# Algebra Qualifying Exam Solutions

## D. Zack Garza

Tuesday 7th July, 2020

## Contents

# Contents

# 1   Problem Session Links

Problem Session 1: Group Theory

- 3.2, Sylow Theory Solution
- 5.1, Class Equation Solution
- 6.1, Sylow Theory Solution
- 6.2, Group Actions Solution
- Bonus: 2.4, Conjugacy Classes Solution

## 2 Spring 2020

### 2.1 1 ?

### 2.2 2 ?

### 2.3 3 ?

### 2.4 4 ?

### 2.5 5 ?

### 2.6 6

Let $R$ be a ring with 1.

#### 2.6.1 a

An $R$-module $M$ is **free** if any of the following conditions hold:

- $M$ admits an $R$-linearly independent spanning set $\{\mathbf{b}_\alpha\}$, so

$$m \in M \implies m = \sum_\alpha r_\alpha \mathbf{b}_\alpha$$

  and

$$\sum_\alpha r_\alpha \mathbf{b}_\alpha = 0_M \implies r_\alpha = 0_R$$

  for all $\alpha$.
- $M \cong \bigoplus_\alpha R$ are isomorphic as $R$-modules.
- There is a nonempty set $X$ and an inclusion $X \hookrightarrow M$ such that for every $R$-modules $N$, every map $X \longrightarrow N$ lifts to a unique map $M \longrightarrow N$, so the following diagram commutes:

$$
\begin{array}{ccc}
 & M & \\
 \uparrow & \overset{\exists! \tilde{f}}{\cdots\cdots} & \\
 X & \overset{f}{\longrightarrow} & N
\end{array}
$$

#### 2.6.2 b

$M$ is **torsionfree** iff $M_t := \left\{ m \in M \mid \operatorname{Ann}(m) \neq 0 \right\} \leq M$ is the trivial submodule, where $\operatorname{Ann}(m) := \left\{ r \in R \mid r \cdot m = 0_M \right\} \trianglelefteq R$.

#### 2.6.3 c

- Let the following be an SES where $F$ is a free $R$-module:

$$0 \longrightarrow N \longrightarrow M \overset{\pi}{\longrightarrow} F \longrightarrow 0.$$

- Since $F$ is free, there is a generating set $X = \{x_\alpha\}$ and a map $\iota : X \hookrightarrow M$ satisfying the 3rd property from (a).

- If we construct a map $f : X \longrightarrow M$, then the universal property of free modules will give a lift $\tilde{f} : F \longrightarrow M$

- Note $\{\iota(x_\alpha)\} \subseteq F$ and $\pi$ is surjective, so choose fibers $\{y_\alpha\} \subseteq M$ such that

$$\pi(y_\alpha) = \iota(x_\alpha).$$

- Define a map

$$f : X \longrightarrow M$$
$$x_\alpha \mapsto y_\alpha.$$

- By the universal property, this yields a map $h : F \longrightarrow M$, commutativity forces $(h \circ \iota)(x_\alpha) = y_\alpha$, i.e. we have a diagram

$$X = \{x_\alpha\}$$

$$0 \longrightarrow N \longrightarrow M \xrightarrow{\;\;\pi\;\;} F \longrightarrow 0$$

- It remains to check that it's a section:

$$f \in F \implies f = \sum_\alpha r_\alpha \iota(x_\alpha)$$

$$\implies (\pi \circ h)(f) = \pi\left(h\left(\sum_\alpha r_\alpha \iota(x_\alpha)\right)\right)$$

$$= \pi\left(\sum_\alpha r_\alpha h(\iota(x_\alpha))\right)$$

$$= \pi\left(\sum_\alpha r_\alpha y_\alpha\right)$$

$$= \sum_\alpha r_\alpha \pi(y_\alpha)$$

$$= \sum_\alpha r_\alpha \iota(x_\alpha)$$

$$:= f$$

- Checking $(h \circ \pi)(m) = m$: seems to be hard!

- Both $\pi \circ h$ and $\mathrm{id}_F$ are two maps that agree on the spanning set $\{\iota(x_\alpha)\}$, so in fact they are *equal*.

Short proof:

- Free implies projective
- Universal property of projective modules: for every surjective $\pi : M \longrightarrow N$ and every $f : P \longrightarrow N$ there exists a unique lift $\tilde{f} : P \longrightarrow M$:

$$
\begin{array}{ccc}
 & & P \\
 & \overset{\exists!\tilde{f}}{\nearrow} & \downarrow f \\
M & \overset{\pi}{\longrightarrow} & N
\end{array}
$$

- Take the identity map:

$$
\begin{array}{ccccccc}
 & & & & F & & \\
 & & \overset{\exists!h}{\nearrow} & & \downarrow \mathrm{id}_F & & \\
0 & \longrightarrow & N & \longrightarrow & M \longrightarrow F & \longrightarrow & 0
\end{array}
$$

### 2.6.4  d

- Claim: if $R$ is a PID and $M$ is a finitely generated $R$-module, then $M \cong M_t \oplus M/M_t$ where $M_t \leq M$ is the torsion submodule.
- Claim: $M/M_t$ is torsionfree, and since a f.g. torsion free module over a PID is free, $M/M_t$ is free.
    - Let $m + M_t \in M/M_t$ and suppose it is torsion, we will show that is must be the zero coset.
    - Then there exists an $r \in R$ such that $r(m + M_t) = M_t$
    - Then $rm + M_t = M_t$, so $rm \in M_t$.
    - By definition of $M_t$, every element is torsion, so there exists some $s \in R$ such $s(rm) = 0_M$.
    - Then $(sr)m = 0_M$ which forces $m \in M_t$
    - Then $m + M_t = M_t$, so $m + M_t$ is the zero coset.
- There is a SES
$$
0 \longrightarrow M_t \longrightarrow M \longrightarrow M/M_t \longrightarrow 0
$$
and since $M/M_t$ is free, by (c) this sequence splits and $M \cong M \oplus M/M_t$.

## 2.7  7 ?

## 2.8  8 ?

# 3  Fall 2019

## 3.1  1

Centralizer:

$$C_G(h) = Z(h) = \left\{ g \in G \mid [g, h] = 1 \right\} \quad \text{Centralizer}$$

Class equation:

$$|G| = \sum_{\substack{\text{One } h \text{ from each} \\ \text{conjugacy class}}} \frac{|G|}{|Z(h)|}$$

Notation:

$$h^g = ghg^{-1}$$

$$h^G = \left\{ h^g \mid g \in G \right\} \quad \text{Conjugacy Class}$$

$$H^g = \left\{ h^g \mid h \in H \right\}$$

$$N_G(H) = \left\{ g \in G \mid H^g = H \right\} \supseteq H \quad \text{Normalizer.}$$

**Theorem 1**: $\left| h^G \right| = [G : Z(h)]$

**Theorem 2**: $\left| \left\{ H^g \mid g \in G \right\} \right| = [G : N_G(H)]$

*Proof:* Let $G \curvearrowright \left\{ H \mid H \leq G \right\}$ by $H \mapsto gHg^{-1}$. Then the $\mathcal{O}_H$ is the set of conjugate subgroups, $\text{Stab}(H) = N_G(H)$. So Orbit-Stabilizer says $\mathcal{O}_h \cong G/\text{Stab}(H)$; then just take sizes.

**Theorem 3**: $\bigcup_{g \in G} H^g = \bigcup_{g \in G} gHg^{-1} \subsetneq G$ for any proper $H \leq G$.

*Proof:* By theorem 2, since each coset is of size $|H|$, which only intersect at the identity, and there are exactly $[G : N_G(H)]$ of them

$$\left| \bigcup_{g \in G} H^g \right| = (|H| - 1)[G : N_G(H)] + 1$$

$$= |H|[G : N_G(H)] - [G : N_G(H)] + 1$$

$$= |G| \frac{|G|}{|N_G(H)|} - \frac{|G|}{|N_G(H)|} + 1$$

$$\leq |H| \frac{|G|}{|H|} - \frac{|G|}{|H|} + 1$$

$$= |G| - ([G : H] - 1)$$

$$< |G|.$$

where we use the fact that $H \subseteq N_G(H) \implies |H| \leq |N_G(H)| \implies \frac{1}{|N_G(H)|} \leq \frac{1}{|H|}$, and since $H < G$ is proper, $[G : H] \geq 2$.

Since $[g_i, g_j] = 1$, we have $g_i \in Z(g_j)$ for every $i, j$.

Then

$$
\begin{aligned}
g \in G &\implies g = g_i^h \quad \text{for some } h \\
&\implies g \in Z(g_{\mathbf{j}})^h \quad \text{for every } j \text{ since } g_i \in Z(g_j) \ \forall j \\
&\implies g \in \bigcup_{h \in G} Z(g_j)^h \quad \text{for every } j \\
&\implies G \subseteq \bigcup_{h \in G} Z(g_j)^h \quad \text{for every } j,
\end{aligned}
$$

which by Theorem 3, if $Z(g_j) < G$ were proper, then the RHS is properly contained in $G$. So it must be the case that that $Z(g_j)$ is not proper and thus equal to $G$ for every $j$.

But $Z(g_i) = G \iff g_i \in Z(G)$, and so each conjugacy class is size one. So for every $g \in G$, we have $g = g_j$ for some $j$, and thus $g = g_j \in Z(g_j) = Z(G)$, so $g$ is central. Then $G \subseteq Z(G)$ and $G$ is abelian.

## 3.2   2

Relevant Ideas:

- The $pqr$ theorem.

- Sylow 3: $|G| = p^n m$ implies $n_p \mid m$ and $n_p \cong 1 \mod p$.

- **Theorem**: If $H, K \leq G$ and any of the following conditions hold, $HK$ is a subgroup:
  - $H \trianglelefteq G$ (wlog)
  - $[H, K] = 1$
  - $H \leq N_G(K)$

- **Theorem**: For a positive integer $n$, all groups of order $n$ are cyclic $\iff n$ is squarefree and, for each pair of distinct primes $p$ and $q$ dividing $n$, $q - 1 \not\equiv 0 \mod p$.

- **Theorem:**

$$
A_i \trianglelefteq G, \quad G = A_1 \cdots A_k, \quad A_k \bigcap \prod_{i \neq k} A_i = \emptyset \implies G = \prod A_i.
$$

- The intersection of subgroups is a again a subgroup.

- Any subgroups of coprime order intersect trivially?

