n$ is such that $Av = \lambda v$, then as $Xv \in V_\lambda$ we know that the characteristic polynomial having distinct roots, means $n$ distinct eigenvalues, hence 1-dimensional eigenspaces. So $Xv \in V_\lambda \implies Xv = \mu v$, similarly $Yv = \xi v$, for $\mu, \xi \in \mathbb{C}$. As such, the eigenvectors of $A$ are eigenvectors of $X, Y$, and as there are $n$-distinct ones, the matricies $X, Y$ are diagonalizable with respect to the basis of eigenvectors.

Hence there exist $B \in GL_n(\mathbb{C})$ such that $BXB^{-1} = D_X, BYB^{-1} = D_Y$, therefore

$$XY = B^{-1}D_XBB^{-1}D_YB = B^{-1}D_XD_YB = B^{-1}D_YD_XB = YX$$

**Note**: Simulatenous diagonalizability comes up often! $A$ is diagonalizable by C-H, but more importantly it's eigenspaces are 1-dimensional...

## 21.2 Question 2

**a)**

**b)**

$N = \{g \in G : gHg^{-1} = H\} = \text{Stab}(H)$, via the action of conjugation. The number of distinct subgroups of $G$ of the form $aHa^{-1}$ is the set of orbits under the action of conjugation of $H$ by $G$, this is the number of orbits of $H$. Via the Orbit-Stabilizer theorem this is

$$|\mathcal{O}_H| = |G : \text{Stab}(H)| = |G : N|$$

**c)**

If $H \neq G$ then $H$ is a proper subgroup of $G$. $H \leq N$, so $|G : N| \leq |G : H|$. Each of the conjugate subgroups contains 1, and has order $H$, so each one contains at most

$$|G : N|(|H| - 1) + 1$$

elements. $|H|-1$ for the order of the conjugate subgroups, and to avoid double counting 1, adding back 1 outside the expression. The number of total conjugate subgroups is $|G:N|$. Thus

$$1+|G:N|(|H|-1) \leq 1+|G:H|(|H|-1) = 1+|G|-|G:H| < |G|$$

As $|G:H| \neq 1$.

## 21.3 Question 3

Let $G$ be a finite abelian group that is not cyclic. By the Fundamental Theorem of Finite Abelian Groups $G$ is isomorphic to the following:

$$G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$$

For not necessarily distinct primes $p_i$ and integers $\alpha_i \geq 1$. Now as $G$ is not cyclic, it does not have a generator, and this occurs when $G \cong \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$. This happens when $\gcd(p_1^{\alpha_1}, ..., p_n^{\alpha_n}) = 1$ by the Chinese Remainder Theorem. For the group we have, therefore, $\gcd(p_1^{\alpha_1}, ..., p_n^{\alpha_n}) \neq 1$, hence two of the prime powers share common factors, which occurs when the primes are the same, WLOG assume this is $p_1, p_2$, i.e.

$$G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_1^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$$

Hence $G$ contains a subgroup of the form $\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_1\mathbb{Z}$

## 21.4 Question 5

The elements of $\mathbb{F}_p^\times$ are the invertible elements of $\mathbb{F}_p$, which are the roots of $x^{p-1}-1$. Each element of $\mathbb{F}p^\times$ has an inverse, and so

$$\sum_{k \in \mathbb{F}_p^\times} \frac{1}{k} = \sum_{k \in \mathbb{F}_p^\times} k = 0$$

## 21.5 Question 6

Consider the polynomial $x^7+2 \in \mathbb{F}_7[x]$, one can check that $2^7 = 2$, and therefore $x^7+2 = (x+2)^7$. Thus roots of $x^7+2$ are $-2 \equiv 5 \mod 7$, and as they all live in $\mathbb{F}_7$ this is the splitting field.

## 21.6 Question 8

Let $G = C_8$, then as $|G| = 8 = 2^3$, $G$ is a 3 dimensional vector space over the finite field $\mathbb{F}_2$, so it's automorphisms are 3×3 invertible matricies over $\mathbb{F}_2$:

$$\mathrm{Aut}(G) \cong GL(G) \cong GL_3(\mathbb{F}_2)$$

Thus the multiplication is gotten by matrix multiplication, there is a total of 168 elements in this group:

$$|GL_3(\mathbb{F}_2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 7 \cdot 6 \cdot 4 = 168$$

I have no idea what they wanted from the description of the multiplication table...

## 21.7 Question 9

Let $\chi$ be an irreducible complex character of a finite group $G$, and let $z \in Z(G)$. Then $z$ has order say $n$, so $z^n = 1 \implies \rho(z)^n = 1$, hence the eigenvalues of $\rho(z)$ are nth roots of unity. As $\chi(z) = trace(\rho(z))$, the character of $z$ is a sum of roots of unity. But as $z \in Z(G)$ we know $zg = gz \, \forall g \in G$, thus $\rho(z)\rho(g) = \rho(g)\rho(z)$, so $\rho(z) = \lambda I$ by Schur's lemma.

Specifically, define the map $Tv = zv$, i.e. $Tv = (\rho(z))(v)$. One can easily check this defines a homomorphisms of G-representations. Then $\rho(z)$ is therefore a scalar by Schurs lemma, specifically a root of unity $\lambda$ via the above discussion. Thus $\chi(z) = \sum \lambda = \dim V \cdot \lambda$.

Now $\chi(1) = trace(I) = \sum 1 = \dim V$, and therefore $\frac{\chi(z)}{\chi(1)} = \frac{\dim V \cdot \lambda}{\dim V} = \lambda$

# 22 January 2005

## 22.1 1

The kernel and image are submodules of $M$, and $N$ respectively. Thus as $\phi$ is nonzero we get that the image is all of $N$ and the kernel is 0, hence an isomorphism.

