Contents

1 Spring 2009 Part II

1.1 5

Let A be a noetherian domain. Suppose that for every maximal ideal $Q \subset A$ the quotient Q/Q^2 is one-dimensional over the field A/Q.

1.1.1 a

Let $P \subset A$ be a nonzero prime ideal. Then there is some maximal $Q \supset P$. Since Q/Q^2 is one-dimensional we see that in the localization A_Q that Q_Q/Q_Q^2 is one-dimensional and thus by Nakayama's lemma QA_Q is principal. Then $PA_Q \subset QA_Q$ but I claim that in any domain no nonzero prime can be strictly contained in a principal ideal. Indeed let R be a noetherian domain and $\mathfrak{p} \subset (x)$. Consider $I = \{r \in R \mid rx \in \mathfrak{p}\}$ which is an ideal. However, if $\mathfrak{p} \neq (x)$ then $x \notin \mathfrak{p}$ so $r \in \mathfrak{p}$ and thus $I = \mathfrak{p}$. Then $\mathfrak{p}x = \mathfrak{p}$ so by Nakayama's lemma there is $1+rx$ such that $(1+rx)\mathfrak{p} = 0$ but $1 + rx \neq 0$ so $\mathfrak{p} = 0$ because R is a domain. Therefore PA_Q is equal to either 0 or QA_Q and thus $P = (0)$ or $P = Q$ proving that P is maximal or zero.

1.1.2 b

Let $K = \operatorname{Frac}(A)$ and $p \in A[x]$ be a monic polynomial. Suppose that $\alpha \in K$ is a root of p. Then I claim that $\alpha \in A_Q$ for each nonzero prime $Q \subset A$. In A_Q let $M = QA_Q = (\varpi)$ then we can write

any element as $a = u\varpi^n$ where u is a unit since either $a \notin M$ or $a \in M^n$ for some power n. Thus we can write, $\alpha = \frac{a}{b} = u\varphi^k$ for possibly negative k Suppose that $k = -\ell$ for $\ell > 0$. Let,

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

then,

$$u^n + a_1 u^{n-1}\varpi^\ell + \cdots + a_n \varpi^{n\ell} = 0$$

and thus $u^n \in M$ but u^n is a unit giving a contradiciton. Therefore, $k \geq 0$ so $\alpha \in A_Q \subset K$. Now I claim that,

$$A = \bigcap_{P \neq (0)} A_P$$

Indeed, one direction is clear. We need to show that if $\beta \in A_P \subset K$ for all nonzero P then $\beta \in A$. Consider the ideal $I = \{a \in A \mid a\beta \in A\}$ then if $I = A$ we see that $\beta \in A$. Suppose $I \subsetneq A$ then there is some maximal ideal $P \subset A$ such that $I \subset P$. Then for each $s \in A \setminus P$ we see that $s \notin I$ so $s\beta \notin A$ and thus $\beta \notin A_P$ contradicting the assumption. Thus $\beta \in A$ proving the claim. Therefore, since $\alpha \in A_P$ for all nonzero P we see that $\alpha in A$ so A is integrally closed.

Suppose that A were not integrally closed. Then let $K = \mathrm{Frac}\,(A)$ be it

2 Fall 2009 Part I

2.1 4

Let G be a nontrivial finite group and p the smallest prime dividing the order of G. Let $H \subset G$ be a subgroup of index p. Suppose that $H \subset G$ is not normal then consider the action of G on the conjugates $C = \{gHg^{-1} \mid g \in G\}$ which is obviously transitive. As G-sets we have $G/N_G(H) \cong C$ but $[G : H]$ is prime and $N_G(H) \neq G$ so $N_G(H) = H$ and thus $|C| = p$. Therefore we get a map $\varphi : G \to S_p$ whose image has order d dividing $p!$ and $|G|$ and thus $d = p$ (since $d = 1$ would imply that the action is not transitive) because p is the mimimal prime dividing $|G|$. Thus the image is cyclic of order p so $\ker\varphi$ has index p and furthermore $\ker\varphi \subset N_G(H) = H$ because elements of the kernel in particular fix H by conjugation so $H = \ker\varphi$ which is normal.

3 Fall 2010 Part I

3.1 1

3.1.1 a

Let G be a finite group of order n and let $\rho : G \to S(G)$ by G acting on itself by left translation. Let G have order m. Let $H = \langle g \rangle \subset G$ and partition G into right H-cosets $Hc_1, Hc_2, Hc_3, \ldots, Hc_k$ where $mk = n$. Then g acts on each partition H as an m-cycle and thus has sign $(-1)^{m-1}$ and therefore the sign of $\rho(g)$ is,

$$(-1)^{(m-1)k} = (-1)^{n-k} = (-1)^{n+k}$$

3.1.2 b

Let G be a finite group of order $2k$ with k odd. Consider the homomorphism $G \to S(G) \to \mathbb{Z}/2\mathbb{Z}$ given by taking the sign. There is an element in G of even order in the Sylow 2-subgroup and

then it has sign $(-1)^{2k+k} = -1$ because k is odd. Therefore this is a nontrivial homomorphism so the kernel is $N \subset G$ which is normal of order k. Furthermore the Sylow 2-subgroup $P \subset G$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By the second isomorphism theorem, $PN = G$ and $P \cap N = \{e\}$ and thus,

$$G = N \rtimes (\mathbb{Z}/2\mathbb{Z})$$

3.2 3

Let $R = \mathbb{C}[x, y]$ be a prime and $P \subset R$ a prime. We know that $\dim R = 2$ and R is a domain so the only prime of height 0 is $P = (0)$. Primes of height 2 must be maximal and thus R/Q is a field but also a finite type $\mathbb{C}$-algebra so $R/Q \cong \mathbb{C}$ (since it is algebraically closed) and thus $Q = (x-a, y-b)$ where $x \mapsto a$ and $y \mapsto b$ under the map $R \to \mathbb{C}$. Thus the case P has height one remains.

Here I claim that in a Noetherian domain, height one primes are principal if and only if it has unique factorization. Using this, we see that $P = (f)$ for some $f \in \mathbb{C}[x, y]$ which must be irreducible else P would obviously not be prime.

Now I justify the claim. If P is a UFD then irreducible elements are prime by looking at factorizations. Then if P has height 1 it is minimal over (f) for some $f \in R$. If f is irreductible then (f) is prime so $P = (f)$ otherwise write $f = r_1 \cdots r_n$ where r_i are irreducible then $r_i \in P$ for some i and $(f) \subset (r_i) \subset P$ and (r_i) is prime so $P = (r_i)$ and thus P is principal. Conversely, if every height one prime is principal then we need to show that irreducible elements are prime. If r is irreducible suppose that $xy \in (r)$. Consider the minimal prime P over (r) then P has height 1 (since (0) is prime) so $P = (g)$ and thus $g \mid r$ so $P = (r)$ because r is irreducible and thus r is prime.

3.3 4

Let G be a group and k a field.

3.3.1 a

The algebra $k[G]$ is defined as the algebra of set maps $G \to k$ with finite support under addition and convolution. Explicitly, this coresponds to polynomials,

$$\sum_{g \in G} a_g \cdot g$$

with finitely many nonzero a_g under the clear addition and polynomial multiplication.

There is an equivalence of categories $\mathrm{Rep}_k(G) \cong \mathrm{Mod}_{k[G]}$. Given a k-linear G-representation V we let $k[G]$ act via,

$$\left(\sum_{g \in G} a_g \cdot g\right) \cdot v = \sum_{g \in G} a_g (g \cdot v)$$

which makes sense because the sum is finite. This gives V the structure of a $k[G]$-representation. Conversely if M is a $k[G]$-module then there is a G-action by $G \subset k[G]$ sending $g \mapsto 1g$ and $(1g)(1 \cdot h) = 1gh$ so this is indeed a G-action. Futhermore, for $\lambda \in k$ we have $v \mapsto \lambda e \cdot v$ gives a k-action so M is also a k-module and $(\lambda \cdot e)(1g) = (\lambda g) = (1g)(\lambda g)$ so these actions commute showing that M gets the structue of a k-linear G-rep. These identifications are clearly inverse.

3.3.2 b

Let A and B be associative k-algebras. Then $A \otimes_k B$ is an associative k-algebra whose operations are generated by the following,

$$\lambda \cdot (a \otimes b) = \lambda a \otimes b = a \otimes \lambda b$$

making $A \otimes_k B$ a k-module but there is a multiplication,

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

which is clearly k-linear. We exend these linearly from elementary tensors.

For any groups G, H consider,

$$k[G] \otimes_k k[H] \to k[G \times H]$$

via sending,

$$g \otimes h \mapsto (g, h)$$

or more explicitly,

$$\left(\sum_{g \in G} a_g g\right) \otimes_k \left(\sum_{h \in H} b_h h\right) \mapsto \sum_{(g,h) \in G \times H} a_g b_h (g, h)$$

This is an algebra map because,

$$(g \otimes h)(g' \otimes h') = (gg' \otimes hh') \mapsto (gg', hh') = (g, h)(g', h')$$

We need to check that this is an isomorphism. It is clear that $k[G \times H]$ is generated over k by $1(g, h)$ and $g \otimes h \mapsto (g, h)$ so the map is surjective. Furthermore, this map admits a well-defined inverse sending $(g, h) \mapsto g \otimes h$ and extended linearly. Thus this is an isomorphism.

3.3.3 c

Let A be an associative k-algebra and A^{op} the opposite algebra. This is an associative k-algebra because $a \cdot (b \cdot c) = (cb)a = c(ba) = (a \cdot b) \cdot c$ and the k-module structue works the same way on A^{op}. Let $A = k[G]$ I claim that $g \mapsto g^{-1}$ defines an isomorphism $A \to A^{\text{op}}$. Indeed,

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g \in G} a'_g g\right) = \sum_{g \in G}\left(\sum_{h \in G} a_h a'_{h^{-1}g}\right) g \mapsto \sum_{g \in G}\left(\sum_{h \in G} a_h a'_{h^{-1}g}\right) g^{-1} = \left(\sum_{g \in G} a'_g g\right)\left(\sum_{g \in G} a_g g\right)$$

so this is a k-algebra map and it is bijective because $g \mapsto g^{-1}$ is bijective $G \to G$. We can say that $k[G]^{\text{op}} = k[G^{\text{op}}]$ but $g \to g^{-1}$ defines an isomorphism $G \to G^{\text{op}}$.

3.4 4

Let $f = X^3 - 2 \in \mathbb{Z}[X]$.

3.4.1 a

By Eisenstein's criterion applied for $p = 2$ notice that f is irreducible over $\mathbb{Q}$. Furthermore, since its splitting field $K/\mathbb{Q}$ is complex it has an element of order 2. Furthermore, consider $\sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2}$ defines an automorphism of order 3. Therefore, $G \subset S_3$ must be S_3.

3.4.2 b

Consider the subgroups of S_3. Consider the subgroups,

(a) trivial: we have $\{e\} \subset S_3 \iff K \subset K$ and $S_3 \subset S_3 \iff \mathbb{Q} \subset K$

(b) index two $\langle r \rangle \subset S_3 \iff \mathbb{Q}(\zeta_3) \subset K$ because this is invariant under the 3-cycle.

(c) index three $\langle \sigma \rangle \subset S_3 \iff \mathbb{Q}(\sqrt[3]{2}) \subset K$ because this is the subfield of real elements. Then the other index three subgroups are conjugates and thus must be conjugates of $\mathbb{Q}(\sqrt[3]{2}) \subset K$ giving the fiels $\mathbb{Q}(\zeta_3^i \sqrt[3]{2}) \subset K$.

3.4.3 c

Over $\mathbb{F}_5$ notice that f factors as $(X-3)(X^2+3X+1)$ and $X^{@}+3X+1$ is irreducible over $\mathbb{F}_5$ so the splitting field of f is quadratic.

Over $\mathbb{F}_7$ we see that f has no roots and thus is irreducible (since would factor into a quadratic and a linear). We need to check that the splitting field does not contain a quadratic subdield wich happens in the case that the discriminant is a square. The discriminant is,

$$\Delta = -27q^2 \equiv_7 4$$

which is a square.

3.5 5

Let $G = \mathrm{GL}_2(\mathbb{F}_q)$ for $q = p^n$. Let Π be the set of one-dimensional subspaces in $V = \mathbb{F}_q^2$. Since $G \circlearrowright V$ by multiplication then it acts on Π.

3.5.1 a

If $\ell \in \Pi$ consider $G_\ell \subset G$. Notice that $|G| = (q^2-1)(q^2-q) = q(q-1)^2(q+1)$ and thus the sylow p-subgroups have order q. Since $G \circlearrowright \Pi$ transitively it suffices to show this for some line ℓ. Choose the line generated by $(1,0)$ then the satiblizer is of the form,

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

therefore the upper triangular matrices,

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

forming a sylow p-subgroup isomorphic to $\mathbb{F}_q$ is normal and thus there is a single one. Now each $\ell \in \Pi$ has a corresponding stabilizer G_ℓ. Each stabilizer fixes a unique line since otherwise they would be diagonalable. Thus there are $q+1$ such subgroups which are all conjugate and each has a Sylow p-subgroup so there are $q+1$ Sylow p-subgroups each of order q.

3.5.2 b

Let ℓ_1, ℓ_2, ℓ_3 be three distinct lines in V. Choose generators $v_1 \in \ell_1$ and $v_2 \in \ell_2$ and $v_3 \in \ell_3$ such that $v_3 = \alpha_1 v_1 + \alpha_2 v_2$ since $\dim V = 2$. Send $e_1 \mapsto \alpha_1 \ell_1$ and $e_2 \mapsto \alpha_2 v_2$ which is a gance of basis and thus given by $g \in G$ but then also $\alpha_1 v_1 + \alpha_2 v_2 = v_3$ so $g \cdot \mathbb{F}_q e_i \mapsto \ell_i$ as required (let $e_3 = e_1 + e_2$ for the purpose of this statemnt).

3.5.3 c

Let P_1, P_2, P_3 be three distinct p-Sylow subgroups of G and Q_1, Q_2, Q_3 are another three distinct p-Sylow sugroups of G. These are in bijective correspondence with the lines $\ell \in \Pi$ and thus there is a $g \in G$ such that,

$$gP_ig^{-1} = Q_i$$

4 Fall 2010 Part II

4.1 1

Let G be a subgroup of a finite p-group H such that the natural homomorphism $G \to H/[H,H]$ is surjective.

We proceed by induction on $|H|$. If $|H| = 1$ then obvious $G = H$ because there is only one subgroups.

Now we proceed by induction on $|H|$. Suppose that N is a nontrivial normal subgroup of H. Then we consider $G/H\cap N \hookrightarrow H/N$ then the map $G/G\cap N \twoheadrightarrow H/N/[H/N, H/N]$ is surjective. Therefore $G/G\cap N = H/N$ and therefore by the second isomorphism theorem $G\cdot N = H$. Let Z be the center of H. Because H is a p-group the center is nontrivial and normal and thus $G\cdot Z = H$. If $G\cap Z$ then we see that $H = G \times Z$ but then G would not surject because the factor Z is abelian and direct. Therefore, must have $G \cap Z$ nontrivial. Let $N = G \cap Z$ which is normal and thus $G \cdot (G \cap Z) = H$ which implies that $G = H$ proving the claim by induction.

4.2 2

Let G be a finite group and $K \subset L$ an extension of fields. Let $W_L = W \otimes_K L$. Let V, V' be n-dimensional K-linear G-representations with $n > 0$.

4.2.1 a

Suppose that there is a nonzero $L[G]$-linear map $V'_L \to V_L$. There is an exact sequence,

$$0 \longrightarrow \mathrm{Hom}_{K[G]}(V', V) \longrightarrow \mathrm{Hom}_K(V', V) \longrightarrow \prod_{g\in G} \mathrm{Hom}_K(V', V)$$

when the second map sends $\varphi \mapsto g\cdot\varphi - \varphi$ for each $g \in G$. Then tensoring by L we get,

$$0 \longrightarrow \mathrm{Hom}_{K[G]}(V', V) \otimes_K L \longrightarrow \mathrm{Hom}_L(V'_L, V_L) \longrightarrow \prod_{g\in G} \mathrm{Hom}_L(V'_L, V_L)$$

because $\mathrm{Hom}_K(V', V) \otimes_K L = \mathrm{Hom}_L(V'_L, V_L)$ since L is flat over K and V' is finite K-module. Therefore because kernels are unqiue we find that,

$$\mathrm{Hom}_{K[G]}(V', V) \otimes_K L \cong \mathrm{Hom}_{L[G]}(V'_L, V_L)$$

and thus if the righthand size is nonzero then we must have $\mathrm{Hom}_{K[G]}(V', V)$ be nonzero.

4.2.2 b

Suppose that K is infinite. Suppose that $p \in K[x_1, \ldots, x_N]$ is zero as a map $K^N \to K$. We prove that $p = 0$ by induction on N. For $N = 1$ this is because a nonzero polynomial has finitely many roots but K is infinite so $p = 0$. Now for general N take any $a_1, \ldots, a_{N-1} \in K$ then $p(a_1, \ldots, a_{N-1}, x_N) \in K[x_N]$ is always zero and thus $p(a_1, \ldots, a_{N-1}, x_N) = 0$ as a polynomial. Therefore, its coefficients $q_i \in K[x_1, \ldots, x_{N-1}]$ are zero as maps $K^{N-1} \to K$ and thus $q_i = 0$ by hypothesis. Therefore $p = 0$ because its coefficients as a polynomial in x_N are identically zero.

Let K be infinite. Since $\dim V' = \dim V$ we can pick some K-linear isomorphism (not as G-reps) $V' \xrightarrow{\sim} V$ identifying them. Now we can consider the map $\det : \mathrm{Hom}_{K[G]}(V', V) \to K$ taking the determinant (viewed as a map $V \to V' \to V$ using the identification) as a polynomial $c_i \in K[x_1, \ldots, x_d]$ where d is the dimension and $x_1, \ldots, x_d \in \mathrm{Hom}_{K[G]}(V', V)$ is a basis because V' and V are vectorspaces of dimension n. If V' and V are not isomorphic as $K[G]$-modules then every $\varphi \in \mathrm{Hom}_{K[G]}(V', V)$ must not be invertible and thus $\det \varphi = 0$. Therefore det must be the zero polynomial. This implies that $\det : \mathrm{Hom}_{L[G]}(V'_L, V_L) \to L$ is the zero polynomial in $L[x_1, \ldots, x_d]$ since $\mathrm{Hom}_{L[G]}(V'_L, V_L) \cong \mathrm{Hom}_{K[G]}(V', V) \otimes_K L$ and therefore there is no isomorphism $V' \to V$ as $L[G]$-modules.

4.3 4

Let A be a commutative ring.

4.3.1 a

Let B be a flat A-algebra, M a finitel presented A-module, and N an A-module. First, if $M = A^n$ then,

$$\begin{aligned}\mathrm{Hom}_A(M, N) \otimes_A B = \mathrm{Hom}_A(A^n, N) \otimes_A B = N^n \otimes_A B = (N \otimes_A B)^{\oplus n} \\ = \mathrm{Hom}_B(B^n, N \otimes_A B) = \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)\end{aligned}$$

Now we consider,

$$A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$$

and apply the natural maps to get an exact sequence (using the flatness of B and the left-exactness of $\mathrm{Hom}(-,-)$ to get exactness)

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(M, N) \otimes_A B & \longrightarrow & \mathrm{Hom}_A(A^n, M) \otimes_A B & \longrightarrow & \mathrm{Hom}_A(A^m, M) \otimes_A B \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) & \longrightarrow & \mathrm{Hom}_B(B^n, M \otimes_A B) & \longrightarrow & \mathrm{Hom}_B(B^m, M \otimes_A B) \end{array}$$

since the rightmost arrows are isomorphisms then by the five lemma we see that $\mathrm{Hom}_A(M, N) \otimes_A B \xrightarrow{\sim} \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$ is an isomorphism.

4.3.2 b

Suppose that,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of A-modules. Suppose that for each maximal ideal $\mathfrak{m} \subset A$ the localized sequence splits. Furthermore suppose that M'' is finitely presented.

First, notice that if the sequence splits then applying any additive functior preserves being split exact. In particular, $\mathrm{Hom}_A(M'', M) \to \mathrm{Hom}_A(M'', M'')$ is surjective. Conversely, suppose this map is surjective. Then the identity map $\mathrm{id} \in \mathrm{Hom}_A(M'', M'')$ is in the image so there is a map $M'' \to M$ composing with $M \to M''$ to the identity so the sequence is split.

Therefore, we see that for each maximal $\mathfrak{m} \subset A$,

$$\mathrm{Hom}_{A_\mathfrak{m}}(M''_\mathfrak{m}, M_\mathfrak{m}) \to \mathrm{Hom}_{A_\mathfrak{m}}(M''_\mathfrak{m}, M''_\mathfrak{m})$$

is surjective. However, since M'' is finitely presented and $A_\mathfrak{m}$ is flat over A we see that,

$$\begin{array}{ccc} \mathrm{Hom}_{A_\mathfrak{m}}(M''_\mathfrak{m}, M_\mathfrak{m}) & \twoheadrightarrow & \mathrm{Hom}_{A_\mathfrak{m}}(M''_\mathfrak{m}, M''_\mathfrak{m}) \\ \| & & \| \\ \mathrm{Hom}_A(M'', M) \otimes_A A_\mathfrak{m} & \twoheadrightarrow & \mathrm{Hom}_A(M'', M'') \otimes_A A_\mathfrak{m} \end{array}$$

and thus $\mathrm{Hom}_A(M'', M)_\mathfrak{m} \to \mathrm{Hom}_A(M'', M)_\mathfrak{m}$ is surjective. Since this holds at each maximal ideal, we see that $\mathrm{Hom}_A(M'', M) \to \mathrm{Hom}_A(M'', M)$ is surjective and thus the sequence splits.

4.4 5

Let F be a field and $V = F^4$ with the skew-symmetric bilinear form,

$$\langle x, y \rangle = x_1 y_3 + x_2 y_4 - x_3 y_1 - x_4 y_2$$

A subspace U of V is isotropic if $\langle x, y \rangle = 0$ for all $x, y \in U$. Let G be the subgroup of $\mathrm{GL}_4(F)$ preserving $\langle -, - \rangle$.

4.4.1 a

Let $U \subset V$ be two dimensional and isotropic. Let $u^1, u^2 \in U$ be a basis. Because $\langle -, - \rangle$ is nondegenerate, we can choose $v^1, v^2 \in V$ such that $\langle u^i, v^j \rangle = \delta_{ij}$. Now if $\langle v^1, v^2 \rangle = a$ then consider $\tilde{v}^1 - au^1$ and then $\langle \tilde{v}^1, v^2 \rangle = 0$ but also $\langle u^i, \tilde{v}^1 \rangle = \delta_{i1}$ because $u^1, u^2 \in U$ is isotropic. Thus u^1, u^2, v^1, v^2 is a basis of V on which the form $\langle -, - \rangle$ takes the same values as on the standard basis e^1, e^2, e^3, e^4. Thus there is an element $g \in G$ taking this basis to the standard basis and thus $gU = U_0$.

4.4.2 b

Let $F = \mathbb{F}_q$. The number of pairs (u^1, u^2) linearly independent with $\langle u^1, u^2\rangle = 0$ is given by $(q^4-1)(q^3-q)$ because the first vector is arbitrary (but nonzero) and the second lies in the 3-dimensional subspace $\ker\langle u^1, -\rangle$ and also not on the span of u^1. Now we need to count this up to the choice of such a basis for U. Since the span is isotropic, any change of basis for the span of u^1 and u^2 gives a basis also trivial for the bracket. Therefore we get,

$$\frac{(q^4-1)(q^3-q)}{(q^2-1)(q^2-q)} = (q^2+1)(q+1)$$

5 Spring 2010 Part I

5.1 1

Let $G = \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$.

5.1.1 a

Exercise 5.1.1. Find an element $\sigma \in G$ of order 8.

Because $p^2 - 1 = (p+1)(p-1)$ there is always an element of order $p+1$ in $\mathbb{F}_{p^2}^\times$. Multiplication by this element gives an automorphism of $(\mathbb{Z}/p\mathbb{Z})^2$ of order 8.

5.1.2 b

Let $P \subset G$ be the Sylow 2-subgroup. Since $|G| = (p^2-1)(p^2-p) = p(p-1)^2(p+1) = 2^5 \cdot 3^2 \cdot 7$ we see that $|P| = 2^5$. Notice that there exists an element $q \in (\mathbb{F}_{7^2})^\times$ of order 2^4 because it is cyclic of order $2^4 \cdot 3$. Furthermore, the Frobenius is an automorphism of order 2 so I claim that

$$P = \left\langle q, F \mid F^2 = q^{16} = 1, FqF = q^7 \right\rangle$$

for some choice of a Sylow 2-group. It suffices to show that $FqF = q^7$ because then clearly this presented group has order 2^5 (because it is a semi-direct product of $\mathbb{Z}/2^4$ and $\mathbb{Z}/2\mathbb{Z}$). Indeed, $F, q \in \mathrm{GL}_2(\mathbb{F}_7)$ acts on $\mathbb{F}_7 \cong \mathbb{F}_{7^2}$ as a $\mathbb{F}_7$-*vectorspace* via sending $x \mapsto x^7$ in terms of the $\mathbb{F}_{7^2}$ structure while $q \in \mathbb{F}_{7^2}^\times$ acts by multiplication. Thus $FqFx = (qx^7)^7 = q^7x$ because $F = (-)^7$ is a Field automorphism and $F^2 = \mathrm{id}$ proving the claim.

5.2 2

Let V, W be vector spaces over an algebraically closed field k with $\dim V = 6$ and $\dim W = 9$. Let $T : V \to V$ and $S : W \to W$ be linear maps whose minimal polynomials are T^6 and S^9. Consider $S \otimes T : W \otimes V \to W \otimes V$.

The minimal polynomial of $S \otimes T$ is $(S \otimes T)^6 = 0$.

$\dim \ker S \otimes T = 9 \cdot 6 - 8 \cdot 5$ because the images of S and T are of codimension one.

We must have $9 \cdot 6 - 8 \cdot 5 = 14$ eigenvectors of eigenvalue zero and therefore 14 Jordan blocks. Now

the largest Jordan block must have size 6 because the minimal polynomial is $(S \otimes T)^6 = 0$. Now consider,

$$\begin{aligned}
\dim \ker (S \otimes T)^1 &= 9 \cdot 6 - 8 \cdot 5 = 14 \\
\dim \ker (S \otimes T)^2 &= 9 \cdot 6 - 7 \cdot 4 = 14 + 12 \\
\dim \ker (S \otimes T)^3 &= 9 \cdot 6 - 6 \cdot 3 = 14 + 12 + 10 \\
\dim \ker (S \otimes T)^4 &= 9 \cdot 6 - 5 \cdot 2 = 14 + 12 + 10 + 8 \\
\dim \ker (S \otimes T)^5 &= 9 \cdot 6 - 4 \cdot 1 = 14 + 12 + 10 + 8 + 6 \\
\dim \ker (S \otimes T)^6 &= 9 \cdot 6 - 3 \cdot 0 = 14 + 12 + 10 + 8 + 6 + 4 = 9 \cdot 6
\end{aligned}$$

Therefore, there are 12 blocks of size at least 2 and 10 blocks of size at least 3 etc down to 4 blocks of size 6. Thus we see that there are 2 blocks of size 1 and two blocks of size 2 and two blocks of size 3 and two blocks of size 4 and two blocks of size 5 and four blocks of size 6.

5.3 3

Exercise 5.3.1. Let A, B be commutative rings containing a field k with B finitely generated over k. Let $\phi : A \to B$ be a k-algebra homomorphism and $\mathfrak{q} \subset B$ a maximal ideal. Show that $\phi^{-1}(\mathfrak{q}) \subset A$ is a maximal ideal.

Indeed, consider $A/\phi^{-1}(\mathfrak{q}) \to B/\mathfrak{q}$ where $B/\mathfrak{q}$ is a field and therefore a finite field extension of k by the Nullstellensatz because it is a finitely generated k-algebra. Then, $A/\phi^{-1}(\mathfrak{q}) \subset B/\mathfrak{q}$ is a domain and a finite dimensional k-vectorspace and thus a field (multiplication is injective thus surjective thus inverses exist) so $\phi^{-1}(\mathfrak{q}) \subset A$ is maximal.

5.4 4

Let α be a root of $x^7 - 12$ and ζ a primitive root of $x^7 - 1$.

5.4.1 a

Suppose that the powers $1, \alpha, \ldots, \alpha^6$ were linearly independent over $\mathbb{Q}[\zeta]$. We know that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ because the two fields are not equal and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$ so there are no notrivial subfields. Since the indexes $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ are relatively prime we know that, $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 7 \cdot 6$ and the product basis is a basis because we have equality $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]$ and thus the powers of α which are independent over $\mathbb{Q}$ must also be intependent over $\mathbb{Q}(\zeta)$ in $\mathbb{Q}(\alpha, \zeta)$.

5.4.2 b

If $\beta \in \mathbb{Q}[\alpha]$ has a conjugate $\zeta^i \beta$ in $\overline{\mathbb{Q}}$ show that $\beta = c\alpha^j$ for some rational number c and some j.

We can write,

$$\beta = \eta_0 + \eta_1 \alpha + \cdots + \eta_6 \alpha^6$$

with $\eta_i \in \mathbb{Q}$ then the conjugate by σ which must take α to another root of $x^7 - 12$ and thus $\sigma(\alpha) = \zeta^k \alpha$ so,

$$\sigma(\beta) = \eta_0 + \eta_1 \zeta^k \alpha + \cdots + \eta_6 \zeta^{6k} \alpha^6$$

but we want,

$$\sigma(\beta) = \zeta^i \beta$$

so by the linear independence all but one η_j are zero proving the claim.

5.4.3 c

Suppose that $\beta \in \mathbb{Q}(\alpha)$ is a root of $x^7 - 11$. Then the conjugates of β in $\overline{\mathbb{Q}}$ are of the form $\zeta^i\beta$ and thus by the previous part $\beta = c\alpha^j$ for some $c \in \mathbb{Q}$. However, $(c\alpha^j)^7 = c^6 12^j$ which cannt equal 11 because 11 is prime and not divisible by 12 giving a contradiction.

5.5 5 (WRITE THIS UP)

6 Spring 2010 Part II

6.1 1

Consider ζ_9 where $G = \mathrm{Gal}\,(\mathbb{Q}(\zeta_9) : \mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Therefore, G contains a normal subgroup of index 3 which corresponds to a Galois subfield of index 3 over $\mathbb{Q}$. Now it suffices to compute this field explicitly.

Let $H = \langle -1 \rangle \subset (\mathbb{Z}/9\mathbb{Z})^\times$ which obviously has order 2 and thus index 3. Then let $K = \mathbb{Q}(\zeta_9)^H$ which is clearly generated by $\eta = \zeta_9 + \bar{\zeta_9}$ because it is invariant under $\zeta_9 \mapsto \zeta_9^{-1}$. This element has trace zero so its minimal polynomial is,

$$x^3 + ax + b$$

We just need to find a and b. First, $-b$ is the norm,

$$\begin{aligned} b &= (\zeta_9 + \zeta_9^{-1})(\zeta_9^2 + \zeta_9^{-2})(\zeta_9^4 + \zeta_9^{-4}) = (\zeta_9^3 + \zeta_9 + \zeta_9^{-1} + \zeta_9^{-3})(\zeta_9^4 + \zeta_9^{-4}) \\ &= \zeta_9^7 + \zeta_9^5 + \zeta_9^3 + \zeta_9 + \zeta_9^{-1} + \zeta_9^{-3} + \zeta_9^{-5} + \zeta_9^{-7} \\ &= \zeta_9^8 + \zeta_9^7 + \zeta_9^6 + \zeta_9^5 + \zeta_9^4 + \zeta_9^3 + \zeta_9^2 + \zeta_9 = -1 \end{aligned}$$

Now we consider,

$$a = -\frac{1 + (\zeta_9 + \zeta_9^{-1})^3}{\zeta_9 + \zeta_9^{-1}}$$

Consider,

$$1 + (\zeta_9 + \zeta_9^{-1})^3 = 1 + \zeta_9^3 + 3\zeta_9 + 3\zeta_9^{-1} + \zeta_9^{-3} = (1 + \zeta_9^3 + \zeta_9^{-3}) + 3(\zeta_9^{-1} + \zeta_9^{-3}) = 3(\zeta_9^{-1} + \zeta_9^{-3})$$

because $\zeta_9^3 = \zeta_3$ and $1 + \zeta_3 + \zeta_3^{-1} = 0$. Therefore $a = -3$ so the minimal polynomial is,

$$x^3 - 3x + 1$$

6.2 2

6.2.1 a

Let $I \subset R$ be a nonzero ideal and R a domain. Suppose that I is a free R-module. If I is free of rank n then there is an injective map $R^n \to R$. Then tensoring with $K = \mathrm{Frac}\,(R)$ we get an injective map $K^n \to K$ implying that $n = 1$ and thus I is principal (it has one generator).

