Algebra Qualifying Exam Solutions

D. Zack Garza

Wednesday 3rd June, 2020

Contents

1 Fall 2018

1.1 1

1.1.1 a

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

Since P is normal in G, we have $gPg^{-1} = P$ for all $g \in G$.

If S_p^j is any other Sylow p-subgroup, we have $gS_p^ig^{-1} = S_p^j$ for some $g \in G$.

But then $P = gPg^{-1} \subseteq gS_p^ig^{-1} = S_p^j$.

1.1.2 b

Suppose P is not contained in M; then $M < MP$ is a proper subgroup, and by maximality of M, $MP = G$.

We can then write

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

$$\implies \Big|M \bigcap P\Big||G| = |M||P|$$

$$(?) \implies |G| \text{ divides } |M||P|$$

$$\implies |G|/|M| \text{ divides } |P|.$$

1.2 2

1.2.1 a

- $G_a = \mathrm{Stab}_G(a) = \left\{ g \in G \;\middle|\; g \curvearrowright a = a \right\}$
- $G_b = \mathrm{Stab}_G(b) = \left\{ g \in G \;\middle|\; g \curvearrowright b = b \right\}$
- $G \cdot x = \mathcal{O}_x = \left\{ g \curvearrowright x \;\middle|\; g \in G \right\}$

Suppose $a, b \in X$ where $a \in G \cdot b$, so they belong to the same orbit. Then $a = h \curvearrowright b$ for some $h \in G$.

Then

$$\begin{aligned} g \in G_a &\iff g \curvearrowright a = a \\ &\iff g \curvearrowright (h \curvearrowright b) = h \curvearrowright b \\ &\iff gh \curvearrowright b = h \curvearrowright b \\ &\iff h^{-1}gh \curvearrowright b = b \\ &\iff h^{-1}gh \in G_b, \end{aligned}$$

so $g \in G_a \iff hgh^{-1} \in G_b$ and so the stabilizers of any two elements in the same orbit are conjugate.

1.2.2 b

Suppose $|H| = n$ and thus $|G| = nm$ for some $m = [G : H] \geq 2$ by Lagrange since H is proper.

Let G act on its subgroups by conjugation,

- The orbit $G \cdot H$ is the set of all conjugate subgroups, and
- The stabilizer of H is $G_H = N_G(H)$.

By orbit-stabilizer,

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

Let $|H| = n$, and note that all conjugate subgroups have the same order.

Then

$$H \leq N_G(H) \implies [G : N_G(H)] \leq [G : H] = m.$$

and each conjugate contains the identity element, so

$$\begin{aligned}
\bigcup_{g\in G} gHg^{-1} &\leq 1 + \sum_{H'\in G\cdot H} (|H'|-1) \\
&= 1 + \sum_{H'\in G\cdot H} n-1 \\
&= 1 + (n-1)|G\cdot H| \\
&= 1 + (n-1)[G:N_G(H)] \\
&\leq 1 + (n-1)[G:H] \\
&= 1 + (n-1)m \\
&= 1 + nm - m \\
&= 1 + |G| - m \\
&= |G| - (m-1) \\
&\leq |G| - 1 \quad \text{since } m \geq 2 \\
&< |G|.
\end{aligned}$$

Todo: not an ideal proof. Doesn't use the first part..?

1.2.3 c

Noting that $G \curvearrowright S$ transitively iff there is only one orbit and $|S/G| = 1$, by Burnside's lemma we have

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

where $S^g = \left\{ s \in S \;\middle|\; g \curvearrowright s = s \;\forall g \in G \right\}$.

We can now note that $S^e = S$ and so $|S^e| \geq 2$, not every other term in the sum can be greater than 1. So there is some g such that $|S^g| = 0$, so g has no fixed points.

■

1.3 3

Let $L/K/F$.

1.3.1 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.

1.3.2 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 $f(x) \coloneqq \min(\alpha, F)$ has no repeated factors, then $f'(x) \coloneqq \min(\alpha, K)$ divides f and thus can not have repeated factors.