## 22.2 2

A basis of $\mathbb{Q}[x]/(x^2)$ is $\{1, x\}$. Let $a(x)+I$ be a polynomial in $\mathbb{Q}[x]/(x^2)$ for $I = (x^2)$. Then dividing by $x^2$ gives $g(x) = q(x)x^2 + r(x)$ where $\deg r(x) < 2$ so $g(x)+I = r(x)+I$ thus $g(x)$ is a linear combination of elements in the basis. To see linear independence, suppose $a_0+a_1x \in I$, then $x^2|a_0+a_1x$, which is impossible, so $a_i = 0$. So we have a basis. The units in $R$ are all of $\mathbb{Q}$, there may be more....

The ideals are in bijection, via the 4th isomorphism theorem with polynomials that divide $x^2$: So the trivial ideal, $x$, and the whole ring.

## 22.3 3

## 22.4 4

## 22.5 5

Use Cayley-Hamilton to get a polynomial that kills $A$, then move $I$ to the other side multiply by $A^{-1}$ and get the result modulo a sign change.

## 22.6 6

Recall by Sylow's theorem that any $p$ subgroup is contained in a Sylow p subgroup by conjugation, so $gKg^{-1} \leq P$, but $K$ is normal so we just have $K \leq P$. We also know that Sylow p subs conjugation to each other, so

$$gKg^{-1} \leq gPg^{-1} \implies K \leq Q$$

for any Sylow $p$ sub $Q$

## 22.7 7

Let $G$ be a finite group

**a**

If $x \in \cap \ker \phi_i$, then $x$ acts trivially on all the irreducible representations. The regular representation is a direct sum of the irreducible representations, and thus $x$ acts trivially on the regular representation. As such $x = x \cdot 1_{KG} = 1_{KG} = 1_G$. The first equality is definition of identity, the second is because $x$ acts trivially on the regular rep (aka the group ring), the third is because the identity of the group ring is the identity of the group.

Alternate solution: If $x \in \cap \ker \phi_i$ then $x \in \ker \rho$ for the regular representation $\rho$. The kernel of the representation is the same as the kernel of the character, which for the regular representation is just the identity element. Hence $\cap \ker \phi_i = \{1\}$

## 22.8 8

## 22.9 9

## 22.10 10

Subfields of $F_{125} = F_{5^3}$ are the fields for which $F_{5^d}$ where $d|3$, thus only $F_5$ and the whole field.

Field automorphisms are of the form $x \mapsto x^{5^n}$, as $x^{5^3} = x$ for $x \in F$ then we get 3 automorphisms: $x \mapsto x$, $x \mapsto x^5$, $x \mapsto x^{25}$

# 23 August 2004

## 23.1 Question 1

An $F[x]$ module over a field $F$ corresponds to a pair $(V, T)$ where $V$ is a vector space over $F$ and $T$ is a linear operator on $T$. The action is given as $x \cdot v = Tv$. Thus for a $\mathbb{Q}[x]$-module homomorphism

$$f : \mathbb{Q}[x]/(1+x^2) \to \mathbb{Q}[x]/(1+x^3)$$

with corresponding pairs $(V, \phi), (W, \psi)$ we show these correspond with linear maps $T : V \to W$ such that $T \circ \phi = \psi \circ T$. The $\mathbb{Q}[x]$-module structure on $V$ is defined as

$$(a_0 + a_1 x)v = a_0 v + a_1 \phi(v)$$

Thus from $f$, the module homomorphism we get a linear map $T$ defined to be $Tv = f(v)$. In order for $f(xv) = xf(v)$ we need that $T \circ \phi(v) = \psi \circ T(v)$ for all $v \in V$ thus the condition that the linear maps commute.

## 23.2 Question 2

Let $A \in M_n(\mathbb{C})$ be a nilpotent matrix with $A^m = 0$. Then $A$ satisfies $x^m = 0$, so the minimal polynomial divides this, and by Cayley Hamilton, the degree of the minimal polynomial is no more than $n$. As such $x^n = 0$.

**Note**: One can also use Jordan form to show that since the eigenvalues of $A$ are all zero, the Jordan form is a block upper triangular matrix with all 0's down the diagonal. Then via induction argue that an upper triangular matrix when raised to the nth power gives the zero matrix.

## 23.3 Question 3

$(I + A^*A)^* = I^* + A^*(A^*)^* = I + A^*A$ so $I + A^*A$ is self adjoint. By the Spectral Theorem, there is an orthonormal basis of eigenvectors of $I + A^*A$ such that the matrix is diagonal, thus this matrix is nonsingular

## 23.4 Question 4

**a**

First note that as $G$ is abelian $(ab)^k = a^k b^k$, thus clearly the order of $ab$ divides the lcm of $m, n$, call this $x$, if the order of $ab$ is $k$, then $a^k b^k = 0$ so $k|m$ and $k|n$. By definition of the lcm, $m|x$ and $n|x$, so we get that $k|x$

**b**

By the above we know that if $k$ is the order of $ab$, $k|m, k|n$ so $k|mn$. Now if we have

$$a^k b^k = 1$$

Then raising both sides to $m$ we get $b^{km} = 1$ so $n|km$, but as the gcd of $m, n$ is 1, $n$ divides $k$, similarly $m|k$, so $nm|k$, and we get the desired result.

## 23.5 Question 5

There are 4 conjugacy classes in $A_4$ with representatives $1, (12)(34), (123), (132)$. Note that although (123), (132) are conjugate in $S_4$, they get conjugated by (23) which is not in $A_4$.

## 23.6 Question 6

We need to show that conjugate matrices have the same ranks.

## 23.7 Question 8

Characters of a direct product are given by tensors of the irreducible representations of the groups. Recall that the character of the tensor of two representations is just the product of the characters. The conjugacy classes of direct sums of groups are just products of the conjugacy classes. Thus the character table for a direct product is gotten by taking the tensor of the two reps.

# 24 January 2004

## 24.1 Question 8

Consider $\rho : \mathbb{Z} \to SL_2(\mathbb{C})$, $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. This is a reducible representation as reducible representations are those which can be put in block upper triangular form with respect to some basis.