### 3.2.1  a

We have

- $n_3 \mid 5 \cdot 7, \quad n_3 \cong 1 \mod 3 \implies n_3 \in \{1, 5, 7, 35\} \setminus \{5, 35\}$
- $n_5 \mid 3 \cdot 7, \quad n_5 \cong 1 \mod 5 \implies n_5 \in \{1, 3, 7, 21\} \setminus \{3, 7\}$
- $n_7 \mid 3 \cdot 5, \quad n_7 \cong 1 \mod 7 \implies n_7 \in \{1, 3, 5, 15\} \setminus \{3, 5\}$

Thus

$$n_3 \in \{1, 7\} \quad n_5 \in \{1, 21\} \quad n_7 \in \{1, 15\}.$$

Toward a contradiction, if $n_5 \neq 1$ and $n_7 \neq 1$, then

$$\left| \mathrm{Syl}(5) \bigcup \mathrm{Syl}(7) \right| = (5-1)n_5 + (7-1)n_7 + 1 = 4(21) + 6(15) = 174 > 105 \text{ elements}$$

using the fact that Sylow $p$-subgroups for distinct primes $p$ intersect trivially (?).

### 3.2.2 b (Todo)

By (a), either $Q$ or $R$ is normal. Thus $QR \leq G$ is a subgroup, and it has order $|Q| \cdot |R| = 5 \cdot 7 = 35$.

By the *pqr* theorem, since 5 does not divide $7 - 1 = 6$, $QR$ is cyclic.

### 3.2.3 c

We want to show $Q, R \trianglelefteq G$, so we proceed by showing **not** $(n_5 = 21$ or $n_7 = 15)$, which is equivalent to $(n_5 = 1$ and $n_7 = 1)$ by the previous restrictions.

Note that we can write

$$G = \{\text{elements of order } n\} \coprod \{\text{elements of order not } n\}.$$

for any $n$, so we count for $n = 5, 7$:

- Elements in $QR$ of order **not** equal to 5: $|QR - Q\{\mathrm{id}\} + \{\mathrm{id}\}| = 35 - 5 + 1 = 31$
- Elements in $QR$ of order **not** equal to 7: $|QR - \{\mathrm{id}\}R + \{\mathrm{id}\}| = 35 - 7 + 1 = 29$

Since $QR \leq G$, we have

- Elements in $G$ of order **not** equal to $5 \geq 31$.
- Elements in $G$ of order **not** equal to $7 \geq 29$.

Now both cases lead to contradictions:

- $n_5 = 21$:

$$|G| = \left| \{\text{elements of order 5}\} \coprod \{\text{elements of order not 5}\} \right|$$
$$\geq n_5(5-1) + 31 = 21(4) + 31 = 115 > 105 = |G|.$$

- $n_7 = 15$:

$$|G| = \left| \{\text{elements of order 7}\} \coprod \{\text{elements of order not 7}\} \right|$$
$$\geq n_7(7-1) + 29 = 15(6) + 29 = 119 > 105 = |G|.$$

### 3.2.4  d

Suppose $P$ is normal and recall $|P| = 3, |Q| = 5, |R| = 7$.

- $P \bigcap QR = \{e\}$ since $(3, 35) = 1$
- $R \bigcap PQ = \{e\}$ since $(5, 21) = 1$
- $Q \bigcap RP = \{e\}$ since $(7, 15) = 1$

We also have $PQR = G$ since $|PQR| = |G|$ (???).

We thus have an internal direct product

$$G \cong P \times Q \times R \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{105}.$$

by the Chinese Remainder Theorem, which is cyclic.

## 3.3  3

Just fiddling with computations. Context hints that we should be considering things like $x^2$ and $a + b$.

### 3.3.1  a

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

Note that this implies $x = -x$ for all $x \in R$.

### 3.3.2  b

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$
$$\implies ab + ba = 0$$
$$\implies ab = -ba$$
$$\implies ab = ba \quad \text{by (a)}.$$

## 3.4  4

Theorem: $F^\times$ is always cyclic for $F$ a field

### 3.4.1  a

Since $|F| = q$ and $[E : F] = k$, we have $|E| = q^k$ and $|E^\times| = q^k - 1$. Noting that $\zeta \in E^\times$ we must have $n = o(\zeta) \,\big|\, |E^\times| = q^k - 1$ by Lagrange's theorem.

### 3.4.2 b

Rephrasing (a), we have

$$n \mid q^k - 1 \iff q^k - 1 \cong 0 \mod n$$
$$\iff q^k \cong 1 \mod n$$
$$\iff m := o(q) \mid k.$$

### 3.4.3 c

Since $m \mid k \iff k = \ell m$, (**claim**) there is an intermediate subfield $M$ such that

$$E \leq M \leq F \quad k = [F : E] = [F : M][M : E] = \ell m,$$

so $M$ is a degree $m$ extension of $E$.

Now consider $M^\times$. By the argument in (a), $n$ divides $q^m - 1 = |M^\times|$, and $M^\times$ is cyclic, so it contains a cyclic subgroup $H$ of order $n$.

But then $x \in H \implies p(x) := x^n - 1 = 0$, and since $p(x)$ has at most $n$ roots in a field. So $H = \left\{ x \in M \mid x^n - 1 = 0 \right\}$, i.e. $H$ contains all solutions to $x^n - 1$ in $E[x]$.

But $\zeta$ is one such solution, so $\zeta \in H \subset M^\times \subset M$. Since $F[\zeta]$ is the smallest field extension containing $\zeta$, we must have $F = M$, so $\ell = 1$, and $k = m$.

> Todo: **revisit**, tricky!

## 3.5   5

> One-step submodule test.

### 3.5.1 a

It suffices to show that

$$r \in R, \ t_1, t_2 \in \text{Tor}(M) \implies rt_1 + t_2 \in \text{Tor}(M).$$

We have

$$t_1 \in \text{Tor}(M) \implies \exists s_1 \neq 0 \text{ such that } s_1 t_1 = 0$$
$$t_2 \in \text{Tor}(M) \implies \exists s_2 \neq 0 \text{ such that } s_2 t_2 = 0.$$

Since $R$ is an integral domain, $s_1 s_2 \neq 0$. Then

$$s_1 s_2 (rt_1 + t_2) = s_1 s_2 r t_1 + s_1 s_2 t_2$$
$$= s_2 r (s_1 t_1) + s_1 (s_2 t_2) \quad \text{since } R \text{ is commutative}$$
$$= s_2 r (0) + s_1 (0)$$
$$= 0.$$

### 3.5.2 b

Let $R = \mathbb{Z}/6\mathbb{Z}$ as a $\mathbb{Z}/6\mathbb{Z}$-module, which is not an integral domain as a ring.

Then $[3]_6 \curvearrowright [2]_6 = [0]_6$ and $[2]_6 \curvearrowright [3]_6 = [0]_6$, but $[2]_6 + [3]_6 = [5]_6$, where 5 is coprime to 6, and thus $[n]_6 \curvearrowright [5]_6 = [0] \implies [n]_6 = [0]_6$. So $[5]_6$ is *not* a torsion element.

So the set of torsion elements are not closed under addition, and thus not a submodule.

### 3.5.3 c

Suppose $R$ has zero divisors $a, b \neq 0$ where $ab = 0$. Then for any $m \in M$, we have $b \curvearrowright m := bm \in M$ as well, but then

$$a \curvearrowright bm = (ab) \curvearrowright m = 0 \curvearrowright m = 0_M,$$

so $m$ is a torsion element for any $m$.

∎

### 3.6   6

> Prime ideal: $\mathfrak{p}$ is prime iff $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Silly fact: 0 is in every ideal!
> **Zorn's Lemma:** Given a poset, if every chain has an upper bound, then there is a maximal element. (Chain: totally ordered subset.)
> **Corollary:** If $S \subset R$ is multiplicatively closed with $0 \notin S$ then $\left\{ I \trianglelefteq R \mid J \bigcap S = \emptyset \right\}$ has a maximal element. (TODO: PROVE)
> **Theorem:** If $R$ is commutative, maximal $\implies$ prime for ideals. (TODO: PROVE)
> **Theorem:** Non-units are contained in a maximal ideal. (See HW?)

### 3.6.1 a

Let $\mathfrak{p}$ be prime and $x \in N$. Then $x^k = 0 \in \mathfrak{p}$ for some $k$, and thus $x^k = xx^{k-1} \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, inductively we obtain $x \in \mathfrak{p}$.

### 3.6.2 b

Let $S = \left\{ r^k \mid k \in \mathbb{N} \right\}$ be the set of positive powers of $r$. Then $S^2 \subseteq S$, since $r^{k_1} r^{k_2} = r^{k_1 + k_2}$ is also a positive power of $r$, and $0 \notin S$ since $r \neq 0$ and $r \notin N$.

By the corollary, $\left\{ I \trianglelefteq R \mid I \bigcap S = \emptyset \right\}$ has a maximal element $\mathfrak{p}$.

Since $R$ is commutative, $\mathfrak{p}$ is prime.

### 3.6.3 c

Suppose $R$ has a unique prime ideal $\mathfrak{p}$.

Suppose $r \in R$ is not a unit, and toward a contradiction, suppose that $r$ is also not nilpotent.

Since $r$ is not a unit, $r$ is contained in some maximal (and thus prime) ideal, and thus $r \in \mathfrak{p}$.

## 3.7  7

Since $r \notin N$, by (b) there is a maximal ideal $\mathfrak{m}$ that avoids all positive powers of $r$. Since $\mathfrak{m}$ is prime, we must have $\mathfrak{m} = \mathfrak{p}$. But then $r \notin \mathfrak{p}$, a contradiction.

### 3.7  7

Galois Theory.
**Galois** = normal + separable.
**Separable**: Minimal polynomial of every element has distinct roots.
**Normal (if separable)**: Splitting field of an irreducible polynomial.

Definition: $\zeta$ is a primitive root of unity iff $o(\zeta) = n$ in $F^{\times}$.
$\varphi(p^k) = p^{k-1}(p-1)$

The lattice:



Let $K = \mathbb{Q}(\zeta)$. Then $K$ is the splitting field of $f(x) = x^n - 1$, which is irreducible over $\mathbb{Q}$, so $K/\mathbb{Q}$ is normal. We also have $f'(x) = nx^{n-1}$ and $\gcd(f, f') = 1$ since they can not share any roots.

Or equivalently, $f$ splits into distinct linear factors $f(x) = \prod_{k \leq n}(x - \zeta^k)$.

Since it is a Galois extension, $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = \varphi(n)$ for the totient function.