Let $R = \mathbb{Z}[\sqrt{-5}]$. We need to show that neither $P = (3, 1+\sqrt{-5})$ nor $Q = (3, 1-\sqrt{-5})$ is prinicpal. Since these are exchanged by the Galois action it suffices to show that P is not principal. Indeed, suppose that $P = (\alpha)$. Then $3 = \alpha\beta$ and $1+\sqrt{-5} = \alpha\gamma$. Taking norms we see that $3^2 = N(\alpha)N(\beta)$ and $6 = N(\alpha)N(\beta)$ meaning that $N(\alpha)$ must divide 9 and 6 and therefore is 1 or 3. However, $a^2 + 5b^2$ cannot equal 3 and is only 1 if $a = \pm 1$ which obviously doesn't work. Therefore P is not principal.

6.2.2 b

Clearly $3R \subset P \cap Q$ since each has 3 as a generator. Furthermore, because $P + Q = R$ (consider $1 + \sqrt{-5} + 1 - \sqrt{-5} - 3 = -1$) we know that $P \cap Q = PQ \subset 3R$ because the products of the generators are all divisible by 3 (each is obvious execpt for $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$). This also shows the surjectivity of the addition map $P \oplus Q \to R$ because it factors as $P \oplus Q \to P + Q \subset R$ and $P + Q = R$ and $P \oplus Q \to P + Q$ is surjective by definition.

6.2.3 c

Consider the exact sequence,

$$0 \longrightarrow 3R \longrightarrow P \oplus Q \longrightarrow R \longrightarrow 0$$

where the kernel is $P \cap Q = 3R$ (embedded as $x \mapsto (x, -x)$) which is isomorphic to R. Because R is a free and thus projective R-module this exact sequence splits so,

$$P \oplus Q \cong R \oplus 3R \cong R^2$$

6.3 3

Exercise 6.3.1. Let G be a finite group and $H \subset G$ a subgroup with prime to p index. Let V be a finite-dimensional G-rep over $\mathbb{F}_p$ whose restriction to H is semisimple. Prove that V is semisimple.

If V is irreducible we are done. Therefore, aiming for induction it suffices to show that if V has a subrepresentation $W \subset V$ then it is complemented. Because $\mathrm{Res}^G_H(V)$ is semi-simple we know that $\mathrm{Res}^G_H(W) \subset mathrmRes^G_H(V)$ is complemented menaing there is a direct sum decomposition in the category of H-representations which is equivalent to the existence of a H-invariant projection map $p : V \to W$ whose kernel gives the complementary invariant subspace. It suffices to modify p such that it is G-invariant. Indeed, let,

$$p'(v) = \frac{1}{[G : H]} \sum_{g \in G/H} g \cdot p(g^{-1} \cdot v)$$

We need to show this is well-defined. First $[G : H]$ in nonzero because it is prime to p so division is ok. Furthermore, we need to show the formula is independent of the choice of left coset representatives. If we choose $g' = gh$ then $g' \cdot p(g'^{-1} \cdot v) = gh \cdot p(h^{-1}g^{-1} \cdot v) = g \cdot p(g^{-1} \cdot v)$ because p is H-invariant. Therefore, this formula is well-defined. Now I claim that p' is a G-invariant projection $V \to W$. If $v \in W$ then $g^{-1} \cdot v \in W$ so $p(g^{-1} \cdot v) = g^{-1} \cdot v$ and thus $p'(v) = v$. Finally, for any $\sigma \in G$,

$$p'(\sigma \cdot v) = \frac{1}{[G : H]} \sum_{g \in G/H} g \cdot p(g^{-1}\sigma \cdot v) = \frac{1}{[G : H]} \sum_{g' \in G/H} \sigma g' \cdot p(g'^{-1} \cdot v) = \sigma p'(v)$$

where $g' = \sigma^{-1}g$ is a new set of coset representatives.

6.4 4

6.4.1 a HOW TO DO IT?

Exercise 6.4.1. Let A be a commutative Noetherian ring. Prove that $A[[x]]$ is Noetherian.

We try to replicate the proof of the Hilbert basis theorem. Let $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ be an ascending chain of ideals of $A[[x]]$. Choose elements $f_i \in I_{i+1} \setminus I_i$ of minimal "degree" where "degree" means the lower degree. Let $a_i \in A$ be the coefficient of the lowest degree term of f_i. Then consider,

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

Since A is noetherian this terminates at $(a_1, \ldots, a_N)$ proving that for each a_n we have,

$$a_n = \sum_{i=1}^{N} u_i a_i$$

for some $u_i \in A$. Now I can choose,

6.4.2 b

Suppose that A is a commutative Artinian ring. Let $\mathfrak{p} \subset A$ be prime. I want to show that $A/\mathfrak{p}$ is a field and thus that $\mathfrak{p}$ is maximal. For any $x \notin \mathfrak{p}$ I need to find some y such that $xy - 1 \in \mathfrak{p}$. Consider the descending chain of ideals,

$$(x) \supset (x^2) \supset (x^3) \supset \cdots$$

which must stabiize. Therefore, we have $(x^n) = (x^{n+1})$ for some n. Therefore, there is a unit u such that $ux^{n+1} = x^n$ and thus $(ux - 1)x^n = 0$. In particular, $(ux - 1)x^n \in \mathfrak{p}$ but $x \notin \mathfrak{p}$ so $ux - 1 \in \mathfrak{p}$ proving that $ux = 1$ in $A/\mathfrak{p}$ so $A/\mathfrak{p}$ is a field.

Now consider a list of maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3, \ldots$. Consider the descending chain,

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \cdots$$

This must stabilize at some point meaning that $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n\mathfrak{m}_{n+1}$. Therefore, $\mathfrak{m}_{n+1} \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n$ which implies that $\mathfrak{m}_{n+1} \supset \mathfrak{m}_i$ for some $i \in \{1, \ldots, n\}$ and therefore there can only be finitely many maximal ideals.

6.5 5

Exercise 6.5.1. Let K be an algebraically closed field and $V \subset K^n$ and $W \subset K^m$ be irrediculbe algebraic sets. Prove that $V \times W \subset K^{n+m}$ is an irreducible algebraic set.

This is equivalent to the question, given two finite type K-algebra domains A, B why is $A \otimes_K B$ a domain. By Noetherian normalization, we may write $A \supset K[x_1, \ldots, x_a]$ and $B \supset K[y_1, \ldots, y_b]$ as integral extensions where $a = \operatorname{trdeg}_K(\operatorname{Frac}(A))$ and $b = \operatorname{trdeg}_K(\operatorname{Frac}(B))$. Consider,

$$A \otimes_K B \supset K[x_1, \ldots, x_a, y_1, \ldots, y_b]$$

which is an integral extension because it factors as,

$$A \otimes_K B \supset A \otimes_K K[y_1, \ldots, y_b] \supset K[x_1, \ldots, x_a, y_1, \ldots, y_b]$$

and base change and composition of integral extensions are integral. It suffices to show that there is a unique point in the fiber over each closed point since each component must map surjectively

for an integral extension. Let $S = K[x_1, \ldots, x_a, y_1, \ldots, y_b]$ and let $\mathfrak{m} \subset S$ be a maximal ideal $\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_a - \alpha_a, y_1 - \beta_1, \ldots, y_b - \beta_b)$ where we are using that K is algebraically closed. Then,

$$A \otimes_K B \otimes_S S/\mathfrak{m} = (A \otimes_{S_1} S_1/\mathfrak{m}_1) \otimes_K (B \otimes_{S_2} S_2/\mathfrak{m})$$

where $S_1 = K[x_1, \ldots, x_a]$ and $S_2 = K[y_1, \ldots, y_b]$ and $\mathfrak{m}_1 = (x_1 - \alpha_1, \ldots, x_a - \alpha_a)$ and $\mathfrak{m}_2 = (y_1 - \beta_1, \ldots, y_b - \beta_b)$. Then $A \otimes_{S_1} S_1/\mathfrak{m} = K$ because it is a field since A is a domain integral over the domain S_1 there is a lying over property by Cohen's theorem so $A \otimes_{S_1} S_1/\mathfrak{m}_1$ is a finitely generated K-algebra and a field meaning that $A \otimes_{S_1} S_1/\mathfrak{m}_1 = K$ by the nullstellensatz. Likewise $B \otimes_{S_2} S_2/\mathfrak{m}_2 = K$ and therefore,

$$A \otimes_K B \otimes_S S/\mathfrak{m} = K \otimes_K K = K$$

and therefore $A \otimes_K B$ must be a domain.

A better way to do this proof it to notice that $A \supset S_1$ satisfies the conditions for going up and going down because it is an integral extension, A is a domain, and S_1 is a normal domain.

7 Fall 2011 Part I

7.1 1

Let p be a prime, $G = \mathrm{GL}_3(\mathbb{Z}/p^5\mathbb{Z})$.

7.1.1 a

Consider the map $\varphi : G \to \mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$ which is surjective because any lift of a matrix over $\mathbb{Z}/p\mathbb{Z}$ will have determinant which reduces to a unit modulo p and thus is a unit in $\mathbb{Z}/p^5\mathbb{Z}$. Furthermore, $\ker\varphi = I + pM_3$ where M_3 is the set of matrices over $\mathbb{Z}/p^4\mathbb{Z}$. Therefore, $|\ker\varphi| = (p^4)^9 = p^{4\cdot 9}$.

7.1.2 b

From the exact sequence,

$$1 \longrightarrow I + pM_3 \longrightarrow G \longrightarrow \mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 1$$

we see,

$$|G| = |\ker\varphi| \cdot |\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})| = p^{4\cdot 9} \cdot (p^3 - 1)(p^3 - p)(p^3 - p^2) = p^{4\cdot 9+3} \cdot (p^3 - 1)(p^2 - 1)(p - 1)$$

Consider $P = (I + pM_3)U$ where U is the group of upper triangular matrices. Then since $N = I + pM_3$ is normal we have,

$$NU/N \cong U/U \cap N$$

and thus $|P| = |U| \cdot |N|/|U \cap N|$. However, $U \cap N$ is upper triangular matrices divisible by p. Then $|U| = p^{5\cdot 3}$ and $|U \cap N| = p^{4\cdot 3}$ and therefore,

$$|P| = p^{5\cdot 3} \cdot p^{4\cdot 9}/p^{4\cdot 3} = p^{4\cdot 9+3}$$

and therefore this is an explicit Sylow p-subgroup.

7.2 2

Let $G = \mathrm{SL}_2(\mathbb{F}_3)$ which has order 24.

7.2.1 a

Consider the action of G on $\mathbb{P}^1_{\mathbb{F}_3}$ which acts through $\mathrm{PSL}_2(\mathbb{F}_3) = G/\{\pm 1\}$. We know that the action is transitive and faithful and $\mathbb{P}^1_{\mathbb{F}_3}$ has 4 elements so $\mathrm{PSL}_2(\mathbb{F}_3)$ is isomorphic to a transitive subgroup of S_4. However, $|\mathrm{PSL}_2(\mathbb{F}_3)| = |G|/2 = 12$ and the only subgroup of S_4 of index 2 is A_4 so $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$.

7.2.2 b

We know that G has 7 conjugacy classes and thus 7 irreducible representations. Let these have dimensions $d_1, \ldots, d_7$ then,

$$d_1^2 + \cdots + d_7^2 = 24$$

with $d_1 = 1$. Now $Q = G/\{\pm 1\}$-reps are exactly G-reps with -1 acting trivially. Furthermore, if V is an irreducible Q-rep then Q is irreducible as a G-rep because any G-invariant subspace would also be Q-invariant.

Now consider the rep theory of A_4. We know that A_4 has a 3-dimensional representation then then $12 - 3^2 = 3$ so there must be three additional one-dimensional representations. Thus G must have at least three one-dimensional representations and one three-dimensional representation. Thus,

$$24 - 3^2 - 3 = 12$$

Now there are three remaining representations so how can,

$$d_1^2 + d_2^2 + d_3^2 = 12$$

Well the only way is for $d_1 = d_2 = d_3 = 2$ proving that G has three representations of dimension two.

7.3 3

7.3.1 a

Let R be a commutative Noetherian domain. Let $x \in R$ be a nonzero nonunit. Let P be the poset of nonzero nonunit elements of R modulo units under divisibility i.e. $x \leq y \iff y \mid x \iff (x) \subset (y)$ (equivalently the poset of principal proper ideals). Consider a totally ordered chain $\{x_i\}_{i \in I} \subset P$. By the noetherian hypothesis every ascending chain in P is finite. Therefore by Zorn's lemma (actually a weakening using the axiom of dependent choice) we see that each $x \in P$ has a maximal element y such that $x \leq y$. If we write $y = y_1 y_2$ where y_1 is a nonunit then $(y) \subsetneq (y_1)$ so y is not maximal unless $(y_1) = (y)$ i.e. y_2 is a unit. Thus y is irreducible and we can write $x = yx_1$. Repeating this process we get a chain $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$ which must stabilize at some point meaning that x_{i+1} is a unit. Therefore, $x = y_1 y_2 \cdots y_{i+1} x_{i+1}$ is a product of irreducibles.

7.3.2 b

Let R be a commutative Noetherian ring. Let $I \subsetneq R$ be a proper ideal. Replacing R with R/I we may assume that $I = (0)$ and we need to show that there is a finite set of primes $\mathbb{P}_1, \ldots, \mathbb{P}_r \subset R$ such that $\mathbb{P}_1 \cdots \mathbb{P}_r = (0)$. Because R is Noetherian, we know that it has finitely many associated primes amoung which are the minimal primes. Therefore,

$$\operatorname{nilrad}(R) = \bigcap_{P \in \operatorname{Ass}_R(R)} P$$

However, $\operatorname{nilrad}(R) \subset R$ is finitely generated and each generator is nilpotent so for some n we know that $(\operatorname{nilrad}(R))^n = (0)$. Thus, if $P_1, \ldots, P_r \in \operatorname{Ass}_R(R)$ are the associated primes then,

$$P_1^n \cdots P_r^n \subset \left(\bigcap P\right)^n \subset (\operatorname{nilrad}(R))^n = (0)$$

7.4 4

Let G be a finite group and $H \subset G$ a subgroup of index 2.

7.4.1 a

Let V be an irreducible complex G-rep. Then,

$$\operatorname{Hom}_H\left(\operatorname{Res}_H^G(V), \operatorname{Res}_H^G(V)\right) = \operatorname{Hom}_G\left(V, \operatorname{Ind}_H^G\left(\operatorname{Res}_H^G(V)\right)\right)$$

we know that there is an embedding $V \to \operatorname{Ind}_H^G\left(\operatorname{Res}_H^G(V)\right)$. Because,

$$\dim \operatorname{Ind}_H^G\left(\operatorname{Res}_H^G(V)\right) = 2 \dim V$$

we see that $\operatorname{Ind}_H^G\left(\operatorname{Res}_H^G(V)\right)$ contains either one or two copies of V and therefore since V is irreducible,

$$\operatorname{Hom}_H\left(\operatorname{Res}_H^G(V), \operatorname{Res}_H^G(V)\right) = \operatorname{Hom}_G\left(V, \operatorname{Ind}_H^G\left(\operatorname{Res}_H^G(V)\right)\right)$$

has either dimension 1, in which case $\operatorname{Res}_H^G(V)$ is irreducible, or dimension 2 in which case $\operatorname{Res}_H^G(V)$ must split into two distinct irreps (since if they were equal it would have dimension 4).

7.4.2 b

Assume that whenever two elements of H are conjugate in G then they are conjugate in H. Since $H \subset G$ has index 2 it is normal and thus G/H acts on the subrepresentations of $\operatorname{Res}_H^G(V)$. However, we know that if $\operatorname{Res}_H^G(V)$ is reducible then,

$$\operatorname{Res}_H^G(V) = V_1 \oplus V_2$$

and the action cannot have any fixed points because V is irreducible so $g \cdot V_1 \cong g * V_1 \cong V_2$. However, $\chi_{g*V_1}(h) = \chi_{V_1}(g^{-1}hg)$ but if $h' = g^{-1}hg$ then h' and h are conjugate in H and thus $\chi_{g*V_1}(h) = \chi_{V_1}(h)$ meaning that V_1 and V_2 have the same characters contradicting the fact that they are nonisomorphic. Thus $\operatorname{Res}_H^G(V)$ is irreducible.

7.5 5

Let p be a prime.

7.5.1 a

Consider the projective resolution,

$$\cdots \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\times p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\times p} \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

where $\mathbb{Z}/p^2\mathbb{Z}$ is a free and thus projective $\mathbb{Z}/p^2\mathbb{Z}$-module. Then we can compute the cohomology of the complex after applying $\mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(-, \mathbb{Z}/p\mathbb{Z})$ to get,

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\times p} \mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \cdots$$

which equals the complex,

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{0} \mathbb{Z}/p\mathbb{Z} \longrightarrow \cdots$$

Therefore,

$$\mathrm{Ext}^i_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$$

for all $i \geq 0$.

7.5.2 b

To prove that $\mathbb{Z}/p^2\mathbb{Z}$ is injective it suffices to show that $\mathrm{Ext}^1_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z}) = 0$. Using the above complex we have to take the cohomology of,

$$0 \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\times p} \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \cdots$$

giving,

$$\mathrm{Ext}^0_{\mathbb{Z}/p^2\mathbb{Z}}\left(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z}\right) = \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad \mathrm{Ext}^1_{\mathbb{Z}/p^2\mathbb{Z}}\left(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z}\right) = 0$$

Now we can choose an injective resolution,

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\times p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\times p} \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \cdots$$

Now we apply the functor $\mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, -)$ to find,

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\times p} \mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z}) \longrightarrow \cdots$$

which equals,

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{0} \mathbb{Z}/p\mathbb{Z} \longrightarrow \cdots$$

and therefore,

$$\mathrm{Ext}^i_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$$

for all $i \geq 0$.

8 Fall 2011 Part II

8.1 1

Let M be a finitely generated nonzero module ocer a commutative ring R and let $I \subset R$ be an ideal.

8.1.1 a

Let $\varphi : M \to M$ be an R-linear map with $\varphi(M) \subset IM$. Then consider the diagram,

$$\begin{array}{ccccc} R^n & \overset{\tilde{\varphi}}{\dashrightarrow} & I \cdot R^n & \hookrightarrow & R^n \\ \downarrow\pi & & \downarrow\pi & & \downarrow\pi \\ M & \xrightarrow{\varphi} & IM & \hookrightarrow & M \end{array}$$

which lifts $\tilde{\varphi} : R^n \to I \cdot R^n \subset R^n$. Thus $\tilde{\varphi}$ is given by a matrix with coefficients a_{ij} in I. Then its characteristic polynomial,

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

has $a_i \in I^i$ because a_i is a polynomial in a_{ij} of degree i. By Cayley-Hamilton,

$$\tilde{\varphi}^n + a_1 \tilde{\varphi}^{n-1} + \cdots + a_n = 0$$

Thus,

$$\pi \circ (\tilde{\varphi}^n + a_1 \tilde{\varphi}^{n-1} + \cdots + a_n) = 0$$

but $\pi \circ \tilde{\varphi} = \varphi \circ \pi$ and thus,

$$(\varphi^n + a_1 \varphi^{n-1} + \cdots + a_n) \circ \pi = 0$$

but π is surjective so we see that,

$$\varphi^n + a_1 \varphi^{n-1} + \cdots + a_n = 0$$

8.1.2 b

If $IM = M$ then we can consider $\varphi = 1$ in the previous proposition to get that,

$$1 + a = 0$$

in $\operatorname{End}(R) M$ where $a \in I$ and thus $(1 + a)M = 0$ for some $a \in I$. Then if $I \subset \operatorname{Jac}(R)$ then $1 + a$ is a unit so if $(1 + a)M = 0$ then $M = 9$. Therefore $IM \neq M$ if $M \neq 0$.

8.2 4

Let A be a finitely generated k-algebra domain and G a finite group acting on A as a k-algebra.

8.2.1 a

Consider $A^G \subset A$. For any $a \in A$ consider the polynomial,

$$f(X) = \prod_{g \in G} (X - g(a))$$

which is invariant under G and therefore $f \in A^G[X]$ and is also clearly monic so a is integral over A^G since $f(a) = 0$. Therefore $A^G \subset A$ is integral.

Then I claim that actually $A^G \subset A$ is finite. Indeed, choose a finite set $x_1, \ldots, x_n \in A$ that generate as a k-algebra then each x_1 is integral over A^G so $A^G[x_1]$ is finite over A^G and continuing we see that $A = A^G[x_1, \ldots, x_n]$ is finite over A^G.

8.2.2 b

Let R be a Noetherian ring. We need to prove that if $B \subset A$ is a finite extension of R-algebra domains and A is a finitely generated R-algebra then B is a finitely generated R-algebra.

Let $x_1, \ldots, x_n \in A$ generate as a R-algebra. Each x_i is integral over B and therefore satisfies some monic polynomial,

$$x_i^{d_i} + \cdots + a_{i0} = 0$$

then consider the subalgebra C generated by the coefficients $a_{i0} \in B$ thus $C \subset B$ but each x_i is integral over C by assumption. Thus A is a finite C-module. Since R is Noetherian we see that A and C are also noetherian so B is a finite C-module because submodules of finite modules are finite over a Noetherian ring. Therefore we just need to show that if $A \subset B$ is finite and A is a finite type R-algebra then B is a finite type A-algebra.

Indeed, we have $R[x_1, \ldots, x_n] \twoheadrightarrow A$ as R-algebras and $A^r \twoheadrightarrow B$ as A-modules and thus $A[y_1, \ldots, y_r] \twoheadrightarrow B$ as A-algebras and thus $R[x_1, \ldots, x_n, y_1, \ldots, y_r] \twoheadrightarrow B$ as R-algebras.

8.3 3

Let $G \subset \mathrm{GL}_n(K)$ be a finite p-group where K is a field of characteristic p. Consider the standard action of G on K^n. First consider $Z(G) \subset G$ which is a nontrivial abelian p-group. In the case $n = 1$ the group consists of p-power roots of unity which are trivial because the Frobenius is injective. In the case $n > 1$ for any $A \in Z(G)$ notice that $A^{p^k} = I$ for some k so $(A - I)^{p^k} = 0$ and therefore A admits an eigenvector $v_A \neq 0$. We need to show that there is a simultaneous eigenvector for all $A \in Z(G)$. Since $AB = BA$ for all $A, B \in G$ this shows that $V_A = \{v \in K^n \mid Av = v\}$ is a $Z(G)$-representation and therefore by the same argument B has an eigenvector in V_A and repeating for each generator gives a fixed point of K^n under $Z(G)$.

Now, take $A \in Z(G)$ then I claim that V_A is a G-invariant subspace. Indeed, for any $B \in G$ we have $A(Bv) = BAv = Bv$ so $Bv \in V_A$. Therefore, $G/Z(G)$ acts on V_A. Since $(A - I)^{p^k} = 0$ we know that V_A is nonempty and $G/Z(G)$ has strictly smaller order. Thus by induction we conclude that V_A has a $G/Z(G)$-invariant vector and thus V has a G-invariant vector.

8.4 5

Suppose that the polynomial,

$$f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$$

is irreducible over $\mathbb{Q}$. Notice that $f(X)$ has roots of the form $\pm\alpha, \pm\beta$. Let E denote the splitting field of f and $G = \mathrm{Gal}\,(E/\mathbb{Q})$.

8.4.1 a

Since f is irreducible we know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ since $f(\alpha) = 0$. It is clear that $E = \mathbb{Q}(\alpha, \beta)$ and thus,

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

Therefore we need to consider $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$. We know that $f = (X - \alpha)(X + \alpha)q$ where $q \in \mathbb{Q}(\alpha)[X]$ is quadratic. Therefore, if q is irreducible then $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. Otherwise q splits and then $\beta \in \mathbb{Q}(\alpha)$ so we find that either $[E : \mathbb{Q}] = 8$ or $[E : \mathbb{Q}] = 4$.

Now in the case that $|G| = 4$ we know that G acts transitively on the roots because f is irreducible. Then by the orbit stabilizer theorem, as G-sets, the set of roots X is isomorphic to G/G_x for any fixed $x \in X$. But $|G| = |X| = 4$ so $G_x = \{e\}$ showing that each nonzero $g \in G$ has no fixed points.

8.4.2 b

First notice that,

$$\alpha = \sqrt{\frac{-a + \sqrt{a^2 - 4b}}{2}} \quad \beta = \sqrt{\frac{-a - \sqrt{a^2 - 4b}}{2}}$$

Thus,

$$\alpha^2 - \beta^2 = \sqrt{a^2 - 4b}$$

moreover,

$$\alpha^2\beta^2 = b$$

thus $\sqrt{b} = \alpha\beta \in E$.

Suppose that $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ then for each $\sigma \in G$ either $\sigma(\alpha) = -\alpha, \beta, -\beta$. In the first case $\sigma(\alpha) = -\alpha$ then $\sigma(\beta) = -\beta$ because it cannot have a fixed point and thus $\sigma(\sqrt{b}) = \sqrt{b}$. If $\sigma(\alpha) = \pm\beta$ then $\sigma(\beta) = \pm\alpha$ because σ has order two and thus $\sigma(\sqrt{b}) = \sqrt{b}$. Thus $\sqrt{b} \in K^G = \mathbb{Q}$ proving that $b \in \mathbb{Q}$ is a square.

If b is a square then $\alpha\beta = \sqrt{b} \in \mathbb{Q}$ must be fixed under the Galois group. Therefore, G cannot contain an element of order 4 because these would send $\alpha\beta \mapsto -\alpha\beta$.

8.4.3 c

Consider,

$$\delta = \sqrt{\frac{a^2 - 4b}{b}} = \frac{\alpha^2 - \beta^2}{\alpha\beta}$$

If $G = \mathbb{Z}/4\mathbb{Z}$ then the generator $\sigma \in G$ acts via a cyclic permutation of the roots. Up to a choice of generator we can assume this permutation is $\alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha$. Therefore,

$$\sigma(\delta) = \frac{\beta^2 - \alpha^2}{-\alpha\beta} = \delta$$

and thus $\delta \in K^G = \mathbb{Q}$ proving that,

$$\delta^2 = \frac{a^2 - 4b}{b}$$

is a square in $\mathbb{Q}$.

Conversely, if $\frac{a^2-4b}{b}$ is a square in $\mathbb{Q}$. Then we must have $\delta \in \mathbb{Q}$ and thus it is fixed under G. However, if $G = (\mathbb{Z}/2\mathbb{Z})$ then there must be the element $\alpha \mapsto \beta$ and $-\alpha \mapsto -\beta$ because there would be three distinct order two elements which sends $\delta \mapsto -\delta$ which we cannot have. Thus $G = \mathbb{Z}/4\mathbb{Z}$.

9 Spring 2011 Part I

9.1 1

9.1.1 a

Let G be a finite group and $H \subset G$ a proper subgroup. Suppose that,

$$G = \bigcup_{g \in G} gHg^{-1}$$

There are at most $[G : H]$ conjugates and each has $|H|$ elements but these are not distinct because each contains e so the number of elements on the right is less than $|H|[G : H] = |G|$ giving a contradiction.

9.1.2 b

Suppose G is a finie transitive group of permutation of a finite set X of n objects, $n > 1$. Let $H = G_{x_0}$ be the subgroup of elements that fix x_0 then the conjugates are the subgroups fixing each element $i \in X$ since G acts transitively on X. Since $n > 1$ and G acts transitively we must have that H is a proper subgroup. Therefore by part (a) there is some element $g \in G$ which lies in no conjugate and thus fixes no element of X.

9.2 2

9.2.1 a

LEt ζ be a complex primitive root of $X^{25} - 1$. We know $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(25) = 5 \cdot 4$. Then if $x^5 - 5$ has a root in $\mathbb{Q}(\zeta)$ then it has every root so we would have the splitting field $E \subset \mathbb{Q}(\zeta)$ of $x^5 - 5$. However, the splitting field $E = \mathbb{Q}(\zeta_5, \sqrt[5]{5})$ which has Galois group D_{10} which is nonabelian but $\mathbb{Q}(\zeta)$ is abelian giving a contradiction.

9.2.2 b HOW TO DO THIS??

If $\alpha^5 = 5$ then consider $E = \mathbb{Q}(\zeta, \alpha)$ and suppose that $\beta^5 = \alpha$. Then E is the splitting field of $x^{25} - 5$.

9.3 3

9.3.1 a

Exercise 9.3.1. Let $q = p^n$ with p prime. How many monic irreducible polynomials of degree 2 are there over $\mathbb{F}_q$? How many of degree 3?

Monic irreducible polynomials correspond to Galois orbits of elements of a algebraic extensions of $\mathbb{F}_q$. Since for every $\alpha \in \overline{\mathbb{F}_q}$ of degree 2 we know that $\alpha \in \mathbb{F}_{q^2}$ we just need to determine the number of Galois orbits in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. There are $(q^2 - q)/2 = q(q-1)/2$ such orbits.

Furthermore, every element $\beta \in \overline{\mathbb{F}_q}$ is degree 3 lies in $\mathbb{F}_{q^3}$ and therefore we just need to consider the number of Galois orbits in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ of which there are $q^3 - q/3 = q(q-1)(q+1)/3$.

9.3.2 b

Consider the group $G = \mathrm{GL}_3(\mathbb{F}_q)$. In each conjugacy class there is a unique element in canonical form,

$$\mathbb{F}_q^3 \cong \mathbb{F}_q[T]/(a_1) \oplus \cdots \oplus \mathbb{F}_q[T]/(a_n)$$

with $a_1 \mid a_2 \mid a_3$ and all are monic. There are three cases. Either $n = 1$ and $\deg a_1 = 3$ or $n = 2$ and $\deg a_1 = 1$ is a linear factor of a_2 with $\deg a_2 = 2$. In the first case, either a_1 is irreducible in which case there are $q(q-1)(q+1)/3$ or it splits into a linear and a quadratic in which case there are $q(q-1)^2/2$ possibilities (none of the roots can be zero since T is invertible) or it totally splits in which case there are $\binom{q-1}{3} + 2\binom{q-1}{2} + (q-1) = (q-1)(q-2)(q-3)/6 + (q-1)^2(q-2) + (q-1)$ possibilities. In the second case, a_2 must so there are $(q-1)^2$ possibilities and then a_1 must be one of the two factors. Therefore we get $(q-1)^2$ taking into account the case that both factors are the same. Finally, it is possible for $a_1 = a_2 = a_3$ are all linear giving $(q-1)$ possibilities. Thus in total there are,

$$q(q-1)(q+1)/3 + q(q-1)^2/2 + (q-1)(q-2)(q-3)/6 + (q-1)^2(q-2) + (q-1) + 2(q-1)^2 + (q-1) = q(q^2-1)$$

conjugacy classes.

9.4 4

9.4.1 a

Let K be algebraically closed. Suppose that $S \subset K^n$ is the set of common zeros of $\{f_i\} \subset K[x_1, \ldots, x_n]$ and thus $S = Z(I)$ with $I = (f_i)$. Suppose that,

$$r = \frac{g}{d} \in K(x_1, \ldots, x_n)$$

is a rational function such that the polynomial d is non-zero at all points of S thus r defines a K-valued rational function on S. Since d does not vanish on S we know that $I' = I + (d)$ has no common zeros and thus by the Nullstellensatz, $I' = (1)$ and therefore we can write,

$$qd + g_1 f_1 + \cdots + g_r f_r = 1$$

Therefore, let $h = gq$ and then,

$$h(x) = g(x)q(x) = \frac{g(x)}{d(x)}[1 - (g_1(x)f_1(x) + \cdots + g_r(x)f_r(x))]$$

but $f_i(x) = 0$ for all $x \in S$ and thus $h(x) = r(x)$.

9.4.2 b

Let $k = \mathbb{Q}$ and $f_1 = x^2 + y^2 - 1$. Consider,

$$r = \frac{1}{y - x}$$

which is well-defined on the vanishing locus of f_1 because $\frac{1}{\sqrt{2}} \notin \mathbb{Q}$. Suppose there were a polynomial $h \in \mathbb{Q}[x, y]$ with $h(x, y) = r(x, y)$ on $S = V(f)$. Then h defines a continuous function $\mathbb{R}^2 \to \mathbb{R}$ and thus on $S^1 \subset \mathbb{R}^2$ it must be bounded because the circle S^1 is compact. However, $r(x, y)$ is unbounded on $S \subset S^1$ by taking rational points on the circle approaching $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$.

Alternatively, if $h(x, y) = r(x, y)$ then $(y-x)h-1$ vanishes on S and thus $(y-x)h-1 = q(x^2+y^2-1)$ but setting $x = y$ we get $1 = -q(2x^2 - 1)$ which is impossible based on degree.

10 Spring 2011 Part II

10.1 1

Let V be a nonzero finite-dimensional vector space over an algebraically clsoed field k and $T : V \to V$ a linear endomorphism.

10.1.1 a

Jordan canonical form says that T is similar to a matrix with block diagonal Jordan blocks unique up to reordering the blocks. Consider V as a $k[T]$-module. Then applying the structure theorem we find that,

$$V \cong k[T]/(a_1) \oplus \cdots \oplus k[T]/(a_n)$$

and each monic polynomial $a_i \in k[T]$ splits into linear factors because k is algebraically closed. Therefore we find that,

$$V \cong \bigoplus_{i=1}^{n} \oplus_{j=1}^{r_i} k[T]/(T - \lambda_{ij})^{n_{ij}}$$

as $k[T]$-modules which proves the existence of Jordan canonical form if we choose the basis $1, (T - \lambda), \ldots, (T - \lambda)^{n-1}$ on each factor giving a Jordan block.