The representation, however, is not decomposable as decomposable, in the $2 \times 2$ case corresponds with being diagonalizable (in general these are block diagonal matricies via Maschke's theorem). For the given representation we have that the Jordan form of

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

is

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

which is not diagonal, hence this is not a decomposable representation

## 24.2 Question 9

If $\mathbb{F}_p$ is a finite field of order $p$, and $K/F$ is a finite extension then $K = \mathbb{F}_{p^n}$. Take the polynomial $(x - a_1) \cdots (x - a_n) + 1$ where $a_1, ..., a_n \in \mathbb{F}_{p^n}$, then this polynomial has no roots in $\mathbb{F}_{p^n}[x]$

## 24.3 Question 10

### a)

$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$

### b)

The roots of the two irreducible polynomials that $x^4 + 4$ decomposes into are $\pm 1 \pm i$, thus the spitting field contains all of these, and as $\pm 1 \in \mathbb{Q}$ the splitting field is $\mathbb{Q}(i)$. The splitting group of $f(x)$ is therefore a degree 2 extension of $\mathbb{Q}$, and so the Galois group is an order 2 group, which means it's $\mathbb{Z}/2\mathbb{Z}$

# 25 August 2003

## 25.1 Question 1

**a)**

$$\begin{aligned}\langle Tf, g\rangle &= \int_0^1 f'(x)g(x)\,dx \\ &= [f(1)g(1) - f(0)g(0)] - \int_0^1 f(x)g'(x)\,dx \\ &= [f(0+1)g(0+1) - f(0)g(0)] - \int_0^1 f(x)g'(x)\,dx \\ &= -\int_0^1 f(x)g'(x)\,dx \\ &= \langle f, T^*g\rangle\end{aligned}$$

Using integration by parts and the fact that $f, g$ are 1-periodic

## 25.2 Question 6

By Sylow's theorems, each Sylow 17-subgroup is cyclic of order 17, as 17 is the largest prime power of 17 dividing the order of $S_{17}$. The number of Sylow 17-subgroups is gotten by finding the number of elements of order 17, as these live in the Sylow 17-subgroups. Each Sylow 17-subgroup has 16 elements of order 17, as we don't count the identity. The elements of order 17 in $S_{17}$ are the 17-cycles. Fixing the first element, there are $(17-1)! = 16!$ possible elements of order 17 in $S_{17}$, thus the number of Sylow 17-subgroups is $n_p = 16!/16 = 15!$. To conclude: We found that the number of elements in each Sylow 17-subgroup of order 17 is 16, and the number of elements in $S_{17}$ of order 17 is 16!, the Sylow 17-subgroups partition the elements of order 17 and that's how we arrive at 15!

## 25.3 Question 7

Let $(V, \rho)$ be a representation of finite group $G$, and

$$W = \{v \in V : \rho(g)v = v, \forall g \in G\}$$

We can decompose $V$ into a direct sum of irreducible representations with multiplicity:

$$V \cong V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}$$

If $V_1$ is the trivial representation, then $W \cong V_1^{n_1}$, so $\dim W = n_1$. Let $\chi_V$ denote the character of $V$, from the decomposition we know

$$\chi_V = \sum n_i \chi_{V_i}$$

, thus taking the inner product of $\chi_V$ with $\chi_{V_1}$ we get

$$\begin{aligned}(\chi_V, \chi_{V_1}) &= \sum n_i (\chi_{V_i}, \chi_{V_1}) \\ &= \begin{cases} n_i & \chi_{V_1} = \chi_{V_i} \\ 0 & \chi_{V_1} \neq \chi_{V_i} \end{cases}\end{aligned}$$

Thus $(\chi_V, \chi_{V_1}) = n_1$ as desired.

# 26 January 2003

## 26.1 Question 1

Let $A \in M_n(\mathbb{C})$ be such that $A^3 = A$. Then $A$ satisfies the polynomial $x^3 = x$, or $x^3 - x = 0$. Over $\mathbb{C}$ this polynomial factors as $x(x^2 - 1) = x(x-1)(x+1)$. Since $x^3 - x = 0$ we know that the minimal polynomial must divide this polynomial, as by definition it's the polynomial of least degree that kills $A$. But each of the roots of $x^3 - x$ are distinct, thus the minimal polynomial has distinct roots. Hence as the minimal polynomial distinct roots, the matrix $A$ is diagonalizable.

## 26.2 Question 2

Let $p$ be prime, and $G$ a $p$-group. Let $H \leq G$ such that $|G : H| = p$. Let $\pi_H$ be the permutation representation gotten by left multiplication of $G$ on the set of left cosets of $H$. Consider the kernel of this map, $\ker \pi_H$. Let $|H : \ker \pi_H| = k$, then

$$|G : \ker \pi_H| = |G : H||H : \ker \pi_H| = pk$$

We have that

$$\pi_H : G \to \text{Perm}(\mathcal{C}_H) \cong S_{|G:H|} \cong S_p$$

Thus $G/\ker \pi_H \leq S_p$, so $pk|p!$, hence $k|(p-1)!$, but $p \nmid (p-1)!$, as all divisors are less than $p$, and $\ker \pi_H \leq G$, which is a $p$-group, so it has order the power of a prime. Thus $|\ker \pi_H| = k = 1$, and as such $|H : \ker \pi_H| = 1$, meaning $H = \ker \pi_H$, the kernel of a homomorphism is normal, so $H \trianglelefteq G$

## 26.3 Question 3

Let $M$ be an $R$-module for commutative ring $R$. Then if $M$ is irreducible, consider the submodule $Rm$ for some $m \in M$. As this submodule contains $rm$, it contains $1m = m \in M$ which is nonzero hence $Rm = M$, thus $M$ is cyclic. I claim that $M \cong R/\text{Ann}(m)$, for $m$ the generator of $M$. This follows from the fact that $f : R \to M$ given by $r \mapsto rm$ is a surjective $R$-module homomorphism, and the kernel of this map is $\text{Ann}(m)$. The result then follows from the 1st Isomorphism theorem.