We can now define maps

$$\tau_j : K \longrightarrow K$$
$$\zeta \mapsto \zeta^j$$

and if we restrict to $j$ such that $\gcd(n, j) = 1$, this yields $\varphi(n)$ maps. Noting that if $\zeta$ is a primitive root, then $(n, j) = 1$ implies that that $\zeta^j$ is also a primitive root, and hence another root of $\min(\zeta, \mathbb{Q})$, and so these are in fact automorphisms of $K$ that fix $\mathbb{Q}$ and thus elements of $\mathrm{Gal}(K/\mathbb{Q})$.

So define a map

$$\theta : \mathbb{Z}_n^{\times} \longrightarrow K$$
$$[j]_n \mapsto \tau_j.$$

from the *multiplicative* group of units to the Galois group.

The claim is that this is a surjective homomorphism, and since both groups are the same size, an isomorphism.

**Surjectivity:**

Letting $\sigma \in K$ be arbitrary, noting that $[K : \mathbb{Q}]$ has a basis $\left\{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\right\}$, it suffices to specify $\sigma(\zeta)$ to fully determine the automorphism. (Since $\sigma(\zeta^k) = \sigma(\zeta)^k$.)

In particular, $\sigma(\zeta)$ satisfies the polynomial $x^n - 1$, since $\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$, which means $\sigma(\zeta)$ is another root of unity and $\sigma(\zeta) = \zeta^k$ for some $1 \leq k \leq n$.

Moreover, since $o(\zeta) = n \in K^\times$, we must have $o(\zeta^k) = n \in K^\times$ as well. Noting that $\left\{\zeta^i\right\}$ forms a cyclic subgroup $H \leq K^\times$, then $o(\zeta^k) = n \iff (n, k) = 1$ (by general theory of cyclic groups).

Thus $\theta$ is surjective.

**Homomorphism:**

$$\tau_j \circ \tau_k(\zeta) = \tau_j(\zeta^k) = \zeta^{jk} \implies \tau_{jk} = \theta(jk) = \tau_j \circ \tau_k.$$

**Part 2:**

We have $K \cong \mathbb{Z}_{20}^\times$ and $\varphi(20) = 8$, so $K \cong \mathbb{Z}_8$, so we have the following subgroups and corresponding intermediate fields:

- $0 \sim \mathbb{Q}(\zeta_{20})$
- $\mathbb{Z}_2 \sim \mathbb{Q}(\omega_1)$
- $\mathbb{Z}_4 \sim \mathbb{Q}(\omega_2)$
- $\mathbb{Z}_8 \sim \mathbb{Q}$

For some elements $\omega_i$ which exist by the primitive element theorem.

## 3.8   8

### 3.8.1  a.

Let $\mathbf{v} \in \Lambda$, so $\mathbf{v} = \sum_{i=1}^n r_i \mathbf{e}_i$ where $r_i \in \mathbb{Z}$ for all $i$.

Then if $\mathbf{x} = \sum_{j=1}^n s_j \mathbf{e}_j \in \Lambda$ is arbitrary, we have $s_j \in \mathbb{Z}$ for all $j$ and

$$\langle \mathbf{v}, \ \mathbf{x} \rangle = \left\langle \sum_{i=1}^n r_i \mathbf{e}_i, \ \sum_{j=1}^n s_j \mathbf{e}_j \right\rangle$$
$$= \sum_{i=1}^n \sum_{j=1}^n r_i s_j \langle \mathbf{e}_i, \ \mathbf{e}_j \rangle \in \mathbb{Z}$$

since this is a sum of products of integers (since $\langle \mathbf{e}_i, \ \mathbf{e}_j \rangle \in \mathbb{Z}$ for each $i, j$ pair by assumption) so $\mathbf{v} \in \Lambda^\vee$ by definition.

**3.8.2 b.**

$\det M \neq 0$:

Suppose $\det M = 0$. Then $\ker M \neq \mathbf{0}$, so let $\mathbf{v} \in \ker M$ be given by $\mathbf{v} = \sum_{i=1}^{n} v_i \mathbf{e}_i \neq \mathbf{0}$.

Note that

$$M\mathbf{v} = 0 \implies \begin{bmatrix} \mathbf{e}_1 \cdot \mathbf{e}_1 & \mathbf{e}_1 \cdot \mathbf{e}_2 & \cdots \\ \mathbf{e}_2 \cdot \mathbf{e}_1 & \mathbf{e}_2 \cdot \mathbf{e}_2 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \end{bmatrix} = \mathbf{0}$$

$$\implies \sum_{j=1}^{n} v_j \langle \mathbf{e}_k, \ \mathbf{e}_j \rangle = 0 \quad \text{for each fixed} \quad k.$$

We can now note that $\langle \mathbf{e}_k, \ \mathbf{v} \rangle = \sum_{j=1}^{n} v_j \langle \mathbf{e}_k, \ \mathbf{e}_j \rangle = 0$ for every $k$ by the above observation, which forces $\mathbf{v} = 0$ by non-degeneracy of $\langle \cdot, \ \cdot \rangle$, a contradiction.

∎

*Alternative proof:*

Write $M = A^t A$ where $A$ has the $\mathbf{e}_i$ as columns. Then

$$\begin{aligned} M\mathbf{x} = 0 &\implies A^t A \mathbf{x} = 0 \\ &\implies \mathbf{x}^t A^t A \mathbf{x} = 0 \\ &\implies \|A\mathbf{x}\|^2 = 0 \\ &\implies A\mathbf{x} = 0 \\ &\implies \mathbf{x} = 0, \end{aligned}$$

since $A$ has full rank because the $\mathbf{e}_i$ are linearly independent.

∎

Let $A = [\mathbf{e}_1^t, \cdots, \mathbf{e}_n^t]$ be the matrix with $\mathbf{e}_i$ in the $i$th column.

**The rows of $A^{-1}$ span $\Lambda^\vee$:**

Equivalently, the columns of $A^{-t}$ span $\Lambda^\vee$.

Let $B = A^{-t}$ and let $\mathbf{b}_i$ denote the columns of $B$, so $\operatorname{im} B = \operatorname{span}\{\mathbf{b}_i\}$.

Since $A \in \operatorname{GL}(n, \mathbb{Z})$, $A^{-1}, A^t, A^{-t} \in \operatorname{GL}(n, \mathbb{Z})$ as well.

$$\mathbf{v} \in \Lambda^\vee \implies \langle \mathbf{e}_i,\ \mathbf{v} \rangle = z_i \in \mathbb{Z} \quad \forall i$$
$$\implies A^t \mathbf{v} = \mathbf{z} := [z_1, \cdots, z_n] \in \mathbb{Z}^n$$
$$\implies \mathbf{v} = A^{-t}\mathbf{z} := B\mathbf{z} \in \operatorname{im} B$$
$$\implies \mathbf{v} \in \operatorname{im} B$$
$$\implies \Lambda^\vee \subseteq \operatorname{im} B,$$

and

$$B^t A = (A^{-t})^t A = A^{-1} A = I$$
$$\implies \mathbf{b}_i \cdot \mathbf{e}_j = \delta_{ij} \in \mathbb{Z}$$
$$\implies \operatorname{im} B \subseteq \operatorname{span} \Lambda^\vee.$$

∎

### 3.8.3 c.

?

# 4 Spring 2019

## 4.1 1

$A$ is diagonalizable iff $\min_A(x)$ is separable. See further discussion here.

Claim: If $A \in \operatorname{GL}(m, \mathbb{F})$ is invertible and $A^n/\mathbb{F}$ is diagonalizable, then $A/\mathbb{F}$ is diagonalizable.

Let $A \in \operatorname{GL}(m, \mathbb{F})$. Since $A^n$ is diagonalizable, $\min_{A^n}(x) \in \mathbb{F}[x]$ is separable and thus factors as a product of $m$ **distinct** linear factors:

$$\min_{A^n}(x) = \prod_{i=1}^m (x - \lambda_i), \quad \min_{A^n}(A^n) = 0$$

where $\{\lambda_i\}_{i=1}^m \subset \mathbb{F}$ are the **distinct** eigenvalues of $A^n$.

Moreover $A \in \operatorname{GL}(m, \mathbb{F}) \implies A^n \in \operatorname{GL}(m, \mathbb{F})$: $A$ is invertible $\iff \det(A) = d \in \mathbb{F}^\times$, and so $\det(A^n) = \det(A)^n = d^n \in \mathbb{F}^\times$ using the fact that the determinant is a ring morphism $\det : \operatorname{Mat}(m \times m) \longrightarrow \mathbb{F}$ and $\mathbb{F}^\times$ is closed under multiplication.

So $A^n$ is invertible, and thus has trivial kernel, and thus zero is not an eigenvalue, so $\lambda_i \neq 0$ for any $i$.

Since the $\lambda_i$ are distinct and nonzero, this implies $x^k$ is not a factor of $\mu_{A^n}(x)$ for any $k \geq 0$. Thus the $m$ terms in the product correspond to precisely $m$ **distinct linear** factors.

We can now construct a polynomial that annihilates $A$, namely

$$q_A(x) := \min_{A^n}(x^n) = \prod_{i=1}^{m}(x^n - \lambda_i) \in \mathbb{F}[x],$$

where we can note that $q_A(A) = \min_{A^n}(A^n) = 0$, and so $\min_A(x) \mid q_A(x)$ by minimality.

We now claim that $q_A(x)$ has exactly $n \cdot m$ distinct linear factors in $\bar{\mathbb{F}}[x]$, which reduces to showing that no pair $x^n - \lambda_i, x^n - \lambda_j$ share a root. and that $x^n - \lambda_i$ does not have multiple roots.

- For the first claim, we can factor

$$x^n - \lambda_i = \prod_{k=1}^{n}(x - \lambda_i^{\frac{1}{n}} e^{\frac{2\pi i k}{n}}) := \prod_{k=1}^{n}(x - \lambda_i^{\frac{1}{n}} \zeta_n^k),$$

  where we now use the fact that $i \neq j \implies \lambda_i^{\frac{1}{n}} \neq \lambda_j^{\frac{1}{n}}$. Thus no term in the above product appears as a factor in $x^n - \lambda_j$ for $j \neq i$.

- For the second claim, we can check that $\dfrac{\partial}{\partial x}(x^n - \lambda_i) = nx^{n-1} \neq 0 \in \mathbb{F}$, and $\gcd(x^n - \lambda_i, nx^{n-1}) = 1$ since the latter term has only the roots $x = 0$ with multiplicity $n - 1$, whereas $\lambda_i \neq 0 \implies$ zero is not a root of $x^n - \lambda_i$.