1.3.3 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.)

1.4 4

Let $m(x)$ be the minimal polynomial of φ. If the polynomial $f(x) = x$ doesn't divide m, then f does not have zero as an eigenvalue, so φ 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

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

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.

1.5 5

1.5.1 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.

1.5.2 b

$\implies$:

If $\left\{ A^j \mathbf{v}_k \;\middle|\; 0 \leq j \leq n-1 \right\}$ 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

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

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

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

■

1.6 6

1.6.1 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.

1.6.2 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.

1.6.3 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.

■

1.7 7

1.7.1 a

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

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

1.7.2 b

We identify $\ker\varphi = \left\{x \in R \;\middle|\; rx = 0\right\}$, 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 $\text{im }\varphi = \left\{y = rx \;\middle|\; x \in R\right\}$. So let $y \in \text{im }\varphi$. Since r is a zero divisor, there exists some $z \in R$ such that $rz = 0$.

But then

$$yz = rxz = xrz = 0z2$$

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

1.7.3 c

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

Let $Z \coloneqq \{z_i\}_{i=1}^n$ be the set of n zero divisors in R. Let φ_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 $R/K_i \coloneqq \{r + K_i\}$. By the first isomorphism theorem, $R/K_i \cong \text{im } \varphi$, and by (b) every element in the image is a zero divisor, so

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

But then

$$|R| = [R : K_i]|K_i| \leq (n)(n) = n^2 < \infty.$$

1.7.4 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 $\left|R^\times\right| \geq 2$ since ± 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

	0	1	t	$1+t$
0	0	0	0	0
1	0	1	t	$1+t$
t	0	t	**0**	t
$1+t$	0	$1+t$	t	1

,

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:

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

■

2 Spring 2018

2.1 1

2.1.1 a

We have

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

and since $e \in Z(G)$, $|Z(G)| \geq 1$. Since $p \mid |G|$, we must have $p \mid |Z(G)| \neq 0$ and so $|Z(G)| \geq p$.

2.1.2 b

Lemma: $G/Z(G)$ cyclic $\iff$ G is abelian.
Proof:

$$\begin{aligned} G/Z(G) = \langle x + Z \rangle &\iff g \in G \implies g + Z = x^m + Z \\ &\iff g(x^m)^{-1} = z \iff g = x^m z \\ &\implies gh = x^m z_1 x^n z_2 = x^n z_2 x^m z_1 = hg. \end{aligned}$$

Since G is a p-group, G has a nontrivial center, so consider $G/Z(G)$.

This could have three possible orders:

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

2.1.3 c

By Sylow, we have $n_5 = 1$ and $n_7 = 1$, so both $P_5, P_7 \trianglelefteq G$, and by recognition of direct products we have $G \cong P_5 \times P_7$.

Since the sizes of both of these groups are p^2 for a prime, by (b) they are abelian, and the direct product of abelian groups is again abelian.

2.1.4 d

By the classification of finite abelian groups and the Chinese Remainder theorem,

- $\mathbb{Z}/(5)^2 \times \mathbb{Z}/(7)^2$
- $\mathbb{Z}/(5^2) \times \mathbb{Z}/(7)^2$
- $\mathbb{Z}/(5)^2 \times \mathbb{Z}/(7^2)$
- $\mathbb{Z}/(5^2) \times \mathbb{Z}/(7^2)$

■

2.2 2

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

2.2.1 a

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

$$\begin{aligned}\alpha_1 &= \sqrt{2+\sqrt{2}} \\ \alpha_2 &= \sqrt{2-\sqrt{2}} \\ \alpha_3 &= -\alpha_1 \\ \alpha_4 &= -\alpha_2.\end{aligned}$$

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

2.2.2 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 $L \coloneqq \mathbb{Q}(\sqrt{2})$, 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

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

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

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

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

2.2.3 c

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

2.3 3

Moral: $H_1 \bigcap H_2 \iff E_1E_2$, $H_1H_2 \iff E_1 \bigcap E_2$.