Now uniqueness holds because of the uniqueness of the structure theorem which tells us that the monic polynomials $a_1 \mid \cdots \mid a_n$ are unique and thus so are the roots λ_{ij} and the multiplicities n_{ij}. The only ambiguity is in reordering.

10.1.2 b

If T is diagonalizable with distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ then clear $(T - \lambda_1) \cdots (T - \lambda_r) = 0$ so the minimal polynomial must divide this and thus has no repeated roots. Conversely, suppose that the minimal polynomial m has no repeated roots. Then since $a_1 \mid \cdots \mid a_n = m$ each a_i has no repeated roots and thus the multplicities $n_{ij} = 1$ so the Jordan canonical form is diagonal and thus T is diagonalizable.

11 Fall 2014 Part II

11.1 1 CHECK THIS

Extensions of abelian groups,

$$0 \longrightarrow \mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z}) \longrightarrow G \longrightarrow \mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z}) \longrightarrow 0$$

From the structure theorem for finitely generated abelian groups we can write $G = \mathbb{Z}^r \oplus T$ where T is a product of cyclic groups. Tensoring with $\mathbb{Q}$ we see that $r = 2$ and thus we just need to think about T. We can have $G = \mathbb{Z}^2 \oplus (\mathbb{Z}/3\mathbb{Z})$ or $\mathbb{Z}^2 \oplus (\mathbb{Z}/9\mathbb{Z})$ or $\mathbb{Z}^2 \oplus (\mathbb{Z}/3\mathbb{Z})^2$.

11.2 3

Let G be a finite group and C_1, C_2, C_3 be conjugacy classes in G.

11.2.1 a

Let χ be an irreducible character of G. Consider,

$$\sum_{x\in C_1, y\in C_2, z\in C_3} \rho(xyz) = \left(\sum_{x\in C_1} \rho(x)\right)\left(\sum_{y\in C_2} \rho(y)\right)\left(\sum_{z\in C_3} \rho(z)\right)$$

for the representation $\rho : G \to \mathrm{GL}_V()$. Each factor is a scalar matrix because it commutes with $\rho(g)$ for all $g \in G$ since G acts on C_i by conjugation and V is irreducible. Therefore,

$$\sum_{x\in C_i} \rho(x) = \left(\frac{1}{\chi(1)} \sum_{x\in C_i} \mathrm{tr}\,(\rho x)\right) \cdot I = \frac{\#C_i \chi(C_i)}{\chi(1)} I$$

because $\chi = \mathrm{tr}\,(\rho)$ is constant on C_i. Therefore,

$$\begin{aligned}\sum_{x\in C_1, y\in C_2, z\in C_3} \chi(xyz) &= \mathrm{tr}\left(\left(\sum_{x\in C_i} \rho(x)\right)\right) = \mathrm{tr}\left(\left(\frac{\#C_1\chi(C_1)}{\chi(1)} \cdot \frac{\#C_2\chi(C_2)}{\chi(1)} \cdot \frac{\#C_3\chi(C_3)}{\chi(1)}\right) I\right) \\ &= \frac{\#C_1 \#C_2 \#C_3 \chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)^2}\end{aligned}$$

11.2.2 b

Consider the set $S = \{(x, y, z) \in C_1 \times C_2 \times C_3 \mid xyz = 1\}$. We know that,

$$G \subset \mathbb{C}[G] \hookrightarrow \mathrm{End}\,(V_1) \times \cdots \mathrm{End}\,(V_n)$$

is an embedding where $V_1, \ldots, V_n$ are the irreducible representations. Furthermore, $\chi(g) = \chi(1) \iff \rho(g) = I$. Therefore, $g = 1$ iff $\chi(g) = \chi(1)$ for all χ. Furthermore, by the orthogonality relations, if $g \neq 1$ then,

$$\sum_{\chi} \chi(g) = 0$$

Therefore,

$$\frac{1}{\#G} \sum_{\chi} \chi(1)\chi(xyz) = 1_S$$

which means that,

$$\#S = \frac{1}{\#G} \sum_{x\in C_1, y\in C_2, z\in C_3} \sum_{\chi} \chi(1)\chi(xyz) = \frac{1}{\#G} \sum_{\chi} \chi(1) \sum_{x\in C_1, y\in C_2, z\in C_3} \chi(xyz)$$
$$= \frac{1}{\#G} \sum_{\chi} \frac{\#C_1\#C_2\#C_3\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)} = \frac{\#C_1\#C_2\#C_3}{\#G} \sum_{\chi} \frac{\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)}$$

11.3 4

Let V be a nonzero finite-dimensional vector space over a field F. A linear endomorphism T of V is semi-simple if every T-stable subspace admits a T-stable linear complement.

11.3.1 a

We view V as a $F[T]$-module via the action of T. Then using the structue theorem we find that as $F[T]$-modules,

$$V \cong F[T]/(a_1) \oplus \cdots \oplus F[T]/(a_n)$$

where $a_1 \mid \cdots \mid a_n$. Therefore, we can choose a basis such that T is block diagonal in terms of companion matrices. Now, it is clear that V is semisimple iff each factor $F[T]/(a_i)$ is semi-simple as a $F[T]$-module. This is equivalent to $F[T]/(a_i)$ being a sum of fields or equivalently $F[T]/(a_i)$ having no nilpotents. Since $F[T]$ is a UFD the quotient having no nilpotents is equivalent to each a_i spliting into distinct irreducible factors. Furthermore, the minimal polynomial of T is a_n and since each $a_i \mid a_n$ we see that semi-simplicity is equivalent to a_n splitting into distinct irreducible factors.

If F is algebraically closed then the minimal polynomial splits into linear factors. Therefore semi-simplicity is equivalent to the roots of the minimal polynomial having multiplicity 1 which is the same as T being diagonalizable using the Jordan canonical form.

11.3.2 b

Let F be algebraically closed. Then each a_i splits into linear factors which are either identical or coprime and therefore,

$$V \cong F[T]/(a_1) \oplus \cdots \oplus F[T]/(a_n) \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{r_i} F[T]/(T-\lambda_{ij})^{n_{ij}}$$

where r_i is the number of independent roots of a_i and n_{ij} is the algebraic multiplicity of the root λ_{ij} in a_i. This gives the Jordan canonical form because it shows that T is similar to a block diagonal matrix whose blocks are given by the action of T on,

$$F[T]/(T-\lambda)^n$$

which gives a matrix of the form $\lambda I + N$ where N has a line of off diagonal 1s and thus is nilpotent of degree n (meaning $N^n = 0$ and $N^{n-1} \neq 0$).

Taking the diagonal part S and the off diagonal part N of the Jordan canonical form we see that $T = S + N$. Then $[S, N] = 0$ because within each block (or factor in the decomposition of V) we have that $S = \lambda I$ for the corresponding root and both S and N are sums of operators with respect to this decomposition. Clearly, S is diagonalizable and thus semi-simple. Furthermore, N is nilpotent by construction.

11.3.3 c

Suppose that $T = S' + N'$ then $S + N = S' + N'$ so $S' - S = N - N'$ and thus $S' - S$ is nilpotent and also semi-simple. However, $\ker(S' - S)$ cannot have a complement unless $\ker(S' - S) = V$ because since this is nilpotent the kernel must be nontrivial and every element eventually maps into the kernel under powers thus there cannot be a complementary $S' - S$-stable subspace. Therefore $\ker(S' - S) = V$ meaning that $S' = S$ and thus $N' = N$ so the decomposition is unique.

11.4 5

Let k be an algebraically closed field, and A and B domains that are finite type k-algebras.

11.4.1 a

Let $X = \mathrm{mSpec}(B)$ for $\mathfrak{m} \in X$ let $\mathfrak{m}_x \subset A \otimes_k B$ be the corresponding prime ideal of the form $A \otimes_k \mathfrak{m}_x$ and thus $(A \otimes_k B)/\mathfrak{m}_x = A$ because $B/\mathfrak{m}_x = k$ (since k is algebraically closed and $B/\mathfrak{m}_x$ is a finite extension of k by the nullstellensatz). Let $f \in A \otimes_k B$ be nonzero. If $f = a \otimes b$ then $\bar{f} = a\varphi_x(b)$ where $\varphi_x : B \to B/\mathfrak{m}_x = \mathbb{C}$ and thus is nonzero if $b \notin \mathfrak{m}_x$ which defines a dense open subset $U \subset X$ since $b \neq 0$.

Now let $f = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ then

$$\bar{f} = a_1\varphi_x(b_1) + \cdots + a_n\varphi_x(b_n)$$

Consider the map of modules $k^n \to A$ via $e_i \mapsto a_i$ which gives a map $k^n \to k^r$ where $k^r \cong \mathrm{span}\{\{\}\, a_1, \ldots a_n\}$. Then there are $\ell_i : k^n \to k^r \to k$ such that $v \in k^n$ maps to zero in A iff $\ell_i(v) = 0$ for each i. Therefore,

$$\bar{f} = 0 \iff \ell_i(a_1)\varphi_x(b_1) + \cdots + \ell_i(a_n)\varphi_x(b_n) = \varphi_x(\ell_i(a_1)b_1 + \cdots + \ell_i(a_n)b_n) = 0 \iff \ell_i(a_1)b_1 + \cdots + \ell_i(a_n)b_n \in \mathfrak{m}$$

each $\ell_i(a_1)b_1 + \cdots + \ell_i(a_n)b_n \in \mathfrak{m}_x$ is a closed condition and thus $\bar{f} \neq 0$ is an open condition. Furthermore, because B is a domain to be dense an open must simply be nonempty and if $\bar{f} = 0$ always then $f = 0$ because its image under $\ell_i \otimes_k B : V \otimes_k B \to B$ is zero but $\ell_i : V \to \mathbb{C}$ are mutually injective and thus so are $\ell_i \otimes_k B$ because B is flat over k.

11.4.2 b

Let R be a k-algebra domain. Suppose that $A \otimes_k R$ is not a domain. Then there is $x, y \in A \otimes_k R$ such that $xy = 0$ then write,

$$x = a_1 \otimes r_1 + \cdots + a_n \otimes r_n \quad \text{and} \quad y = a_1' \otimes r_1' + \cdots + a_n' \otimes r_n'$$

and thus $A \otimes_k k[r_1, \ldots, r_n, r_1', \ldots, r_n'] \subset A \otimes_k B$ is not a domain so we may assume that $R = B$ is finitely generated. Then if $f, g \in A \otimes_k B$ with $fg = 0$ then $\bar{f}\bar{g} = 0$ at each $\mathfrak{m}_x$ but B is a domain so $\bar{f} = 0$ or $\bar{g} = 0$ but there are dense opens $U_f, U_g \subset X$ such that $\bar{f} \neq 0$ on U_f and $\bar{g} \neq 0$ on U_g so $\bar{f}\bar{g} \neq 0$ on $U_f \cap U_g$ which is dense. Thus $A \otimes_k B$ is a domain.

11.4.3 c

Let K/k be an extension of fields. By Noetherian normalization there is an integral extension $k[x_1, \ldots, x_d] \subset A$ where $d = \dim A$. Then $K[x_1, \ldots, x_d] \subset A \otimes_k K$ is also integral so,

$$\dim A \otimes_k K = \dim K[x_1, \ldots, x_d] = \dim A$$

12 Spring 2012 Part I

12.1 1

Let R be a finite-dimensional k-algebra.

12.1.1 a

Let R be a commuatvie integral domain. Then the multiplication map $x : R \to R$ for each $x \neq 0$ is injective since R is a domain. Thus because R is a finite k-vector space it is also surjective so there is some $y \in R$ such that $xy = 1$ and thus R is a field.

12.1.2 b

Suppose that R is not commutative. Suppose that $rs = 1$. There is an embedding $R \subset \operatorname{End}(k) R$ as k-algebras. Then if $rs = 1$ as matrices then $sr = 1$ as well so this equation holds in R. Now I will prove this claim. We see that r and s are bijective linear maps and thus $s : R \to R$ is surjective so there is some $t \in R$ such that $st = 1$. Then $t = (rs)t = r(st) = r$ and thus $st = sr = 1$.

12.2 4

Let G be a finite group and F a field and V a nonzero finite-dimensional F-linear G-rep.

12.2.1 a

Consider $G = \mathbb{Z}/p\mathbb{Z}$ and $F = \mathbb{F}_p$ and $V = \mathbb{F}_p^2$ with the following action,

$$1 \mapsto A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Clearly the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is fixed by the action however there is no G-invariant complement because otherwise this matrix would be diagonalizable (V would split into G-invariant one-dimensional subspaces) but $(A - I)^2 = 0$ and $A - I \neq 0$ so there is no way A can be diagonalizable.

12.2.2 b

Suppose $|G|$ is nonzero in F. It suffices to show that for any $W \subset V$ subrepresentation there is a G-invariant projection because then its kernel is a G-invariant complement. It suffices to construct a projection map $V \to V^G$ and then apply this to $\operatorname{Hom}(V, W)$ to get a G-invariant projection. Consider,

$$v \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot v$$

which clearly is a map $V \to V^G$ which is the identity on V^G. This makes sense because $|G|$ is invertible in F.

13 Spring 2012 Part II

13.1 1

13.1.1 a

Let A be a Noetherian ring then $A[x]$ is Noetherian.

To prove this consider an ideal I. Choose a sequence $f_i \in I \setminus I_i$ of minimal degree where $I_i = (f_0, \ldots, f_{i-1})$. Then the degrees $d_i = \deg f_i$ are increasing because otherwise the smaller degree f_i would have appeared earlier.

Let a_i be the leading coefficent of f_i. Then consider the sequence of ideals,

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

which must stabilize because A is noetherian so there is some N such that for each a_i for $i > N$ we have,

$$a_i = \sum_{j<N} \alpha_i a_i$$

with $\alpha_i \in A$. Therefore, consider,

$$g_i = \sum_{j<N} \alpha_j X^{d_i - d_j} f_j$$

has leading coefficient the same as f_i and thus,

$$f_N - g_N \in I \setminus I_N$$

because $g_N \in I_N$ but $f_N \notin I_N$ has smaller degree contradicting minimality. Thus I must be finitely generated.

13.1.2 b

Let A be Noetherian and $J \subset A$ an ideal. Define,

$$G_J(A) = A \oplus J \oplus J^2 \cdots$$

We know that $J = (x_1, \ldots, x_n)$ because A is Noetherian. There is a surjection of A-algebras,

$$A[x_1, \ldots, x_n] \twoheadrightarrow G_J(A)$$

and therefore $G_J(A)$ is Noetherian.

13.2 3

Let $f : A \to B$ be a ring homomorphism.

13.2.1 a

We say that B is integral over A if each $b \in B$ satisfies some monic polynomial $p \in A[x]$ or equivalently if the subring $A[b] \subset B$ (this means the image of A in B adjoined b) is finite over A.

If $A \to B$ is finite, take $b \in B$ then consider,

$$\begin{array}{ccc} A^n & \xrightarrow{\varphi} & A^n \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ B & \xrightarrow{\times b} & B \end{array}$$

which lifts to a commutative square because A^n is projective. Let $p \in A[x]$ be the characteristic polynomial of φ which is monic. Then $p(\varphi) = 0$ by Cayley-Hamilton and thus $\pi(p(\varphi)) = 0$. However,

$$\pi \circ (a \cdot \varphi^n) = a \cdot \pi(\varphi^n) = a \cdot b^n \cdot \pi$$

by the diagram and therefore because π is surjective we see that since $\pi(p(\varphi)) = 0$ we get that, $p(b) = 0$ in B proving that b is integral.

13.2.2 b

Let $A \to B$ be finite then I claim that $f^*(V(I)) = V(f^{-1}(I))$. First, if $\mathfrak{p}' \supset I$ then $f^{-1}(\mathfrak{p}') \supset f^{-1}(I)$ so $f^*(V(I)) \subset V(f^{-1}(I))$. Then consider $A/f^{-1}(I) \to B/I$ which is finite and injective and whose topoolgical map is $f^* : V(I) \to V(f^{-1}(I))$. Thus it suffices to show that $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective if $A \to B$ is finite and injective. This follows directly from Cohen's theorem. (DO THIS!!)

13.3 4

Let p be an odd prime and ζ_p a primitive p-th root of unity.

13.4 a

We know $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Then $\mathbb{Q}(\zeta_p)$ contains a subfield L whose Galois group over $\mathbb{Q}$ is $\mathbb{Z}/5\mathbb{Z}$ exactly when $\mathbb{Z}/5\mathbb{Z}$ is a quotient of $\mathbb{Z}/(p-1)\mathbb{Z}$ exactly when $5 \mid p-1$.

13.4.1 b

Let $F = \mathbb{Q}(\zeta_n)$ where $n = pq$ for two distinct primes $p, q \equiv 1 \mod 5$ (e.g. take $p = 11$ and $q = 31$). Then,

$$\operatorname{Gal}(F/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/(q-1)\mathbb{Z})$$

Let σ_1 and σ_2 be generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/q\mathbb{Z})^\times$ respectively inside $\operatorname{Gal}(F/\mathbb{Q})$. Then consider $H = \langle \sigma_1^5, \sigma_2^5 \rangle \subset G$ which for $E = F^H$ gives explicitly $H = \operatorname{Gal}(F/E)$ inside $\operatorname{Gal}(F/\mathbb{Q})$. Because the group is abelian, $H \subset G$ is normal and thus $E = F^H$ is Galois over $\mathbb{Q}$ with,

$$\operatorname{Gal}(E/\mathbb{Q}) = G/H = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

13.5 5

13.5.1 a

Let G be a group and $H \subset G$ a subgroup of finite index $n > 0$. Then $G \circlearrowright G/H$ by left multiplication giving a map $G \to S_n$. The kernel is a normal subgroup $N \subset G$. Then $[G : N] = |\operatorname{im}(G \to S_n)| \leq |S_n| = n!$.

13.5.2 b DO THIS PROPERLY

Let G be a group which is generated by two elements. A subgroup $H \subset G$ of index three determines an action $G \circlearrowright G/H$ and thus a homomorphism $\varphi_H : G \to S_3$. Furthermore, $\ker \varphi_H = K_H$ where,

$$K_H = \bigcap_{g \in G} gHg^{-1}$$

Recall that G acts on conjugates of H transitively by conjugation. The stabilizer of H under this action is $N_G(H)$ so if $N_G(H) \subset G$ is normal then $G/N_H(G)$ acts on the conjugates simply transitively. In general, by the orbit-stabilizer theorem there is an isomorphism of G-sets $G/N_G(H) \xrightarrow{\sim} \{gHg^{-1} \mid g \in G\}$ and thus there are exactly $[G : N_H(G)]$ conjugates of H which divides the index $[G : H]$.

Therefore for $[G : H] = 1$ either H is normal or there are exactly three conjugates. Now I claim that if $\varphi_H \sim \varphi_{H'}$ where $\sim$ means they are equal as maps to S_3 up to permuting the set on which S_3 acts i.e. up to inner automorphism then H and H' are conjugate. Indeed, such a map specifies the action up to isomorphism. Since H is the stabilizer of the distinguished point of G/H but an automorphism of the G-set G/H may mess up the distinguished point the stablizer becomes the stabilizer of some coset gH which is just the conjugate gHg^{-1}.

Actually, given any transitive action $\varphi : G \to S_3$ on a the three point set $\{1, 2, 3\}$ we can recover an index three subgroup $H \subset G$ as the stabilizer of 1. However, there is still an ambiguity of how to assign $\{1, 2, 3\}$ to G/H so we need to ignore swapping 2 and 3 and thus only look at maps $G \to S_3$ up to conjugation by $(2\,3)$.

Therefore, we need to count maps $G \to S_3$. Since $G = \langle \sigma, \tau \rangle$ such maps are determined by the images of σ and τ. Furthermore, the image must be transitive since the desired action is transitive. The transitive subgroups of $S_3 = \langle r, f \rangle$ are S_3 and $\langle r \rangle$. There are at most $6 \cdot 6$ possible choices for where to send the generators σ and τ. Now conjugating by the transposition $f = (2\,3)$ only fixes e and f and thus there are $4 \cdot 4/2$ possible maps sending σ and τ to not e and f up to conjugation and 2 maps sending $\sigma \mapsto f$ and 2 maps sending $\tau \mapsto f$ up to conjugation and 1 map sending $\sigma \mapsto e$ and 1 map sending $\tau \mapsto e$ up to conjugation and one additional map sending $\sigma \mapsto e$ and $\tau \mapsto r$ (we cannot send both $\sigma, \tau \mapsto e$ or $\sigma, \tau \mapsto f$ or $\sigma \mapsto e$ and $\tau \mapsto f$ or $\sigma \mapsto f$ and $\tau \mapsto e$ because then the image would not be transitive) so we get at most $8 + 2 + 2 + 1 + 1 + 1 = 17$ maps up to conjugation and thus at most 17 subgroups of index 3.

14 Fall 2012 Part I

14.1 1 DO THIS!!

Let A be an $n \times m$ integer matrix defining a linear map $f_A : \mathbb{Z}^m \to \mathbb{Z}^n$. The transpose then defines $f_{A^\top} : \mathbb{Z}^n \to \mathbb{Z}^m$.

By the normal form for modules over a PID we can choose bases of $\mathbb{Z}^m$ and $\mathbb{Z}^n$ such that A is diagonal and thus $A^\top$ is also diagonal with the same entries proving that their torson (which comes from the nonzero entries on the diagonal) subgroups of the cokernel are equal.

14.2 2 DO THIS FUCKER

Let $G = \mathrm{SL}_n(\mathbb{F}_p)$ for a prime p and an integer $n > 1$.

14.2.1 a

We see that,

$$|G| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})/(p-1) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1)\cdots(p^2 - 1)$$

Consider the standard flag,

$$0 \subset \mathrm{span}\{e_1\} \subset \mathrm{span}\{e_1, e_2\} \subset \cdots \subset \mathrm{span}\{e_1, \ldots, e_n\}$$

Consider the subgroup preserving this flag. This is the subgroup P of upper triangular matrices. Consider the subgroup P of upper triangular matrices with diagonal equal to 1. Then clearly $|P| = p^{\frac{n(n-1)}{2}}$ so this is a Sylow p-subgroup.

14.2.2 b

Consider the subgroup $P_i \subset P$ having zeros up through the i-th off diagonal. Then P_0

14.3 3 DO THIS FUCKER

14.4 4

Let R be a commutative ring.

14.4.1 a

Let $f : M \to M$ be an endomorphism of a finite R-module. Then view M as an $R[T]$-module via the action of $T \cdot m = f(m)$. Then $(T)M = M$ because f is surjective so since M is finite, by Nakayama, there is some $qT \in (T)$ such that $(1 + qT)M = 0$ and therefore for each $m \in M$ if $Tm = 0$ then $(1 + qT)m = 0$ so $m = 0$ and thus f is injective.

14.4.2 b

Suppose that R is Noetherian and $f : R \to R$ is a ring homomorphism. Suppose that $f : R \to R$ is surjective. Consider the ascending chain,

$$\ker f \subset \ker f^2 \subset \ker f^3 \subset \cdots$$

which must stabilize because R is Noetherian. Therefore $\ker f^n = \ker f^{n+1}$ so if $f^{n+1}(x) = 0$ then $f^n(x) = 0$. Since f is surjective, for any $x \in \ker f$ we can choose $y \in R$ such that $x = f^n(y)$ and thus $f(x) = 0$ so $f^{n+1}(y) = 0$ and thus $f^n(y) = 0$ meaning that $x = 0$ so f is injective.

14.4.3 c

Consider $R = k[x_1, x_2, x_3, \dots]$ and the map $R \to R$ sending $x_1 \mapsto 0$ and $x_{i+1} \mapsto x_i$. This is clearly surjective because each x_i is in the image but also clearly not injective because $x_1 \mapsto 0$.

14.5 5 DO THIS FUCKER

14.5.1 a

15 Fall 2012 Part II

15.1 9

Let G be a group, V a nonzero dinite-dimensional vector sapce over an algebraically closed field k and $\rho : G \to \mathrm{GL}(V)$ a representation. Let $E = \mathrm{End}_G V$.

15.1.1 a

If V is decomposable then the map $V_1 \oplus V_2 \to V_1 \oplus V_2$ given by $\mathrm{id} : V_1 \to V_1$ and $0 : V_1 \to V_2$ and $0 : V_2 \to V_1 \oplus V_2$ is not of the required form.

Now suppose that V is not decomposable. Let $T \in E$ then T has some eigenvector $\lambda \in k$ because k is algebraically closed. Then $V_\lambda^{(n)} = \ker (T - \lambda I)^n$ are nontrivial G-subrepresentations. If $V_\lambda^{(n+1)} = V_\lambda^{(n)}$ then if $(T - \lambda I)v \in V_\lambda^{(n)}$ then $(T - \lambda I)^{n+1} v = 0$ so $v \in V_\lambda^{(n+1)} = V_\lambda^{(n)}$ and thus $(T - \lambda I)^n$ decomposes V into $V_\lambda^{(n)}$ and $\mathrm{im}\,(T - \lambda I)^n$ since if $v \in \mathrm{im}\,(T - \lambda I)^n \cap V_\lambda^{(n)}$ then $v = (T - \lambda I)^n u$ and thus $u \in V_\lambda^{(n)}$ so $v = 0$. Furthermore since $T - \lambda I \in \mathrm{End}_G(V)$ this gives a decomposition of V. Since we know that $V_\lambda^{(n)}$ is nontrivial we must have $V_\lambda^{(n)} = V$ and thus $(T - \lambda I)^n = 0$ proving the claim.

15.1.2 b

Suppose that V is not decomposable. For any $T \in E$ we can write $T = \lambda I + N$. If $\lambda = 0$ then T is nilpotent. If $\lambda \neq 0$ then $(T - \lambda I)^n = 0$ and therefore,

$$T^{-1} = (T - \lambda I + \lambda I)^{-1} = \lambda^{-1}[I + (I - \lambda^{-1}T) + (I - \lambda^{-1}T)^2 + \cdots + (I - \lambda^{-1}T)^{n-1}]$$

because calling this Q then,

$$(I - \lambda^{-1}T)Q = Q - \lambda^{-1} I \implies TQ = I$$

so T is invertible. Furthermore, let $N \in E$ be nilpotent and $F \in E$. Clearly FN and NF are not invertible since N has a nontrivial kernel and not full rank so FN and NF are nilpotent. Furthermore, for $N, N' \in E$ nilpotent suppose that $N + N'$ is invertible then $F(N + N') = I$ and thus,

$$I - FN = FN'$$

which implies that FN' is invertible since FN is nilpotent giving a contradiction. Therefore $N + N'$ is not invertble and thus nilpotent. Thus the nilpotent elements $I \subset E$ form a subalgebra. Then for any $T = \lambda I + N'$ we have,

$$TN = \lambda N + NN'$$

is nilpotent and,

$$NT = \lambda N + N'N$$

is also nilpotent so the nilpotent matrices form a two sided ideal I.

15.1.3 c BETTER PROOF?

Since E is a finite dimensional F-module we know that $I \subset E$ is also a finite dimensional F-module. Then the chain $I \supset I^2 \supset \cdots$ must stabilize so $I^{n+1} = I^n$ for some n. Then by Nakayama's lemma, there is some $R \in I$ such that $(1-R) \cdot I^n = 0$ but R is nilpotent so $1-R$ is invertible and thus $I^n = 0$.

16 Fall 2013 Part I

16.1 1

Let G be a finite group. Let a G-module be a finite-dimensional $\mathbb{C}[G]$-module.

16.1.1 a

Let $V_1, \ldots, V_h$ be pairwise non-isomorphic irreducible G-modules and,

$$V = \bigoplus_{i=1}^{j} V_i^{\oplus d_i}$$

Then $V \cong \mathbb{C}[G]$ as a $\mathbb{C}[G]$-modules. Then, by Schur's lemma there is no mapping between V_i and V_j for $i \neq j$ so,

$$\operatorname{End}(G)(V) = \bigoplus_{i=1}^{h} \operatorname{Hom}_G\left(V_i^{d_i}, V_i^{d_i}\right) = \bigoplus_{i=1}^{h} M_{d_i}(\mathbb{C})$$

where $\operatorname{Hom}_{\mathscr{G}}\left(V_i^{d_i}, V_i^{d_i}\right) = M_{d_i}(\mathbb{C})$ is given by $d_i \times d_i$ matrices because the G-maps $V_i \to V_i$ are just giving by a scalar by Schur's lemma so the entire map is determined by the matrix of maps between the factors.

16.1.2 b

Suppose that V is a nonzero G-module that is not irreducible. Consider the ring $\operatorname{End}(G) V \otimes V$. Since V is not irreducible there is either $V_1^{\oplus 2} \subset V$ or $V_1 \oplus V_2 \subset V$ where V_1, V_2 are irreps. In these cases either,

$$(V_1 \otimes V_1)^{\oplus 4} \subset V^{\otimes 2}$$

or

$$(V_1 \otimes V_1) \oplus (V_1 \otimes V_2)^{\otimes 2} \oplus (V_2 \otimes V_2) \subset V$$

in either case some irreducible W must be contained in V to some power $d > 1$ (either as $W \subset V_1 \otimes V_1$ or $W \subset V_1 \otimes V_2$). Therefore, $\operatorname{End}(G) W^d \subset \operatorname{End}(G) V$ but $\operatorname{End}(G) W^d = M_d(\mathbb{C})$ which is noncommutative since $d > 1$.

16.2 2

16.2.1 a

Let $\gamma \in \mathrm{GL}_3(\mathbb{Z})$ have finite order. Then γ is diagonalizable over $\mathbb{C}$ and its eigenvalues are roots of unity. Furthermore, the characteristic polynomial of γ is monic $p \in \mathbb{Z}[x]$ of degree 3 so each λ is an algebraic integer of degree 3. Thus we can only have ζ_n if $\phi(n) \leq 3$. Therefore the possible n are $2, 3, 4, 6$. Furthermore, the three eigenvalues must all be roots of the same polynomial of order 3 so we cannot have i and ζ_3 simultaneously. Thus the order $n \leq 6$.

16.2.2 b

Consider the polynomial $x^3 + 1 = 0$. Thus our matrix has $\det A = -1$ and $\mathrm{tr}\,(A) = 0$ so consider,

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

then $\gamma^3 = -I$ so it satisfies our minimal polynomial and thus $\gamma^6 = I$ but $\gamma^2 \neq I$ and $\gamma^3 \neq I$ so γ has order 6.

16.3 3

16.3.1 a

If A is a Dedekind domain and I, J are nonzero ideals. Consider the surjective map $I \otimes_A J \to IJ$ defined by $a \otimes b \mapsto ab$. It suffices to prove that J is a flat A-module since this implies that for any ideal $I \subset A$ we have $I \otimes_A J \to IJ$ an isomorphism. Then for each prime $\mathfrak{p} \subset A$ we have $I_\mathfrak{p} \subset A_\mathfrak{p}$ but $A_\mathfrak{p}$ is a DVR (or a field for $\mathfrak{p} = (0)$) and in particular a PID meaning that $I_\mathfrak{p}$ is principal and thus a free and thus flat. Therefore I is flat since its localization at each prime is flat.

16.3.2 b

Let $A = \mathbb{C}[x, y]$ and $I = J = \mathfrak{m} = (x, y)$. Consider the map,

$$\mathfrak{m} \otimes_A \mathfrak{m} \twoheadrightarrow \mathfrak{m}^2$$

If this map is an isomorphism then after tensoring with $\mathbb{C} \cong A/\mathfrak{m}$ it is still an isomorphism. However,

$$(\mathfrak{m} \otimes_A \mathfrak{m}) \otimes_A A/\mathfrak{m} = (\mathfrak{m} \otimes A/\mathfrak{m}) \otimes_{A/\mathfrak{m}} (\mathfrak{m} \otimes A/\mathfrak{m}) = (\mathbb{C}x \oplus \mathbb{C}y) \otimes_\mathbb{C} (\mathbb{C}x \oplus \mathbb{C}y)$$

is a four dimensional $\mathbb{C}$-vector space. However,

$$\mathfrak{m}^2 \otimes_A A/\mathfrak{m} = \mathbb{C}x^2 \oplus \mathbb{C}xy \oplus \mathbb{C}y^2$$

is three dimensional proving that we cannot have had an isomorphism.

16.4 4

Let $A \subset B$ be commutative rings.

16.4.1 a

We say that B is integral over A if each $b \in B$ satisfies some monic polynomial $p \in A[x]$. Suppose that B is a finite A-module. Then there is a surjection $\pi : A^n \twoheadrightarrow B$. Thus for $b \in B$ consider the diagram,

$$\begin{array}{ccc} A^n & \xrightarrow{\varphi} & A^n \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ B & \xrightarrow{b\cdot} & B \end{array}$$

Let $p \in A[x]$ be the characteristic polynomial of φ which is monic. Then by Cayley-Hamilton $p(\varphi) = 0$. Then, $\pi \circ p(\varphi) = 0$. For each $x \in A^n$ we have,

$$\pi(a \cdot \varphi^n(x)) = a \cdot \pi \circ \varphi^n(x)) = a \cdot b^n \cdot \pi(x)$$

and therefore $p(b) \cdot \pi(x) = 0$ but since π is surjective we have $p(b) = 0$ in b (take $\pi(x) = 1$).