Now as $M \cong R/\text{Ann}(m)$, the submodules of $M$ are the same as the ideals of $R/\text{Ann}(m)$, and as $M$ is irreducible, this means that the ideals of $R/\text{Ann}(m)$ are either 0 or $R/\text{Ann}(m)$, the 4th isomorphism theorem for Rings says that the ideals of $R/\text{Ann}(m)$, $J/\text{Ann}(m)$, are in bijection with ideals $J \subset R$ that contain $\text{Ann}(m)$. Thus these ideals are either $R$ or $\text{Ann}(m)$, meaning $\text{Ann}(m)$ is maximal.

If $\text{Ann}(m)$ is a maximal ideal of $R$ and $M$ is cyclic, then $M \cong R/\text{Ann}(m)$, so submodules are in bijection with ideals of $R/\text{Ann}(m)$. But $\text{Ann}(m)$ being maximal means that $R/\text{Ann}(m)$ is a field,

so the only ideals are 0 and $R/\text{Ann}(m)$, thus the only submodules of $M$ are 0 and $M$. Hence $M$ is irreducible.

**Note**: There are two statements regarding a module being irreducible: $M$ is irreducible iff $M$ is cyclic for *any* nonzero element as a generator, and $M$ is irreducible if and only if it's isomorphic to $R/I$ for *some* maximal ideal $I$ of $R$. So one direction $\Leftarrow$ is true because we have some maximal ideal ($\text{Ann}(m)$), but for the other direction we need both statements, cyclic and the annihilator being maximal, in order to be true.

## 26.4 Question 4

Let $p(x)$ be a nonzero polynomial of degree $n \geq 1$. The field $\mathbb{F}_q[x]/(p(x))$ has coset representatives

$$c_0 + (p(x)), ..., c_{n-1}x^{n-1} + (p(x))$$

So $n$-total coset representatives, there are $q$ choices for each $c_i$, thus $q^n$ total elements in the field.

## 26.5 Question 5

Take $\alpha_1, ..., \alpha_n \in \mathbb{C}$, with $\alpha_l^2 \in \mathbb{Q}$. Let $F = \mathbb{Q}(\alpha_1, .., \alpha_n)$, and assume $\sqrt[3]{2} \in F$, then

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

So $3|[F : \mathbb{Q}]$, but

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha_1, .., \alpha_{n-1})] \cdots [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$$

Each extension is either 1 or 2, depending on if $\alpha_i \in \mathbb{Q}$ or not. If not then we know $\alpha_i^2 \in \mathbb{Q}$. So $[F : \mathbb{Q}]$ is a power of 2, which cannot be true if 3 divides it.

## 26.6 Question 6

Let $f(x) = (x^2 + 1)(x^2 - 2)(x^2 - 3)(x^2 - 4)$, the roots of this polynomial are $\pm i, \pm\sqrt{2}, \pm\sqrt{3}, \pm 2$. The splitting field contains every root of the polynomial, thus $F = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, 2) = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$

## 26.7 Question 9

Let $A$ be a set of order less than or equal to 4, and let $Q_8$ act on $A$. By the Orbit-Stabilizer theorem for $a \in A$,

$$|\text{Stab}(a)| = |Q_8 : \mathcal{O}_a|$$

Now, as $\mathcal{O}_a \subseteq A$ and $\text{Stab}(a) \leq Q_8$ the order of the orbit of $a$ can be 1,2,4, which means the order of the Stabilizer can be 2,4,8 by Lagrange. As such the stabilizer of $a$, as a subgroup of $Q_8$ must contain the subgroup $\langle -1 \rangle \simeq \mathbb{Z}_2$. Consider the homomorphism

$$\pi_A : Q_8 \to \text{Perm}(A)$$

The kernel of this associated map is defined as the intersection of all stabilizers:

$$\ker \pi_A = \{g \in G : g \cdot a = a, \forall a \in A\} = \{g \in G : g \in \text{Stab}(a), \forall a \in A\} = \bigcap_{a \in A} \text{Stab}(a)$$

We've shown that the subgroup $\langle -1 \rangle$ is contained in all the stabilizers of the action of $Q_8$ on $A$. As such $\langle -1 \rangle \leq \ker \pi_A$, so $\pi_A$ is not an injective map, and as $\text{Perm}(A) \cong S_{|A|} \cong S_4$ we know that $Q_8$ is not isomorphic to a subgroup of $S_4$.

# 27 August 2002

## 27.1 Question 2

### a)

If $G$ is a noncyclic group of order $p^2$, then $G$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. The irreducible representations over $\mathbb{C}$ can be described by the character table. In the direct product of groups, the characters are gotten via the tensor product of representations: If $\chi_V, \chi_W$ are characters of $\mathbb{Z}_p$, then $\chi_{V\otimes W}$ is a character of $\mathbb{Z}_p \times \mathbb{Z}_p$ since the character of a tensor product of representations is the product of the characters. The character table of $\mathbb{Z}_p$ is given by

| | $0$ | $1$ | $2$ | $\cdots$ | $p-1$ |
|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $\cdots$ | $1$ |
| $\chi_2$ | $1$ | $\omega$ | $\omega^2$ | $\cdots$ | $\omega^{m-1}$ |
| $\chi_3$ | $1$ | $\omega^2$ | $\omega^4$ | $\cdots$ | $\omega^{m-2}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | |
| $\chi_{p-1}$ | $1$ | $\omega^{m-1}$ | $\omega^{m-2}$ | $\cdots$ | $\omega$ |

Where $\omega$ is a $p$th root of unity, therefore the characters of $\mathbb{Z}_p \times \mathbb{Z}_p$ are given by $\chi_{(i,j)}((a,b)) = \chi_i(a)\chi_j(b)$. The product of two irreducible characters is only irreducible if one of them is 1 dimensional, in our case every character is 1 dimensional, so we have $p^2$ irreducible representations.