But now since $q_A(x)$ has exactly distinct linear factors in $\bar{\mathbb{F}}[x]$ and $\min_A(x) \mid q_A(x)$, $\min_A(x) \in \mathbb{F}[x]$ can only have distinct linear factors, and $A$ is thus diagonalizable over $\mathbb{F}$.

■

## 4.2   2

### 4.2.1   (a)

Go to a field extension. Orders of multiplicative groups for finite fields are known.

We can consider the quotient $K = \dfrac{\mathbb{F}_p[x]}{\langle \pi(x) \rangle}$, which since $\pi(x)$ is irreducible is an extension of $\mathbb{F}_p$ of degree $d$ and thus a field of size $p^d$ with a natural quotient map of rings $\rho : \mathbb{F}_p[x] \longrightarrow K$.

Since $K^\times$ is a group of size $p^d - 1$, we know that for any $y \in K^\times$, we have by Lagrange's theorem that the order of $y$ divides $p^d - 1$ and so $y^{p^d} = y$.

So every element in $K$ is a root of $q(x) = x^{p^d} - x$.

Since $\rho$ is a ring morphism, we have

$$\rho(q(x)) = \rho(x^{p^d} - x) = \rho(x)^{p^d} - \rho(x) = 0 \in K$$
$$\iff q(x) \in \ker \rho$$
$$\iff q(x) \in \langle \pi(x) \rangle$$
$$\iff \pi(x) \mid q(x) = x^{p^d} - x \quad \text{"to contain is to divide".}$$

■

## 4.2.2 (b)

> Some potentially useful facts:
>
> - $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
> - $x^{p^d} - x \mid x^{p^n} - x \iff d \mid n$
> - $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \mid n$
> - $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic $f_i$ of degree $d$ dividing $n$.

Claim: $\pi(x)$ divides $x^{p^n} - x \iff \deg \pi$ divides $n$.

$\implies$ : Let $L \cong \mathbb{GF}(p^n)$ be the splitting field of $\varphi_n(x) := x^{p^n} - x$; then since $\pi \mid \varphi_n$ by assumption, $\pi$ splits in $L$. Let $\alpha \in L$ be any root of $\pi$; then there is a tower of extensions $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$.

Then $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$, and so

$$
\begin{aligned}
n &= [L : \mathbb{F}_p] \\
&= [L : \mathbb{F}_p(\alpha)]\,[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \\
&= \ell d,
\end{aligned}
$$

for some $\ell \in \mathbb{Z}^{\geq 1}$, so $d$ divides $n$.

$\impliedby$ : If $d \mid n$, use the fact (claim) that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic $f_i$ of degree $d$ dividing $n$. So $f = f_i$ for some $i$.

■

## 4.3  3

> - Sylow theorems:
> - $n_p \cong 1 \mod p$
> - $n_p \mid m$.

It turns out that $n_3 = 1$ and $n_5 = 1$, so $G \cong S_3 \times S_5$ since both subgroups are normal.

There is only one possibility for $S_5$, namely $S_5 \cong \mathbb{Z}/(5)$.

There are two possibilities for $S_3$, namely $S_3 \cong \mathbb{Z}/(3^2)$ and $\mathbb{Z}/(3)^2$.

Thus

- $G \cong \mathbb{Z}/(9) \times \mathbb{Z}/(5)$, or
- $G \cong \mathbb{Z}/(3)^2 \times \mathbb{Z}/(5)$.

■

## 4.4  4

Concepts Used:

- Notation: $X/G$ is the set of $G$-orbits

- Notation: $X^g = \left\{ x \in x \mid g \cdot x = x \right\}$
- Burnside's formula: $|G||X/G| = \sum |X^g|$.

### 4.4.1 a

Strategy: Burnside.

- Define a sample space $\Omega = G \times G$, so $|\Omega| = |G|^2$.

- Identify the event we want to analyze: $A := \left\{ (g, h) \in G \times G \mid [g, h] = 1 \right\}$.

    - Define and note:
    $$A_g := \left\{ (g, h) \mid h \in H, [g, h] = 1 \right\} \implies A = \coprod_{g \in G} A_g.$$

- Set $n$ be the number of conjugacy classes, note we want to show $P(A) = n/|G|$.

- Let $G$ act on itself by conjugation, which partitions $G$ into conjugacy classes.

    - What are the orbits?
    $$\mathcal{O}_g = \left\{ hgh^{-1} \mid h \in G \right\},$$
    which is the conjugacy class of $g$.

    - What are the fixed points?
    $$X^g = \left\{ h \in G \mid hgh^{-1} = g \right\},$$
    which are the elements of $G$ that commute with $g$, which is precisely $A_g$.

- Note $|X/G| = n$, the number of conjugacy classes.

- Note that
$$|A| = \left| \coprod_{g \in G} A_g \right| = \sum_{g \in G} |A_g| = \sum_{g \in G} |X^g|.$$

- Apply Burnside
$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

- Rearrange and use definition:
$$n|G| = |X/G||G| = \sum_{g \in G} |X^g|$$

- Compute probability:
$$P(A) = \frac{|A|}{|\Omega|} = \frac{\sum_{g \in G} |X^g|}{|G|^2} = \frac{|X/G||G|}{|G|^2} = \frac{n|G|}{|G|^2} = \frac{n}{|G|}.$$

∎

### 4.4.2 b

Class equation:

$$|G| = Z(G) + \sum_{\substack{\text{One } x \text{ from each} \\ \text{conjugacy class}}} [G : Z(x)]$$

where $Z(x) = \left\{ g \in G \;\middle|\; [g, x] = 1 \right\}$.

### 4.4.3 c

> Todo: revisit.

As shown in part 1,

$$\mathcal{O}_x = \left\{ g \curvearrowright x \;\middle|\; g \in G \right\} = \left\{ h \in G \;\middle|\; ghg^{-1} = h \right\} = C_G(g),$$

and by the class equation

$$|G| = |Z(G)| + \sum_{\substack{\text{One } x \text{ from each} \\ \text{conjugacy class}}} [G : Z(x)]$$

Now note

- Each element of $Z(G)$ is in its own conjugacy class, contributing $|Z(G)|$ classes to $n$.

- Every other class of elements in $G \setminus Z(G)$ contains at least 2 elements

  - Claim: each such class contributes **at least** $\dfrac{1}{2}|G \setminus Z(G)|$.

Thus

$$n \leq |Z(G)| + \frac{1}{2}|G \setminus Z(G)|$$
$$= |Z(G)| + \frac{1}{2}|G| - \frac{1}{2}|Z(G)|$$
$$= \frac{1}{2}|G| + \frac{1}{2}|Z(G)|$$

$$\implies \frac{n}{|G|} \leq \frac{1}{2}\frac{|G|}{|G|} + \frac{1}{2}\frac{|Z(G)|}{|G|}$$
$$= \frac{1}{2} + \frac{1}{2}\frac{1}{[G : Z(G)]}.$$

### 4.5  5

### 4.5.1 a

Suppose $\mathrm{Tor}(M)$ has rank $n \geq 1$. Then let $\mathbf{r}$ be a generating element.

However, since $\mathbf{r} \in \mathrm{Tor}(M)$, there exists an $s \in R \setminus 0_R$ such that $s\mathbf{r} = 0_M$.

But then $s\mathbf{r} = 0$ with $s \neq 0$, so $\{\mathbf{r}\}$ is by definition not linearly independent.

$\blacksquare$

### 4.5.2  b

Let $n = \mathrm{rank}\, M$, and let $\mathcal{B} = \{\mathbf{r}_i\}_{i=1}^n \subseteq R$ be a generating set. Let $M' := M/\mathrm{Tor}(M)$ and $\pi : M \longrightarrow M'$ be the canonical quotient map.

**Claim:** $\pi(\mathcal{B})$ is a basis for $M'$.

**Linearly Independent:**

Let $\mathcal{B}' = \pi(\mathcal{B}) = \{\mathbf{r}_i + \mathrm{Tor}(M)\}_{i=1}^n$ and suppose that

$$\sum_{i=1}^n s_i(\mathbf{r}_i + \mathrm{Tor}M) = \mathbf{0}_{M'}.$$

Since $x = 0 \in M' \iff x \in \mathrm{Tor}(M)$,

$$\sum_{i=1}^n s_i\mathbf{r}_i \in \mathrm{Tor}(M) \implies \exists \alpha \neq 0_R \in R \text{ such that } \alpha_i \sum s_i\mathbf{r}_i = \mathbf{0}_M.$$

But since $R$ is an integral domain and $\alpha \neq 0$, we must have $s_i = 0$ for all $i$.

**Spanning:**

Write $\pi(\mathcal{B}) = \{\mathbf{r}_i + \mathrm{Tor}(M)\}_{i=1}^n$.

Letting $\mathbf{x} \in M'$ be arbitrary, we can write $\mathbf{x} = \mathbf{m} + \mathrm{Tor}(M)$ for some $\mathbf{m} \in M$ where $\pi(\mathbf{m}) = \mathbf{x}$.

But since $\mathcal{B}$ is a basis for $M$, we have $\mathbf{m} = \sum_{i=1}^n s_i\mathbf{r}_i$, and so

$$\begin{aligned}
\mathbf{x} &= \pi(\mathbf{m}) \\
&= \pi(\sum_{i=1}^n s_i\mathbf{r}_i) \\
&= \sum_{i=1}^n s_i\pi(\mathbf{r}_i) \\
&= \sum_{i=1}^n s_i(\mathbf{r}_i + \mathrm{Tor}(M)),
\end{aligned}$$

which expresses $\mathbf{x}$ as a linear combination of elements in $\mathcal{B}'$.

### 4.5.3 c

**$M$ is not free: Claim**: If $I \trianglelefteq R$ is a free $R$-module, then $I$ is a principal ideal.

*Proof:* Let $I = \langle B \rangle$ for some basis – if $B$ contains more than 1 element, say $m_1$ and $m_2$, then $m_2 m_1 - m_1 m_2 = 0$ is a linear dependence, so $B$ has only one element $m$.

But then $I = \langle m \rangle = R_m$ is cyclic as an $R$- module and thus principal as an ideal of $R$. The result follows by the contrapositive.

**$M$ is rank 1**: For any module, we can take an element $M \neq 0_M$ and consider its cyclic module $Rm$.

Thus the rank of $M$ is at least 1, since $\{m\}$ is a subset of a spanning set. It can not be linearly dependent, since $R$ is an integral domain and $M \subseteq R$, so $\alpha m = 0 \implies \alpha = 0$.