16.4.2 b

Let $A \subset B$ be domains with B integral over A. If A is a field then for each $b \in B$ we know that there is a monic $p \in A[x]$ such that $p(b) = 0$. Then,

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0$$

and therefore,

$$b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = -a_n$$

Therefore,

$$-a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) \cdot b = 1$$

which proves that b is invertible in B and thus B is a field.

Now suppose that B is a field. Then for any $a \in A$ we know that $a^{-1} \in B$ satisfies some polynomial $p \in A[x]$ and thus,

$$a^{-n} + c_1 a^{-n+1} + \cdots + c_n = 0$$

Therefore,

$$a^{-1} = -(c_1 + c_2 a + \cdots + c_n a^{n-1})$$

so we see that $a^{-1} \in A$ and thus A is a field.

16.4.3 c

Let A be a domain with $K = \operatorname{Frac}(A)$. Let L be a finite extension of K. Let B be the set of elements of L which are integral over A. For $b, b' \in B$ we know that $A[b]$ is finite over A and then $A[b, b']$ is finite over $A[b]$ so $A[b, b']$ is finite over A. Therefore $A[b, b']$ is integral over A so $b + b', bb' \in A[b, b']$ are integral over A and thus $B \subset L$ is a subring.

Consider $F = \operatorname{Frac}(B) \subset L$. Let $S = A \setminus \{0\}$ then $K \subset S^{-1}B$ is an integral extension and therefore $S^{-1}B$ is a field but $S^{-1}B \subset F$ and thus $S^{-1}B = F$ because F is a field. Now for each $x \in L$ it satisfies some polynomial $p \in K[x]$ because L/K is fintie so clearing denominators we get $p \in A[x]$ and,

$$c_0 x^n + \cdots + c_n = 0$$

but then let $y = c_0 x$ and thus,

$$y^n + c_1 y^{n-1} + c_2 c_0 y^{n-2} + \cdots + c_n c_0^{n-1} = 0$$

and thus $y \in B$ showing that $x \in F$ and thus $L = F$.

17 Fall 2013 Part II

17.1 1

Let us say that $H \subset G$ is malnormal if $gHg^{-1} \cap H = \{1\}$ for all $g \in G \setminus H$.

Let G be a finite group acting transitively on S. We call G a Frobenious group if no nontrivial element $g \neq 1$ of G fixes more than one element of S.

17.1.1 a

Choose $x \in S$ and set $H = G_x$. If G is Frobenius then $G_x \cap G_y = \{1\}$ for $x \neq y$ since any element of the intersection would fix x and y. However, since the action is transitive these are conjugate subgroups and thus $G_x \cap gG_x g^{-1} = \{1\}$ for each $g \in G \setminus G_x$ so G_x is malnormal. Conversely, if G_x is malnormal and $x \neq y$ then $G_x \cap G_y = \{1\}$ so there is no nontrivial element fixing any pair so G is Frobenius.

17.1.2 b

Let,

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q) \right\} \quad \text{and} \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q) \right\}$$

Let G act on $S = \mathbb{F}_q$ via the action,

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot z = az + b$$

Then $H = G_0$. Furthermore $G \circlearrowright S$ is Frobenius because if $az + b = z$ then $(1-a)z = b$ and thus either $a = 1$ and $b = 0$ or $z = (1-a)^{-1}b$ so if the element is nontrivial then there is a unique fixed point. Therefore by (a) we see that $H = G_0$ is malnormal.

17.2 3

17.2.1 a

Let A, B be local rings and $f : A \to B$ is a flat local map. We want to show that for any A-module N we have $B \otimes_A N = 0$ imply that $N = 0$. First we reduce to the case that N is finitely generated.

If N is not finitely generated then for every $N' \subset N$ finitely generated consider $B \otimes_A N' \subset B \otimes_A N$ (because B is flat it is still injective) but $B \otimes_A N = 0$ so $B \otimes_A N' = 0$ and thus $N' = 0$ proving that $N = 0$ because N' contained an arbitrary element.

Thus we may assume that N is finitely generated. Consider the injection of fields $A/\mathfrak{m}_A \hookrightarrow B/\mathfrak{m}_B$. Now the $A/\mathfrak{m}_A$-module $N \otimes_A A/\mathfrak{m}_A$ is flat because $A/\mathfrak{m}_A$ is a field and thus we get an injection,

$$N \otimes_A A/\mathfrak{m}_A \hookrightarrow N \otimes_A B/\mathfrak{m}_B = (N \otimes_A B) \otimes_B B/\mathfrak{m}_B$$

Since $N \otimes_A B = 0$ we see that $N \otimes_A A/\mathfrak{m}_A = 0$. Therefore $N = \mathfrak{m}_A N$ and N is finitely generated so by Nakayama we see that $N = 0$ proving the claim.

17.2.2 b

Suppose that $f : A \to B$ is faithfully flat. Then f is obviously flat. Take $\mathfrak{p} \in \operatorname{Spec}(A)$ and suppose that it is not in the image of $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$. Then I claim that $B \otimes_A A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = 0$ indeed $\operatorname{Spec}(B \otimes_A A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})$ is the fiber over $\mathfrak{p}$ which we know is empty and thus $B \otimes_A A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = 0$ because it has no prime ideals. This contradicts the fact that $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \neq 0$ proving that f^* must be surjective.

Suppose that $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective. For each $\mathfrak{p} \in \operatorname{Spec}(A)$ choose $\mathfrak{P} \in \operatorname{Spec}(B)$ mapping $\mathfrak{P} \mapsto \mathfrak{p}$ and then we get a local map of local rings $f : A_\mathfrak{p} \to B_\mathfrak{P}$. Since f is flat then $A_\mathfrak{p} \to B_\mathfrak{P}$ is flat because any $A_\mathfrak{p}$-module N is an A-module and $B_\mathfrak{P} \otimes_{A_\mathfrak{p}} N = (B \otimes_A N)_\mathfrak{P}$ which is an exact functor. Therefore, f is faithfully flat in the sense that for any $A_\mathfrak{p}$-module N we have $N \otimes_{A_\mathfrak{p}} B_\mathfrak{P} = 0$ implies that $N = 0$. Then if N is an A-module such that $B \otimes_A N = 0$ then $B_\mathfrak{P} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} = 0$ and thus $N_\mathfrak{p} = 0$ for each prime $\mathfrak{p}$ proving that $N = 0$ and thus f is faithfully flat.

17.2.3 c

Let f be faithfully flat. For submodules $M, M' \subset N$ suppose that $M \otimes_A N \subset M' \otimes_A B$ inside $N \otimes_A B$. Consider the submodule $\tilde{M} = M + M' \subset N$ then $\tilde{M} \otimes_A B = M' \otimes_A B$ inside $N \otimes_A B$. Consider the exact sequence,

$$0 \longrightarrow M' \longrightarrow \tilde{M} \longrightarrow C \longrightarrow 0$$

applying $- \otimes_A B$ we find that $C \otimes_A B = 0$ by flatness and the above equality and thus $C = 0$ by faithful flatness showing that $M' = \tilde{M}$ in N and thus $M \subset M'$ in N.

Therefore, if $f(a) \mid f(a')$ then $a'B \subset aB$. Since $A \to B$ is flat for any ideal $I \subset A$ we have $I \otimes_A B \to IB$ is an isomorphism. Therefore, $a'A \otimes_A B \subset aA \otimes_A B$ and hence $a'A \subset aA$ proving that $a \mid a'$ in A.

17.2.4 4

Let $f \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree 4 with roots $\alpha, \beta, \gamma, \delta$.

17.2.5 a

Consider,

$$g(x) = (x - (\alpha\beta + \gamma\delta))(x - (\alpha\gamma + \beta\delta))(x - (\alpha\delta + \beta\gamma))$$

Notice that this is symmetric in swapping any of the roots $\alpha, \beta, \gamma, \delta$ and therefore the coefficients can be written as a polynomial of the elementary symmetric polynomials in the roots which are in

$\mathbb{Q}$ and thus $g \in \mathbb{Q}[x]$. Furthermore, the discriminant of g is,

$$\begin{aligned}\Delta_g &= (\alpha\beta + \gamma\delta - \alpha\gamma - \beta\delta)^2(\alpha\beta + \gamma\delta - \alpha\delta - \beta\gamma)^2(\alpha\gamma + \beta\delta - \alpha\delta - \beta\gamma)^2 \\ &= (\alpha-\delta)^2(\beta-\gamma)^2(\alpha-\gamma)^2(\beta-\delta)^2(\alpha-\beta)^2(\gamma-\delta)^2 = \Delta_f\end{aligned}$$

so g has the same discriminant as f.

17.2.6 b

If $f \in \mathbb{Z}[x]$ then the roots $\alpha, \beta, \gamma, \delta$ are integral over $\mathbb{Z}$ and therefore sums and products of them are integral over $\mathbb{Z}$ so the coefficients of g are integral over $\mathbb{Z}$ but also the coefficents of g are in $\mathbb{Q}$. Since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ this proves that $g \in \mathbb{Z}[x]$.

17.2.7 c

The Galois group of f over $\mathbb{Q}$ is a subgroup of S_4 because it acts faitfully on the roots since the roots generate the splitting field. A generic polynomial has $G = S_4$. If Δ_f is a square in $\mathbb{Q}$ then generically $G = A_4$ because it must preserve the square root of the discriminant and thus all permutations of the roots must be even. The groups $D_4, Z_4, Z_2 \times Z_2$ are all the transitive subgroups of S_4 and since f is irreducible the action must be transitive on the roots. Thus the Galois group must be amoung these listed groups.

In the case $G = S_4$ the group acts transitively on the three roots of g so g is irreducible. In the case $G = S_4$ the group still acts transitively on the three roots of g so g is irreducible. In the case $G = Z_4$ we get a cyclic permutation $\alpha \mapsto \beta \mapsto \gamma \mapsto \delta$ which sends $\alpha\gamma + \beta\delta \mapsto \beta\delta + \gamma\alpha$ so there is a fixed root and thus g is reducible. In the case $G = D_4$ it contains Z_4 but the swap $\alpha \iff \beta$ does not fix this one root so g is irreducible. In the case $G = Z_2 \times Z_2$ the transpositions $\alpha \iff \beta$ and $\gamma \iff \delta$ fix $\alpha\beta + \gamma\delta$ and thus g is reducible.

17.2.8 5

Let k be an algebraically closed field.

17.2.9 a

One form of the Nullstellensatz states that for any ideal $J \subset k[x_1, \ldots, x_n]$ we have,

$$I(Z(J)) = \sqrt{J}$$

If $J, J' \subset k[x_1, \ldots, x_n]$ are radical ideals such that $J \supset J'$ then it is obious that $Z(J) \subset Z(J')$ since if $f(x) = 0$ for all $f \in J$ then $f(x) = 0$ for all $f \in J'$. Now suppose that $Z(J) \subset Z(J')$ then $I(Z(J)) \supset I(Z(J))$ because if $f(Z(J')) = 0$ then $f(Z(J)) = 0$ because $Z(J) \subset Z(J')$ but then $J = I(Z(J))$ and $J' = I(Z(J))$ so $J \supset J'$.

The maximal ideals of $k[x_1, \ldots, x_n]$ are of the form $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$. By the previous discussion, the maximal ideals must correspond to minimal closed sets which are obviously the points. Then if $Z(J) = \{a\}$ then $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n) \subset J$ so we have equality since $k[x_1, \ldots, x_n]/\mathfrak{m}_a = k$ is a field so $\mathfrak{m}_a$ is already maximal.

17.2.10 b

The Zariski topology on k^n is defined by making the closed sets exactly the vanishing loci of ideals $I \subset k[x_1, \ldots, x_n]$. This is a topology because if $Z_i = Z(I_i)$ are closed then,

$$\bigcap_i Z_i = Z\left(\sum_i I_i\right)$$

and,

$$Z_1 \cup Z_2 = Z(I_1 \cap I_j)$$

17.2.11 c

If P is prime then suppose that $Z(P) = Z(I_1) \cup Z(I_2) = Z(I_1 I_2)$. Then $P = \sqrt{I_1 I_2} \supset I_1 I_2$ and thus $P \supset I_1$ or $P \supset I_2$ by prime avoidance so either $Z(P) = Z(I_1)$ or $Z(P) = Z(I_2)$ so $Z(P)$ is irreducible.

Suppose that $Z(J)$ is irreducible. Then for each $fg \in J$ we know that $Z(J) \subset Z(f) \cup Z(g)$ so either $Z(J) \subset Z(f)$ or $Z(J) \subset Z(g)$ and thus $\sqrt{(f)} \subset J$ or $\sqrt{(g)} \subset J$ and thus $f \in J$ or $g \in J$.

18 Spring 2013 Part I

18.1 1

18.1.1 a

Let $A \subset B$ be nonzero commutative rings where B is integral over A. We will use three properties that hold for integral extensions,

(a) the lying over property: $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective

(b) the going up property: if $\mathfrak{p}' \mapsto \mathfrak{p}$ and $\mathfrak{p} \subset \mathfrak{q}$ then there is $\mathfrak{p}' \subset \mathfrak{q}'$ with $\mathfrak{q}' \mapsto \mathfrak{q}$

(c) the incompatibility property, the primes $\mathfrak{p}' \mapsto \mathfrak{p}$ do not satisfy any inclusions (i.e. the fibers are zero dimensional).

Then given a maximal chain,

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

of primes in A there is a prime $\mathfrak{p}_0' \subset B$ such that $\mathfrak{p}_0' \mapsto \mathfrak{p}_0$ by lying ove. Then by going up there are primes $\mathfrak{p}_i' \subset B$ such that $\mathfrak{p}_i' \subset \mathfrak{p}_{i+1}'$ and $\mathfrak{p}_i' \mapsto \mathfrak{p}_i$. Since $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$ we see that $\mathfrak{p}_i' \neq \mathfrak{p}_{i+1}'$ and thus we get a length n chain in B so $\dim A \leq \dim B$. Furthermore, for a maximal chain,

$$\mathfrak{p}_0' \subsetneq \cdots \subsetneq \mathfrak{p}_n'$$

in B then applying f^* we get,

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

where we know that $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$ because otherwise $\mathfrak{p}_i' \subsetneq \mathfrak{p}_{i+1}'$ both lie over $\mathfrak{p}_i$ which cannot happen by the lying over property. Thus there is a chain in A of length n so $\dim B \leq \dim A$. Therefore $\dim A = \dim B$.

18.1.2 b

Let A be a finite type k-algebra (with k infinite) and a domain. Then there exists a finite injection $k[x_1, \ldots, x_d] \hookrightarrow A$ of k-algebras such that $d = \dim A = \operatorname{trdeg}_k(\operatorname{Frac}(A))$.

(HOW TO PROVE THIS!!)

18.1.3 c

Let K/k be an extension of finite fields and B be a finitely generated k-algebra domain. We know that $B \supset k[x_1, \ldots, x_d]$ is an finite extension where $d = \dim B$ by Noetherian normalization. Then K/k is flat so,

$$K[x_1, \ldots, x_n] \hookrightarrow B \otimes_k K$$

is a finite injection. Thus,

$$\dim B \otimes_k K = \dim K[x_1, \ldots, x_d] = d = \dim B$$

18.2 2

Let $R = \mathbb{Z}[t]$ and make $\mathbb{Z}/n\mathbb{Z}$ an R-module by letting t act through the identity.

18.2.1 a

Consider the finite projective resolution,

$$0 \longrightarrow R \xrightarrow{1 \mapsto (t-1\ -2)} R^2 \xrightarrow{e_1 \mapsto 2\, e_2 \mapsto t-1} R \xrightarrow{t \mapsto 1} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

18.2.2 b

Then we apply the functor $\operatorname{Hom}_R(-, \mathbb{Z}/4\mathbb{Z})$ to this complex to get,

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{1 \mapsto (0\ 2)} (\mathbb{Z}/4\mathbb{Z})^2 \xrightarrow{e_1 \mapsto 2\, e_2 \mapsto 0} \mathbb{Z}/4\mathbb{Z}$$

therefore,

$$\operatorname{Ext}^i_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & i = 0 \\ (\mathbb{Z}/2\mathbb{Z})^2 & i = 1 \\ \mathbb{Z}/2\mathbb{Z} & i = 2 \\ 0 & i > 2 \end{cases}$$

18.3 3

Let $G = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.

18.3.1 a

Consider the exact sequence,

$$1 \longrightarrow I + 3M_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow G \xrightarrow{\varphi} \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow 1$$

therefore,

$$|G| = |I + 3M_2(\mathbb{Z}/3\mathbb{Z})| \cdot |\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 3^4 \cdot (3^2 - 1)(3^2 - 3) = 3^5 \cdot 2^4$$

18.3.2 b

Clearly if the order of $g \in G$ is a power of 3 then its image in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ has order a power of 3. Conversely suppose that $\varphi(g)$ has order a power of 3. Therefore, $g^{3^k} \in \ker \varphi = I + 3M_2(\mathbb{Z}/3\mathbb{Z})$ but every element in there has order dividing 3^4 and thus g has 3-power order.

18.3.3 c

The Sylow 2-subgroup $P \subset G$ maps isomorphically onto its image in $\mathrm{GL}_2(\mathbb{F}_3)$ because it has prime order to the kernel and thus their intersection is trivial.

Therefore, it suffices to show that $P = \mathbb{F}_9^\times \rtimes \mathbb{Z}/2\mathbb{Z}$ has an embedding in $\mathrm{GL}_2(\mathbb{F}_3)$ since $|P| = 2^4$ which is the correct order. We know that $P \subset \mathrm{GL}_2(\mathbb{F}_3)$ as follows. Indeed, $\mathbb{F}_9^\times \hookrightarrow G$ by the action by multiplication on $\mathbb{F}_9$. Furthermore, F acts on $\mathbb{F}_9$ giving the correct group.

18.4 5

(I AM CONFUSED WHAT ABOUT A METRIC IN WHICH CASE MAXIMAL ISOTROPIC IS TRIVIAL)

Let V be a $\mathbb{C}$-vector space of even dimension $2n$ and $B : V \times V : \mathbb{C}$ a symmetric nondegenerate biliear form. Let O_B be the subgroup of $\mathrm{GL}(V)$ preserving B. We say that $W \subset V$ is isotropic if $B(w, w') = 0$ for all $w, w' \in W$.

18.4.1 a

Consider the map $\varphi : V \to W^*$ via $v \mapsto B(v, -)$ then $W^\perp = \ker \varphi$ and likewise this is surjective because B is nondegenerate. Thus,

$$\dim V = \dim W^\perp + \dim W^* = \dim W^\perp + \dim W$$

However if W is coisotropic then $W \subset W^\perp$ so we see that,

$$\dim W \leq n$$

Suppose that $\dim W = n$ and W is isotropic. Then if $W \subset U$ and U is isotropic then $\dim U \leq n$ proving that $U = W$ so W is maximal. Conversely, if W is maximal then consider the biliear form B on $W^\perp/W$ which cannot have any isotropic subspaces or else W would not be maximal. Thus $W = W^\perp$ and therefore $\dim W = n$.

18.4.2 b

Let W be maximal isotropic and suppose that $g \in O_B$ satisfies $gW = W$.

19 Spring 2013 Part II

19.1 1

Let A be a commuative ring and G a finite group of automorphisms of A.

19.1.1 a

For each $a \in A$ consider the polynomial,

$$f(x) = \prod_{\sigma \in G} (x - \sigma(a))$$

which is invariant under G and thus has coefficients in A^G (because they are symmetric polynomials in $\sigma(a)$ for $\sigma \in G$). Furthermore f is clearly monic so $A^G \subset A$ is integral.

19.1.2 b

Let K be an algebraically closed field. It suffices to show that if $f : A \to B$ is an integral extension of commutative rings and $A \to K$ is a map then it extends to $B \to K$. We know that $\varphi : A \to K$ factors through $A/\ker\varphi \hookrightarrow K$ and thus $\ker\varphi = \mathfrak{p}$ is a prime ideal. Thus φ factors as $A \to A/\mathfrak{p} \to \operatorname{Frac}(A/\mathfrak{p}) \to K$ where $A/\ker f$ is a domain and $\operatorname{Frac}(A/\ker f)$. Then $\ker f$ is a prime ideal and $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective so there is some prime $\mathfrak{p}' \in \operatorname{Spec}(B)$ such that $\mathfrak{p} = f^{-1}(\mathfrak{p}')$. Therefore consider the diagram,

$$\begin{array}{ccccccc} B & \longrightarrow & B/\mathfrak{p}' & \longrightarrow & \operatorname{Frac}(B/\mathfrak{p}') & \dashrightarrow & K \\ \uparrow & & \uparrow & & \uparrow & \nearrow & \\ A & \longrightarrow & A/\mathfrak{p} & \longrightarrow & \operatorname{Frac}(A/\mathfrak{p}') & & \end{array}$$

If K is not algebraically closed this is false. For example, let $K = \mathbb{Q}$ and $A = \mathbb{Q}(\sqrt{2})$ with $G = \operatorname{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)$ then $A^G = \mathbb{Q}$ but the identity $\mathrm{id} : \mathbb{Q} \to \mathbb{Q}$ cannot extend to $\mathbb{Q}(\sqrt{2})$ because there is no embedding of fields $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}$.

19.1.3 c

Let $K = \overline{\mathbb{Q}}$ and $A = \mathbb{Q}(\sqrt{2})$ with $G = \operatorname{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)$. Then $A^G = \mathbb{Q}$ and take the unique map $A^G \to K$ via the embedding $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$. However, the are two extensions to $\mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ given by the standard and composing with the nontrivial element of the Galois group to give $\sqrt{2} \mapsto -\sqrt{2}$.

19.2 3

Let G be a non-abelian finite group that is simple.

19.2.1 a DO THIS!!

A_5 is a non-abelian finite simple group. Suppose that $N \subset A_5$ were normal. Then N cannot contain any transposition because otherwise it would contain every transposition by conjugation. Since A_5 contains the 3-cycles and is generated by the 3-cycles.

19.2.2 b

Let G have even order. Suppose that $\rho : G \to \mathrm{GL}_2(\mathbb{C})$ is irreducible. Then $\ker\rho$ is normal and $\ker\rho \neq G$ else the action would be trivial so $\ker\rho = \{e\}$ and thus ρ is faithful.

Since $[G, G] \subset G$ is normal and G is nonabelian we have $G^{\mathrm{ab}} = 0$ and thus the only one-dimensional

representation of G is trivial. Therefore $\det \rho = 1$ so $\rho : G \to \mathrm{SL}_2(\mathbb{C})$ is injective.

Now consider the elements of order two $a \in G$ such that $a^2 = e$. Since $g \mapsto g^{-1}$ pairs all elements such that $g^2 \neq e$ and G has even order there must be an even number of elements with $g^2 = e$ and thus there must be some element $a \in G$ of order two. However, $\rho(a)^2 = \rho(a^2) = \rho(e) = I$ and thus $\rho(a) = -I$ because $\det \rho(a) = 1$ and $\rho(a) \neq I$ since it is injective (the other roots have negative determinant) and thus $\rho(a) \in Z(\mathrm{GL}_2(\mathbb{C}))$ so $a \in Z(G)$ because ρ is injective. Howefer, $Z(G) \subset G$ is normal and $Z(G) \neq G$ because G is nonabelian giving a contradiction.

19.2.3 4

Let K be an algebraically closed subbfield of $\mathbb{C}$ and $J \subset K[x_1, \ldots, x_n]$ an ideal. Let $Z = Z(J)$ in $\mathbb{C}^n$.

19.2.4 a

Suppose that $p \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes on $Z \cap K^n$. The polynomial p defines a continuous map $\mathbb{C}^n \to \mathbb{C}$ (in the Euclidean topology) and since $Z \cap K^n$ is dense in Z because $Z \cap K^n = Z(J)$ and p vanishes on $Z \cap K^n$ then p vanishes on Z.

Let,

$$p(x) = \sum_{i,j} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

Then for each $x \in Z \cap K^n$ we get an equation,

$$\sum_{i,j} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} = 0$$

which is a linear equation in the $a_{i_1,\ldots,i_n}$. Then we can choose a basis $c_\alpha \in \mathbb{C}/K$ then write,

$$a_{i_1,\ldots,i_n} = \sum_\alpha c_\alpha b^\alpha_{i_1,\ldots,i_n}$$

Then we get a system,

$$\sum_\alpha \sum_{i,j} c_\alpha b^\alpha_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} = 0$$

therefore since c_α form a basis each,

$$p_\alpha = \sum_{i,j} b^\alpha_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

vanishes on $Z \cap K^n$ and $p_\alpha \in K[x_1, \ldots, x_n]$ then,

$$p = \sum_\alpha p_\alpha$$

(all the sums are finite because each a sum is finite and there are finitely many coefficients). Therefore, by the Nullstellensatz, $p_\alpha \in J$ and thus p_α vanishes on Z and thus p vanishes on Z.

19.2.5 b

Let Z' be the closure of $Z \cap K^n$ in the Zariski topology on $\mathbb{C}^n$. Since $Z \supset Z \cap K^n$ and Z is closed so $Z \supset Z'$. Then $Z' = Z(J')$ for some ideal $J' \subset \mathbb{C}[x_1, \ldots, x_n]$. If $p \in J'$ then p vanishes on Z' and thus on $Z \cap K^n$ and thus p vanishes on Z so $p \in J$ and thus $J' \subset J$ proving that $Z' = Z(J') \supset Z = Z(J)$ and thus $Z = Z'$.

19.2.6 c

It suffices to show that if $Z \subset \mathbb{C}^n$ is Zariski closed then $Z \cap K^n \subset K^n$ is Zariski closed. If $Z = Z_{\mathbb{C}}(I)$ then there is an ideal $I' \subset K[x_1, \ldots, x_n]$ such that $Z = Z_{\mathbb{C}}(I')$ by the argument in part (1). Then I claim that $Z \cap K^n = Z_K(I')$. Indeed, if $x \in Z \cap K^n$ then $p(x) = 0$ for all $p \in I'$ so $x \in Z_K(I')$. If $x \in Z_K(I')$ then $p(x) = 0$ for all $p \in I'$ so $x \in Z$ but $x \in K^n$ by definition so $x \in Z \cap K^n$. Therefore $Z \cap K^n = Z_K(I')$ so $Z \cap K^n$ is Zariski closed.

20 Fall 2012 Part II

20.1 10

Let $G = \mathrm{SL}_3(\mathbb{F}_p)$ where p is an odd prime. Let ℓ be a prime divisor of $p^2 + p + 1$.

20.1.1 a

Suppose that $\ell > 3$. Notice that $|G| = (p^3 - 1)(p^3 - p)(p^3 - p^2)/(p - 1) = p^3(p^3 - 1)(p^2 - 1)$. Now $\ell \mid p^3 - 1$ but does not divide p^3 or $p^2 - 1$ because in the first case then $\ell \mid 1$ and in the second case then $\ell \mid p + 2$ and either $\ell \mid p - 1$ or $\ell \mid p + 1$ which can only happen if $\ell = 3$. Therefore, it suffices to show that G has a cyclic subgroup of order $p^2 + p + 1$.

Indeed, consider the mulitplication action $\mathbb{F}_{p^3} \circlearrowright \mathbb{F}_{p^3}$. giving a cyclic subgroup inside $\mathrm{GL}_3(\mathbb{F}_p)$ of order $(p^3 - 1)$. We need to find which elements lie in $\mathrm{SL}_3(\mathbb{F}_p)$. These are elements $z \in \mathbb{F}_p^\times$ with $\det z = 1$ but,

$$\det z = z \cdot z^p \cdot z^{p^2} = z^{p^2+p+1}$$

Therefore, this is the cyclic subgroup of order $p^2 + p + 1$ inside $\mathrm{SL}_3(\mathbb{F}_p)$.

20.1.2 b

Suppose that $\ell = 3$. If $p = 3$ then we can take the upper triangular matrices which are not cyclic but have order a power of p. Now let $p \neq 3$ and consider the Frobenius element $F \in \mathrm{SL}_3(\mathbb{F}_p)$ (it has determinant 1 because it commutes with taking the determinant of an element). Furthermore consider $z \in \mathbb{F}_{p^3}^\times$ of order 3 which exists because $3 \mid p^3 - 1$ by Fermat's little theorem. Furthermore, $FzF^{-1} = z^p$ but if we choose $z \notin \mathbb{F}_p$ then $z \neq z^p$ and therefore the ℓ-Sylow subgroup is not commutative and thus cannot be cyclic.

21 Spring 2014 Part I

21.1 1

Let p be a prime.

21.1.1 a

Let H be a finite p-group. Let $\rho : H \to \mathrm{GL}(V)$ be an action on a nonzero finite-dimensional F_p-vector space. This is an action on a finite set of order p^n. The orbits have size p^k because H is a p-group and therefore the number of fixed points is divisible by p. However, the origin is fixed so there is at least one nonzero fixed element which spans a fixed line.

21.1.2 b

Now let V be a finite-dimensional $\overline{F_p}$-vectorspace. Since H is finite, by adjoining all the entries in the matrices (which are algebraic over $\mathbb{F}_p$ by definition) in the image of $H \to \mathrm{GL}_V()$ we obtain an H-rep V' on a finite-dimensional F_q-vectorspace for some $p = q^k$ such that $V = V' \otimes_{\mathbb{F}_p} \mathbb{F}_q$. Since V' is finite the same argument gives a fixed line in V' and thus a fixed line in V.

21.1.3 c

Let G be a finite group with p-Sylow subgroup G_p. Let V be a nontrivial irreducible $\overline{F_p}$-linear representation of G. Since $\mathrm{Res}^G_{G_p}(V)$ is a representation of a p-group G_p by (b) we see that there is a fixed line $\ell \subset \mathrm{Res}^G_{G_p}(V)$. Therefore,

$$W = \sum_{g \in G/G_p} g \cdot \ell \subset V$$

is a G-invariant subspace and thus $W = V$. Therefore, choosing a generator $v \in \ell$ we see that $\{g \cdot v\}_{v \in G/G_p}$ spans V and moreover,

$$\sum_{g \in G/G_p]} g \cdot v \in V^G$$

and $V^G = (0)$ since V is irreducible so v is in the span of $\{g \cdot v\}_{g \neq e}$ and thus,

$$\dim V \leq [G : G_p] - 1$$

21.2 2

Let R be a commutative ring.

21.2.1 a

Let R' be a flat R-algebra. Choose a free resolution $P_\bullet \to M$ then for any R-module N we consider the complex,

$$(R' \otimes_R P_\bullet) \otimes_{R'} (R' \otimes_R N) = R' \otimes_R (P_\bullet \otimes_R N)$$

Because R' is flat $R' \otimes_R P_\bullet$ is an exact complex of free R'-modules. Then because R' is R-flat $R' \otimes_R -$ commutes with taking cohomology so,

$$\mathrm{Tor}_i^{R'}(R' \otimes_R M, R' \otimes_R N) \cong H^i(R' \otimes_R (P_\bullet \otimes_R N)) \cong R' \otimes_R H^i(P_\bullet \otimes_R N) \cong \mathrm{Tor}_i^R(M, N)$$

Now we need to prove that this isomorphism is natural. Functoriality in N is obvious from the construction and the functoriality of the tensor product and of cohomology given a morphism of complexes. Now suppose we have a map $\alpha : M \to M'$ of R-modules. Then choosing free resolutions $P_\bullet \to M$ and $P'_\bullet \to M$ there is a lift $\alpha_\bullet : P_\bullet \to P'_\bullet$ of α to a morphism of complexes. Therefore, we get a diagram of complexes,

$$\begin{array}{ccc} (R' \otimes_R P_\bullet) \otimes_{R'} (R' \otimes_R N) & = & R' \otimes_R (P_\bullet \otimes_R N) \\ \downarrow \alpha & & \downarrow \alpha \\ (R' \otimes_R P'_\bullet) \otimes_{R'} (R' \otimes_R N) & = & R' \otimes_R (P'_\bullet \otimes_R N) \end{array}$$

where this commutes because the tensor product isomorphism are natural. Taking H^i immediately gives the natural square,

$$\begin{array}{ccc} \operatorname{Tor}_i^{R'}(R' \otimes_R M, R' \otimes_R N) & = & \operatorname{Tor}_i^{R}(M, N) \\ \downarrow \alpha & & \downarrow \alpha \\ \operatorname{Tor}_i^{R'}(R' \otimes_R M', R' \otimes_R N) & = & \operatorname{Tor}_i^{R}(M', N) \end{array}$$

21.2.2 b

Let R be a domain and $\xi \in \operatorname{Tor}_n^R(M, N)$ with $n > 0$. Indeed, we know that $K = \operatorname{Frac}(R)$ is flat over R and thus,

$$K \otimes_R \operatorname{Tor}_n^R(M, N) \cong \operatorname{Tor}_n^K(K \otimes_R M, K \otimes_R N) = 0$$

for $n > 0$ because all K-modules are flat since K is a field. Therefore, everything in $\operatorname{Tor}_n^R(M, N)$ is torsion since $1 \otimes \xi = 0$ implies that $r\xi = 0$ for some $r \neq 0$ such that $r^{-1} \otimes r\xi = 0$.