### b)

Consider the group homomorphism

$$\varphi : \mathbb{Z}_p \to GL_2(\mathbb{R})$$
$$n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Then clearly this is nontrivial, and we show it's a homomorphism:

$$\varphi(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So we send the additive identity to the multiplicative identity. Furthermore

$$\varphi(a+b) = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \varphi(a)\varphi(b)$$

## 27.2 Question 3

Let $T$ be a diagonalizable linear operator on a finite dimensional vector space $V$, let $U \subset V$ be a subspace that is $T$ invariant.

### a)

Let $S$ be the restriction of $T$ to $U$. As $T$ is diagonalizable, the minimal polynomial $m_T(x)$ of $T$ splits into distinct roots, and $m_T(T) = 0$. If $S$ is the restriction of $T$ to an invariant subspace, then $m_T(S) = 0$, as the restriction of the minimal polynomial $m_T(x)$ to $U$ is just $m_S(x)$, the minimal polynomial of $S$. Thus the minimal polynomial of $S$ divides the minimal polynomial of $T$. But as we said above, $m_T(x)$ splits into distinct roots, so $m_S(x)$ must also split into distinct roots, thus $S$ is diagonalizable.

### b)

As $T$ is diagonalizable on $V$ there is a basis of eigenvectors, and that there is a direct sum decomposition of $V$ into the eigenspaces of $T$:

$$F^n = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_n}$$

From here we note by part a that each eigenspace of $S$ is a subspace of the eigenspace of $T$, $W_{\lambda_i} \subset V_{\lambda_i}$. In each of these eigenspaces which $S$ and $T$ share, take the complement of $W_{\lambda_i}$, and for the eigenvalues of $T$ that are not eigenvalues of $S$, take the whole eigenspace. Formally:

$$U = (U \cap V_{\lambda_1}) \oplus \cdots \oplus (U \cap V_{\lambda_n})$$

, then

$$V = (U \cap V_{\lambda_1}) \oplus \cdots \oplus (U \cap V_{\lambda_n}) \oplus W_{\lambda_1} \oplus \cdots \oplus W_{\lambda_n}$$

Where we extend a basis of $U \cap V_{\lambda_i}$ to a basis of $V_{\lambda_i}$, then take $W_{\lambda_i}$ to be the complement subspace formed by the eigenvectors in the basis of $V_{\lambda_i}$, not in $U \cap V_{\lambda_i}$

## 27.3 Question 5

If $G$ is of order 10 and abelian, then by the Fundamental theorem $G \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^m\mathbb{Z}$ where $|\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^m\mathbb{Z}| = 10$. Hence $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and we note that as $\gcd(2, 5) = 1$,

$$G \cong \mathbb{Z}/10\mathbb{Z}$$

If $G$ is nonabelian, then by Lagrange, if $x \in G$ is not the identity it has order $2, 5, 10$. Having order 10 yields the cyclic case above, so $x$ could have either 2 or 5 order (or trivially order 1). Let $x$ be an element of order 5, and $y$ and element of order 2. $1, x, x^2, x^3, x^4$ and $y, xy, x^2y, x^3y, x^4y$, the element $yx$ is one of the later elements.

# 28 January 2002

## 28.1 Question 2

Let $V$ be a finite dimensional real vector space, and $P \in \text{End}(V)$ idempotent. As $P^2 = P$, then $P$ satisfies $x^2 - x = 0 \implies x(x-1) = 0$ so the minimal polynomial of $P$ divides $x^2 - x$ thus $P$ is diagonalizable as the minimal polynomial has no repeated roots. $P$ has eigenvalues 0, 1 or both, and so we have a decompostion of $V$ into the eigenspaces of $P$: $V_0, V_1$, so $V = V_0 \oplus V_1$, these are the $U$, $W$ we're looking for. Then clearly $P$ is a projection as $u+w \in V \implies P(u+w) = P(u)+P(w) = u \in V_1$

This problem can also be solved without appealing to diagonalizability: For any $v \in V$ we can write $v = Pv + (v - Pv)$, so take $U = P(V)$ and $W = (id_V - P)(V)$. Then clearly we have that $Pv = P^2(v) + Pv - P^2v = Pv + Pv - Pv = Pv$, so $P$ is the projection onto the image of $V$ under $P$. The intersection is trivial since $v \in P(V) \cap (id_V - P)(V)$ means that $Pw = v$ and $v - Pw = v$, so $v = v + Pw \implies Pv = Pv + P^2w \implies Pw = 0$ so $v$ is zero.

## 28.2 Question 3

### a)

The minimal polynomial is linear or quadratic. If it's quadratic by Cayley Hamilton it's necessarily the charactersitic polynomial. If the minimal polynomial is linear, then the other invariant factor is the same as the minimal polynomial and hence is equal to a scalar matrix. The same min polynomial gives the same charactersitic polynomial hence same list of invariant factors.

### b)

We'll show that the elements of order 3 in 3x3 real matricies have only one possible rational canonical form. If $A$ is an element of order 3 in $GL_2(\mathbb{R})$, $A^3 = I$ so $A$ satisfies $x^3 - 1 = (x-1)(x^2+x+1)$, so the minimal polynomial divides this. It must be the case that the minimal polynomial and hence the charactersitic polynomial is $x^2+x+1$ since if the min polynomial is $x-1$ then $A$ does not have order 3, and the min poly is degree 1 or 2 so it's $x^2+x+1$. Thus Cayley-Hamilton says this is also the charactersitic polynomial thus the only possible RCF is

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

## 28.3 Question 6

Let $G$ be a group of order 75

## 28.4 Question 8

### a)

Let $\mathbb{C}[G]$ be a module over itself, with basis elements the $g \in G$. Then we have an action given by permuting the basis elements by left multiplication:

$$g \cdot g_i = g_j$$

In this basis, the matrix will have 1 if $g \cdot g_j = g_i$ and zero otherwise, but the only element which will fix all elements of $G$ is the identity, thus the trace of this matrix is either $|G|$, or zero. Hence the character is as stated.