However, the rank is at most 1 since $R$ is commutative. If we take two elements $\mathbf{m}, \mathbf{n} \in M$, then since $m, n \in R$ as well, we have $nm = mn$ and so

$$(n)\mathbf{m} + (-m)\mathbf{n} = 0_R = 0_M$$

is a linear dependence. 2 **$M$ is torsion-free**:

Let $x \in \mathrm{Tor} M$, then there exists some $r \neq 0 \in R$ such that $rx = 0$. But $x \in R$ and $R$ is an integral domain, so $x = 0$, and thus $\mathrm{Tor}(M) = \{0_R\}$.

$\blacksquare$

## 4.6  6

### 4.6.1 a

Define the set of proper ideals

$$S = \left\{ J \mid I \subseteq J < R \right\},$$

which is a poset under set inclusion.

Given a chain $J_1 \subseteq \cdots$, there is an upper bound $J := \bigcup J_i$, so Zorn's lemma applies.

### 4.6.2 b

$\implies$ :

We will show that $x \in J(R) \implies 1 + x \in R^\times$, from which the result follows by letting $x = rx$.

Let $x \in J(R)$, so it is in every maximal ideal, and suppose toward a contradiction that $1 + x$ is **not** a unit.

Then consider $I = \langle 1 + x \rangle \trianglelefteq R$. Since $1 + x$ is not a unit, we can't write $s(1 + x) = 1$ for any $s \in R$, and so $1 \notin I$ and $I \neq R$

So $I < R$ is proper and thus contained in some maximal proper ideal $\mathfrak{m} < R$ by part (1), and so we have $1 + x \in \mathfrak{m}$. Since $x \in J(R)$, $x \in \mathfrak{m}$ as well.

But then $(1 + x) - x = 1 \in \mathfrak{m}$ which forces $\mathfrak{m} = R$.

$\Longleftarrow$

Fix $x \in R$, and suppose $1 + rx$ is a unit for all $r \in R$.

Suppose towards a contradiction that there is a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$ and thus $x \notin J(R)$.

Consider

$$M' := \left\{ rx + m \mid r \in R, \ m \in M \right\}.$$

Since $\mathfrak{m}$ was maximal, $\mathfrak{m} \subsetneq M'$ and so $M' = R$.

So every element in $R$ can be written as $rx + m$ for some $r \in R, m \in M$. But $1 \in R$, so we have

$$1 = rx + m.$$

So let $s = -r$ and write $1 = sx - m$, and so $m = 1 + sx$.

Since $s \in R$ by assumption $1 + sx$ is a unit and thus $m \in \mathfrak{m}$ is a unit, a contradiction.

So $x \in \mathfrak{m}$ for every $\mathfrak{m}$ and thus $x \in J(R)$.

### 4.6.3 c

- $\mathfrak{N}(R) = \left\{ x \in R \mid x^n = 0 \text{ for some } n \right\}$.
- $J(R) = \text{Spec}_{\max}(R) = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$.

We want to show $J(R) = \mathfrak{N}(R)$.

$\mathfrak{N}(R) \subseteq J(R)$:

We'll use the fact $x \in \mathfrak{N}(R) \implies x^n = 0 \implies 1 + rx$ is a unit $\iff x \in J(R)$ by (b):

$$\sum_{k=1}^{n-1} (-x)^k = \frac{1 - (-x)^n}{1 - (-x)} = (1 + x)^{-1}.$$

$J(R) \subseteq \mathfrak{N}(R)$:

Let $x \in J(R) \setminus \mathfrak{N}(R)$.

Since $R$ is finite, $x^m = x$ for some $m > 0$. Without loss of generality, we can suppose $x^2 = x$ by replacing $x^m$ with $x^{2m}$.

If $1 - x$ is not a unit, then $\langle 1 - x \rangle$ is a nontrivial proper ideal, which by (a) is contained in some maximal ideal $\mathfrak{m}$. But then $x \in \mathfrak{m}$ and $1 - x \in \mathfrak{m} \implies x + (1 - x) = 1 \in \mathfrak{m}$, a contradiction.

So $1 - x$ is a unit, so let $u = (1 - x)^{-1}$.

Then

$$(1 - x)x = x - x^2 = x - x = 0$$
$$\implies u(1 - x)x = x = 0$$
$$\implies x = 0.$$

## 4.7 7

Work with matrix of all ones instead. Eyeball eigenvectors. Coefficients in minimal polynomial: size of largest Jordan block Dimension of eigenspace: number of Jordan blocks

### 4.7.1 a

Let $A$ be the matrix in the question, and $B$ be the matrix containing 1's in every entry.

- Noting that $B = A + I$, we have

$$B\mathbf{x} = \lambda\mathbf{x}$$
$$\iff (A + I)\mathbf{x} = \lambda\mathbf{x}$$
$$\iff A\mathbf{x} = (\lambda - 1)\mathbf{x},$$

  so we will find the eigenvalues of $B$ and subtract one from each.

- Note that $B\mathbf{v} = \left[\sum v_i, \sum v_i, \cdots, \sum v_i\right]$, i.e. it has the effect of summing all of the entries of $\mathbf{v}$ and placing that sum in each component.

- We proceed by finding $p$ eigenvectors and eigenvalues, since the JCF and minimal polynomials will involve eigenvalues and the transformation matrix will involve (generalized) eigenvectors.

- Claim: each vector of the form $\mathbf{p}_i := \mathbf{e}_1 - \mathbf{e}_{i+1} = [1, 0, 0, \cdots, 0 - 1, 0, \cdots, 0]$ where $i \neq j$ is also an eigenvector with eigenvalues $\lambda_0 = 0$, and this gives $p - 1$ linearly independent vectors spanning the eigenspace $E_{\lambda_0}$

  - Compute

$$B\mathbf{p}_i = [1 + 0 + \cdots + 0 + (-1) + 0 + \cdots + 0] = [0, 0, \cdots, 0]$$

  - So every $\mathbf{p}_i \in \ker(B)$, so they are eigenvectors with eigenvalue 0.
  - Since the first component is fixed and we have $p - 1$ choices for where to place a $-1$, this yields $p - 1$ possibilities for $\mathbf{p}_i$
  - These are linearly independent since the $(p - 1) \times (p - 1)$ matrix $\left[\mathbf{p}_1^t, \cdots, \mathbf{p}_{p-1}^t\right]$ satisfies

$$\det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix} = (1) \cdot \det \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix} = (-1)^{p-2} \neq 0.$$

  where the first equality follows from expanding along the first row and noting this is the first minor, and every other minor contains a row of zeros.

- Claim: $\mathbf{v}_1 = [1, 1, \cdots, 1]$ is an eigenvector with eigenvalue $\lambda_1 = p$.

  - Compute

$$B\mathbf{v} = \left[\sum_{i=1}^{p} 1, \sum_{i=1}^{p} 1, \cdots, \sum_{i=1}^{p} 1\right] = [p, p, \cdots, p] = p[1, 1, \cdots, 1] = p\mathbf{v}_1,$$

  thus $\lambda_1 = p$

- dim $E_{\lambda_1} = 1$ since the eigenspaces are orthogonal and $E_{\lambda_0} \oplus E_{\lambda_1} \le F^p$ is a subspace, so $p > \dim(E_{\lambda_0}) + \dim E_{\lambda_1} = p - 1 + \dim E_{\lambda_1}$ and it isn't zero dimensional.

- Using that the eigenvalues of $A$ are $1 + \lambda_i$ for $\lambda_i$ the above eigenvalues for $B$,

$$\text{Spec }(B) := \{(\lambda_i, m_i)\} = \{(p, 1), (0, p-1)\} \implies \chi_B(x) = (x - p)x^{p-1}$$
$$\implies \text{Spec }(A) = \{(p-1, 1), (-1, p-1)\} \implies \chi_A(x) = (x - p + 1)(x+1)^{p-1}$$

> Note: we can always read off the *characteristic* polynomial from the spectrum.

- The dimensions of eigenspaces are preserved, thus

$$JCF_{\mathbb{Q}}(A) = J_{p-1}^1 \oplus (p-1)J_{-1}^1 = \left[\begin{array}{c|c|c|c|c|c} p-1 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

- The matrix $P$ such that $A = PJP^{-1}$ will have columns the bases of the generalized eigenspaces.

- In this case, the generalized eigenspaces are the usual eigenspaces, so

$$P = [\mathbf{v}_1, \mathbf{p}_1, \cdots, \mathbf{p}_{p-1}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

### 4.7.2  b

For $F = \mathbb{F}_p$, all eigenvalues/vectors still lie in $\mathbb{F}_p$, but now $-1 = p-1$, making $(x - (p-1))(x+1)^{p-1} = (x+1)(x+1)^{p-1}$, so $\chi_{A,\mathbb{F}_p}(x) = (x+1)^p$, and the Jordan blocks may merge.

- A computation shows that $(A + I)^2 = pA = 0 \in M_p(\mathbb{F}_p)$ and $(A+I) \ne 0$, so $\min_{A,\mathbb{F}_p}(x) = (x+1)^2$.
  - Thus the largest Jordan block corresponding to $\lambda = -1$ is of size 2
- Can check that $\det(A) = \pm 1 \in \mathbb{F}_p^{\times}$, so the vectors $\mathbf{e}_1 - \mathbf{e}_i$ are still linearly independent and thus $\dim E_{-1} = p - 1$
  - So there are $p - 1$ Jordan blocks for $\lambda = 0$.

Summary:

$$\min_{A,\mathbb{F}_p}(x) = (x+1)^2$$
$$\chi_{A,\mathbb{F}_p}(x) \equiv (x+1)^p$$
$$\dim E_{-1} = p - 1.$$

Thus

$$JCF_{\mathbb{F}_p}(A) = J_{-1}^2 \oplus (p-2)J_{-1}^1 = \begin{bmatrix} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 \end{bmatrix}.$$

To obtain a basis for $E_{\lambda=0}$, first note that the matrix $P = [\mathbf{v}_1, \mathbf{p}_1, \cdots, \mathbf{p}_{p-1}]$ from part (a) is singular over $\mathbb{F}_p$, since

$$\begin{aligned} \mathbf{v}_1 + \mathbf{p}_1 + \mathbf{p}_2 + \cdots + \mathbf{p}_{p-2} &= [p-1, 0, 0, \cdots, 0, 1] \\ &= [-1, 0, 0, \cdots, 0, 1] \\ &= -\mathbf{p}_{p-1}. \end{aligned}$$

We still have a linearly independent set given by the first $p-1$ columns of $P$, so we can extend this to a basis by finding one linearly independent generalized eigenvector.