21.2.3 c DO THIS BETTER

The non-torsion element of $\operatorname{Ext}_{\mathbb{Z}}^1(\mathbb{Q}/\mathbb{Z}, \mathbb{Z})$ corresponds to the nontrivial extension,

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Such extensions have a group operation from the homological algebra construction of Ext or explicitly by Baer sum where

$$E_1 + E_2 = \{(a, b) \in E_1 \times E_2 \mid \pi_1(a) = \pi_2(b)\}/(\iota_1(n), -\iota_2(n))$$

given the well-defined map $\pi = \pi_1 = \pi_2$ on $E_1 + E_2$. In our case, let's consider the square of our extension,

$$E_1 + E_2 = \{(a, b) \in \mathbb{Q}^2 \mid [a] = [b]\}/(n, -n)\} \cong \mathbb{Q}$$

via sending $(a, b) \mapsto a + b$ then the new map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ is via $a \mapsto \frac{1}{2}[a]$ which gives a new extension

21.3 3

Let G be a group of order $56 = 7 \cdot 8$. LEt P_2 and P_7 be 2-Sylow and 7-Sylow subgroups respectively.

21.3.1 a

Suppose that P_2 and P_7 are both normal. By the second isomorphism theorem we know that,

$$P_2P_7/P_2 \cong P_7$$

because $P_2 \cap P_7 = \{e\}$ (since they have coprime orders) and thus $|P_2P_7| = |P_2| \cdot |P_7|$. Therefore $G = P_2 \times P_7$. In general if $N, M \subset G$ are normal such that $N \cap M = \{e\}$ then they commute in this way.

To prove this, consider $x \in N$ and $y \in M$ then $xyx^{-1}y^{-1} \in N \cap M$ by normality used twice and thus $xyx^{-1}y^{-1} = e$ so $xy = yx$.

21.3.2 b

Suppose that neither P_2 nor P_7 is normal. Then by the Sylow theorems there are,

$$m_2 = 2k_2 + 1 \mid 7 \quad \text{and} \quad m_7 = 7k_7 + 1 \mid 8$$

subgroups of each type so we see that there must be 7 Sylow 2-subgroups and 8 Sylow 7-subgroups. Since the 7-Sylows have prime order no two can intersect except at e and thus there must be $8 \cdot 6$ elements of order 7 in G. This leaves only 8 elements of order divisible by 2 so there cannot be more than one 2-Sylow.

21.3.3 c

We can consider $\mathbb{Z}/8\mathbb{Z} \circlearrowright \mathbb{Z}/7\mathbb{Z}$ nontrivially since $(\mathbb{Z}/7\mathbb{Z})^\times = \mathbb{Z}/6\mathbb{Z}$ has an element of order 7. This gives a semi-direct product with non-normal $P_2 \cong \mathbb{Z}/8\mathbb{Z}$. Furthermore, we can consider $P_2 = (\mathbb{Z}/2\mathbb{Z})^3$ and $\mathbb{Z}/7\mathbb{Z} \circlearrowright P_2$ by the order 7 automorphism $\sigma \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ defined by considering the generator in $\mathbb{F}_8^\times$ which has order 7. This gives a semi-direct product with $P_7 \cong \mathbb{Z}/7\mathbb{Z}$ non-normal.

21.4 4

(I THINK YOU NEED NOETHERIAN?)

Let B be a domain, $K = \mathrm{Frac}\,(B)$ and K' a finite separable extension of K.

21.4.1 a

Suppose that $P', Q' \in \mathrm{Spec}\,(B')$ lie above $\mathfrak{p} \in \mathrm{Spec}\,(B)$ and $P' \subset Q'$. Then consider $(B_\mathfrak{p}/\mathfrak{p})_\mathfrak{p} \hookrightarrow (B'/P')_\mathfrak{p}$ is an integral extension and $(B/\mathfrak{p})_\mathfrak{p}$ is a field so $(B'/P')_\mathfrak{p}$ is a field. However, Q' is also a prime of $(B'/P')_\mathfrak{p}$ and thus $P' = Q'$.

Let $X \to \mathrm{Spec}\,(K)$ be an integral dominant map and X integral. Then $X = \mathrm{Spec}\,(L)$ for some algebraic extension of K. Indeed for each $x \in X$ there is an affine open $\mathrm{Spec}\,(A)$ containing x such that A is a domain and $K \subset A$ is a integral extension (injective because the map is dominant) and thus A is a field so x is the generic point and $X = \mathrm{Spec}\,(L)$ where $L = A$ is an algebraic extension of K.

Then for $f : X \to Y$ an integral dominant morphism of schemes. Then for any integral subscheme $Z \subset Y$ with an integral subscheme $W \subset f^{-1}(Z)$ mapping dominantly onto Z we see that $W \to Z$ is an integral dominant map of integral schemes. Take the generic point $\eta \in Z$ then each integral subscheme of the fiber $V \subset f^{-1}(\eta)$ maps $V \to \eta$ is dominant and integral with V integral so $V = \xi$ where $\xi \to \eta$ is an algebraic extension of fields. Therefore the irreducible components of the fiber over $\eta \in Y$ are points.

Furthermore, if $X \to Y$ is dominant and finite then for each integral subscheme $Z \subset Y$ with generic point $\eta \in Z$ then $f^{-1}(\eta) \to \eta$ is finte and dominant so $f^{-1}(\eta) = \mathrm{Spec}\,(A)$ is affine and $K \to A$ where $K = \mathcal{O}_{Z,\eta}$ so A is a finite K-module so $\mathrm{Spec}\,(A)$ is finite.

21.4.2 b

Let K'/K be Galois and B integrally closed. For each prime $\mathfrak{q} \subset B$ I claim that the fibers of $\mathrm{Spec}\,(B') \to \mathrm{Spec}\,(B)$ are finite (THIS HOLDS IF NOETHERIAN).

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes above $\mathfrak{p}_1$ ordered such that $\mathfrak{p}_1 \not\supset \mathfrak{p}_j$ for $j > 1$ i.e. $\mathfrak{p}_1$ is minimal (there are no relations by part (a) so there is actually no requirement on the order). Then by prime avoidance, there is some,

$$x \in \mathfrak{p}_1 \setminus \bigcup_{i=2}^{n} \mathfrak{p}_n$$

otherwise $\mathfrak{p}_1$ would lie above some $\mathfrak{p}_j$ for $j > 1$. Now consider,

$$y = \prod_{\sigma \in G} \sigma(x)$$

Then $y \in (K')^G = K$. Therefore,

$$y \in \mathfrak{p}_1 \cap K = \mathfrak{p}_1 \cap B' \cap K = \mathfrak{p}_1 \cap B = \mathfrak{q}$$

because $B' \cap K = B$ since B is integrally closed in K. Therefore, $y \in \mathfrak{p}_i$ for each i meaning that for each i there is some $\sigma(x) \in \mathfrak{p}_i$ and thus $x \in \sigma^{-1}(\mathfrak{p}_i)$. However, $\sigma^{-1}(\mathfrak{p}_i) = \mathfrak{p}_j$ for some j since it is a prime lying above $\mathfrak{q}$. However, $x \in \mathfrak{p}_j$ and thus $\mathfrak{p}_j = \mathfrak{p}_1$. Therefore $\mathfrak{p}_i = \sigma(\mathfrak{p}_1)$ so the Galois group acts transitively.

21.5 5

Let V be a nonzero finite-dimensional vector space over a field k with characteristic not equal to 2. Let ω_1, ω_2 be symplectic forms on V.

21.5.1 a

Consider the isomorphism $A : V \xrightarrow{\omega_1} V^* \xrightarrow{\omega_2^{-1}} V$ which takes $v \mapsto \omega_1(-, v) \mapsto u$ such that $\omega_2(-, u) = \omega_1(-, v)$ and thus,

$$\omega_1(x, y) = \omega_2(x, Ay)$$

Furthermore, this equation uniquely determines A by the above isomorphisms. In this case,

$$\omega_1(Ax, y) = -\omega_1(y, Ax) = -\omega_2(y, x) = \omega_2(x, y) = \omega_1(x, Ay)$$

21.5.2 b

For any $v \in V$ let W be the span of $\{A^i v\}$. If $i + j$ is odd then we have,

$$\omega_1(A^i v, A^j v) = \omega_1(A^r v, A^{r+1} v) = \omega_2(A^r v, A^r v) = 0$$

where $2r + 1 = i + j$. If $i + j$ is even then,

$$\omega_1(A^i v, A^j v) = \omega_1(A^r v, A^r v) = 0$$

where $i + j = 2r$. Thus W is ω_1-isotroptic.

21.5.3 c

Assume that $k = \bar{k}$. Let V_λ and V_μ be the generalized eigenspaces of A with eigenvalues $\lambda \neq \mu$. If $v \in V_\lambda$ and $u \in V_\mu$ then $(A-\lambda)^n v = 0$ and $(A-\mu)^m v = 0$. Therefore, consider,

$$\omega_1((A-\lambda)^n v, u) = \omega_1(v, (A-\lambda)^n u)$$

Notice that,

$$(A-\lambda)^n = (A-\mu+\mu-\lambda)^n = (\mu-\lambda)^n \left[I + \frac{A-\mu}{\mu-\lambda} \right]^n$$

But $A-\mu$ is nilpotent on V_μ and therefore $A-\lambda$ is invertible on V_μ. However, $\omega_1((A-\lambda)^n v, u) = 0$ for sufficiently large n and thus,

$$\omega_1(v, (A-\lambda)^n u) = 0$$

for any $u \in V_\mu$ but since this operator is surjective we can choose u to hit any $u' \in V_\mu$ we want so we see that $\omega_1(v, u') = 0$ as required.

Now let $v \in V_\lambda \cap V_\lambda^\perp$. By the Joran canonical form we project any $u \in V$ onto the generalized eigenspaces,

$$u = \sum_\mu u_\mu$$

and then,

$$\omega_1(v, u) = \omega_1(v, u_\lambda)$$

because $\omega_1(V_\lambda, V_\mu) = 0$ for $\lambda \neq \mu$. But $v \in V_\lambda^\perp$ and thus,

$$\omega_1(v, u) = \omega_1(v, u_\lambda) = 0$$

Therefore $v = 0$ since u is arbitrary. Therefore V_λ is symplectic.

21.5.4 d

Assume that $k = \bar{k}$. Let m_A and p_A be the minimal and characteristic polynomials of A respectively. Since the eigenspaces V_λ are symplectic they have even size $2n$. Therefore each linear factor in p_A appears an even number of times. Furthermore, we know that $(A-\lambda)^n v$ is isotropic meaning that each Jordan factor is an isotropic subspace so it has at most dimension n. Therefore, the minimal polynomial has at most n copies of the linear factor $(T-\lambda)$. This shows that $m_A^2 \mid p_A$.

22 Spring 2014 Part II

22.1 1 DO THIS!!!

Let A be a Noetherian domain with $L = \text{Frac}\,(A)$ and B a finitely generated A-algebra with injective structue map $f : A \to B$.

22.1.1 a

PROVE NOETHERIAN NORMALIZATION!!!

22.1.2 b

We know that $B \otimes_A K$ is a finite type K-algebra and therefore there is a finite extension $K[x_1, \dots, x_d] \subset B \otimes_A K$ because $B \otimes_A K$ is nonzero since $A \to B$ is injective. Now by clearing denominators we can assume that $A[x_1, \dots, x_d] \subset B \subset B \otimes_A K$. Now since B is finitely generated as an A-algebra we know that B is finitely generated over $A[x_1, \dots, x_d]$ so,

$$B = A[x_1, \dots, x_d][y_1, \dots, y_r]/(f_1, \dots, f_k)$$

using that A is noetherian. But we know that $B \otimes_A K$ is finite over $K[x_1, \dots, x_d]$ so each y_i becomes integral over K so it satisfies some monic $p_i \in K[x_1, \dots, x_n][x]$ let a be the product of the denominators of all coefficients in the p_i then $p_i \in A_a[x_1, \dots, x_d][x]$ and therefore y_i is integral over $A_a[x_1, \dots, x_d]$ and thus,

$$A_a[x_1, \dots, x_d] \subset B_a$$

is finite.

22.1.3 c

We know that $\operatorname{Spec}(A_a) \to \operatorname{Spec}(A)$ is open and dense. Furthermore, $A_a[x_1, \dots, x_n] \subset B_b$ is finite and thus $\operatorname{Spec}(B_a) \to \operatorname{Spec}(A_a[x_1, \dots, x_n])$ is surjective but $\operatorname{Spec}(A_a[x_1, \dots, x_n]) \to \operatorname{Spec}(A_a)$ is surjective so we see that $\operatorname{Spec}(B_a) \to \operatorname{Spec}(A_a)$ is surjective and thus $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ hits at least the dense open $\operatorname{Spec}(A_a)$.

22.2 3

Let p be an odd prime and k a field of char not p.

22.2.1 a

Let $K = k(\zeta_p)$ be the splitting field of $X^p - 1$ over k. Let $\Gamma = \operatorname{Gal}(K/k)$ then for each $\sigma \in \Gamma$ we have $\sigma(\zeta_p) = \zeta_p^{n_\sigma}$ then send $\sigma \mapsto n_\sigma \in (\mathbb{Z}/p\mathbb{Z})^\times$. This is injective because if $\sigma(\zeta_p) = \zeta_p$ then σ fixes all the roots so it is trivial.

If $k = \mathbb{Q}$ then $X^{p-1} + \cdots + 1$ is irreducible and therefore there is an automorphism sending $\zeta_p \mapsto \zeta_p^n$ for each $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ because these are the roots of $X^{p-1} + \cdots + 1$.

Now let $k = \mathbb{F}_7$. The roots of unity are $\mathbb{F}_7^\times$ which has order 6. Therefore, $X^6 - 1$ aready has all its roots in $\mathbb{F}_7$. This means that $\zeta_p^{\frac{p-1}{2}} \in k$ so we get the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ which is coprime to 6.

22.2.2 b FINISH THIS

Let $K = \mathbb{Q}(\zeta_7)$ then $G = \operatorname{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2 \cong \mathbb{Z}/6\mathbb{Z}$ and thus has a unique index 3 subgroup and therefore K has a unique subfield F of degree 3 over $\mathbb{Q}$. The subgroup is $\langle -1 \rangle \subset (\mathbb{Z}/7\mathbb{Z})^\times$ and therefore is generated by $b = \zeta_7 + \zeta_7^{-1}$ being fixed by the element $\sigma : \zeta_7 \mapsto \zeta_7^{-1}$.

22.3 5

This is just Fall 2014 A4.

23 Fall 2015 Part I

23.1 1

Let p be a prime and $G = \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

23.1.1 a

Consider the reduction map $\varphi : \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ which is surjective because any lift of an invertible matrix must have a unit determinant (since it is nonzero mod p and thus coprime to p) so it is invertible. Furthermore, if $A \in \ker\varphi$ then $A - I \in pM_2(\mathbb{Z}/p\mathbb{Z})$. Thus we get an exact sequence,

$$0 \longrightarrow M_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

Then we know that $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = (p^2-1)(p^2-p)|$ and $|M_2(\mathbb{Z}/p^2\mathbb{Z})| = (\mathbb{Z}/p\mathbb{Z})^4 = p^4$. Therefore,

$$|G| = p^5(p-1)^2(p+1)$$

23.1.2 b

Let $U \subset G$ be the group of upper triangular matrices with diagonal I. Then $U \cong (\mathbb{Z}/p^2\mathbb{Z})$ via the map

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

I claim that $S = U(I + pM_2(\mathbb{Z}/p\mathbb{Z}))$ is a Sylow p-subgroup. It suffices to show that $|S| = p^5$. Indeed, consider,

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1+pa & pb \\ pc & 1+pd \end{pmatrix} = \begin{pmatrix} 1+p(a+uc) & u+p(b+ud) \\ pc & 1+pd \end{pmatrix}$$

Therefore, we can recover u only up to its image under $(\mathbb{Z}/p^2\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})$. Perhaps more rigorously, consider the second isomorphism theorem with $N = I + pM_2(\mathbb{Z}/p\mathbb{Z}) = \ker\varphi$ normal in G. Then,

$$UN/N \cong U/N \cap U$$

However, $U \cap N$ is the set of upper triangular matrices in the kernel which is isomorphic to $(\mathbb{Z}/p\mathbb{Z}) \subset (\mathbb{Z}/p^2\mathbb{Z})$. Therefore, we see that $|UN| = |N| \cdot |U|/|N \cap U| = p^4 \cdot p^2/p = p^5$ proving the claim.

23.1.3 c REALLY DO THIS

Because all the Sylow p-subgroups are conjugate we just need to prove this claim for $S = UN$. It is not difficult to check that the only matrices in the center of UN are the diagonal ones which is a subgroup of $M_2(\mathbb{Z}/p\mathbb{Z})$ isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

23.2 2

Let R be a Noetherian ring and M, N be R-modules.

23.2.1 a

Let M be finitely generated and N be finite as a set. Since R is Noetherian submodules of finitely generated modules are finitely generated. Therefore, there exists a resolution of M by finite free modules,

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

Then we can compute directly,

$$\operatorname{Tor}_i^R(M,N) = H^i(F_\bullet \otimes_R N)$$

However, $F_i \otimes_R N$ is a finite set because it is a finite direct sum of modules which are finite as sets (the cartesian product of finite sets is finite) and therefore the homology of this complex is stricly smaller than each term so $\operatorname{Tor}_i^R(M,N)$ is finite as a set.

23.2.2 b

Suppose that M, N are finite as sets and that their orders are coprime. For $k \in M$ the multiplication map $M \xrightarrow{k\times} M$ induces the multiplication by k map on $\operatorname{Tor}_i^R(M,N) \to \operatorname{Tor}_i^R(M,N)$. Likewise for the multiplication map $N \to N$. Now if k is coprime to $|M|$ this map is an isomorphism while if k is equal to $|M|$ then it is zero (because by Lagrange's theorem the order of each element of a finite group divides the order of the group). Therefore, multiplication by $|M|$ is both an isomorphism on $\operatorname{Tor}_i^R(M,N)$ (because $|M|$ is coprime to $|N|$ so multiplication by $|M|$ is an isomorphism $N \to N$) and the zero map (because this map is also induced by multiplication $M \to M$ which is the zero map). Therefore $\operatorname{Tor}_i^R(M,N) = 0$.

23.2.3 c

Let R be a domain and $I \subset R$ be a nonzer proper ideal. Consider the exact sequence,

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

Then, tensoring by R/I we get,

$$\operatorname{Tor}_1^R(R/I,R) \longrightarrow \operatorname{Tor}_1^R(R/I,R/I) \longrightarrow R/I \otimes_R I \longrightarrow R/I \longrightarrow R/I \longrightarrow 0$$

but R is flat so $\operatorname{Tor}_1^R(R/I,R) = 0$ and therefore, $\operatorname{Tor}_1^R(R/I,R/I) = \ker(R/I \otimes_R I \to R/I) = I/I^2$. Thus it suffices to show that $I^2 \subsetneq I$. Otherwise, if $I^2 = I$ then because R is Noetherian we see that I is finitely generated so by Nakayama's lemma, $rI = 0$ for some $r - 1 \in I$ but R is a domain and I is nonzero so $r = 0$ and thus $1 \in I$ so $I = R$ a contradiction. Thus $I^2 \subsetneq I$ and thus $\operatorname{Tor}_1^R(R/I,R/I) \neq 0$.

23.3 3 DO THIS ONE!!

Let K be a finite field of order $q = p^n$ where p is prime and let $\mathbb{F}_p \subset K$ be the order p subfield.

23.3.1 a

Consider $f(X) = X^q - X$ then we know that every element of K satisfies this because $K^\times$ is cyclic of order $q-1$ and obviously $f(0) = 0$. Therefore, K is generated by roots of f of which there are exactly q so f must split into linear factors in f because it has degree q. Thus K is the splitting field of f.

Now clearly the Frobenius $F : x \mapsto x^p$ is a field Automorphism fixing the prime subfield. Furthermore, $F^n = \mathrm{id}$ but $F^k \neq \mathrm{id}$ for $k < n$ since otherwise $x^{p^k} - x$ would have p^n solutions which is impossible. Therefore, F generates a subgroup of the Galois group which is of size $[K : \mathbb{F}_p]$ and thus $\mathrm{Gal}\,(K/\mathbb{F}_p) \cong \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

23.3.2 b

Let $x_1, \ldots, x_n \in K$ be a $\mathbb{F}_p$ basis for K. Let M be the matrix $M_{ij} = x_i^{p^j}$. Let $\sigma_j = F^i \in G$ enumerate the Galois entires. Then $M_{ij} = \sigma_j(x_i)$.

Suppose that $\det M = 0$ then consider the map $M : \mathbb{F}_q^n \to \mathbb{F}_q^n$ given by sending $(\alpha_1, \ldots, \alpha_n)$ to $(M_{ij}\alpha_j)_i$ and thus there is a nontrivial solution,

$$\alpha_1\sigma_1(x_i) + \cdots + \alpha_n\sigma_n(x_i) = 0$$

Therefore, for any $x \in \mathbb{F}_q$ we can write,

$$x = \beta_1 x_1 + \cdots + \beta_n x_n$$

and thus summing we find,

$$\alpha_1\sigma_1(x) + \cdots + \alpha_n\sigma_n(x) = 0$$

for all $x \in \mathbb{F}_q$ which contradicts the linear independence of characters $\mathbb{F}_q^\times \to \mathbb{F}_q$. Therefore $\det M \neq 0$.

23.3.3 c

Let $n = 4$. Take $a \in \mathbb{F}_p$. I want to show that $X^2 - a$ has a root in K. Either $X^2 - a$ has a root in $\mathbb{F}_p$ or $X^2 - a$ is irreducicble and therefore its splitting field F is an extension of $\mathbb{F}_p$ of index 2. However, we have shown that then F must be the splitting field of $X^{p^2} - X$ so there is exactly one such field of this order. Moreover, because $\mathrm{Gal}\,(K/\mathbb{F}_p) = \mathbb{Z}/4\mathbb{Z}$ there is a subgroup of index 2 and thus the unique field F of order p^2 must lie inside and thus $X^2 - a$ has a solution in K.

Explicitly, consider the subfield $F \subset \mathbb{F}_3[x]/(x^4 - x - 1)$ of elements such that $x^{3^2} = x$. Then I claim this contains a square root of -1.

23.4 4

Let A, B be commutative rings and $A \to B$ making B an A-algebra.

23.4.1 a

We say that $b \in B$ is integral over A if there is a monic polynomial $p \in A[x]$ with $p(b) = 0$ in B. If every element $b \in B$ is integral over A then we say that B is integral over A.

23.4.2 b DO THIS!!

Let A be a domain and $B = A[T]/(a_0T^n + a_1T^{n-1} + \cdots + a_n)$ with $a_0 \neq 0$. Clearly if $a_0 \in A^\times$ then B is integral over A since T is an integral element (just divide the defining equation by a_0) and sums and products of integral elements are integral.

Now suppose that B is integral over A. Then $T \in B$ is integral over A so $B = A[T]$ is a finite A-module. However, I claim that if a_0 is not a unit then B is not a finite A-module. Indeed, consider T^k for sufficiently large k the elements $1, T, T^2, \ldots, T^k$ cannot be independent and thus,

$$T^k + b_1T^{k-1} + \cdots + b_k = 0$$

However, this polynomial must be in the ideal (f) and thus equals fg but then the leading term shows that a_0 is a unit.

23.4.3 c DO THIS!!

Exercise 23.4.1. Let k be a field and nonzero $f = a_0(X)T^n + a_1(X)T^{n-1} + \cdots + a_n(X)$ with $a_i(X) \in k[X]$ let $B = k[X,T]/(f)$. For $U = X + T^{n+1}$ prove that B is integral over the subalgebra $k[U]$.

We can write,

$$f = a_0(U - T^{n+1})T^n + \cdots + a_n(X - T^{n+1})$$

Then expanding the leading term has degree $d_i(n+1) + i$ where d_i is the degree of a_i and this is the maximal such $d_i(n+1) + i$. However, this term comes from the leading term in $a_i(U - T^{n+1})$ which has no powers of X and thus the leading term in f (in terms of T) is a scalar. Therefore by part (b) we see that,

$$k[X,T]/(f) = k[U][T]/(f)$$

is integral over $k[U]$ because the leading term of $f \in (k[U])[T]$ is a unit.

24 Spring 2015 Part I

24.1 1

Let G be a finite group.

24.1.1 a

Let $\pi : G \to \mathrm{GL}_V()$ be an irreducible complex representation and χ be its character. If $\pi(g) = cI$ for some $c \in \mathbb{C}$ then c is a root of unity since G is finite and thus $\chi(g) = c \dim V$ so $|\chi(g)| = \dim V$. Suppose that $g \in G$ has $|\chi(g)| = \dim V$. Then $\pi(g)$ is diagonalizable and its eigenvalues are roots of unity so,

$$|\chi(g)| = |\lambda_1 + \cdots + \lambda_n| \leq |\lambda_1| + \cdots + \cdots |\lambda_n| = n$$

with equality if and only if $\lambda_1 = \cdots = \lambda_n$ and thus $\chi(g) = \lambda I$.

24.1.2 b

If $|\chi(g)| = \chi(1)$ we have shown that $\rho(g) = cI$ and thus $\rho(gxg^{-1}x^{-1}) = \rho(g)\rho(x)\rho(g)^{-1}\rho(x)^{-1} = I$. Furthermore, we know that,

$$G \subset \mathbb{C}[G] \hookrightarrow \operatorname{End}(V_1) \times \cdots \times \operatorname{End}(V_n)$$

where $V_1, \ldots, V_n$ are the irreducible representations by sending $g \mapsto g \mapsto (\rho_i(g))$ thus $gxg^{-1}x^{-1} = e$ because it is sent to I in each $\operatorname{End}(V_i)$.

Conversely, suppose that $g \in Z(G)$. Then $\rho(g) : V \to V$ is an intertwiner because $\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g)$ and thus because V is irreducible then by Schur's Lemma we have $\rho(g) = \lambda I$ and thus $\chi(g) = \lambda \dim V$ so $|\chi(g)| = \chi(1)$.

24.2 2

Let R be a Dedekind domain.

24.2.1 a

In general flat implies torsion-free because if N is flat then $N \otimes R \to N \otimes K$ is injective where $K = \operatorname{Frac}(R)$ but the torsion dies. Conversely, suppose that N is a torsion-free R-module. Then $N_{\mathfrak{p}}$ is a torsion-free $R_{\mathfrak{p}}$-module for each prime but $R_{\mathfrak{p}}$ is a PID and thus by the structure theorem $N_{\mathfrak{p}}$ is free and thus flat. Therefore N is flat because we can check flatness at each prime.

It is clear that $\mathfrak{m} = (x, y) \subset \mathbb{C}[x, y]$ is a torsion-free $\mathbb{C}[x, y]$-module. However, it is not flat because $\mathfrak{m} \otimes \mathfrak{m} \to \mathfrak{m}^2$ has the nonzero element $x \otimes y - y \otimes x$ in its kernel.

24.2.2 b

Let $I, J \subset R$ be ideals. Consider the exact sequence,

$$0 \longrightarrow J \longrightarrow R \longrightarrow R/J \longrightarrow 0$$

then applying $R/I \otimes_R -$ we find,

$$\operatorname{Tor}_1^R(R/I, R) \longrightarrow \operatorname{Tor}_1^R(R/I, R/J) \longrightarrow R/I \otimes_R J \longrightarrow R/I \longrightarrow R/I \otimes_R R/J \longrightarrow 0$$

But R is free so $\operatorname{Tor}_1^R(R/I, R) = 0$ and thus

$$\operatorname{Tor}_1^R(R/I, R/J) = \ker(R/I \otimes_A J \to R/I) = \ker(J/IJ \to R/I) = (I \cap J)/IJ$$

Now suppose that $I, J \neq 0$. If $I + J = (1)$ write $i + j = 1$ and then for each $x \in I \cap J$ we can write $x = xi + xj \in IJ$ since $x \in I$ and $x \in J$ and thus $IJ = I \cap J$ so $\operatorname{Tor}_1^R(R/J, R/J) = 0$. Conversely, suppose that $IJ = I \cap J$. Then factor into prime ideals,

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \quad \text{and} \quad J = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_n^{r_n}$$

If $\mathfrak{p}_i = \mathfrak{q}_j$ then $IJ \subset \mathfrak{p}_i^{e_i + r_i}$ but $I \cap J \not\subset \mathfrak{p}_i^{e_i + r_i}$ because $\mathfrak{p}_i^{e_i} \cap \mathfrak{p}_i^{r_i} = \mathfrak{p}_i^{\max\{e_i, r_i\}}$ and the powers get strictly smaller. Therefore the primes must be disjoint and thus $I + J = (1)$ because the nonzero primes are maximal ideals.

In $\mathbb{C}[x, y]$ we need to find two ideals I, J such that $I \cap J = IJ$ but $I + J \neq (1)$. Indeed consider (x) and (y) then $(x) \cap (y) = (xy) = (x)(y)$ but $(x) + (y) = (x, y)$.

24.3 4

Let A be a commutative ring.

24.3.1 a

Let S, T be multiplicative subsets of A such that S and T intersect the same prime ideals of A nontrivially. That is for each $\mathfrak{p} \subset A$ we have $S \cap \mathfrak{p} \neq \varnothing \iff T \cap \mathfrak{p} \neq \varnothing$. Consider the map $A \to S^{-1}A$. If $f \in T$ then if $f \in \mathfrak{p}(S^{-1}A)$ then there is some $u, s \in S$ and $p \in \mathfrak{p}$ such that $u(fs - p) = 0$ then $ufs \in \mathfrak{p}$ so either $us \in \mathfrak{p}$ or $f \in \mathfrak{p}$ so either $S \cap \mathfrak{p} \neq \varnothing$ or $T \cap \mathfrak{p} \neq \varnothing$ so in either case $S \cap \mathfrak{p} \neq \varnothing$ and thus $\mathfrak{p}(S^{-1}A) = S^{-1}A$ and thus f is a unit in $S^{-1}A$ since it is not contained in any prime ideal. Therefore $A \to S^{-1}A$ factors uniquely through $A \to T^{-1}A$ giving a map $T^{-1}A \to S^{-1}A$. Swapping S and T gives a map $S^{-1}A \to T^{-1}A$ and their compositions extend to universal maps $A \to S^{-1}A$ and $A \to T^{-1}A$ and thus are the identities so $S^{-1}A \to T^{-1}A$ is an isomorphism of A-algebras.

24.4 5

Let F be an algebraically closed field and let

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

24.4.1 a

Since M acts on the standard basis as a 3-cycle we know that $M^3 = I$ and thus $x^3 - 1$ is the minmal and characteristic polynomial. As long as 3 is invertible in F this factors as,

$$x^3 - 1 = (x - 1)(x - \zeta_3)(x - \zeta_3^2)$$

which factors into distinct linear factors and thus M is diagonalizable so its Jordan normal form is,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{pmatrix}$$

otherwise F has characteristic 3 and the minimal polynomial is,

$$(x - 1)^3$$

Therefore, in this case the Jordan normal form is,

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

24.4.2 b

Let F has characteristic 3 and suppose that $TM = MT$. Notice that $e_1 + e_2 + e_3 = (I + M + M^2)e_i$ for each i. Thus, $\operatorname{im}(I + M + M^2) = F(e_1 + e_2 + e_3)$.

Suppose that T is not invertible then $Tv = 0$ for some nonzero v. Consider $(T - M)^3 = M^3(TM^{-1}I)^3$

Let T be nonzero and not invertible. In this basis $M = I + N$ so if $MT = TM$ then $NT = TN$. Suppose that $Tv = 0$ then $Nv \in \ker T$ so if $v = a_1e_1 + a_2e_2 + a_3e_3 \in \ker T$ then $N^2v = a_3e_1 \in \ker T$ so either $a_3 = 0$ or $e_1 \in \ker T$. If $a_3 = 0$ then $v = a_1e_1 + a_2e_2$ so $Nv = a_2e_1 \in \ker T$ so either $a_2 = 0$ or $e_1 \in \ker T$ if $a_2 = 0$ then $v = a_1e_1$ and $a_1 \neq 0$ because $v \neq 0$ so $e_1 \in \ker T$. Therefore, $e_1 \in \ker T$. Now $NTe_2 = Te_1 = 0$ so $Te_2 = \lambda_1e_1$. Furthermore, $NTe_3 = TNe_3 = Te_2 = \lambda_1e_1$ so $Te_3 = \lambda_1e_2 + \lambda_2e_1$ and thus $T^3 = 0$.

If the characteristic is not 3 then we can let $T(e_1+e_2+e_3) = 0$ and is a projection to the complement and thus is not invertible or nilpotent but commutes with M.

25 Spring 2015 Part II

25.1 2 DO THIS ONE BETTER

Let $p > 2$ be an odd prime.

25.1.1 a

Exercise 25.1.1. Let G be a finite group and P a p-Sylow subgroup of G. Let N be the normalizer of P. Let $x, y \in C(P)$ where $C(P)$ is the centralizer. Show that if $x, y \in G$ are conjugate then they are conjugate in N.

We know that for any $z \in P$ that $yzy^{-1} = z$ so $zyz^{-1} = y$ and thus $P \subset C(y)$. Suppsose that $x = gyg^{-1}$ for $g \in G$. Since $x \in C(P)$ we see that $gyg^{-1}zgy^{-1}g^{-1} = z$ for all $z \in P$ and thus

$$y(g^{-1}zg)y^{-1} = g^{-1}zg$$

so we see that $y \in C(g^{-1}Pg)$ and therefore $g^{-1}Pg \subset C(y)$ is another Sylow p-subgroup so they are conjugate in $C(y)$ and thus there is some $q \in C(y)$ such that $g^{-1}Pg = q^{-1}Pq$ and thus $gq^{-1} \in N$. Furthermore, $gq^{-1}yqg^{-1} = gyg^{-1} = x$ proving the proposition.