### b)

Let $\chi$ be a character of a representation $\rho : G \to GL(V)$ with $d = (\chi, \chi_1)$, the multiplicity of the trivial rep inside $\chi$, and $\chi(g) = 0$ for all nonidentity element of $G$. Then,

$$(\chi, \chi_1) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi_1(g)} = \frac{1}{|G|}\chi(1) = d$$

As a result $\chi(1) = d|G| = d\chi^{reg}(1)$, and since it's zero on every other element of $G$ we get the result.

## 28.5 Question 9

Let $K$ be a finite field with an odd number of elements, say $p$. Then we know that

$$x^p - x = \prod_{\alpha \in K} (x - \alpha)$$

Now let take the nonzero element of this field to obtain

$$x^{p-1} - 1 = \prod_{\alpha \in K^\times} (x - \alpha)$$

Take $x = 0$ so that

$$-1 = \prod_{\alpha \in K^\times} (-\alpha) = \prod_{\alpha \in K^\times} (-1)^{p-1}(\alpha)$$

Thus

$$-1^p = \prod_{\alpha \in K^\times} \alpha$$

And since the order of $K$ is odd we get the desired result.

## 28.6 Question 10

### a)

The subfields of $\mathbb{Q}(\sqrt{2}, i)$ can be gotten by finding the Galois group then using the Fundamental Theorem. First one can check that this is a degree 4 extension of $\mathbb{Q}$. So we have two possible choices for Galois group. If one does part b we can immediately see what the Galois group is: Galois groups of cyclotomic field extensions is the group $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus immediately yielding $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$, each of these elements has order 2 mod 8, hence we get the Klein 4 group. Hence we have 4 total subgroups, 3 of which are nontrivial, yielding 3 nontrival field extensions, corresponding to $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}i)$

Or,

$K$ is the splitting field of the separable polynomial $(x^2 - 2)(x^2 + 1)$, so it's Galois. The possible Galois automorphisms are those that send $\sqrt{2} \mapsto \pm\sqrt{2}$ and $i \mapsto \pm i$, there are 4 possible automorphisms, and the nonidentity ones have order 2, thus yielding the Klein 4 group.

### b)

The element we'll choose is the 8th root of unity $\frac{1+i}{\sqrt{2}}$

# 29 January 2001

## 29.1 Question 4

Use RCF, 4 possible orbits? Corresponding to the minimal polynomial?

## 29.2 Question 6

Let $p, q$ be prime numbers $q < p$ such that $q \nmid p - 1$. Prove every group of order $pq$ is cyclic.

# 30 August 2000

## 30.1 Question 1

We have a theorem: Each irreducible $p(x)$ in $\mathbb{F}_p[x]$ of degree $n$ divides $x^{p^n} - x$ and is separable.

For us, $x^8 - x = x^{2^3} - x$, and so every irreducible polynomial of degree 3 in $\mathbb{F}_2[x]$ will appear. We can check that there is only $x^3+x+1, x^3+x^2+1$. Now, we can factor the polynomial as follows:

$$x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + \cdots + x + 1) = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

## 30.2 Question 2

### a)

First, since there are 5 conjugacy classes, there must be 5 characters. So there is a single missing row to the table. The order of the group is the sum of conjugacy class sizes, so $|G| = 20$. This is also equal to the sum of squares of the dimensions of the representations. So $\chi_5(1) = 4$. Next we can just use column orthogonality to see that $\chi_5(a) = -1, \chi_5(b) = \chi_5(c) = \chi_5(d) = 0$.... Which when checking seems wrong... I'm not sure if I'm making a very silly error or if this character table is flawed.

### b)

$\ker(\chi_2) = \{g \in G : \chi_2(g) = \chi_2(1)\}$, so the order is the number of elements in $G$ that, give 1 when evaluated on $\chi_2$. By the character table this is the number of elements in $G$ conjugate to $1, a, d$, whose sizes are 1,4,5 respectively, thus $|\ker \chi_2| = 10$

## 30.3 Question 3

### a)

$|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$, the largest power of $p$ that appears in the order allowable by Lagrange is the order of the Sylow $p$-subgroup. In this case it's $p$

### b)

We have that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order $p$, so is therefore a part of the Sylow $p$-subgroup. The number of distinct Sylow $p$-subgroups is gotten by $n_p \equiv 1 \mod p$ and $n_p | (p-1)^2(p+1)$

## 30.4 Question 8

**a)**

$$\begin{aligned}\langle Sv, v\rangle &= \langle (TT^* + T^*T)v, v\rangle \\ &= \langle TT^*v, v\rangle + \langle T^*Tv, v\rangle \\ &= \langle T^*v, T^*v\rangle + \langle Tv, Tv\rangle \\ &= ||T^*v||^2 + ||Tv||^2 \\ &\geq 0\end{aligned}$$

**b)**

First let $v \in \ker(T) \cap \ker(T^*)$ then $T^*v = Tv = 0$, and thus clearly $Sv = (TT^* + T^*T)v = TT^*v + T^*Tv = 0$, hence $\ker(T) \cap \ker(T^*) \subseteq \ker(S)$

Next let $v \in \ker(S)$, then $Sv = (TT^* + T^*T)v = TT^*v + T^*Tv = 0$, so by part a we have

$$\langle Sv, v\rangle = \langle (TT^* + T^*T)v, v\rangle = ||T^*v||^2 + ||Tv||^2 = 0$$

So $||T^*v||^2 = -||Tv||^2$, but this only holds when both of these are 0, thus $Tv = T^*v = 0$, and hence $v \in \ker(T) \cap \ker(T^*)$, thus we have equality.