Solving $(A - I\lambda)\mathbf{x} = \mathbf{v}_1$ is our only option (the others won't yield solutions). This amounts to solving $B\mathbf{x} = \mathbf{v}_1$, which imposes the condition $\sum x_i = 1$, so we can choose $\mathbf{x} = [1, 0, \cdots, 0]$.

Thus

$$P = [\mathbf{v}_1, \mathbf{x}, \mathbf{p}_1, \cdots, \mathbf{p}_{p-2}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

## 4.8  8

Concepts used:

- $\zeta_n := e^{\frac{2\pi i}{n}}$, and $\zeta_n^k$ is a primitive $n$th root of unity $\iff \gcd(n, k) = 1$
  - In general, $\zeta_n^k$ is a primitive $\dfrac{n}{\gcd(n, k)}$th root of unity.
- $\deg \Phi_n(x) = \varphi(n)$
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ (proof: for a nontrivial gcd, the possibilities are $p, 2p, 3p, 4p, \cdots, p^{k-2}p, p^{k-1}p$.)
- $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$

Let $K = \mathbb{Q}(\zeta)$

### 4.8.1  a

- $\zeta := e^{2\pi i/8}$ is a primitive 8th root of unity
- The minimal polynomial of an $n$th root of unity is the $n$th cyclotomic polynomial $\Phi_n$

- The degree of the field extension is the degree of $\Phi_8$, which is

$$\varphi(8) = \varphi(2^3) = 2^{3-1} \cdot (2-1) = 4.$$

- So $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

### 4.8.2 b

- $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(8)^\times \cong \mathbb{Z}/(4)$ by general theory
- $\mathbb{Z}/(4)$ has exactly one subgroup of index 2.
- Thus there is exactly **one** intermediate field of degree 2 (a quadratic extension).

### 4.8.3 c

- Let $L = \mathbb{Q}(\zeta, \sqrt[4]{2})$.

- Note $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$

  - $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta)$
    * $\zeta_8^2 = i$, and $\zeta_8 = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$ so $\zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}$.
  - $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i, \sqrt{2})$:
    * $\zeta = e^{2\pi i/8} = \sin(\pi/4) + i\cos(\pi/4) = \dfrac{\sqrt{2}}{2}(1+i)$.

- Thus $L = \mathbb{Q}(i, \sqrt{2})(\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$.

  - Uses the fact that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ since $\sqrt[4]{2}^2 = \sqrt{2}$

- Conclude

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})]\, [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

using the fact that the minimal polynomial of $i$ over any subfield of $\mathbb{R}$ is always $x^2 + 1$, so $\min_{\mathbb{Q}(\sqrt[4]{2})}(i) = x^2 + 1$ which is degree 2.

# 5 Fall 2018

## 5.1 1

Concepts Used:

- Sylow 2: All Sylow $p$-subgroups are conjugate.
- $|HK| = |H||K|/\left|H \bigcap K\right|$.
- Lagrange's Theorem: $H \leq G \implies |H| \,\Big|\, |G|$

### 5.1.1 a

- Every $p$-subgroup is contained in some Sylow $p$-subgroup, so $P \subseteq S_p^i$ for some $S_p^i \in \mathrm{Syl}_p(G)$.

- $P \trianglelefteq G \iff gPg^{-1} = P$ for all $g \in G$.

- Let $S_p^j$ be any other Sylow $p$-subgroup,

- Since Sylow $p$-subgroups are all conjugate $gS_p^i g^{-1} = S_p^j$ for *some* $g \in G$.

- Then

$$P = gPg^{-1} \subseteq gS_p^i g^{-1} = S_p^j.$$

### 5.1.2  b

- If $P$ is not contained in $M$, then $M < MP$ is a proper subgroup

- By maximality of $M$, $MP = G$

- Note that $M \bigcap P \le P$ and $|P| = p^c$ implies $\left| M \bigcap P \right| = p^a$ for some $a \le c$ by Lagrange

- Then write

$$G = MP \iff |G| = \frac{|M||P|}{|M \bigcap P|}$$

$$\iff \frac{|G|}{|M|} = \frac{|P|}{|M \bigcap P|} = \frac{p^c}{p^a} = p^{c-a} := p^b$$

where $a \le c \implies 0 \le c - b \le c$ so $0 \le b \le c$.

### 5.2  2

Concepts used:

- Orbit: $G \cdot x := \left\{ g \cdot x \mid g \in G \right\} \subseteq X$
- Stabilizer: $G_x := \left\{ g \in G \mid g \cdot x = x \right\} \le G$
- Orbit-Stabilizer: $G \cdot x \simeq G/G_x$.
- $abc \in H \iff b \in a^{-1} H c^{-1}$
- Set of orbits for $G \curvearrowright X$, notated $X/G$.
- Set of fixed points for $G \curvearrowright X$, notated $X^g$.
- Burnside's Lemma: $|X/G| \cdot |G| = \displaystyle\sum_{g \in G} |X^g|$
    - Number of orbits equals average number of fixed points.

### 5.2.1  a

- Fix $x$ and let $y \in G_x$ be another element in the orbit of $x$.
- Then there exists a $g \in G$ such that $g \cdot x = y$, so $x = g^{-1} \cdot y$

- Then

$$h \in G \cdot x \iff h \cdot x = x \quad \text{by being in the stabilizer}$$
$$\iff h \cdot (g^{-1} \cdot y) = g^{-1} \cdot y \quad \text{using that } x, y \text{ are in the same orbit}$$
$$\iff (ghg^{-1}) \cdot y = y$$
$$\iff ghg^{-1} \in G_y \quad \text{by the defn of the stabilizer}$$
$$\iff h \in g^{-1}G_y g,$$

so every $h \in G \cdot x$ is conjugate to some element in $G_y$.

### 5.2.2 b

Let $G$ act on its subgroups by conjugation,

- The orbit $G \cdot H$ is the set of all subgroups conjugate to $H$, and

- The stabilizer of $H$ is $G_H = N_G(H)$.

- By orbit-stabilizer,

$$G \cdot H = [G : G_H] = [G : N_G(H)].$$

- Since $|H| = n$, and all of its conjugate also have order $n$.

- Note that

$$H \leq N_G(H) \implies |H| \leq |N_G(H)| \implies \frac{1}{|N_G(H)|} \leq \frac{1}{|H|},$$

- Now *strictly* bound the size of the union by overcounting their intersections at the identity:

$$\left| \bigcup_{g \in G} gHg^{-1} \right| < (\text{Number of Conjugates of } H) \cdot (\text{Size of each conjugate})$$

$$\quad\quad \textit{strictly overcounts since they intersect in at least the identity}$$
$$= [G : N_G(H)]|H|$$
$$= \frac{|G|}{|N_G(H)|}|H| \quad \text{since } G \text{ is finite}$$
$$\leq \frac{|G|}{|H|}|H|$$
$$= |G|.$$

### 5.2.3 c

- Let $G \curvearrowright X$ transitively where $|X| \geq 2$
- An action is transitive iff there is only one orbit, so $|X/G| = 1$.
- Apply Burnside's Lemma

$$1 = |X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| \implies |G| = \sum_{g \in G} |X^g|$$

- Note that $X^e = X$, since the identity must fix every element, so $|X^e| \geq 2$.
- Not *every* other term in the sum can be greater than 1, otherwise the RHS is greater than the size of $G$
- Thus we must have $|X^g| = 0$ for some $g \in G$, i.e. $g$ has no fixed points in $X$.

## 5.3 3

Let $L/K/F$.

### 5.3.1 a

**False**: Take $L/K/F = \mathbb{Q}(\zeta_2, \sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}$.

Then $L/F$ is Galois, since it is the splitting field of $x^3 - 2$ and $\mathbb{Q}$ has characteristic zero.

But $K/F$ is not Galois, since it is not the splitting field of any irreducible polynomial.

### 5.3.2 b

**True**: If $L/F$ is Galois, then $L/K$ is normal and separable:

- $L/K$ is normal, since if $\sigma : L \hookrightarrow \overline{K}$ lifts the identity on $K$ and fixes $L$, i-t also lifts the identity on $F$ and fixes $L$ (and $\overline{K} = \overline{F}$).

- $L/K$ is separable, since $F[x] \subseteq K[x]$, and so if $\alpha \in L$ where $f(x) := \min(\alpha, F)$ has no repeated factors, then $f'(x) := \min(\alpha, K)$ divides $f$ and thus can not have repeated factors.

### 5.3.3 c

**False**: Use the fact that every quadratic extension is Galois, and take $L/K/F = \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}$.

Then each successive extension is quadratic (thus Galois) but $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial (noting that it does not split $x^4 - 2$ completely.)

## 5.4 4

Let $m(x)$ be the minimal polynomial of $\varphi$. If the polynomial $f(x) = x$ doesn't divide $m$, then $f$ does not have zero as an eigenvalue, so $\varphi$ is nonsingular and since 0 is nilpotent, $\varphi + 0$ works.

Otherwise, write $\varphi(x) = x^m \rho(x)$ where $\gcd(x, \rho(x)) = 1$.

Then

$$V \cong \frac{k[x]}{m(x)} \cong \frac{k[x]}{(x^m)} \oplus \frac{k[x]}{(\rho)} := U \oplus W$$

by the Chinese Remainder theorem.

We can now note that $\varphi|_U$ is nilpotent because it has characteristic polynomial $x^m$, and $\varphi|_W$ is nonsingular since $\lambda = 0$ is not an eigenvalue by construction.

## 5.5 5

### 5.5.1 a

Letting $\mathbf{v}$ be fixed, since $\left\{A^j \mathbf{v}\right\}$ spans $V$ we have

$$B\mathbf{v} = \sum_{j=0}^{n-1} c_j A^j \mathbf{v}.$$

So let $p(x) = \sum_{j=0}^{n-1} c_j x^j$. Then consider how $B$ acts on any basis vector $A^k \mathbf{v}$.

We have

$$
\begin{aligned}
BA^k \mathbf{v} &= A^k B\mathbf{v} \\
&= A^k p(A)\mathbf{v} \\
&= p(A)A^k \mathbf{v},
\end{aligned}
$$

so $B = p(A)$ as operators since their actions agree on every basis vector in $V$.

### 5.5.2 b

$\implies :$

If $\left\{A^j \mathbf{v}_k \mid 0 \le j \le n-1\right\}$ is linearly independent, this means that $A$ does satisfy any polynomial of degree $d < n$.