25.1.2 b

Let $G = \mathrm{GL}_2(\mathbb{F}_p)$. Let P be the Sylow p-subgroup of upper triangular matrices and let N be its normalizer.

25.2 4

Let F be a field and V a finite-dimensional F-vector space. This is a $G = \mathrm{GL}_V()$-module automatically. Let $T = F$ be the 1-dimensional trivial G-module.

25.2.1 a

The G-module structue on V^* is $\varphi \mapsto \varphi \circ g^{-1}$ and $V \otimes V^*$ via $v \otimes \varphi \mapsto g \cdot v \otimes \varphi \circ g^{-1}$. Then consider the isomorphism,

$$V \otimes V^* \xrightarrow{\sim} \mathrm{Hom}_F(V, V)$$

given by,

$$v \otimes \varphi \mapsto (u \mapsto v\varphi(u))$$

Then,

$$g \cdot v \otimes \varphi \circ g^{-1} \mapsto (u \mapsto g \cdot v\varphi(g^{-1} \cdot u)) = g \cdot (u \mapsto v\varphi(u))$$

25.2.2 b

There is a natural G-invariant element $\mathrm{id} \in \mathrm{Hom}_F(V, V)$ which corresponds to, after choosing a basis $e_1, \ldots, e_n$, the tensor,

$$q = e_1 \otimes e_1 + \cdots + e_n \otimes e_n$$

Sending $1 \mapsto q$ gives a G-module map $T \to V \otimes V^*$. Furthermore, we can define $V \otimes V^* \to T$ via $e_i \otimes e_j \mapsto \delta_{ij}$ which is taking the trace. This G-invariant because the trace is invariant under conjugation. Furthermore, this is nonzero because there exist matrices of any trace.

25.2.3 c

Let $A = \ker \tau \subset \mathrm{Hom}_F(V, V)$ is the subrepresentation of traceless matrices. Suppose that F has characteristic $p > 0$ and $p \mid \dim V$. Then, for example, I is traceless. However, $I \in \mathrm{Hom}_G(V, V) = (\mathrm{Hom}_F(V, V))^G$ and is nonzero so A^G is nontrivial and thus A cannot be irreducible.

25.3 5 HOW TO DO THIS!!!

Let A be a PID

25.3.1 a

For any finitely generated A-module M there is an isomorphism,

$$M \cong R/(a_1) \oplus \cdots R/(a_n)$$

where $(a_1) \supset \cdots \supset (a_n)$. Furthermore, the ideals $(a_i) \subset R$ are unique.

25.3.2 b

26 Fall 2015 Part II

26.0.1 6

Let k be an algebraically closed field and V a finite dimensional k vector space of dimension n. Let $T : V \to V$ be a k-linear endomorphism of V. A vector $v \in V$ is called *cyclic* for T if the set of vectors $\{T^n v \mid n \geq 0\}$ spans V.

26.0.2 a

Since $\dim V = n$ it suffices to show that $\{v, Tv, \dots, T^{n-1}v\}$ is independent. Otherwise, we would have,

$$T^k v = \sum_{\ell=0}^{k-1} \alpha_\ell T^\ell v$$

for some $k \leq n-1$. Therefore, we see that $\dim \operatorname{span}\{T^n v\} \leq k$ because the vectors $v, Tv, \dots, T^{k-1}v$ span the space showing that v is not cyclic.

26.0.3 b

Let T admit a cyclic vector v and $A : V \to V$ commute with T. Then we know that $AT = TA$. Consider, the basis $v, Tv, \dots, T^{n-1}v$. Now,

$$Av = \alpha_0 v + \cdots + \alpha_{n-1} T^{n-1} v$$

because this set spans V. I claim that,

$$A = \alpha_0 I + \cdots + \alpha_{n-1} T^{n-1}$$

Indeed, it suffices to check this on the basis elements. We have,

$$AT^k v = T^k A v = T^k(\alpha_0 v + \cdots + \alpha_{n-1} T^{n-1} v) = \alpha_0(T^k v) + \cdots + \alpha_{n-1} T^{n-1}(T^k v)$$

proving the claim.

26.0.4 c

If v is a cyclic vector for T then,

$$v, Tv, \dots, T^{n-1}v$$

is a basis an in particular is independent. This shows that T cannot satisfy a degree $\leq n-1$ polynomial because if,

$$\alpha_0 I + \cdots + \alpha_{n-1} T^{n-1} = 0$$

then applying this equation to v contradicts the independence. Therefore, the minimal polynomial of T has degree at least n but the characteristic polynomial of T has degree n and is divisible my the minimal polynomial so they are equal.

Conversely, suppose the minimal polynomial of T is the characteristic polynomial. Then the action of T on V makes V a $k[T]$-module so by the structure theorem we have,

$$V \cong k[T]/(p_1) \oplus \cdots \oplus k[T]/(p_n)$$

where $p_1 \mid \cdots \mid p_n$ and thus $p = p_n$ is the minimal polynomial. Since $\deg p = n$ we see that $\dim_k k[T]/(p) = n$ but $\dim V = n$ so we see that,

$$V \cong k[T]/(p)$$

and therefore the element $v \in V$ corresponding to $1 \in k[T]/(p)$ is cyclic because $1 \in k[T]/(p)$ is cyclic because $T^0, \dots, T^{n-1}$ form a k-basis and the T-action is preserved by this isomorphism.

26.1 7

26.1.1 a

Exercise 26.1.1. Let $p > 2$ be a prime and S_p be the symmetric group. Prove that S_p is generated by any p-cycle σ and any transposition τ.

Since all k-cycles are conjugate we may assume that $\sigma = (1 \cdots p)$ and $\tau = (1\,2)$. It suffices to show that all transpositions are generated because we can clearly build any permutation from transpositions. First notice that,

$$\sigma^k \tau \sigma^{-k} = (1+k\,2+k)$$

Then consider,

$$(2\,3)(1\,2)(2\,3) = (1\,3)$$

by this process we get $(1\,a)$ for all a. Then conjugating by σ we get $(1+k\,a+k)$ for all k which gives all transpositions.

26.1.2 b

Let $f = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$. By Einsenstein's criterion, the prime 5 divides the last two coefficents but not the first and 5^2 does not divide the last coefficient thus f is irreducible.

Notice that $f' = 10X^4 - 10$ has only two real roots and thus f can have at most three real roots. Therefore the splitting field $L/\mathbb{Q}$ is complex so complex conjugation is an automorphism ($L/\mathbb{Q}$ is Galois so any embedding $L \to \overline{\mathbb{Q}}$ is automatically an automorphism) of order 2.

Since f is irreducible we know that $G = \mathrm{Gal}\,(L/\mathbb{Q})$ acts transitively on the roots. Then by the orbit stabilizer theorem $|G| = |G_\alpha| \cdot 5$ because there are five roots so $|G|$ is divisible by 5 so the Sylow 5 subgroup has at leat one element of order 5 in G.

Thus $G = \mathrm{Gal}\,(L/\mathbb{Q})$ contains an element of order 2 and of order 5. In fact, we can easily see that f has exactly three real roots so τ transposes the two complex roots. Since $G \subset S_5$ these elements must correspond to a transposition and a 5 cycle which generate all of S_5 by above.

26.1.3 c

We have shown that $G = S_5$ which is not a solvable group (because A_5 is simple) and therefore there cannot be a tower of abelian extensions constructing $L/\mathbb{Q}$ proving that the roots of f cannot be written in terms of radicals (since adjoining radicals and roots of unity produce abelian extensions).

26.2 8

26.2.1 a

Let $K = \mathbb{Q}(\sqrt{-31})$ let R be the integral closure of $\mathbb{Z}$ in K. I claim that $R = \mathbb{Z}[\alpha]$. First I need to show that $\mathbb{Z}[\alpha] \subset R$. It suffices to show that α is integral where,

$$\alpha = \frac{1+\sqrt{-31}}{2}$$

Indeed consider the polynomial,

$$x^2 - x + 8$$

whose roots are,

$$\frac{1 \pm \sqrt{-31}}{2}$$

Not we need to show that $R \subset \mathbb{Z}[\alpha]$. For any $\beta \in K$ we know that its minimal polynomial has degree at most 2 (because $\mathbb{Q}[\beta] \subset K$) then if $\beta \in R$ this polynomial must be monic by definition so,

$$\beta^2 + a\beta + b = 0$$

Therefore,

$$\beta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

For $\beta \in K$ we must have $a^2 - 4b = 31$ and thus $\beta \in \mathbb{Z}[\alpha]$ proving the claim.

It is a general fact that $\mathbb{Z}[\alpha] \cong \mathbb{Z}[t]/(m(t))$ where $m(t)$ is the minimal polynomial which in this case is $t^2 - t + 8$. This is because the kernel of $\mathbb{Z}[t] \to \mathbb{Z}[\alpha]$ is a prime ideal of $\mathbb{Z}[t]$ which is not everything at the generic point and thus is $(p(t))$ (an arbitrary prime ideal is of the form $(p(t), q)$ where q is a rational prime or zero).

26.2.2 b

It is clear that $2R \subset (2, \alpha)$ and $2R \subset (2, 1 - \alpha)$ which are swapped by complex conjugation. We need to show that $\mathfrak{m}, \mathfrak{m}'$ are maximal. Indeed, $R/\mathfrak{m} \cong \mathbb{Z}/2$ because any element can be written as $a + b\alpha$ and $\alpha \mapsto 0$ in $R/\mathfrak{m}$ and $2a \mapsto 0$. Likewise $R/\mathfrak{m}' \cong \mathbb{Z}/2$ so we see that both are prime. It is obvious that $\mathfrak{m}\mathfrak{m}' \subset 2R$ since $\alpha(1 - \alpha) = 8$. Furthermore, if $2a + 2b\alpha \in 2R$ then $2a + 2b\alpha = 2a(1 + \alpha) + 2(b - a)\alpha \in \mathfrak{m}\mathfrak{m}'$ so $2R \subset \mathfrak{m}\mathfrak{m}'$ and thus $2R = \mathfrak{m}\mathfrak{m}'$.

It is also clear that $R/2R$ has no nilpotents and thus its factorization has no ramification. Therefore we cannot have $\mathfrak{m} = \mathfrak{m}'$ proving that these are distinct.

Now if $x + \alpha y \in R^\times$ then $N_{K/Q}(x + \alpha y) = 1$ because it is a unit and positive in $\mathbb{Z}$ so $x^2 + xy + 8y^2 = 1$. But $x^2 + xy + 4y^2 = \frac{1}{2}x^2 + \frac{1}{2}(x + y)^2 + \frac{16-1}{2}y^2$ and thus $(x + y)^2 \leq 2$ so $7y^2 \leq 2$ and thus $y = 0$ so $x^2 = 1$ giving $x = \pm 1$. Thus $R^\times = \{\pm 1\}$.

Now we need to show that $\mathfrak{m}$ is not principal (which shows that its complex conjugate $\mathfrak{m}'$ is also not principal). Indeed, suppose that $\mathfrak{m} = (\beta)$. Then $2 = \beta\gamma$ and $\alpha = \beta\gamma'$ so $N(2) = N(\beta)N(\gamma)$ and $N(\alpha) = N(\beta)N(\gamma')$ but $N(2) = 4$ and $N(\alpha) = 8$ so we must have $N(\beta) = 4$. However, this implies that if $\beta = x + \alpha y$ then $y = 0$ and thus $\beta = 2$ but we can see that 2 does not divide α because its quotient would have norm 2 which is impossible.

26.3 9

Let V, V' be finite dimensional $\mathbb{C}$ representations of a finite group G.

26.3.1 a

The G-action on V^* is given by $\rho(g) \cdot \varphi : v \mapsto \varphi(\rho(g^{-1}) \cdot v)$. The G-action on $V \otimes_{\mathbb{C}} V'$ is induced by $v \otimes v' \mapsto \rho(g) \cdot v \otimes \rho'(g) \cdot v'$ and the G-action on $\mathrm{Hom}_{\mathbb{C}}(V, V')$ is given by,

$$\rho(g) \cdot f : v' \mapsto \rho(v) \cdot f(\rho'(g^{-1}) \cdot v')$$

Consider the maps,

$$\mathrm{Sym}_2(V) \oplus \bigwedge^2 V \to V \otimes_{\mathbb{C}} V \to \mathrm{Hom}_{\mathbb{C}}(V^*, V)$$

sending $(g, \omega) \mapsto g + \omega$ viewing $\mathrm{Sym}_2(V), \bigwedge^2 V \subset V^{\otimes 2}$ via $[x \otimes y] \mapsto \frac{1}{2}(x \otimes y \pm y \otimes x)$ and the second map sending $x \otimes y \mapsto (\varphi \mapsto \varphi(x)y)$. We need to show that these are G-equivariant. The first is obvious because the G-action is induced by the inclusions. Now consider the second map. We have,

$$\rho(g) \cdot (x \otimes y) = (\rho(g) \cdot x \otimes \rho(g) \cdot y) \mapsto (\varphi \mapsto \rho(g) \cdot y\varphi(\rho(g) \cdot x))$$

This is exactly the G-action on $\mathrm{Hom}_{\mathbb{C}}(V^*, V)$ which sends a map f to $\rho(g) \cdot f : \varphi \mapsto \rho(g) \cdot f(\rho(g)^{-1} \cdot \varphi)$ and if $f(\varphi) = y\varphi(x)$ then,

$$\rho(g) \cdot f(\rho(g)^{-1} \cdot \varphi) = \rho(g) \cdot y(\rho(g)^{-1} \cdot \varphi)(x) = \rho(g) \cdot y\varphi(\rho(g) \cdot x)$$

26.3.2 b

Let χ be the character of V. If we choose a basis of V as $e_1, \ldots, e_n$ then we can represent $\rho(g)$ by the matrix M_{ij} such that $\rho(g) \cdot e_j = M_{ij}e_i$. Now consder the dual basis $e^1, \ldots, e^n$ of V^*. We have,

$$(\rho(g) \cdot e^j)(e_i) = e^j(\rho(g^{-1}e_i) = e^j(M^{-1}_{ki}e_k) = (M^{-1})_{ji}$$

proving that,

$$\rho(g) \cdot e^j = (M^{-1})_{ji}e^i$$

and therefore the dual representation has the inverse transpose matrix. Thus $\chi_{V^*} = \mathrm{tr}\left((M^{-1})^\top\right) = \mathrm{tr}(M^{-1})$. Furthermore, M has finite order as a matrix (because G is finite) thus M is diagonalizable with eigenvalues which are roots of unity and M^{-1} has the inverse roots of units so we see that $\mathrm{tr}(M^{-1}) = \overline{\mathrm{tr}(M)}$.

Therefore, $\chi = \overline{\chi}$ if and only if $\chi_V = \chi_{V^*}$ but characters determine the representation so this holds if and only if $V \cong V^*$ as G-representations. Therefore, consider the isomorphism,

$$(V \otimes_{\mathbb{C}} V)^* \cong V^* \otimes_{\mathbb{C}} V^* \cong \mathrm{Hom}_{\mathbb{C}}(V, V^*)$$

an isomorphism corresponds to a G-invariant isomorphism inside $\mathrm{Hom}_{\mathbb{C}}(V, V^*)$. Because the above isomorphism is G-invariant and isomorphisms correspond to nondegenerate bilinear forms $V \times V \to \mathbb{C}$ (which of course is the same as an element of $(V \otimes_{\mathbb{C}} V)^*$ by the universal property of the tensor product) we see that the data of a G-isomorphism $V \xrightarrow{\sim} V^*$ is the same as the data of a G-invariant nondegenerate form $B : V \times V \to \mathbb{C}$.

If V is irreducible and there is a nonzero G-invariant bilinear form $B : V \times V \to \mathbb{C}$ this corresponds to a nonzero G-equivariant map $V \to V^*$. Because these are irreducible, by Shur's Lemma any nonzero map is an isomorphism and thus B must be nondegenerate. Furthermore, from the isomorphisms we know that,

$$\mathrm{Hom}_G(V, V^*) \subset \mathrm{Hom}_{\mathbb{C}}(V, V^*) \xrightarrow{\sim} \mathrm{Sym}_2(V^*) \oplus \bigwedge^2 V^*$$

corresponding to the space of G-invariant forms inside $(V \otimes V)^*$ under the natural isomorphisms. Since this space is one dimensional by Shur's lemma it is either inside $\mathrm{Sym}_2(V^*)$ or $\bigwedge^2 V^*$ and thus all are symmetric or all are alternating (there is really only one such G-invariant form up to scaling so this is not surprising).

26.3.3 c

We can choose a basis of $\bigwedge^2 V$ as $\frac{1}{2}(e_i \otimes e_j - e_j \otimes e_i)$. Applying the transformation,

$$\rho(g) \cdot e_{ij} = \tfrac{1}{2}(M_{ki}e_k \otimes M_{\ell j}e_\ell - M_{\ell j}e_\ell \otimes M_{ki}e_k) = M_{ki}M_{\ell j}\tfrac{1}{2}(e_k \otimes e_\ell - e_\ell \otimes e_k) = M_{ki}M_{\ell j}e_{k\ell}$$

if we restrict to pairs $i < j$ then we see that,

$$\rho(g) \cdot e_{ij} = M_{ki}M_{\ell j}e_{k\ell} - M_{ki}M_{\ell j}e_{\ell k}$$

Therefore, the trace of this transformation is,

$$\operatorname{tr}(\rho(g)) = \sum_{i<j}[M_{ii}M_{jj} - M_{ji}M_{ij}] = \frac{1}{2}\left[\sum_{i,j} M_{ii}M_{jj} - \sum_{i,j} M_{ij}M_{ji}\right] = \tfrac{1}{2}[(\operatorname{tr}(M))^2 - \operatorname{tr}\left(M^2\right)]$$

where I used that the combination $M_{ii}M_{ii} - M_{ji}M_{ij}$ is automatically zero if $i = j$. Thus, $\chi_\wedge(g) = \frac{1}{2}[\chi(g)^2 - \chi(g^2)]$.

Now suppose that $\chi(g)$ is real and V is irreducible. Then,

$$\langle \chi, \chi \rangle = \frac{1}{|G|}\sum_{g\in G} \overline{\chi(g)}\chi(g) = \frac{1}{|G|}\sum_{g\in G} \chi(g)^2 = 1$$

because χ is the character of an irreducible representation. Therefore,

$$\dim\left(\bigwedge^2 V\right)^G = \frac{1}{|G|}\sum_{g\in G}\chi_\wedge(g) = \sum_{g\in G}\tfrac{1}{2}[\chi(g)^2 - \chi(g^2)] = \frac{1}{2}\left[1 - \sum_{g\in G}\chi(g^2)\right]$$

However, the dimension must be equal to one if we have a nonzero G-invariant alternating form (it is at least one because a nonzero B is G-invaraint but by Shur's lemma we know the dimension is at most one) and therefore,

$$\sum_{g\in G}\chi(g^2) = 1$$

such that the above formula gives $\dim(\bigwedge^2 V)^G = 1$.

26.4 10

26.4.1 a

Let F be an algebraically closed field. The maximal ideals of $F[x_1, \ldots, x_n]$ are of the form $\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ for $\alpha_i \in F$.

26.4.2 b

Let K be a field and $\overline{K}$ its algebraic closure and $\operatorname{Aut}\left(\overline{K}/K\right)$ be the group of automorphisms of $\overline{K}/K$. For $a \in \overline{K}^n$ define,

$$\mathfrak{m}_a = \{f \in K[x_1, \ldots, x_n] \mid f(a) = 0\}$$

I claim that $\mathfrak{m}_a$ is a maximal ideal. Indeed. consider the evaluation map $K[x_1, \ldots, x_n] \to \overline{K}$ given by sending $f \mapsto f(a)$. Then $\mathfrak{m}_a = \ker(f \mapsto f(a))$ so to show that $\mathfrak{m}_a$ is maximal it suffices to show

that the image is a field. I claim that if $A \subset \overline{F}$ is a K-algebra then A is a field. Indeed, for each $a \in A$ we know that $K[a] \subset A$ but $a^{-1} \in K[a]$ because $a \in \overline{K}$ is algebraic over K. Therefore A contains all inverses proving that it is a field.

Consider the map $a \mapsto \mathfrak{m}_a$ I claim this gives a bijection between the Aut $\left(\overline{K}/K\right)$-orbits of $\overline{K}^n$ and mSpec $(K[x_1, \ldots, x_n])$. First let $\mathfrak{m} \subset K[x_1, \ldots, x_n] = S$ be any maximal ideal. Then $S/\mathfrak{m}$ is a fintiely generated K-algebra and a field and thus is a finite extension of K by the nullstellensatz. Therefore, there is an embedding $S/\mathfrak{m} \hookrightarrow \overline{K}$ so consider the images of x_i under $S \to S/\mathfrak{m} \hookrightarrow \overline{K}$ which define $a \in \overline{K}^n$. Then $\mathfrak{m} = \ker(S \to \overline{K})$ is exactly $f \in S$ such that $f(a) = 0$ because this map evaluates $x_i \mapsto a_i$. Therefore $a \mapsto \mathfrak{m}_a$ is surjective.

Finally, $\mathfrak{m}_a = \mathfrak{m}_b$ if and only if a and b are conjugate under the Galois group. Indeed, suppose $\mathfrak{m}_a = \mathfrak{m}_b$ then $S/\mathfrak{m}_a \cong S/\mathfrak{m}_b$ as fields over K sending $x_i \mapsto x_i$. Furthermore, a, b fix embeddings $S/\mathfrak{m}_a \hookrightarrow \overline{K}$ and $S/\mathfrak{m}_b \hookrightarrow \overline{K}$ and we can extend the map $S/\mathfrak{m}_a \to S/\mathfrak{m}_b$ to an automorphism $\overline{K} \to \overline{K}$. Therefore we get an automorphism taking $a \mapsto b$ because the embeddings take $x \mapsto a$ and $x \mapsto b$ respectively.

26.4.3 c

First notice that $\mathfrak{m}_a = (x-a) \cap K[x_1, \ldots, x_n]$ where $(x-a) = (x_1 - a_1, \ldots, x_n - a_n) \subset \overline{K}[x_1, \ldots, x_n]$ is the corresponding maximal ideal in the larger ring. This is because $(x-a)$ is exactly the ideal of $f \in \overline{K}[x_1, \ldots, x_n]$ such that $f(a) = 0$ so this aligns with the definition of $\mathfrak{m}_a$.

Let K be a field of characteristic zero. Let $Z \subset \overline{K}^n$ be the zero set of $f(x_1, \ldots, x_n) \in \overline{K}[x_1, \ldots, x_n]$. Assume that Z is stable under the Aut $\left(\overline{K}/K\right)$-action. Consider the ideal,

$$I = I(Z) = \{f \in K[x_1, \ldots, x_n] \mid \forall z \in Z : f(z) = 0\} = \bigcap_{z \in Z} \{f \in K[x_1, \ldots, x_n] \mid f(z) = 0\}$$
$$= \bigcap_{z \in Z} \mathfrak{m}_z = K[x_1, \ldots, x_n] \cap \bigcap_{z \in Z} (x - z) = K[x_1, \ldots, x_n] \cap g\overline{K}[x_1, \ldots, x_n]$$

where we have,

$$g\overline{K}[x_1, \ldots, x_n] = \bigcap_{z \in Z} (x - z)$$

because we can assume that g is irreducible and the ring is Jacobson so (g) is the intersection of the maximal ideals containing it and,

$$(g) \subset (x - z) \iff g \in (x - z) \iff g(z) = 0 \iff z \in Z$$

Now I claim that,

$$V(I) = \{a \in \overline{K}^n \mid \forall f \in I : f(a) = 0\} = Z$$

and that I is principal which together prove the claim.

To see this, notice that,

$$Z \subset V(I)$$

because if $z \in Z$ then $f(z) = 0$ for all $f \in I$.

Furthermore, consider,

$$J = g\overline{K}[x_1, \ldots, x_n] \cap K[x_1, \ldots, x_n]$$

We know that for all $f \in J$ and $z \in Z$ we have $f \in \mathfrak{m}_z$ so $J \subset I$. Furthermore, if $\mathfrak{m}_a$ is maximal with $J \subset \mathfrak{m}_a$ then in

27 Fall 2016 Part I

27.1 1 DO THIS!!

27.2 2

27.2.1 a

Let k be a finite field. Then its characteristic is p for some $p > 0$ because otherwise it would contain $\mathbb{Q}$ which is infinite. Then consider k as a vector space over its prime subfield $\mathbb{F}_p$ and thus $|k| = p^n$ where n is the dimension. Notice that k is the splitting field of $x^{p^n} - x$ since $k^\times$ is cyclic of order $p^n - 1$ every element satisfies this polynomial and thus k is generated by the roots of this polynomial over $\mathbb{F}_p$. Since splitting fields are unique this proves uniqueness.

27.2.2 b

Let $p \neq 5$ be prime. Let K be the splitting field of $f = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + 1)$ over $\mathbb{F}_p$. If K is quadratic then $|K| = p^2$ and thus $K^\times$ is a cyclic group of order $p^2 - 1$ containing all 5-th roots of unity and thus $5 \mid p^2 - 1$ but if $5 \mid p - 1$ then $\mathbb{F}_p$ would contain all 5-th roots of unity so $K = \mathbb{F}_p$ and thus $5 \mid p + 1$. Conversely, if $5 \mid p + 1$ then the unique quadratic extension contains all roots of unity and it is obviously the smallest such extension so it is the splitting field.

27.3 3

27.3.1 a DO THIS PART!!

27.3.2 b

Let $G \subset \mathrm{GL}_n(\mathbb{R})$ be a finite subgroup which acts irreducible on $\mathbb{R}^n$. Let F be the space of quadratic forms which becomes a G-action and consider F^G. The averaging map $F \to F^G$ takes the standard quatratic form Q to a nonzero form because $Q(v) > 0$ for $v \neq 0$ and this remains true of the average because each term $Q(g \cdot v) > 0$ is positive so the sum is positive. Thus $\dim F^G = 1$.

Now suppose that $Q, Q' \in F^G$ then choose a basis $v_1, \ldots, v_n$ for which Q and Q' are both diagonal with matrices D, D'. Then because Q and Q' are G-invariant these diagonal matrices must commute with the G-action (since Q uniquely determines the values a_i including the ordering once a basis is fixed) and thus by Shur's lemma D and D' are scalar matrices and thus Q and Q' are dependent so $\dim F^G \leq 1$. Thus $\dim F^G = 1$.

27.4 4

Let G be a finite group and $Q \subset G$ a normal subgroup with prime index p.

27.4.1 a

Let $\psi : Q \to \mathbb{C}^\times$ be a character. Suppose that $\mathrm{Ind}_Q^G(\psi)$ is reducible. Then,

$$\mathrm{Hom}_G\left(\mathrm{Ind}_Q^G(\psi), \mathrm{Ind}_Q^G(\psi)\right) = \mathrm{Hom}_G\left(\psi, \mathrm{Res}_Q^G\left(\mathrm{Ind}_Q^G(\psi)\right)\right) = \bigoplus_{g \in G/Q} \mathrm{Hom}_G(\psi, g * \psi)$$

so for some $g \notin Q$ we must have $\psi = \psi \circ c_g^{-1}$ and since g generates G/Q we see that $\psi \circ c_g^{-1} = \psi$ for all $g \in G$. For any sequence of groups,

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

there is the inflation restriction sequence,

$$1 \longrightarrow H^1(G/N, A^N) \longrightarrow H^1(G, A) \longrightarrow H^1(N, A)^{G/N} \longrightarrow H^2(G/N, A^N) \longrightarrow H^2(G, A)$$

Therefore, if A is a trivial G-module then,

$$1 \longrightarrow \mathrm{Hom}\,(G/N, A) \longrightarrow \mathrm{Hom}\,(G, A) \longrightarrow \mathrm{Hom}\,(N, A)^{G/N} \longrightarrow H^2(G/N, A) \longrightarrow H^2(G, A)$$

therefore we can extend any map $N \to A$ invariant under the G/N conjugation action to $G \to A$ if $H^2(G/N, A) = 0$. In our case $A = \mathbb{C}^\times$ and G/N is finite cyclic to by Tate's theorem,

$$H^2(G/N, A) = \hat{H}^0(G/N, A) = \mathrm{coker}\,\mathrm{Nm}$$

where $\mathrm{Nm} : A \to A^G$ is the map,

$$a \mapsto \sum_{g \in G/N} g \cdot a = |G/N|a$$

which in our case is surjective because $\mathbb{C}^\times$ is divisible and thus $H^2(G/N, A) = 0$. Therefore $\psi : Q \to \mathbb{C}^\times$ extends to a character $\psi' : G \to \mathbb{C}^\times$.

27.4.2 b

Let V be an irreducible G-representation. Then $\mathrm{Res}^G_Q(V)$ splits into 1-dimensional representations because Q is abelian. For any $\psi \subset \mathrm{Res}^G_Q(V)$ consider,

$$\mathrm{Hom}_G\left(\mathrm{Ind}^G_Q(\psi), V\right) = \mathrm{Hom}_G\left(\psi, \mathrm{Res}^G_Q(V)\right) \neq 0$$

If $\mathrm{Ind}^G_Q(\psi)$ is irreducible then $\mathrm{Ind}^G_Q(\psi) \cong V$ because V is also irreducible and thus $\dim V = p$ because $\dim \mathrm{Ind}^G_Q(\psi) = [G : Q] \cdot 1 = p$. Otherwise, ψ extends to $\psi' : G \to \mathbb{C}^\times$ so $\psi = \mathrm{Res}^G_Q(\psi')$ and thus,

$$\mathrm{Ind}^G_Q(\psi) = \mathrm{Ind}^G_Q\left(\mathrm{Res}^G_Q(\psi')\right) = \mathbb{C}[G/Q] \otimes \psi'$$

which splits into 1-dimensional irreducible representations because $\mathbb{C}[G/Q]$ splits since G/Q is abelian. Therefore V must be 1-dimensional since it is equal to an irreducible factor of $\mathrm{Ind}^G_Q(\psi)$.

27.5 5

Let k be an algebraically closed field and $n \geq 1$ an integer.

27.5.1 a

Proposition 27.5.1. Let X be a nonempty Noetherian topological space. Then X has finitely many irreducible components (maximal irreducible sets) and thus we can write,

$$X = Z_1 \cup \cdots \cup Z_n$$

where $Z_i \neq Z_j$ are closed irreducible subsets. Moreover this decomposition is unique up to reordering.

We proceed by Noetherian induction. This trivially holds for the empty set. Now let $Z \subset X$ be closed. If Z is irreducible we are done. Otherwise write $Z = Z_1 \cup Z_2$ with both $Z_1, Z_2 \subsetneq Z$ closed. Then by the induction hypothesis Z_1, Z_2 have finitely many irreducible components. Each component of Z is contained in Z_1 or Z_2 by irreducibility and thus Z has finitely many irreducible components thus proving the claim by induction.

27.5.2 b

Let $I \subset k[X_1, \ldots, x_n] = R$ be a radical proper ideal. Because R is Noetherian we see that R/I is Noetherian so $X = \operatorname{Spec}(R/I)$ is Noetherian. Therefore X has finitely many irreducible components which are of the form $V(\mathfrak{p})$ for minimal primes $\mathfrak{p} \supset I$. Since $V(\mathfrak{p})$ uniquely determines $\mathfrak{p}$ via,

$$\mathfrak{p} = \bigcap_{\mathfrak{q} \in V(\mathfrak{p})} \mathfrak{q}$$

we see that there are finitely many minimal primes over I. Furthermore, by Zorn's lemma, every irreducible set is contained in some component (for a general space) and thus each prime above I contains a minimal such element.

27.5.3 c

Let,

$$C = \{(x, y, z) \in k^3 \mid x^4 = y^3, x^5 = z^3, y^5 = z^4\}$$

Since k is algebraically closed, $x = t^3$ is surjective and thus $y = t^4$ and $z = t^5$ so we see that C is the image of $t \mapsto (t^3, t^4, t^5)$ and the continuous image of an irreducible set is irreducible.

28 Fall 2016 Part II

28.1 5

Let $A = \mathbb{Z}[\sqrt{-5}]$ and define the ideal $P = (2, 1 + \sqrt{-5}) \subset A$.

28.1.1 a

It is clear that $A/P = \mathbb{Z}/2\mathbb{Z}$ as a ring where $\sqrt{-5} \mapsto -1$ because $1 + \sqrt{-5} \in P$. Therefore P is maximal because $\mathbb{Z}/2\mathbb{Z}$ is a field. Suppose that P were principal then $P = (\alpha)$. Therefore $2 = \alpha\beta$ and $1 + \sqrt{-5} = \alpha\beta'$. Taking norms we see that,

$$N(\alpha)N(\beta) = 4 \quad \text{and} \quad N(\alpha)N(\beta') = 6$$

and therefore $N(\alpha) = 1, 2$. However, it is impossible for $a^2 + 5b^2 = 2$. Thus $a^2 + 5b^2 = 1$ so $a = \pm 1$ and $b = 0$ but then $(\alpha) = R$ which does not work. Thus P is not principal.