# 31 January 2000

## 31.1 Question 1

Looking back this problems seems difficult to solve without some knowledge of representation theory of compact groups

## 31.2 Question 4

### a)

If $F$ is a field with $p(x)$ and irreducible element of $F[x]$ then as $F[x]$ is a Euclidean domain, it's a UFD. In a UFD, nonzero prime elements are irreducible, and moreover $p(x)$ is prime, as irreducible elements are always prime. If $(p)$ is the ideal of all polynomials divisible by $p(x)$, as $F[x]$ is a PID, this ideal is principal, generated by $p(x)$. As $p(x)$ is irreducible, it's a prime ideal, and in a PID nonzero prime ideals are maximal. $p(x) \in (p(x))$ so it's nonzero hence $F[x]/(p)$ is a field.

### b)

Check it has no roots.

### c)

A basis for $F_2[x]/(x^2+x+1)$ is $\{1, x\}$. First we show linear independence: If $a_0 \cdot 1 + a_1 x + (x^2+x+1) = 0 + (x^2+x+1)$, then $a_0 + a_1 x \in (x^2+x+1)$, but the degree of $a_0 + a_1 x$ is less then the degree of the polynomial generating the ideal, thus this occurs only when $a_0 = a_1 = 0$.

To see it spans consider a polynomial $g(x) \in F_2[x]$, dividing this by $1 + x + x^2$ yields $g(x) = (1 + x + x^2)f(x) + r(x)$ where $\deg r(x) < 2$ or $r(x) = 0$. Moding by $I$ gives $g(x) + I = r(x) + I$, so $g(x) + I$ can be written as a linear combination of polynomials with degree less than 2, hence $\{1, x\}$ spans the set. Thus we have a basis.

Next we want to find the Galois group of $F_2[x]/(x^2+x+1)$ over $F_2$ in terms of the basis $\{1, x\}$. As $x^2+x+1$ is irreducible, the extension $F_2[x]/(x^2+x+1)$ is a field extension of the finite field $F_2$, then $F_2(\alpha) \cong F_2[x]/(x^2+x+1)$ where $\alpha$ is a root of $x^2+x+1$. Now the extension is over the finite field, hence is Galois, and moreover is cyclic generated by the Frobenius morphism $\alpha \mapsto \alpha^2$. The extension $F_2(\alpha)/F_2$ is a degree 2 extension with $\mathrm{Gal}(F_2(\alpha)/F_2) = \{x \mapsto x, x \mapsto x^2\}$. Where these are the Frobenius morphism and its square. Now $x^2 = -1 - x$. On an element $a + b\alpha$ of $F_2(\alpha)$ we have $\varphi(a + b\alpha) = (a + b\alpha)^2 = a^2 + b^2\alpha^2 = a + b\alpha^2 = a + b(-1 - \alpha)$ as $a^2 = a$ in the field of order 2.

## 31.3 Question 5

If $A, B$ have finite order, then there exists $n, k$ such that $A^n = I, B^k = I$, respectively. Then $A, B$ have minimal polynomials dividing $x^n - 1, x^k - 1$ respectively. Thus the min poly has distinct roots and therefore is diagonalizable. They commute so we can apply the standard theorem of commuting diagaonalizable operators being simultaneously diagonalizable.

## 31.4 Question 6

First we prove the following proposition: $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$

*Proof.* Let $\varphi_g$ be the action of conjugation by $g \in N_G(H)$: $h \mapsto ghg^{-1}$. Since $gHg^{-1} = H$ this action is a map from $H$ to itself. Moreover since $\varphi_1 = \mathrm{Id}$, and $\varphi_g \circ \varphi_h = \varphi_{gh}$ this is an a bijection. Moreover it's a homomorphism as

$$\varphi_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \varphi_g(h)\varphi_g(k)$$

The map $\psi : N_G(H) \to \mathrm{Aut}(H) \leq S_{|H|}$ defined by $\psi(g) = \varphi_g$ by sending $g \mapsto \varphi_g$ yields the homomorphism into $\mathrm{Aut}(H) \leq S_{|H|}$. The kernel of this map is the sent of elements in $G$ such that $\varphi_g = 1 \implies ghg^{-1} = h$, which are precisely the elements in the centralizer of $H$. The first isomorphism theorem gives the result. □

Now with the above, if we replace $H$ with $G$ we get $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$, and as $Z(G)$ is trivial, then $|G|$ divides the order of the automorphism group.

## 31.5 Question 7

### a)

Recall that we have the standard Hermitian inner product on $\mathbb{C}^2$ as given by $\langle x, y\rangle = \overline{x}^T y$. The averaging procedure in question states that given this inner product we need to compute the following:

$$\{x, y\} = \frac{1}{|G|}\sum_{i \in G}\langle g^i x, g^i y\rangle$$

Where $\{,\}$ is a $G$-invariant inner product. Given that $A$ is an element of order 3 we can make a faithful two-dimensional representation as follows:

$$\rho : \mathbb{Z}_3 \to GL_2(\mathbb{C}) \qquad \rho(i) = A^i$$

From here we can compute the above:

$$\begin{aligned}\{x,y\} &= \frac{1}{3}\sum_{i=0}^{2}\langle A^i x, A^i y\rangle \\ &= \frac{1}{3}\sum_{i=0}^{2}\overline{\overline{A^i x}}^T A^i y \\ &= \frac{1}{3}\sum_{i=0}^{2}\overline{A^i}^T \overline{x}^T A^i y \\ &= \frac{1}{3}\sum_{i=0}^{2}{A^i}^T \overline{x}^T A^i y \\ &= \overline{x}^T \frac{1}{3}\sum_{i=0}^{2}{A^i}^T A^i y\end{aligned}$$

Thus take $B = \frac{1}{3}\sum_{i=0}^{2}{A^i}^T A^i$, then the form

$$\{x,y\} = \overline{x}^T B y$$

is $G$ invariant

**b)**

We start with the standard basis for $\mathbb{C}^2$: $\{e_1, e_2\}$. The we use Gram-Schmidt.