So $\deg m_A(x) = n$, and since $m_A(x)$ divides $\chi_A(x)$ and both are monic degree polynomials of degree $n$, they must be equal.

$\impliedby :$

Let $A \curvearrowright k[x]$ by $A \curvearrowright p(x) \coloneqq p(A)$. This induces an invariant factor decomposition $V =^{\cong} \bigoplus k[x]/(f_i)$. Since the product of the invariant factors is the characteristic polynomial, the largest invariant factor is the minimal polynomial, and these two are equal, there can only be one invariant factor and thus the invariant factor decomposition is

$$V \cong \frac{k[x]}{(\chi_A(x))}$$

as an isomorphism of $k[x]$-modules.

So $V$ is a cyclic $k[x]$ module, which means that $V = k[x] \curvearrowright \mathbf{v}$ for some $\mathbf{v} \in V$ such that $\operatorname{Ann}(\mathbf{v}) = \chi_A(x)$.

> I.e. there is some element $\mathbf{v} \in V$ whose orbit is all of $V$.

But then noting that monomials span $k[x]$, we can write

$$
\begin{aligned}
V &\cong k[x] \curvearrowright \mathbf{v} \\
&:= \left\{ f(x) \curvearrowright \mathbf{v} \ \middle| \ f \in k[x] \right\} \\
&= \operatorname{span}_k \left\{ x^k \curvearrowright \mathbf{v} \ \middle| \ k \geq 0 \right\} \\
&:= \operatorname{span}_k \left\{ A^k \mathbf{v} \ \middle| \ k \geq 0 \right\}.
\end{aligned}
$$

Moreover, we can note that if $k \geq \deg \chi_A(x)$, then $A^k$ is a linear combination of $\left\{ A^j \ \middle| \ 0 \leq j \leq n-1 \right\}$, and so

$$
\begin{aligned}
V &\cong \operatorname{span}_k \left\{ A^k \mathbf{v} \ \middle| \ k \geq 0 \right\} \\
&= \operatorname{span}_k \left\{ A^k \mathbf{v} \ \middle| \ 1 \leq k \leq n-1 \right\}.
\end{aligned}
$$

∎

## 5.6  6

### 5.6.1  a

By the correspondence theorem, submodules of $M/N$ biject with submodules $A$ of $M$ containing $N$. So

- $M$ is maximal:
- $\iff$ no such (proper, nontrivial) submodule $A$ exists
- $\iff$ there are no (proper, nontrivial) submodules of $M/N$
- $\iff$ $M/N$ is simple.

### 5.6.2  b

Identify $\mathbb{Z}$-modules with abelian groups, then by (a), $N$ is maximal $\iff$ $M/N$ is simple $\iff$ $M/N$ has no nontrivial proper subgroups.

By Cauchy's theorem, if $|M/N| = ab$ is a composite number, then $a \mid ab \implies$ there is an element (and thus a subgroup) of order $a$. In this case, $M/N$ contains a nontrivial proper cyclic subgroup, so $M/N$ is not simple. So $|M/N|$ can not be composite, and therefore must be prime.

### 5.6.3  c

Let $G = \left\{ x \in \mathbb{C} \ \middle| \ x^n = 1 \text{ for some } n \in \mathbb{N} \right\}$, and suppose $H < G$ is a proper subgroup.

Then there must be a prime $p$ such that the $\zeta_{p^k} \notin H$ for all $k$ greater than some constant $m$ – otherwise, we can use the fact that if $\zeta_{p^k} \in H$ then $\zeta_{p^\ell} \in H$ for all $\ell \leq k$, and if $\zeta_{p^k} \in H$ for all $p$ and all $k$ then $H = G$.

But this means there are infinitely many elements in $G \setminus H$, and so $\infty = [G : H] = |G/H|$ is not a prime. Thus by (b), $H$ can not be maximal, a contradiction.

∎

## 5.7 7

### 5.7.1 a

Let $\varphi$ denote the map in question, it suffices to show that $\varphi$ is $R$-linear, i.e. $\varphi(s\mathbf{x}+\mathbf{y}) = s\varphi(\mathbf{x})+\varphi(\mathbf{y})$:

$$
\begin{aligned}
\varphi(s\mathbf{x} + \mathbf{y}) &= r(s\mathbf{x} + \mathbf{y}) \\
&= rs\mathbf{x} + r\mathbf{y} \\
&= s(r\mathbf{x}) + (r\mathbf{y}) \\
&= s\varphi(\mathbf{x}) + \varphi(\mathbf{y}).
\end{aligned}
$$

### 5.7.2 b

We identify $\ker \varphi = \left\{ x \in R \mid rx = 0 \right\}$, and since $r \neq 0$ by assumption, this implies each such $x$ is a zero divisor by definition (and $\ker \varphi$ is nonempty by assumption).

Similarly, we identify $\operatorname{im} \varphi = \left\{ y = rx \mid x \in R \right\}$. So let $y \in \operatorname{im} \varphi$. Since $r$ is a zero divisor, there exists some $z \in R$ such that $rz = 0$.

But then

$$ yz = rxz = xrz = x \cdot 0 = 0 $$

since $R$ is commutative, so $y$ is a zero divisor.

### 5.7.3 c

See 1964 Annals "Properties of rings with a finite number of zero divisors"

Let $Z := \{z_i\}_{i=1}^n$ be the set of $n$ zero divisors in $R$. Let $\varphi_i$ be the $n$ maps $x \mapsto z_i x$, and let $K_i = \ker \varphi_i$ be the corresponding kernels.

Fix an $i$. By (b), $K_i$ consists of zero divisors, so

$$ |K_i| \leq n < \infty \quad \text{for each } i. $$

Now consider $R/K_i := \{r + K_i\}$. By the first isomorphism theorem, $R/K_i \cong \operatorname{im} \varphi$, and by (b) every element in the image is a zero divisor, so

$$ [R : K_i] = |R/K_i| = |\operatorname{im} \varphi_i| \leq n. $$

But then

$$ |R| = [R : K_i] \cdot |K_i| \leq n \cdot n = n^2. $$

**5.7.4 d**

By (c), if there are exactly 2 zero divisors then $|R| \leq 4$. Since every element in a finite ring is either a unit or a zero divisor, and $|R^\times| \geq 2$ since $\pm 1$ are always units, we must have $|R| = 4$.

Since the characteristic of a ring must divide its size, we have char $R = 2$ or 4.

Using the hint, we see that only $\mathbb{Z}/(4)$ has characteristic 4, which has exactly 2 zero divisors given by $[0]_4$ and $[2]_4$.

If $R$ has characteristic 2, we can check the other 3 possibilities.

We can write $\mathbb{Z}/(2)[t]/(t^2) = \left\{ a + bt \ \middle| \ a, b \in \mathbb{Z}/(2) \right\}$, and checking the multiplication table we have

$$
\begin{array}{c|cccc}
 & 0 & 1 & t & 1+t \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & t & 1+t \\
t & 0 & t & \mathbf{0} & t \\
1+t & 0 & 1+t & t & 1
\end{array} \ ,
$$

and so we find that $t, 0$ are the zero divisors.

In $\mathbb{Z}/(2)[t]/(t^2 - t)$, we can check that $t^2 = t \implies tt^2 = t^2 \implies t(t^2 + 1) = 0 \implies t(t+1) = 0$, so both $t$ and $t + 1$ are zero divisors, along with zero, so this is not a possibility.

Similarly, in $\mathbb{Z}/(2)[t]/(t^2 + t + 1)$, we can check the bottom-right corner of the multiplication table to find

$$
\left[
\begin{array}{c|cc}
 & t & 1+t \\
\hline
t & 1+t & 1 \\
t & 1 & t
\end{array}
\right] \ ,
$$

and so this ring only has one zero divisor.

Thus the only possibilities are:

$$R \cong \mathbb{Z}/(4)$$
$$R \cong \mathbb{Z}/(2)[t]/(t^2).$$

■

# 6 Spring 2018

## 6.1 1

Concepts Used:

- Centralizer: $C_G(x) = \left\{ g \in G \ \middle| \ [gx] = 1 \right\}$.

- Class Equation: $|G| = |Z(G)| + \sum [G : C_G(x_i)]$

- $G/Z(G)$ cyclic $\iff$ $G$ is abelian.

  > *Proof:*
  >
  > $$\begin{aligned} G/Z(G) = \langle xZ \rangle \iff g \in G &\implies gZ = x^m Z \\ &\iff g(x^m)^{-1} \in Z \\ &\iff g = x^m z \quad \text{for some} \quad z \in Z \\ &\implies gh = x^m z_1 x^n z_2 = x^n z_2 x^m z_1 = hg. \end{aligned}$$

- Every group of order $p^2$ is abelian.

- Classification of finite abelian groups.

### 6.1.1  a

Strategy: get $p$ to divide $|Z(G)|$.

- Apply the class equation:

$$|G| = |Z(G)| + \sum [G : C_G(x_i)].$$

- Since $C_G(x_i) \le G$ and $|G| = p^k$, by Lagrange $|C_G(x_i)| = p^\ell$ for some $0 \le \ell \le k$.

- Since $|G| = p^k$ for some $k$ and $Z(G), C_G(x_i) \le G$ are subgroups, their orders are powers of $p$.

- Use

$$[G : C_G(x_i)] = 1 \iff C_G(x_i) = G \iff \left\{ g \in G \,\middle|\, g x_i g^{-1} = x_i \right\} = G \iff x_i \in Z(G).$$

  - Thus every index appearing in the sum is greater than 1, and thus equal to $p^{\ell_i}$ for some $1 \le \ell_i \le k$
  - So $p$ divides every term in the sum

- Rearrange

$$|G| - \sum [G : C_G(x_i)] = |Z(G)|.$$

- $p$ divides both terms on the LHS, so must divide the RHS, so $|Z(G)| \ge p$.

### 6.1.2  b

Strategy: examine $|G/Z(G)|$ by cases.

- 1: Then $G = Z(G)$ and $G$ is abelian.
- $p$: Then $G/Z(G)$ is cyclic so $G$ is abelian
- $p^2$: Not possible, since $|Z(G)| > 1$ by (a).