28.1.2 b

In any DVR $(R, \mathfrak{m})$ we know that the only nontrivial ideals are $\mathfrak{m}^n$ so if $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ then $(a) \subset \mathfrak{m}$ is not contained in P^2 so we must have $(a) = \mathfrak{m}$ and thus a is a uniformizer. For the case $R = A_P$ and $\mathfrak{m} = PA_P$ we need to check that $a \in P \setminus P^2$ implies that $a \in \mathfrak{m} \setminus \mathfrak{m}^2$. It is obvious that $a \in \mathfrak{m}$ so we just need to show that $a \notin \mathfrak{m}^2$. Supppose that $a \in \mathfrak{m}^2$ then $a = bs^{-1}$ for $b \in P^2$ and $s \in A \setminus P$ and

thus $b = as$. Since P is maximal we can write $sr = 1 + c$ with $c \in P$ and thus $rb = asr = a - ac$ so $a = rb + ac \in P^2$ giving a contradiction. Thus $a \notin \mathfrak{m}^2$.

It suffices to show that $1 + \sqrt{-5} \notin P^2$. However, I claim that $P^2 = 2A$. Of the products of the generators, the only non-obvious calculation is,

$$(1 + \sqrt{-5})^2 = 1 + 6 + 2\sqrt{-5} = 2(3 + \sqrt{-5})$$

However, $1 + \sqrt{-5} \notin 2A$ because the coefficients are odd.

28.2 2

Let $G = S_3$ and $H = \langle (1\,2) \rangle$ is a subgroup of order 2. Let M be the $\mathbb{F}_2[G]$-module corresponding to the trivial G-representation so $\dim_{\mathbb{F}_2}(M) = 1$.

28.2.1 a

Let $R = \mathbb{F}_2[H]$ and $S = \mathbb{F}_2[G]$. Let N be a finitely generated S-module. If N is projective then N_R is projective because $\mathrm{Hom}_R(N_R, -) = \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, -))$ and S is free over R so this is an exact functor. Now suppose that N_R is projective. Since $R = \mathbb{F}_2[x]/(x^2 - 1)$ is a commutative ring and actually local then projective modules are free so we see that N_R is a free R-module of finite rank. Now, given a surjection $f : A \twoheadrightarrow B$ of S-modules and an S-map $\varphi : N \to B$ we can lift to a map $\tilde{\varphi} : N_R \to A_R$ of R-modules. Then we can take the averaging map $\mathrm{Hom}_R(N_R, A_R) \to \mathrm{Hom}_S(N, A)$ sending,

$$\tilde{\varphi} \mapsto \sum_{g \in G/H} g \circ \tilde{\varphi} \circ g^{-1}$$

However, because $f \circ \tilde{\varphi} = \varphi$ and f and φ are S-maps,

$$f \circ \left(\sum_{g \in G/H} g \circ \tilde{\varphi} \circ g^{-1} \right) = \sum_{g \in G/H} f \circ g \circ \tilde{\varphi} \circ g^{-1} = \sum_{g \in G/H} g \circ f \circ \tilde{\varphi} \circ g^{-1} = \sum_{g \in G/H} g \circ \varphi \circ g^{-1} = |G/H|\varphi$$

Therefore $|G/H|^{-1}$ (which exists in $\mathbb{F}_2$ since $|G/H| = 3$) times the average gives a lift.

28.2.2 b

Let P be the G-rep given by acting through $G \to G/\langle (1\,2\,3) \rangle \cong H$ on $\mathbb{F}_2^2$ by the swap action $(1\,2) \cdot e_1 = e_2$. I claim this is a projective R-module because $\mathbb{F}_2[H] \to P$ sending $1 \mapsto e_1$ and $(1\,2) \mapsto e_2$ is an isomorphism. Thus P is a projective G-representation. Furthermore, the map $P \to M$ by sending $e_i \mapsto 1$ is surjective and G-invariant and thus makes M a quotient by P.

Suppose there were two such P, P' which are G-modules equiped with a quotient map $P \twoheadrightarrow M$ and $P' \twoheadrightarrow M$ and $\dim_{\mathbb{F}_2}(P) = \dim_{\mathbb{F}_2}(P') = 2$. Then by projectivity we get lifts $P \to P'$ and $P' \to P$ as G-representations. The composition $P \to P' \to P$ is G-invariant and so its kernel is either trivial or one-dimensional (the map is not zero because it commutes with $P \twoheadrightarrow M$). By inspection the only nontrivial G-invariant subspace is the span of $e_1 + e_2$ and then if this maps to zero it means that e_1 and e_2 map to the same place so the images of e_1 and e_2 are fixed in P' and thus $P' = M \oplus M$ which is not projective since P'_R is not a free Rmodule. Thus the kernel must be trivial so for dimension reasons $P \cong P'$.

28.2.3 c

Consider the following resolution,

$$\cdots \longrightarrow P \xrightarrow{e_i \mapsto e_1+e_2} P \longrightarrow M \longrightarrow 0$$

Therefore we find,

$$\mathrm{Ext}^i_{\mathbb{F}_2[G]}(M, M) = H^i(\mathrm{Hom}_{\mathbb{F}_2[G]}(-, M)(P_\bullet)) = M$$

for all $i \geq 0$.

28.3 3 DO THIS

28.4 4 DO THIS

28.5 5 DO THIS

29 Spring 2016 Part I

29.1 2 FINISH THIS!!

Let k be a field and V a k-vectorspace. We say that $W \subset V$ is affine if,

$$w_1, \ldots, w_n \in W, a_1, \ldots, a_n \in k \text{ such that } \sum a_i = 1 \implies \sum a_i w_i \in W$$

29.1.1 a

If $W = \{v + u \mid u \in U\}$ for some subspace $U \subset V$ and vector $v \in V$ then,

$$\sum a_i(v + u_i) = \sum a_i v + \sum a_i u_i = v + \sum a_i u_i \in W$$

so W is affine. Conversely suppose that W is affine. Fix some $v \in W$ and consider $U = \{w - v \mid w \in W\}$. For any $w_1 - v, w_2 - v \in U$ we see that $v, w_1, w_2 \in W$ and $1+1-1 = 1$ so $w_1 + w_2 - v \in W$ and thus $(w_1 - v) + (w_2 - v) = (w_1 + w_2 - v) - v \in U$ so U. Also if $\lambda \in k$ then $\lambda + (1 - \lambda) = 1$ so $\lambda w + (1 - \lambda)v \in W$ and therefore $v + \lambda(w - v) \in W$ so $\lambda(w - v) \in U$ and thus U is a subspace such that $W = v + U$. Furthermore, chosing a different $v' \in W$ shifts U by $v' - v \in U$ and thus leaves U the same so U is unique.

29.1.2 b

Consider the 2-dimensional affine subspaces $W \subset \mathbb{F}_q^3$. There are $q + 1$ dimension two subspaces (given by choosing a linear functional up to scaling). For each U

29.2 3

Let (V, ρ) be a finite-dimensional $\mathbb{C}$-linear representation of a finite group G with character χ_ρ.

29.2.1 a

Let $G \subset H$ with H finite. Then,

$$\mathrm{Ind}_G^H(\rho) = \mathbb{C}[H] \otimes_{\mathbb{C}[G]} V$$

where $\mathbb{C}[H]$ acts on the left on $\mathbb{C}[H]$. Then we have,

$$\mathrm{Hom}_G\left(V, \mathrm{Res}_G^H(W)\right) = \mathrm{Hom}_G\left(\mathrm{Ind}_G^H(V), W\right)$$

In fact, $\mathrm{Ind}_G^H(-)$ is also a right adjoint to $\mathrm{Res}_G^H(-)$.

29.2.2 b

Consider the character of the $G \times G$-representation $(V \otimes V', \rho \otimes \rho')$ where (g, g') acts via $\rho(g) \otimes \rho'(g')$. Then,

$$\chi_{\rho\otimes\rho'}(g, g') = \mathrm{Tr}(\rho(g) \otimes \rho'(g')) = \mathrm{Tr}(\rho(g)) \cdot \mathrm{Tr}(\rho'(g')) = \chi_\rho(g)\chi_{\rho'}(g')$$

because we can choose a basis $e_i \otimes e_j$. Now,

$$\langle \chi_{\rho\otimes\rho'}, \chi_{\rho\otimes\rho'} \rangle = \frac{1}{|G|^2} \sum_{(g,g')\in G\times G} \overline{\chi_\rho(g)\chi_{\rho'}(g')}\chi_\rho(g)\chi_{\rho'}(g') = \left(\frac{1}{|G|}\sum_{g\in G}|\chi_\rho(g)|^2\right)\left(\frac{1}{|G|}\sum_{g'\in G}|\chi_{\rho'}(g')\right) = \langle \chi_\rho, \chi_\rho \rangle \langle \chi$$

This number is 1 if and only if ρ is irreducible and thus $\rho \otimes \rho'$ is irreducible iff ρ and ρ' are irreducible.

29.2.3 c

Let ρ and ρ' be irreducible G-representations and 1_G be the trivial character. Let $H = G \times G$ and $G \subset H$ diagonally $g \mapsto (g, g)$. Consider,

$$\mathrm{Hom}_H\left(\mathrm{Ind}_G^H(1_G), \rho \otimes \rho'\right) = \mathrm{Hom}_G\left(1_G, \mathrm{Res}_G^H(\rho \otimes \rho')\right)$$

Furthermore,

$$\dim \mathrm{Hom}_G\left(1_G, \mathrm{Res}_G^H(\rho \otimes \rho')\right) = \left\langle \chi_1, \chi_{\mathrm{Res}_G^H(\rho\otimes\rho')} \right\rangle = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)\chi_{\rho'}(g) = \langle \overline{\chi_\rho}, \chi_{\rho'} \rangle = \begin{cases} 1 & \chi_{\rho'} = \overline{\chi_\rho} \\ 0 & \text{else} \end{cases}$$

by orthogonality of characters. Therefore, $\rho \otimes \rho'$ appears as a subrepresentation n $\mathrm{Ind}_G^H(1_G)$ if and only if $\chi_{\rho'} = \overline{\chi_\rho}$ and in such cases it appears with multiplicity one.

29.3 5

Let K be a field of characteristic not equal to 2. Consider Galois extensions L/K with $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

29.3.1 a

Consider the elements $\sigma_1 = (1, 0)$ and $\sigma_2 = (0, 1)$. Then the fixed fields L^{σ_1} and L^{σ_2} are of degree 2 and thus $L^{\sigma_1} = K(\sqrt{a})$ and $L^{\sigma_2} = K(\sqrt{b})$. Now it suffices to show that $L = L^{\sigma_1}L^{\sigma_2}$. We know that the compositum coresponds to the subgroup $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{e\}$ proving that $L = L^{\sigma_1}L^{\sigma_2} = K(\sqrt{a}, \sqrt{b})$. Finally, if a/b is a square then $L = K(\sqrt{a})$ contradicting the size of the Galois group being 4 so we must have $a, b, a/b$ nonsquares in K.

29.3.2 b

Let $c \in L^\times$ be a nonsquare and let $E = L(\sqrt{c})$. Suppose that E/K is Galois then $\mathrm{Gal}\,(L/K) = \mathrm{Gal}\,(E/K)\,/\mathrm{Gal}\,(E/L)$. For each $\sigma \in \mathrm{Gal}\,(L/K)$ choose a lift to $\sigma' \in \mathrm{Gal}\,(E/K)$ then we know that,

$$\frac{\sigma(c)}{c} = \frac{\sigma'(c)}{c} = \left(\frac{\sigma'(\sqrt{c})}{\sqrt{c}}\right)^2$$

We need to show that,

$$\frac{\sigma'(\sqrt{c})}{\sqrt{c}} \in L$$

We get an action $\mathrm{Gal}\,(L/K) \circlearrowright \mathrm{Gal}\,(E/L)$ by lifing. Indeed, for any $\tau \in \mathrm{Gal}\,(E/L)$ and $\sigma \in \mathrm{Gal}\,(L/K)$ choose a lift σ' and then $\sigma'\tau\sigma'^{-1}$ has trivial image in $\mathrm{Gal}\,(L/K)$ and thus lies in $\mathrm{Gal}\,(E/L)$ which is a well-defined action because if $\sigma'' = \sigma'\tau'$ so

$$\sigma''\tau\sigma''^{-1} = \sigma'\tau'\tau\tau'^{-1}\sigma'^{-1} = \sigma'\tau\sigma'^{-1}$$

because $\mathrm{Gal}\,(E/L) \cong \mathbb{Z}/2\mathbb{Z}$ is abelian. However, $\mathrm{Aut}\,(\mathbb{Z}/2\mathbb{Z})$ is trivial so this must be the trivial action meaning that σ' and τ commutes. Thus,

$$\tau\left(\frac{\sigma'(\sqrt{c})}{\sqrt{c}}\right) = \frac{\sigma'(\tau(\sqrt{c}))}{\tau(\sqrt{c})} = \frac{\sigma'(\sqrt{c})}{\sqrt{c}}$$

because $\tau(\sqrt{c}) = \pm\sqrt{c}$ since it must permute roots of $X^2 - c$. Therefore, $\frac{\sigma(c)}{c}$ is a square in L.

Conversely, if $\frac{\sigma(c)}{c} \in L$ is a square then we need to show that E/K is Galois. Equivalently we need to show that every K-embedding of $E \hookrightarrow \overline{K}$ is an automorphism. Indeed, consider such an embedding $\sigma : E \to \overline{K}$. Then restricting to L we get an automorphism $L \to L \subset \overline{K}$ over K because L/K is Galois and thus $\frac{\sigma(c)}{c}$ is a square. However, it is clear that $\sigma(E) = L(\sqrt{\sigma(c)})$ because $\sigma(\sqrt{c})$ solves $x^2 - \sigma(c)$. However, $\sqrt{\sigma(c)} = \sqrt{\frac{\sigma(c)}{c}} \cdot \sqrt{c}$ and the first term is an element of L so we se that $\sigma(E) = L(\sqrt{\sigma(c)}) = L(\sqrt{c}) = E$ and thus E/K is Galois.

29.3.3 c

Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $c = (3 - \sqrt{3})(2 - \sqrt{2})$. Consider the norm for $L/\mathbb{Q}(\sqrt{2})$,

$$N(c) = (3 - \sqrt{3})(3 + \sqrt{3})(2 - \sqrt{2})^2 = 6(2 - \sqrt{2})^2$$

However, 6 is not a square in $\mathbb{Q}(\sqrt{2})$ because then 3 would be a square. Therefore c cannot be a square in L.

Now we need to consider $\frac{\sigma(c)}{c}$. For two signs $\eta_1, \eta_2 \subset \{\pm 1\}$ we need to compute,

$$\frac{(3 - \eta_1\sqrt{3})(2 - \eta_2\sqrt{2})}{(3 - \sqrt{3})(2 - \sqrt{2})} = \frac{3 - \eta_1\sqrt{3}}{3 - \sqrt{3}} \cdot \frac{2 - \eta_2\sqrt{2}}{2 - \sqrt{2}}$$

In the case $\eta_i = 1$ that term is 1 and thus a square. Thus we need to consider,

$$\frac{3 + \sqrt{3}}{3 - \sqrt{3}} = \frac{(3 + \sqrt{3})^2}{9 - 3} = \frac{(3 + \sqrt{3})^2}{6} = \frac{(3 + \sqrt{3})^2}{(\sqrt{2}\sqrt{3})^2}$$

which is a square. Similarly,

$$\frac{2+\sqrt{2}}{2-\sqrt{2}} = \frac{(2+\sqrt{2})^2}{4-2} = \frac{(2+\sqrt{2})^2}{2} = \frac{(2+\sqrt{2})^2}{(\sqrt{2})^2}$$

is also a square. Therefore, $E = L(\sqrt{c})$ is Galois.

30 Spring 2016 Part II

30.1 1

Let J be an $n \times n$ matrix over an algebraically closed field k with characteristic not 3. Let the minimal polynomial of J be $(T-\lambda)^n$ for some $\lambda \in k^\times$. Then the Jordan canonical form of J has one Jordan block of size n with eigenvalue λ. Thus we can write $J = \lambda I + N$ where N is a nilpotent matrix of degree n. Then,

$$J^3 = \lambda^3 I + 3N + 3N^2 + N^3$$

Now $3N + 3N^2 + N^3 = (3 + 3N + N^2)N$ is nilpotent of degree n because $(3 + 3N + N^2)$ is invertible and commutes with N so it preserves nilpotence degree. Therefore the minimal polynomial of J^3 is $(J^3 - \lambda^3)^n = 0$ and thus J has a single Jordan block of size n with eigenvalue λ^3.

30.2 2

30.2.1 a

Consider the projective resolution,

$$0 \longrightarrow \mathbb{Z} \xrightarrow{6} \mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z} \longrightarrow 0$$

30.2.2 b

After applying the functor $- \otimes_{\mathbb{Z}} \mathbb{Z}/8\mathbb{Z}$ we get the complex,

$$0 \longrightarrow \mathbb{Z}/8\mathbb{Z} \xrightarrow{6} \mathbb{Z}/8\mathbb{Z}$$

and thus,

$$\operatorname{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & i = 0 \\ \mathbb{Z}/4\mathbb{Z} & i = 1 \\ 0 & i > 1 \end{cases}$$

30.2.3 c

Applying the functor $\operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/9\mathbb{Z})$ we get the complex,

$$0 \longrightarrow \mathbb{Z}/9\mathbb{Z} \xrightarrow{6} \mathbb{Z}/9\mathbb{Z}$$

and thus,

$$\operatorname{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}) = \begin{cases} \mathbb{Z}/3\mathbb{Z} & i = 0 \\ \mathbb{Z}/3\mathbb{Z} & i = 1 \\ 0 & i > 1 \end{cases}$$

30.3 4

Let A be a commutative ring $f : A \to B$ a finite type ring homomorphism. Let $\mathfrak{m} \subset B$ be maximal and $\mathfrak{p} = f^{-1}(\mathfrak{m})$ be a prime of A.

30.3.1 a

Because localization is exact, there is an exact sequence,

$$0 \longrightarrow \mathfrak{p}A_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}(A/\mathfrak{p})_{\mathfrak{p}} \longrightarrow 0$$

and therefore $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong (A/\mathfrak{p})_{\mathfrak{p}} = \text{Frac}\,(A/\mathfrak{p})$ because $\mathfrak{p}$ is the zero ideal in the domain $A/\mathfrak{p}$. Let $K = \text{Frac}\,(A/\mathfrak{p})$.

30.3.2 b

The fiber of the map $f^* : \text{Spec}\,(B) \to \text{Spec}\,(A)$ over the point $\mathfrak{p}$ is given by $\text{Spec}\,(B')$ where,

$$B' = B \otimes_A K$$

Explicitly, $B' = (B \otimes_A A/\mathfrak{p})_{\mathfrak{p}} = (B/\mathfrak{p}B)_{\mathfrak{p}}$. Since $\mathfrak{m} \mapsto \mathfrak{p}$ we see that $\mathfrak{p}B \subset \mathfrak{m}$ and therefore $\mathfrak{m}$ corresponds to an ideal in $B/B\mathfrak{p}$. Then localization at $\mathfrak{p}$ preserves it because $f(A \setminus \mathfrak{p}) \cap \mathfrak{m} = \varnothing$ since $\mathfrak{p} = f^{-1}(\mathfrak{m})$. Therefore there is such an ideal $\mathfrak{m}' \subset B'$ explcicitly $\mathfrak{m}' = (\mathfrak{m}/\mathfrak{p}B)_{\mathfrak{p}}$. Furthermore,

$$B'/\mathfrak{m}' = [(B/\mathfrak{p}B)/(\mathfrak{m}/\mathfrak{p}B)]_{\mathfrak{p}} = [B/\mathfrak{m}]_{\mathfrak{p}} = B/\mathfrak{m}$$

where the last step follows becaues $B/\mathfrak{m}$ is a field and thus localization does nothing.

Now B' is a finitely generated K-algebra because $A \to B$ is finite type and $B/\mathfrak{m} = B'/\mathfrak{m}'$ is a field and a finitely generated K-algebra and thus a finite field extension of K. Thus $B/\mathfrak{m}$ is a finite K-module so through the map $A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = K$ we see that $B/\mathfrak{m}$ is a finite $A_{\mathfrak{p}}$-module.

30.3.3 c

Choose a set of generators $x_1, \ldots, x_n \in B/\mathfrak{m}$ as an A-algebra. We can write $B/\mathfrak{m} = A[x_1, \ldots, x_n]/I$. However, since B is finite over $A_{\mathfrak{p}}$ we know that x_i is integral over $A_{\mathfrak{p}}$ so it satisfies some monic $p_i \in A_{\mathfrak{p}}[x]$. By taking $t \in A \setminus \mathfrak{p}$ to be the product of the denominators of the coefficients of all p_i we can see that $p_i \in A_t[x]$ and thus $x_i \in B/\mathfrak{m}$ is integral over A_t and thus $B/\mathfrak{m}$ is a finite A_t-module.

30.3.4 d

Consider $A_t/\mathfrak{p}A_t = (A/\mathfrak{p})_t$. We know that $B/\mathfrak{m}$ is a finitely generated A_t-module and thus a finitely generated $A_t/\mathfrak{p}A_t$-module. However, $A_t/\mathfrak{p}A_t \subset K \subset B/\mathfrak{m}$ and thus K is finite over $A_t/\mathfrak{p}A_t$ but then each element is algebraic so $A_t/\mathfrak{p}A_t \subset K$ is a finite extension of domains and hence $A_t/\mathfrak{p}A_t$ is a field (and thus $A_t/\mathfrak{p}A_t = K$) meaning that $\mathfrak{p}A_t$ is maximal.

30.4 5

30.4.1 a

Let L be a quadratic extension of a field F with characteristic not 2 and let $h \in F[x]$ be an irreducible cubic. If h is reducible in $L[x]$ it must have a linear factor and thus a root $\alpha \in L$ but then $F(\alpha) \subset L$ has degree 3 over F because h is irreducible of degree 3 which is a contradiction to $[L : F] = 2$. Therefore $x^3 - x - 2$ is irreducible over $\mathbb{F}_{25}$ since it is irreducible over $\mathbb{F}_5$ because it has no root (easy computation).

30.4.2 b

With $f = x^3 - x - 2$ in $\mathbb{F}_{25}[x]$ let $K = \mathbb{F}_{25}[x]/(f)$ and α be the image of x in K. We know that the roots $\alpha_1, \alpha_2, \alpha_3$ have $\alpha_1 + \alpha_2 + \alpha_3 = 0$ and $\alpha_1\alpha_2\alpha_3 = 2$. We know that $\alpha_1 = \alpha$. The Frobenius $x \mapsto x^5$ acts on the roots so,

$$\alpha^5 = \alpha^2(\alpha + 2) = \alpha^3 + 2\alpha = \alpha + 2 + 2\alpha^2 = 2\alpha^2 + \alpha + 2$$

is another root of f. Since $\alpha_1 + \alpha_2 + \alpha_3 = 0$ we see that,

$$\alpha_3 = 3(\alpha^2 + \alpha + 1)$$

30.4.3 c

Now we compute,

$$N_{K/\mathbb{F}_5}(\alpha) = \alpha_1^2\alpha_2^2\alpha_3^2 = 2^2 = -1$$

31 Fall 2018 Part II

31.1 1

Let V be a finite $\mathbb{C}$ vector space and let $B : V \times V \to \mathbb{C}$ be a non-degenerate symmetric bilinear form. Let $T : V \to V$ be a nilpotent linear transformation such that,

$$B(Tx, y) = -B(x, Ty)$$

Let $\dim \ker T = 1$.

31.2 4

31.2.1 a

Let A be an integrally closed noetherian domain with fraction field F and F'/F is a finite extension. Let A' be the integral closure in F'.

Choose a basis $e_1, \ldots, e_n$ of F' over F. Since $F' = \mathrm{Frac}\,(A')$ (any element of F' has a multiple that is integral over A) then $D(Ae_1 + \cdots + Ae_n) \subset A'$. Furthermore, let $f_i = De_i$ then consider the bilinear form $B(x, y) = \mathrm{tr}\,(xy)$. If $a \in A'$ then a is monic over A and thus $\mathrm{tr}\,(a)$ is monic over A but $\mathrm{tr}\,(a) \in F$ so $\mathrm{tr}\,(a) \in A$ because A is integrally closed. This is symmetric and non-degenerate because for each $x \neq 0$ there is y such that $xy = N(x) \in A$ and then $\mathrm{tr}\,(xy) = nN(x) \neq 0$. Consider

the dual basis f_i^* pulled back through B as an isomorphism to the dual space i.e. $B(f_i, f_j^*) = \delta_{ij}$. I claim that $A' \subset f_1^* A + \cdots + f_n^* A$. Indeed, if $a \in A'$ then $B(a, b)$ lies in A for $b \in f_1 A + \cdots f_n A$ so a is in the span of f_i^*. To see this, suppose that $a \in F'$ such that $B(a, f_i) \in A$ for each i. We know that $a = s_1 f_1^* + \cdots + s_n f_n^*$ for $s_i \in F$ and then $B(a, f_i) = s_i \in A$ so a is in the A-span of the f_i.

32 Fall 2019 Part I

32.1 1

Let G be a simple group of order $n = 168 = 2^3 \cdot 3 \cdot 7$.

32.1.1 a

The Sylow p-subgroups of G have order 7. Furthermore, they are all conjugate to eachother and the number of Sylow 7 subgroups is,

$$n_7 = 1 + 7k \mid 2^3 \cdot 3$$

Since G is simple n_7 cannot be 1 and therefore $n_7 = 8$. Now two distinct Sylow p subgroups have distinct elements (except e) because they have prime order and every non identity element is a generator and thus has order 7. Furthermore, every order 7 element generates a Sylow-7 subgroup. Therefore the number of such elements is,

$$(7 - 1) \cdot n_7 = 6 \cdot 8 = 48$$

32.1.2 b

Let P be a Sylow-7 subgroup. We know that $[G : N_G(P)] = n_7 = 8$. Furthermore, the transitive G-action on Sylow-7 subgroups has stabilizer at P equal to $N_G(P)$ so there is an isomorphism of G-sets $G/N_G(P) \xrightarrow{\sim} \mathrm{Syl}_7(G)$. Now inside $N_G(P)$ we have a Sylow-3 subgroup $Q \subset N_G(G)$ (which is also Sylow-3 inside G because their orders are both divisible extactly by 3). Let $g \in P$ be an element of order 7. Then because g generates P we see that $C_G(g) \subset C_G(P) \subset N_G(P)$. Furthermore, since P is abelian we see that $P \subset C_G(g)$. Therefore, $C_G(g) = C_G(P)$ has either order 7 or order $3 \cdot 7$. Suppose that $C_G(g)$ has order $3 \cdot 7$. Then $Q \subset C_G(g)$ by standard arguments $C_G(g) \cong Q \times P \cong \mathbb{Z}/21\mathbb{Z}$. Therefore $C_G(g)$ has an element of order 21 but I claim that G does not. If x is such an element then $x^7 \in Q$ but then $x^3 \in C_G(Q) \subset N_G(Q)$ has order 7 so $N_G(Q)$ has order divisible by 7. Therefore $n_3 = |G|/|N_G(G)|$ is not divisible by 7. Therefore $n_3 \mid 8$ by the third Sylow theorem. Thus we must have $n_3 = 4$ because it cannot be normal. Therefore, G acts on $\mathrm{Syl}_3(G)$ transtiviely by conjugation giving a map $G \to \mathrm{Sym}(\mathrm{Syl}_3(G))$ whose kernel is normal. Since G is simple this kernel is trivial (the map is nontrivial) but $|\mathrm{Sym}(\mathrm{Syl}_3(G))| = 4! = 8 \cdot 3$ which is less than 168 giving a contradiction. Therefore we cannot have an element of order 21 so we must have that $C_G(g)$ has order 7.

Therefore the orbits under conjugation of elements of order 7 have size $|G|/|C_G(g)| = 8 \cdot 3$ and thus there are $48/24 = 2$ such orbits.

32.2 2

Let A be a commutative ring and M, N be A-modules and $B : M \times N \to A$ a bilinear form.

32.2.1 a

Let $m_1, \ldots, m_r \in M$ consider the map,

$$\beta_{m_1,\ldots,m_r} : \wedge^r N \to A$$

defined on elementry forms by sending,

$$\beta_{m_1,\ldots,m_r}(n_1 \wedge \cdots \wedge n_r) = \det B(m_i, n_j)$$

It suffices to show that such a map is well-defined on elementary forms or equivalent to define a map $\beta : N^r \to A$ and check that it is linear in each factor and alternating. This follows directly from properties of the determinant. If we consider,

$$\beta(n_2 \wedge n_1 \wedge \cdots \wedge n_r)$$

is the determinant with the first two rows swapped giving,

$$\beta(n_2 \wedge n_1 \wedge \cdots \wedge n_r) = -\beta(n_1 \wedge n_2 \wedge \cdots \wedge n_r)$$

as required. Linearity in each n_i follows from the multilinearity of the determinant and bilinerity of B. Finally, the determinant is alternating so by the universal property there is a map $\beta : \wedge^r N \to A$.

32.2.2 b

Consider the map,

$$\wedge^r(B) : \wedge^r M \times \wedge^r N \to A$$

defined by sending

$$(m_1 \wedge \cdots \wedge m_r, n_1 \wedge \cdots \wedge n_r) \mapsto \beta_{m_1,\ldots,m_r}(n_1 \wedge \cdots \wedge n_r)$$

This map clearly has the required propety so it suffices to show that $\wedge^r M \to (\wedge^r N)^*$ via $m_1 \wedge \cdots \wedge m_r \mapsto \beta_{m_1,\ldots,m_r}$ is well-defined. Clearly the map $M^r \to (\wedge^r N)^*$ is well-defined. It is linear in each factor because B is bilinear and because the determinant is multilinear. It is alternating because the determinant is alternating. Thus is descends to a map $\wedge^r N \to (\wedge^r M)^*$.

32.2.3 c

This follows immediately from the fact that the determinant of a matrix is the same as its transpose since,

$$\wedge^r(B)(n_1 \wedge \cdots \wedge n_r, m_1 \wedge \cdots \wedge m_r) = \det B(n_i, m_j) = \det B(m_j, n_i) = \det \left(B(m_i, n_j)\right)^\top$$

32.3 3

32.3.1 a

Consider the group $G = \mathrm{GL}_3(\mathbb{F}_5)$. Then $|G| = (5^3-1)(5^3-5)(5^3-5^2) = 5^3(5^3-1)(5^2-1)(5-1)$.

We make use of rational canonical form. For each conjugacy class there is a unique element such that $\mathbb{F}_5^3$ is decomposed as a $\mathbb{F}_5[x]$-module as,

$$\mathbb{F}_5[x]/(p_1) \oplus \cdots \oplus \mathbb{F}_5[x]/(p_r)$$

where $p_1 \mid \cdots \mid p_r$. Where $m = p_r$ is the minimal polynomial. We need to consider the cases $m \mid x^2-1$ or $m \mid x^3-1$ or $m \mid x^5-1$. Now in the case of order 5 the matrix satisfies $x^5-1 = (x-1)^5$ but it satisfies a characteristic polynomial of degree 3 thus its minimal polynomial is either $(x-1)$ or $(x-1)^2$ or $(x-1)^3$. Now $x-1$ gives just the identity so we can igore this case. However both the other options work. There are a few different cases to consider.

For $m \mid x^2-1 = (x-1)(x+1)$ we consider three cases. Either $m = (x-1)$ (giving the identiy which does not have order 2) or $m = (x+1)$ giving $T = -I$ which does have order two giving the case $p_1 = p_2 = p_3 = x+1$ or $m = x^2-1$ and $p_1 = x-1$ or $p_2 = x-1$ giving two different possibilites. Thus there are three conjugacy classes of order 2 elements.

For $m \mid x^3-1 = (x-1)(x^2+x+1)$ we know x^2+x+1 is irreducible. Thus either $m = x-1$ giving the identity (which we don't consider it has order 1) or $m = x^2+x+1$ but then $p_1 \mid m$ cannot happen unless $p_1 = m$ but then we get an even dimensional space which contradicts our space being $\mathbb{F}_3$. Thus $m = x^3-1$ giving $p_1 = x^3-1$ and a single possibility (corresponding to the matrix representation of the frobenius for $\mathbb{F}_{5^3}/\mathbb{F}_5$ choosing a $\mathbb{F}_5$ basis of $\mathbb{F}_{5^3}$). Therefore there is only one conjugacy class of order 3.

Finally we consider order 5. We know that either $m = (x-1)^3$ in which case $p_1 = (x-1)^3$ is the only possibility giving a single conjugacy class or $m = (x-1)^2$ and $p_1 = (x-1)$ and $p_2 = (x-1)^2$ giving a single other conjugacy class. Therefore there are two total conjugacy classes of order five elements.

32.3.2 b

It is true that M and $M^\top$ are always similar over any field K.

First, if K is algebraically closed then it suffices to show that M and $M^\top$ have the same Jordan normal form since a matrix is similar to its Jordan normal form. Obviously if M is in Jordan normal form then $M^\top$ perserves the block structure but flips it. Thus it suffices to show that if M consists of a single Jordan block then $M^\top$ is similar to M. This is given by sending a basis $e_1, \ldots, e_n$ to the basis $e_n, \ldots, e_1$ which swaps the off diagonal from the top to the bottom.