## 31.6 Question 8

**a)**

Let $V = \{(z_1, ..., z_5) : \sum z_i = 0\}$. Clearly $S_5$ leaves $V$ invariant as permuting the entries still yields a zero sum. Any permutation of $S_5$ when applied to the indicies of the elements may permute their ordering, but their sum will still be 0.

To see that $S_5$ acts irreducibly on $V$ we need to show there are no nontrivial invariant subspaces of $V$. One way we can do this is to find the character of $V$ and then use the inner product to see that it computes to 0. The character $\chi_V$ of $V$ can be gotten by subtracting the character of the trivial representation, from the character of the permutation representation which is computed by finding the number of fixed points of the action of each $\sigma \in S_5$ on the elements of $\mathbb{C}^5$. Doing this one gets the following:

$$\chi_V((1)) = 4, \chi_V((12)) = 2, \chi_V((123)) = 1$$

$$\chi_V((1234)) = 0, \chi_V((12)(34)) = 0, \chi_V((123)(45)) = -1, \chi_V((12345)) = -1$$

Using the inner product:

$$\frac{1}{|S_5|}\sum d_i \chi_V(\sigma)\overline{\chi_V(\sigma)}$$

We find that $(\chi_V, \chi_V) = \frac{1}{120}(1 \cdot 4^2 + 10 \cdot 2^2 + 20 \cdot 1^2 + 15 \cdot 0^2 + 30 \cdot 0^2 + 20 \cdot (-1)^2 + 24 \cdot (-1)^2) = 1$, hence it's irreducible.

**b)**

The number of nonisomorphic irreducible complex representations of $S_5$ is equal to the number of conjugacy classes of $S_5$ is equal to the number of partitions of $S_5$ which is 7.

## 31.7 Question 9

**a)**

Let $V$ be a finite dimensional vector space over $\mathbb{Q}$, and let $T : V \to V$ be a nonsingular linear map such that $T^{-1} = T + I$, then multiplying by $T$ yields $I = T^2 + T$, or $T^2 + T - I = 0$. This means that $T$ satisfies $x^2 + x - 1$, so the minimal polynomial divides this polynomial. The minimal polynomial is irreducible and so is this polynomial via the Rational Roots Test, hence this is the minimal polynomial. By Cayley-Hamilton the minimal polynomial divides the characteristic polynomial, and the degree of the characteristic polynomial is the dimension of the vector space. The minimal polynomial has degree 2, so the degree of the characteristic polynomial must be even, the sum of an even number and odd or even number is even, thus the dimension of $V$ is even.

**b)**

If the dimension of $V$ is two, the characteristic polynomial has degree 2, and is thus equal to the minimal polynomial. Thus the only invariant factor of $T$ is $x^2 + x - 1$, so the Rational Canonical Form for $T$ is

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

# 32 January 1997

## 32.1 Question 1

Let $K$ be a finite field with $q$ elements. We'll prove a more general result that will immediately yield what we desire: The number of monic irreducible polynomials of degree $p$, for $p$ a prime, over a finite field of order $q$ is $\frac{q^p-q}{p}$.

First recall that the field $F_{q^p}$ is the splitting field of $x^{q^p}-x$, and that every monic irreducible polynomial of degree $p$ divides $x^{q^p}-x$. The first fact can be seen by using that every element of $F_{q^p}$ satisfies $x^{q^p}=x$ seen using that the multiplicative group of this field is cyclic with order $q^p-1$, so $x^{q^p}-x$ has every element of this extension as a root, thus it's the splitting field. The other fact comes from using that $K[x]/(p(x))$ for an irreducible polynomial $p(x)$ of order $p$ has order $q^p$, so $x^{q^p}=x$ in this field. Reduce $x^{q^p}$ mod $p(x)$ to get the result.

Now $[F_{q^p}:K]=p$, so via a result that two polynomial over a finite field divide one another if and only if the field extensions of their respective orders are subfields, we know that any polynomial that divides $x^{q^p}-x$ has order 1 or $p$.

First we count the number of linear polynomials. A linear polynomial dividing $x^{q^p}-x$ means it's of the form $x-\alpha$ where $\alpha\in K$, as $x^{q^p}-x$ is separable this is all of them, hence there are $q$ monic linear polynomials.

Next we count the number of degree $p$ polynomials. If we multiply all the polynomials together that divide $x^{q^p}-x$ together, we get back $x^{q^p}-x$ hence this has degree $q^p$. So if $y$ is the number of degree $p$ polynomials we'd have $yp+q=q^p$, thus

$$y=\frac{q^p-q}{p}$$

To solve the desired problem substitute $p=2,3$

## 32.2 Question 3

Consider the subspace $\ker(A^2+A+1)$, this is clearly nonzero, as otherwise $x^2+x+1$ wouldn't be a factor of the characteristic polynomial. For any vector $v\in\ker(A^2+A+1)$, $x^2+x+1$ is the minimal degree polynomial for which $(A^2+A+1)v=0$. Thus the vectors $v, Av$ form a basis for this subspace of dimension 2. This is due to the fact that

$$c_0+c_1Av+c_dA^2v=0$$

cannot happen unless the degree is less than 2. As such $T^iv\in\ker(A^2+A+1)$ so it's invariant of dimension 2.

## 32.3 Question 4

Let $\alpha = \cos(2\pi/7)$. Recall $\alpha = \frac{\zeta+\zeta^{-1}}{2}$ for $\zeta = e^{2\pi i/7}$, so $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$, and as $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(7) = 6$, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. As such, and the fact that $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ we know every subgroup is normal, which thus corresponds to normal extensions (Galois), so our extension is Galois, and moreover is necessarily equal to $\mathbb{Z}/3\mathbb{Z}$ being of degree 3.