### 6.1.3 c

- By Sylow

  - $n_5 \mid 7^2, \quad n_5 \cong 1 \mod 5 \implies n_5 \in \{1, 7, 49\} \setminus \{7, 49\} = \{1\} \implies n_5 = 1$
  - $n_7 \mid 5^2, \quad n_7 \cong 1 \mod 7 \implies n_7 \in \{1, 5, 25\} \setminus \{5, 25\} = \{1\} \implies n_7 = 1$

- By recognition of direct products, $G = S_5 \times S_7$

  - By above, $S_5, S_7 \trianglelefteq G$
  - Check $S_5 \bigcap S_7 = \{e\}$ since they have coprime order.
  - Check $S_5 S_7 = G$ since $|S_5 S_7| = 5^2 7^2 = |G|$

- By (b), $S_5, S_7$ are abelian since they are groups of order $p^2$

- The direct product of abelian groups is abelian.

### 6.1.4 d

1. $\mathbb{Z}_{5^2} \times \mathbb{Z}_{7^2}$
2. $\mathbb{Z}_5^2 \times \mathbb{Z}_{7^2}$
3. $\mathbb{Z}_{5^2} \times \mathbb{Z}_7^2$
4. $\mathbb{Z}_5^2 \times \mathbb{Z}_7^2$

■

## 6.2   2

Not the nicest proof! Would be better to replace the ad-hoc computations at the end..

### 6.2.1 a

Note that $g(x) = x^2 - 4x + 2$ has roots $\beta = 2 \pm \sqrt{2}$, and so $f$ has roots

$$\alpha_1 = \sqrt{2 + \sqrt{2}}$$
$$\alpha_2 = \sqrt{2 - \sqrt{2}}$$
$$\alpha_3 = -\alpha_1$$
$$\alpha_4 = -\alpha_2.$$

and splitting field $K = \mathbb{Q}(\{\alpha_i\})$.

### 6.2.2 b

$K$ is the splitting field of a separable polynomial and thus Galois over $\mathbb{Q}$. Moreover, Since $f$ is irreducible by Eisenstein with $p = 2$, the Galois group is a transitive subgroup of $S^4$, so the possibilities are:

- $S_4$
- $A_4$

- $D_4$
- $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$
- $\mathbb{Z}/(4)$

We can note that $g$ splits over $L := \mathbb{Q}(\sqrt{2})$, an extension of degree 2.

We can now note that $\min(\alpha, L)$ is given by $p(x) = x^2 - (2 + \sqrt{2})$, and so $[K : L] = 2$.

We then have

$$[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = (2)(2) = 4.$$

This $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, which leaves only two possibilities:

- $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$
- $\mathbb{Z}/(4)$

We can next check orders of elements. Take

$$\sigma \in \mathrm{Gal}(K/\mathbb{Q})$$
$$\alpha_1 \mapsto \alpha_2.$$

Computations show that

- $\alpha_1^2 \alpha_2^2 = 2$, so $\alpha_1 \alpha_2 = \sqrt{2}$
- $\alpha_1^2 = 2 + \sqrt{2} \implies \sqrt{2} = \alpha_1^2 - 2$

and thus

$$\sigma^2(\alpha_1) = \sigma(\alpha_2)$$
$$= \sigma\left(\frac{\sqrt{2}}{\alpha_1}\right)$$
$$= \frac{\sigma(\sqrt{2})}{\sigma(\alpha_1)}$$
$$= \frac{\sigma(\alpha_1^2 - 2)}{\alpha_2}$$
$$= \frac{\alpha_2^2 - 2}{\alpha_2}$$
$$= \alpha_2 - 2\alpha_2^{-1}$$
$$= \alpha_2 - \frac{2\alpha_1}{\sqrt{2}}$$
$$= \alpha_2 - \alpha_1\sqrt{2}$$
$$\neq \alpha_1,$$

and so the order of $\sigma$ is strictly greater than 2, and thus 4, and thus $\mathrm{Gal}(K/\mathbb{Q}) = \left\{\sigma^k \ \middle|\ 1 \leq k \leq 4\right\} \cong \mathbb{Z}/(4)$.

### 6.2.3  c

?? The subgroup of index 2 $\left\langle \sigma^2 \right\rangle$ corresponds to the field extension $Q(\sqrt{2})/\mathbb{Q}$.

## 6.3    3

Moral: $H_1 \bigcap H_2 \iff E_1 E_2, H_1 H_2 \iff E_1 \bigcap E_2$.

### 6.3.1  a

By the Galois correspondence, it suffices to show that the fixed field of $H_1 \bigcap H_2$ is $E_1 E_2$.

Let $\sigma \in H_1 \bigcap H_2$; then $\sigma \in \text{Aut}(K)$ fixes both $E_1$ and $E_2$.

Not sure if this works – compositum is not literally product..?

Writing $x \in E_1 E_2$ as $x = e_1 e_2$, we have

$$\sigma(x) = \sigma(e_1 e_2) = \sigma(e_1)\sigma(e_2) = e_1 e_2 = x,$$

so $\sigma$ fixes $E_1 E_2$.

### 6.3.2  b

That $H_1 H_2 \subseteq G$ is clear, since if $\sigma = \tau_1 \tau_2 \in H_1 H_2$, then each $\tau_i$ is an automorphism of $K$ that fixes $E_i \supseteq \mathbb{Q}$, so each $\tau_i$ fixes $\mathbb{Q}$ and thus $\sigma$ fixes $\mathbb{Q}$.

That it is a subgroup follows from the fact that elements commute. (?)

To see this, let $\sigma = \sigma_1 \sigma_2 \in H_1 H_2$.

Note that $\sigma_1(e) = e$ for all $e \in E_1$ by definition, since $H_1$ fixes $E_1$, and $\sigma_2(e) \in E_1$ (?).

Then

$$\sigma_1(e) = e \quad \forall e \in E_1 \implies \sigma_1(\sigma_2(e)) = \sigma_2(e)$$

and substituting $e = \sigma_1(e)$ on the RHS yields

$$\sigma_1 \sigma_2(e) = \sigma_2 \sigma_1(e),$$

where a similar proof holds for $e \in E_2$ and thus for arbitrary $x \in E_1 E_2$.

### 6.3.3  c

By the Galois correspondence, the subgroup $H_1 H_2 \leq G$ will correspond to an intermediate field $E$ such that $K/E/\mathbb{Q}$ and $E$ is the fixed field of $H_1 H_2$.

But if $\sigma \in H_1 H_2$, then $\sigma = \tau_1 \tau_2$ where $\tau_i$ is an automorphism of $K$ that fixes $E_i$, and so $\sigma(x) = x \iff \tau_1 \tau_2(x) = x \iff \tau_2(x) = x \,\&\, \tau_1(x) = x \iff x \in E_1 \bigcap E_2$.

# 7 Spring 2013

## 7.1 6

Lemma: every $\mathbf{v} \in V$ is $T$-cyclic $\iff \chi_T(x)/\daleth$ is irreducible.

### 7.1.1 a

Let $f$ be the characteristic polynomial of $T$.

$\implies$ :

- By contrapositive, suppose there is a proper nonzero invariant subspace $W < V$ with $T(W) \subseteq W$, we will show the characteristic polynomial $f := \chi_{V,T}(x)$ is reducible.
- Since $T(W) \subseteq W$, the restriction $g := \chi_{V,T}(x)\big|_W : W \longrightarrow W$ is a linear operator on $W$.
- Claim: $g$ divides $f$ in $\mathbb{F}[x]$ and $\deg(g) < \deg(f)$.
  - Matrix-dependent proof:
    * Choose an ordered basis for $W$, say $\mathcal{B}_W := \{\mathbf{w}_1, \cdots, \mathbf{w}_k\}$ where $k = \dim_F(W)$
    * Claim: this can be extended to a basis of $V$, say $\mathcal{B}_V := \{\mathbf{w}_1, \cdots, \mathbf{w}_k, \mathbf{v}_1, \cdots, \mathbf{v}_j\}$ where $k + j = \dim_F(V)$.
      · Note that since $W < V$ is proper, $j \geq 1$.
    * Restrict $T$ to $W$ to get $T_W$, then let $B = [T_W]_{\mathcal{B}_W}$ be the matrix representation of $T_W$ with respect to $\mathcal{B}_W$.
    * Now consider the matrix representation $[T]_{\mathcal{B}_V}$, in block form this is given by

    $$[T]_{\mathcal{B}_V} = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}$$

    where we've used that $W < V$ is proper to get the existence of $C, D$ (there is at least one additional row/column since $j \geq 1$ in the extended basis.)
    * Now expand along the first column block to obtain

    $$\chi_{T,V}(x) := \det([T]_{\mathcal{B}_V} - xI) = \det(B - xI) \cdot \det(D - xI) := \chi_{T,W}(x) \cdot \det(D - xI).$$

    * Claim: $\det(D - xI) \in xF[x]$ is nontrivial
    * The claim follows because this forces $\deg(\det(D - xI)) \geq 1$ and so $\chi_{T,W}(x)$ is a proper divisor of $\chi_{T,V}(x)$.
- Thus $f$ is reducible.

$\impliedby$

- Suppose $f$ is reducible, then we will produce a proper $T$-invariant subspace.
- Claim: if $f$ is reducible, there exists a nonzero, noncyclic vector $\mathbf{v}$.
- Then $\operatorname{span}_k \left\{ T^j \mathbf{v} \right\}_{j=1}^d$ is a $T$-invariant subspace that is nonzero, and not the entire space since $\mathbf{v}$ is not cyclic.

### 7.1.2 b

Characterization of diagonalizability: $T$ is diagonalizable over $F \iff \min_{T,F}$ is squarefree in $\overline{F}[x]$?

[Margin note: Is there a proof without matrices? What if $V$ is infinite dimensional?]

[Margin note: How to extend basis?]

[Margin note: Why?]

- Let $\min_{T,F}(x)$ be the minimal polynomial of $T$ and $\chi_{T,F}(x)$ be its characteristic polynomial.
- By Cayley-Hamilton, $\min_{T,F}(x)$ divides $\chi_{T,F}$
- Since $\chi_{T,F}$ is irreducible, these polynomials are equal.
- Claim: $T/F$ is diagonalizable $\iff$ $\min_{T,F}$ splits over $F$ and is squarefree.
- Replace $F$ with its algebraic closure, then $\min_{T,F}$ splits.
- Claim: in characteristic zero, every irreducible polynomial is separable
    - Proof: it must be the case that either $\gcd(f, f') = 1$ or $f' \equiv 0$, where the second case only happens in characteristic $p > 0$.
    - The first case is true because $\deg f' < \deg f$, and if $\gcd(f, f') = p$, then $\deg p < \deg f$ and $p \mid f$ forces $p = 1$ since $f$ is irreducible.
- So $\min_{T,F}$ splits into distinct linear factors
- Thus $T$ is diagonalizable.