This I have shown that M and $M^\top$ are similar over $\overline{K}$. In general I claim that if A and B are similar over $\overline{K}$ they are similar over K. Indeed, we can write,

$$AC = CB$$

for some $C \in \mathrm{GL}_n(\overline{K})$. I can write $C = C_1 a_1 + \cdots + C_k a_k$ where $a_i \in \overline{K}$ are K-independent elements (e.g. choose a basis for the finite extension generated by the coefficients of C) and the C_i are matrices over K. Since,

$$AC_1 a_1 + \cdots + AC_k a_k = C_1 B a_1 + \cdots + C_k B a_k$$

and the matrices all have coefficients in K and the a_i are independent we see that for each i,

$$AC_i = C_i B$$

and thus the same is true for any linear combination. Thus we just need some,

$$\tilde{C} = C_1 x_1 + \cdots + C_k x_k$$

that is invertible. Consider the polynomial,

$$p(x_1, \ldots, x_n) = \det(C_1 x_1 + \cdots + C_k x_k)$$

which is nonzero because $p(a_1, \ldots, a_n) \neq 0$ since C is invertible. Thus p is not the zero polynomial. If K is infinite, this implies that p is not the zero function $K^k \to K$ and thus there is some nonzero value of p on K^k and thus some invertible $\tilde{C}$ showing that A and B are similar. However, if K is finite (FIX THIS!!)

32.4 4

Let p be a prime and $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime ideal (p). Let $P \subset \mathbb{Z}_{(p)}[x]$ be a prime ideal.

32.4.1 a

Suppose that $p \in P$. Clearly $(p) \subset P$. Suppose that $f \in P \setminus (p)$. Suppose that $f \mod p$ is reducible then $f = gh + pq$ for polynomials $g, h, q \in \mathbb{Z}_{(p)}[x]$. Since $pq \in P$ we see that $gh \in P$ and thus either $g \in P$ or $h \in P$. Continuing and using the fact that $\mathbb{Z}_{(p)}[x]$ is noetherian we conclude that there is some $f \in P \setminus (p)$ such that its reduction is irreducible. Now,

$$\mathbb{Z}_{(p)}[x]/(p, f) \xrightarrow{\sim} \mathbb{F}_p[x]/(f)$$

which is a field because f is irreducible and thus (p, f) is maximal so $P = (p, f)$ since $(p, f) \subset P$. Furthermore, I just showed that all such ideals (p, f) are maximal and therefore prime.

32.4.2 b

If $p \notin P$ then we could have $P = (0)$ but otherwise choose a nonzero $f \in P$. If every $f \in P$ has every coefficent divisible by p then $P \subset (p)$ in which case for each $g \in P$ we have $g = pr$ for some r so $r \in P$ because P is prime and thus $pP = P$ so by Nakayama's lemma (again using Noetherian-ness to get that P is finitely generated) there is $r = 1 - kp$ such that $(1 - kp)P = 0$ and thus $P = (0)$. since $1 - kp$ is a unit.

Otherwise we can choose some $f \in P$ with,

$$f = a_0 x^n + \cdots + a_n$$

where $p \not| a_i$ for some i. Suppose that f is reducible over $\mathbb{Q}$ then $f = gh$ for $g, h \in \mathbb{Q}[x]$. Write,

$$g = \sum b_i p^{-e_i} x^i \quad \text{and} \quad h = \sum b_i' p^{-e_i'} x^i$$

Therefore there is some power of p (namely the maximum of e_i) such that $p^n g, p^m h \in \mathbb{Z}_{(p)}[x]$ and $(p^n g)(p^n h) = p^{n+m} f \in P$ so either $(p^n g)$ or $(p^m h) \in P$ and the degree is reduced and notice that not every coefficent of $p^n g$ and $p^m g$ is divisible by p. Therefore, choosing f to have minimal degree for the property of not every coefficient being divisible by p we see that $f \in \mathbb{Q}[x]$ is irreducible. Now I claim that $P = (f)$. If $g \in P$ then either $g \in f\mathbb{Q}[x]$ or $ag + bf = 1$ for $a, b \in \mathbb{Q}[x]$ since $f\mathbb{Q}[x]$ is a maximal ideal of $\mathbb{Q}[x]$. Then choose n large enough such that $p^n a, p^n b \in \mathbb{Z}_{(p)}[x]$ then $p^n(ag + bf) = p^n$ so $p^n \in P$ which we know is not possible for any n since P is prime. Thus we must have $g \in f\mathbb{Q}[x]$ and thus $g = fa$ for $a \in \mathbb{Q}[x]$. Then choosing p^n again such that $p^n a \in \mathbb{Z}_{(p)}[x]$

we get that $p^n g = f p^n a$. However, f and $p^n a$ both reduce mod p to nonzero polynomials which proves that $p^n = 1$ else $p^n g$ which is their product would reduce to a zero polynomial mod p since $g \in \mathbb{Z}_{(p)}[x]$. Thus $g \in (f)$ so $P = (f)$.

Now I need to show that (f) is prime for any such polynomial. Suppose that $ab = fg$ then viewing this equation in $\mathbb{Q}[x]$ we see that either $a = fc$ or $b = fc$ for $c \in \mathbb{Q}[x]$. Choosing a suitible p^n we get WLOG $p^n a = f(p^n c)$ but f is nonzero mod p and $p^n c$ is nonzero mod p so $p^n c$ must be as well but $c \in \mathbb{Z}_{(p)}[x]$ so $p^n = 1$ and thus $a \in (f)$. Thus (f) is prime. However (f) is never maximal. We know that f has positive degree (else $(f) = P$ since f is not divisible by p). Thus we cannot have $p \in (f)$. However, suppose that $pa + fb = 1$ for $a, b \in \mathbb{Z}_{(p)}[x]$. Then reducing mod p we have $fb = 1$ so we must have that $f = u + pa$ for some $a \in \mathbb{Z}_{(p)}[x]$ and $u \in \mathbb{Z}_{(p)}^{\times}$. However, then $(p, f) = (1)$ because u is a unit. Thus (f) is never maximal.

32.5 5

Let $f : A \to B$ be an injective K-algebra map between domains finitely generated over a field K. Let $Q(A)$ and $Q(B)$ be the fraction fields.

32.5.1 a

By noetherian normalization, for any finitely generated K-algebra domain A we have that $\dim A = \operatorname{trdeg}_K(Q(A))$. Therefore, using that, for $K \subset F \subset E$,

$$\operatorname{trdeg}_K(E) = \operatorname{trdeg}_K(F) + \operatorname{trdeg}_F(E)$$

we see that,

$$\dim B = \operatorname{trdeg}_K(Q(B)) = \operatorname{trdeg}_K(Q(A)) + \operatorname{trdeg}_{Q(A)}(Q(B)) = \dim A + \operatorname{trdeg}_{Q(A)}(Q(B))$$

and therefore,

$$\operatorname{trdeg}_{Q(A)}(Q(B)) = \dim B - \dim A$$

Now since $Q(A) \otimes_A B$ is the same as localization at $A \setminus \{0\} \subset B$ we see that $Q(A) \otimes_A B$ is a domain and is finitely generated over $Q(A)$ since B is finitely generated over K and thus over A. Therefore,

$$\dim (Q(A) \otimes_A B) = \operatorname{trdeg}_{Q(A)}(Q(Q(A) \otimes_A B))$$

However, since $Q(A) \otimes_A B$ is a localization of B, its fraction field is $Q(B)$ and thus,

$$\dim (Q(A) \otimes_A B) = \operatorname{trdeg}_{Q(A)}(Q(B)) = \dim B - \dim A$$

32.5.2 b

Noetherian normalization says that for any finitely generated K-algebra domain A there are algebraically independent elements $x_1, \ldots, x_n \in A$ such that $K[x_1, \ldots, x_n] \subset A$ is a finite extension of domains with $n = \dim A$.

We apply this to the domain $B' = Q(A) \otimes_A B$ which is finitely generated over the field $Q(A)$. Therefore we get a finite extension $Q(A)[T_1, \ldots, T_d] \subset B'$ where $d = \dim (Q(A) \otimes_A B) = \dim B - \dim A$. By clearing denominators we may assume that $T_i \in B$. Let $C = A[T_1, \ldots, T_d]$. Since B is finitely generated over A by $y_1, \ldots, y_n \in B$ we see that B' is finitely generated over $Q(A)$ by $y_1, \ldots, y_n \in B$.

Since B' is finite over $Q(A)[T_1, \ldots, T_d]$ we must have that each y_i is integral over $Q(A)[T_1, \ldots, T_d]$ and thus y_i satisfies some monic polynomial $p_i \in Q(A)[T_1, \ldots, T_d][x]$. Let $a \in A \setminus \{0\}$ be the product of all the denominators of the coefficients of the p_i and thus $p_i \in A_a[T_1, \ldots, T_d][x]$ meaning that each y_i is integral over $A_a[T_1, \ldots, T_d]$. Therefore $A_a[T_1, \ldots, T_d] \subset B_a$ is an finite extension since B_a is obtained by adjoinging the finitely many y_i which are each integral and thus give a finite extension.

33 Fall 2019 Part II

33.1 1

Let k be a finite field with q elements.

33.1.1 a

A monic irreducible polynomial q generates a field extension $K = \mathbb{F}_q[x]/(q)$ of $\mathbb{F}_q$ of degree $n = \deg q$. There is a unique field of order q^n and therefore this must be it. Since K/k is Galois and q is irreducible the Galois groups permutes the roots. Therefore monic irreducible polynomials correspond exactly to Galois-orbits of elements in K that do not lie in any proper subfield.

In the case $d = 2$ thus means any element $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ determines such a monic irreducible so there are $(q^2 - q)/2 = q(q-1)/2$ such monic irreducibles.

For the case $d = 3$ we have $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ up to the Galois action and thus there are $(q^3 - q)/3 = q(q-1)(q+1)/3$ possible.

For $d = 4$ we need to be careful because there is a subfield $\mathbb{F}_{q^2} \subset \mathbb{F}_{q^4}$ whose mininal polynomial is quadratic and thus there are $(q^4 - q^2)/4 = q^2(q-1)(q+1)/4$ such polynomials.

For $d = 5$ we have $\mathbb{F}_{q^5} \setminus \mathbb{F}_q$ and thus there are $(q^5 - q)/5 = q(q-1)(q+1)(q^2+1)/5$ possibilities.

For $d = 6$ we need to be especially careful because there are $\mathbb{F}_{q^2} \subset \mathbb{F}_{q^6}$ and $\mathbb{F}_{q^3} \subset \mathbb{F}_{q^6}$ so by inclusion-exclusion there are $(q^6 - q^3 - q^2 + q)/6$ monic irreducibles of degree 6.

33.1.2 b

Let p be a polynomial of degree 5 over k. Let K be its splitting field. We know that $\mathrm{Gal}\,(K/k) = (\mathbb{Z}/n\mathbb{Z})$ generated by Frobenius where $n = [K : k]$ as a general fact about finite fields. Now by adding linear factors we can make p have an irreducible part of any degree up to 5. Therefore we can have $\mathrm{Gal}\,(K/k) = (\mathbb{Z}/n\mathbb{Z})$ for $n = 1, 2, 3, 4, 5$ by the primitive element theorem which says that there exists some element such that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is generated by a single element α and thus its minimal polynomial has degree n.

Furthermore, suppose that q is irreducble of degree n. Then I claim that its splitting field E/k has degree n. Indeed consider $k(\alpha) \subset E$ where α is a root of q. Then we know that $\mathrm{Gal}\,(E/k)$ acts transitively on the roots but this is generated by Frobenius and $\alpha^p \in k(\alpha)$ so $k(\alpha)$ contains all the roots. Thus $E = k(\alpha)$ and thus $[E : k] = \deg \alpha = n$.

However, we can also have $q = ab$ where a has degree 2 and b has degree 3 (all other factorings must have at least one linear factor). In this case K contains $\alpha, \beta \in K$ where $a(\alpha) = 0$ and $b(\beta) = 0$.

Then $k(\alpha)$ and $k(\beta)$ are subfields containing the roots of a and of b respectively of degrees 2 and 3. Furthermore, $k(\alpha)k(\beta) = K$ since K is generated by the roots. Therefore, $[K : k] = 6$ since it is divisble by 3 and 2 and is at most 6 by the compositum equality. Thus $\mathrm{Gal}\,(K/k) = \mathbb{Z}/6\mathbb{Z}$.

33.2 7

Let A be a local ring with maximal ideal $\mathfrak{m}$ and M be a nonzero A-module.

33.2.1 a

We know that $\mathrm{Ext}^i_A\,(A/\mathfrak{m}, M)$ is an $A/\mathfrak{m}$-module and thus is $\mathfrak{m}$-torsion. Explicitly, choosing an injective resolution of $M \to I^\bullet$ we know that,

$$\mathrm{Ext}^i_A\,(A/\mathfrak{m}, M) = H^i(\mathrm{Hom}_A\,(A/\mathfrak{m}, I^\bullet))$$

naturally giving the structure of an $A/\mathfrak{m}$-module. Even more explicitly, the complex $\mathrm{Hom}_A\,(A/m, I^\bullet)$ is killed by $a \in \mathfrak{m}$ because if $\varphi : A/\mathfrak{m} \to I^i$ is a map then $a\varphi = 0$ since $a\varphi(x) = \varphi(ax) = 0$ since $ax \in \mathfrak{m}$.

33.2.2 b

Suppose there exist $a_1, \ldots, a_r \in \mathfrak{m}$ such that for all i the element a_i is not a zero-divisor of $M/(a_1, \ldots, a_{i-1})M$. We will prove that $\mathrm{Ext}^i_A\,(A/m, M) = 0$ for $i = 0, \ldots, r-1$ and $\mathrm{Ext}^r_A\,(A/\mathfrak{m}, M) \cong \mathrm{Hom}_A\,(A/\mathfrak{m}, M/(a_1, \ldots, a_r)M)$ as A-modules.

To prove this we proceed by induction. The case $r = 0$ is obvious by the definition of Ext. Now we proceed with an induction hypothesis. Consider the exact sequence,

$$0 \longrightarrow M \xrightarrow{\times a_1} M \longrightarrow M/a_1M \longrightarrow 0$$

Then we take the Ext sequence,

$$\mathrm{Ext}^{i-1}_A\,(A/\mathfrak{m}, M) \longrightarrow \mathrm{Ext}^{i-1}_A\,(A/\mathfrak{m}, M/a_1M) \longrightarrow \mathrm{Ext}^i_A\,(A/\mathfrak{m}, M) \xrightarrow{\times a_1} \mathrm{Ext}^i_A\,(A/\mathfrak{m}, M)$$

Now $M' = M/a_1M$ has a regular sequence $a_2, \ldots, a_r$ of length $r-1$ so by hypothesis,

$$\mathrm{Ext}^i_A\,(A/\mathfrak{m}, M') = \begin{cases} 0 & i < r-1 \\ \mathrm{Hom}_A\,(A/m, M/(a_1, \ldots, a_n)M) & i = r-1 \end{cases}$$

However, from (a) we know that $\times a_1 : \mathrm{Ext}^i_A\,(A/\mathfrak{m}, M) \to \mathrm{Ext}^i_A\,(A/\mathfrak{m}, M)$ is the zero map and therefore we see that for $i - 1 < r - 1$ i.e. $i < r$ that $\mathrm{Ext}^i_A\,(A/\mathfrak{m}, M) = 0$. Furthermore for $i = r$ we get the sequence,

$$0 \longrightarrow \mathrm{Ext}^{r-1}_A\,(A/\mathfrak{m}, M/a_1M) \longrightarrow \mathrm{Ext}^r_A\,(A/\mathfrak{m}, M) \longrightarrow 0$$

and thus,

$$\mathrm{Ext}^r_A\,(A/\mathfrak{m}, M) \cong \mathrm{Ext}^{r-1}_A\,(A/\mathfrak{m}, M/a_1M) \cong \mathrm{Hom}_A\,(A/\mathfrak{m}, M/(a_1, \ldots, a_n)M)$$

33.2.3 c

Let A denote $\mathbb{C}[X,Y]_{(X,Y)}$ and $\mathfrak{m}$ the maximal ideal. We have a regular sequence $X, Y \in A$ because Y is not a zero divisor in $A/(X)$ because (X) is a prime ideal because $X\mathbb{C}[X,Y]$ is prime and does not intersect the localizing set. Therefore,

$$\operatorname{Ext}_A^i(A/\mathfrak{m}, A) = 0$$

for $i = 0, 1$ and,

$$\operatorname{Ext}_A^2(A/\mathfrak{m}, A) = \operatorname{Hom}_A(A/\mathfrak{m}, A/(X,Y)) = \operatorname{Hom}_A(A/\mathfrak{m}, A/\mathfrak{m}) = A/\mathfrak{m} \cong \mathbb{C}$$

33.3 8

Let A be a symmetric unitary $n \times n$ complex matrix. Let λ be an eigenvalue of A.

33.3.1 a

Notice that if $Av = \lambda v$ then $\overline{A}^\top Av = \lambda \overline{A}^\top v$ but $\overline{A}^\top A = I$ so $\overline{A}^\top v = \lambda^{-1} v$ (we cannot have $\lambda = 0$ because A is invertible). Furthermore, $\langle Av, v\rangle = \lambda \langle v, v\rangle$ but $\langle Av, v\rangle = \langle v, A^* v\rangle = \langle v, \lambda^{-1} v\rangle = \overline{\lambda^{-1}} \langle v, v\rangle$. Since $\langle v, v\rangle \neq 0$ we have $\lambda^{-1} = \overline{\lambda}$ and thus $\lambda\overline{\lambda} = 1$.

Now let $V_\lambda \subset \mathbb{C}^n$ be the eigenspace. If $Av = \lambda v$ then $\overline{A}\overline{v} = \overline{\lambda}\overline{v}$. However, $\overline{A} = A^{-1}$ and thus $\overline{\lambda} A \overline{v} = \overline{v}$ but $\overline{\lambda} = \lambda^{-1}$ so $A\overline{v} = \lambda \overline{v}$ so $\overline{v} \in V_\lambda$.

33.3.2 b

For any $v \in V_\lambda$ we can take $v = v_R + i v_I$ where $v_R = \frac{1}{2}(v + \overline{v})$ and $v_L = \frac{1}{2i}(v - \overline{v})$ where $v_R, v_L \in \mathbb{R}^n \cap V_\lambda$ proving that V_λ is the span of $\mathbb{R}^n \cap V_\lambda$ over $\mathbb{C}$.

33.3.3 c

By the spectral theorem, there is a decomposition,

$$\mathbb{C}^n \cong \bigoplus_\lambda V_\lambda$$

However, we know that V_λ is the $\mathbb{C}$-span of $V_\lambda \cap \mathbb{R}^n$. Therefore $\mathbb{R}^n$ is the $\mathbb{R}$-span of $V_\lambda \cap \mathbb{R}^n$ because otherwise $\mathbb{C}^n$ could not be the $\mathbb{C}$-span of the spaces $V_\lambda \cap \mathbb{R}^n$. Therefore choosing an orthonormal basis of each $V_\lambda \cap \mathbb{R}^n$ which are mutually orthogonal in $\mathbb{R}^n$ we find an orthonormal basis $v_1, \ldots, v_n \in \mathbb{R}^n$ consisting of eigenvectors.

33.3.4 d

The unique matrix g that takes the basis $v_1, \ldots, v_n$ to the standard basis is orthogonal because these are both orthonormal bases. Furthermore this is a basis of eigenvectors of A so gAg^{-1} is diagonal since $gAg^{-1}e_i = gAv_i = \lambda_i g v_i = \lambda_i e_i$.

33.4 9

Let A be a noetherian ring. We will show that the following are equivalent:

(a) The Zariski topology on $\operatorname{Spec}(A)$ is discrete.

(b) All prime ideals of A are maximal and $\operatorname{Spec}(A)$ is a finite set.

(c) A is Artinian.

We show that $(c) \implies (b) \implies (a) \implies (b) \implies (c)$. If A is Artinian then let $\mathfrak{p}$ be a prime. For any $x \notin \mathfrak{p}$ we can consider,

$$(x) \supset (x^2) \supset (x^3) \supset \cdots$$

which must stabilize. Therefore $(x^n) = (x^{n+1})$ for some n. Thus there is a unit $u \in A^\times$ such that $ux^n = ux^{n+1}$ so $x^n(ux - 1) = 0$. Therefore $ux - 1 \in \mathfrak{p}$ because $x \notin \mathfrak{p}$ meaning that x is a unit in $A/\mathfrak{p}$ and thus $A/\mathfrak{p}$ is a field so $\mathfrak{p}$ is maximal. Thus all primes are maximal. Furthermore we can form a list of maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ then consider,

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \cdots$$

which must stabilize and therefore for some N we have $\mathfrak{m}_1 \cdots \mathfrak{m}_N = \mathfrak{m}_1 \cdots \mathfrak{m}_n$ for all $n \geq N$. Therefore, $\mathfrak{m}_n \supset \mathfrak{m}_1 \ldots \mathfrak{m}_N$ but if $\mathfrak{m}_n \not\supset \mathfrak{m}_i$ for $i = 1, \ldots, N$ then choose $x_i \in \mathfrak{m}_i \setminus \mathfrak{m}_n$ then $x_1 \ldots x_N \in \mathfrak{m}_1 \cdots \mathfrak{m}_N$ but not in $\mathfrak{m}_n$ giving a contradiction so $\mathfrak{m}_n \supset \mathfrak{m}_i$ for some $i = 1, \ldots, N$ and since $\mathfrak{m}_i$ is maximal we see that $\mathfrak{m}_n = \mathfrak{m}_i$ so $\mathfrak{m}_1, \ldots, \mathfrak{m}_N$ are all the maximal ideals proving (b). Now suppose (b). Then $\operatorname{Spec}(A)$ is a finite topological space in which every point is closed and thus is discrete because every subset is a finite union of singletons which are closed so every set is closed proving (a).

Now suppose (a). We know that $\operatorname{Spec}(A)$ is always quasi-compact so if it is discrete it must be finite. Furthermore, every point is closed which implies that each prime $\mathfrak{p} \in \operatorname{Spec}(A)$ is maximal so we conclude (b). Now assume (b). To show that A is Artinian it suffices to prove that A has finite length as an A-module. In fact, I will show that every finitely generated A-module M has finite length. We can always build a composition series,

$$(0) = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

where $M_{i+1}/M_i \cong A/\mathfrak{p}_i$ for some prime. To see this, we build M_1 by choosing an associated prime of M_n which exists because A is noetherian and M is finitely generated. This gives an embedding $A/\mathfrak{p} \hookrightarrow M$ defining M_1. Quotienting by M_1 we proceed inducively to build the sequence. Because M is finite over a Noetherian ring it is a Noetherian module so this process eventually terminates at M. Now we use the fact that,

$$\ell_A(M) = \ell(M_{n-1}) + \ell_A(A/\mathfrak{p}_{n-1})$$

from the exact squnece and $A/\mathfrak{p}_{n-1}$ is a field so $\ell_A(A/\mathfrak{p}_{n-1}) = 1$. Therefore,

$$\ell_A(M) = \ell_A(A/\mathfrak{p}_1) + \cdots + \ell_A(A/\mathfrak{p}_{n-1}) = n - 1$$

is finite proving that M is an artinian module and in particular A is artinian.

33.5 10

Let G be a finite group and $H \subset G$ a subgroup. Assume that every irreducible complex representation of G remains irreducible when restricted to H.

33.5.1 a

Let V be an irreducible representaton of H. Choose an irreducible subrepresentation $W \subset \mathrm{Ind}_H^G(V)$. Then, using Frobenius reciprocity,

$$\mathrm{Hom}_H\left(V, \mathrm{Res}_H^G(W)\right) = \mathrm{Hom}_G\left(\mathrm{Ind}_H^G(V), W\right) \neq 0$$

However, $\mathrm{Res}_H^G(W)$ is irreducible by the hypothesis and V is irreducible so by Shur's lemma this implies that $V \cong \mathrm{Res}_H^G(W)$ and thus V extends to the G-representation W.

33.5.2 b

Suppose that $a, b \in H$ are conjugate in G. We know that a, b are conjugate in H if $\chi(a) = \chi(b)$ for every irreducible character of H. However, since each irreducible representation of H extends to an irreducible representation of G we know that the chracter extends as well to $\chi' : G \to \mathbb{C}$. Then, $\chi'(a) = \chi'(b)$ because χ' is a class function on G but $\chi'|_H = \chi$ so $\chi(a) = \chi(b)$ proving that a and b are conjugate in H.

33.5.3 c

Consider $\mathrm{GL}_2(\mathbb{F}_5) \subset \mathrm{GL}_2(\mathbb{F}_{25})$. We know that two matrices in the $\mathrm{GL}_2(\mathbb{F}_5)$ are similar in $\mathrm{GL}_2(\mathbb{F}_{25})$ if and only if they are similar in $\mathrm{GL}_2(\mathbb{F}_5)$.

34 Spring 2019 Part I

34.1 1

34.1.1 a

The minimal polynomial of a is $(x^2-2)^2 - 2$. Thus its conjugates are $\pm\sqrt{2 \pm \sqrt{2}}$. Then the Galois group of the splitting field is abelian so every subfield is Galois over $\mathbb{Q}$.

34.1.2 b

The splitting field of $x^4 + 1$ is $\mathbb{Q}(\zeta_8)$. Thus the Galois group is $(\mathbb{Z}/8\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

34.2 2

34.2.1 a

Consider the quotient map $A_4 \twoheadrightarrow C_3$. Thus each irreducible representation of C_3 (which are the characters $C_3 \to \mathbb{C}^\times$) gives an irreducible representation of A_4. Thus we have three irreducible representations of A_4 of dimension 1. But $|A_4| = 12$ and A_4 has the following conjugacy classes, e, the three cycles, $(1\,2)(3\,4)$ and $(1\,3)(2\,4)$. Therefore we are missing one irrep and it has $d^2 = 12 - 3$ so $d = 3$.

Now we work out the character table.

34.2.2 b

Let A_4 act by permutation on $\mathbb{C}^4$. Then $\chi(g) = 4$ if $g = e$ and $\chi(g) = 1$ iff g is a 3-cycle and $\chi(g) = 0$ iff g is a pair of flips. Therefore, from the table we see that $\chi = \chi_1 + \chi_3$ and this gives the required decomposition.

34.2.3 c

34.3 3

Let $I = (x, y)$ and $J = (z, w)$ and $K = (x - z, y - w)$ be ideals of the ring $A = \mathbb{C}[x, y, z, w]$.

34.3.1 a

It is clear that $IJ = (xz, xw, yz, yw)$. It suffices to show that $I \cap J = IJ$. Now if $f \in I \cap J$ then $f = ax + by = cw + dy$. Setting $x = 0$ and $y = 0$ we see that $f = 0$ so $c \in I$ and $d \in I$ and thus $f \in IJ$.

34.3.2 b

Define a map by sending $f \in A/IJ$ to $(\bar{f}_1 \in A/J, \bar{f}_2 \in A/I)$ which satisfies $\bar{f}_1(0,0) = \bar{f}_2(0,0) = f(0,0,0,0)$. This is injective because if $f \in I \cap J$ then $f \in IJ$ so its zero. Furthermore, this is surjective because for any (f, g) such that $h = f - g \in I + J$. Suppose that $f(0,0) = u$ is nonzero then we can consider $f + g - u$. Then this maps to f and g.

34.3.3 c

Consider the projective resolution,

$$0 \longrightarrow A \xrightarrow{y-w\ x-z} A^2 \xrightarrow{x-z\ y-w} A \longrightarrow A/K \longrightarrow 0$$

then apply the functor $A/IJ \otimes_A -$ to get the complex,

$$A/IJ \longrightarrow A/IJ \oplus A/IJ \longrightarrow A/IJ$$

taking homology gives,

$$\operatorname{Tor}_i^A(A/IJ, A/K) = \begin{cases} \mathbb{C}[x,y]/(x,y)^2 & i = 0 \\ \mathbb{C}[x,y]/ \end{cases}$$

34.4 4

34.4.1 a

Consider $x^6 - 1 = (x^3 - 1)(x^3 + 1)$ but $x^3 - 1 = (x - 1)^3$ over $\mathbb{F}_3$. Furthermore, $x^3 + 1 = (x + 1)^3$ so $x^6 - 1 = (x - 1)^3(x + 1)^3$.

34.4.2 b

Conjugacy classes of elements $g \in \mathrm{GL}_2(\mathbb{F}_3)$ are given by rational canonical form. We have $p_1 \mid p_2$ or just p_1. By dimensionality reasons we have $p_1 = p_2$ is linear or p_1 by itself is quadratic. Now the minimal polynomial must divide $x^6 - 1$ and must have degree 2 or be linear. If it is linear since it divides $(x-1)^3(x+1)^3$ then $m = x+1$ or $m = x-1$. The second possibility gives I and the second gives $-I$ which are in their own classes.

For degree two there are three cases. $m = (x-1)^2$ gives a conjugacy class represented by the jordan block,

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

Likewise the case $m = (x+1)^2$ is represented by the Jordan block,

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

and finally $m = (x-1)(x+1)$ is represented by the diagonalizable matrix,

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

34.4.3 c

Now we consider $g \in \mathrm{GL}_3(\mathbb{F}_3)$. By dimensionality there are three cases: either $p_1 = p_2 = p_3$ is linear or $p_1 \mid p_2$ with p_1 linear and p_2 quadratic or p_1 is cubic. The first case gives I and $-I$. The second case gives $p_1 = (x-1)$ and $p_2 = (x-1)^2$ or $p_1 = (x-1)$ and $p_2 = (x-1)(x+1)$ or $p_1 = (x+1)$ and $p_2 = (x-1)(x+1)$ or $p_1 = (x+1)$ and $p_2 = (x+1)^2$ giving four possible conjugacy classes. The final case we have either $p_1 = (x-1)^3$ or $p_1 = (x-1)(x+1)^2$ or $p_1 = (x-1)^2(x+1)$ or $p_1 = (x-1)^3$ giving another four possibilities for a total of 10 conjugacy classes.

34.5 5

Consider extensions of abelian groups,

$$0 \longrightarrow \mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \longrightarrow 0$$

Tensoring with $\mathbb{Q}$ we see that the rank of G is two. Thus write $G = \mathbb{Z}^2 \times T$ where T is torsion. Furthermore, T is generated by at most two elements. We can assume that the first $\mathbb{Z} \mapsto \mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ since this map is surjective. Therefore, we have a surjection $\mathbb{Z} \times T \to \mathbb{Z}/10\mathbb{Z}$ and the kernel is $\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Therefore the possibilities are as follows:

(a) $G = \mathbb{Z}^2 \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

(b)

34.6 10

Let k be a field.

34.6.1 a

Let K/k be a finitely generated k-algebra and a field. We induct on the number of generators of K over k. The base case is trivial. Suppose that the result holds for $n-1$ generators. Now, consider $y_1, \dots, y_n \in K$ algebra generators. These cannot be algebrically independent because then $\dim K = n$. Therefore, there is some relation,

$$f(y_1, \dots, y_n) = 0$$

We set $z_i = y_i - y_n^{r^i}$ and consider,

$$f(z_1 + y_n^r, \dots, z_{n-1} + y_n^{r^{n-1}}, y_n) = 0$$

a monomial in here looks like,

$$\alpha \left(\prod_{i=1}^{n-1} (z_i + y_n^{r^{i-1}})^{a_i} \right) y_n^{a_n} = \alpha y_n^{a_1 r + \cdots + a_{n-1} r^{n-1} + a_n} + \cdots$$

where $\alpha \in k$. Since this leading exponent in y_n is a unique base r number, as long as r is larger than each exponent in f then there is a single monomial with the greatest term because the exponent uniquely determines the a_i by base r expansion. Therefore, this is the leading term in y_n so dividing by α we see that y_n satsifies a monic polynomial over $k[z_1, \dots, z_{n-1}] \subset K$ and therefore K is finite over $k[z_1, \dots, z_{n-1}]$ which is a subfield because it has an integral extension which is a field. By the induction hypothesis $k[z_1, \dots, z_{n-1}]$ is finite over k and thus K is finite over k.

34.6.2 b

Let $f : A \to B$ is a k-algebra map of finitely-generated k-algebras and $\mathfrak{m} \subset B$ be a maximal ideal. Then consider $A/f^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$. Now $B/\mathfrak{m}$ is a field and a finite type k-algebra so its a finite k-module and thus $A/f^{-1}(\mathfrak{m})$ is a finite k-module but also a domain and thus a field so $f^{-1}(\mathfrak{m})$ is maximal.

However, consider $\mathbb{Z} \to \mathbb{Q}$ which sends the maximal ideal $(0) \mapsto (0)$ but (0) is not maximal in $\mathbb{Z}$.

34.6.3 c

Let A be a finitely generated k-algebra. Suppose that $a \in \mathfrak{m}$ for each maximal ideal $\mathfrak{m}$. Then consider a maximal ideal $\mathfrak{m} \subset A_a$ which by above pulls back to a maximal ideal $\mathfrak{m}A$ but then $a \in \mathfrak{m}A$ so $f(a) \in \mathfrak{m}$ which is not possible because $a \in A_a$ is a unit. Therefore A_a has no maximal ideals so $A_a = (0)$ and thus $a^n \cdot 1 = 0$ so a is nilpotent.