2.3.1 a

By the Galois correspondence, it suffices to show that the fixed field of $H_1 \bigcap H_2$ is E_1E_2.

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

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

Writing $x \in E_1E_2$ as $x = e_1e_2$, we have

$$\sigma(x) = \sigma(e_1e_2) = \sigma(e_1)\sigma(e_2) = e_1e_2 = x,$$

so σ fixes E_1E_2.

2.3.2 b

That $H_1H_2 \subseteq G$ is clear, since if $\sigma = \tau_1\tau_2 \in H_1H_2$, then each τ_i is an automorphism of K that fixes $E_i \supseteq \mathbb{Q}$, so each τ_i fixes $\mathbb{Q}$ and thus σ fixes $\mathbb{Q}$.

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

To see this, let $\sigma = \sigma_1\sigma_2 \in H_1H_2$.

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 $x \in E_1E_2$.

2.3.3 c

By the Galois correspondence, the subgroup $H_1H_2 \leq G$ will correspond to an intermediate field E such that $K/E/\mathbb{Q}$ and E is the fixed field of H_1H_2.

But if $\sigma \in H_1H_2$, then $\sigma = \tau_1\tau_2$ where τ_i is an automorphism of K that fixes E_i, and so $\sigma(x) = x \iff \tau_1\tau_2(x) = x \iff \tau_2(x) = x \;\&\; \tau_1(x) = x \iff x \in E_1 \bigcap E_2$.

3 Fall 2019

3.1 1

Centralizer:

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

Class equation:

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

Notation:

$$\begin{aligned} h^g &= ghg^{-1} \\ h^G &= \left\{ h^g \;\middle|\; g \in G \right\} \quad \text{Conjugacy Class} \\ H^g &= \left\{ h^g \;\middle|\; h \in H \right\} \\ N_G(H) &= \left\{ g \in G \;\middle|\; H^g = H \right\} \supseteq H \quad \text{Normalizer.} \end{aligned}$$

Theorem 1: $\left|h^G\right| = [G : Z(h)]$
Theorem 2: $\left|\left\{ H^g \;\middle|\; g \in G \right\}\right| = [G : N_G(H)]$
Proof: Let $G \curvearrowright \left\{ H \;\middle|\; H \leq G \right\}$ 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

$$\begin{aligned} \left| \bigcup_{g \in G} H^g \right| &= (|H| - 1)[G : N_G(H)] + 1 \\ &= |H|[G : N_G(H)] - [G : N_G(H)] + 1 \\ &= |G| \frac{|G|}{|N_G(H)|} - \frac{|G|}{|N_G(H)|} + 1 \\ &\leq |H| \frac{|G|}{|H|} - \frac{|G|}{|H|} + 1 \\ &= |G| - ([G : H] - 1) \\ &< |G|. \end{aligned}$$

where we use the fact that $H \subseteq N_G(H) \implies |H| \leq |N_G(H)| \implies \dfrac{1}{|N_G(H)|} \leq \dfrac{1}{|H|}$, 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

pqr Theorem.

3.2.1 a

Recall $n_p \mid m$ and $n_p \cong 1 \mod p$.

An easy check:

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

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

$$(5-1)n_5 + (7-1)n_7 + 1 = 4(21) + 6(15) > 105 \text{ elements.}$$

3.2.2 b

If $H, K \leq G$ and $H \trianglelefteq G$ then $HK \leq G$ is a subgroup. Proof: Check closure under products, needs normality.
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, $q - 1 \neq 0 \mod p$.
Theorem: If $G = A_1 A_2 \cdots A_n = \prod A_k$ and $A_i \bigcap \prod_{k \neq i} A_i = \{e\}$ for all i, then $A \cong A_1 \times \cdots \times A_n$.

Either Q or R is normal, so $QR \leq G$ is a subgroup of order $|Q| \cdot |R| = 5 \cdot 7 = 35$.

By the theorem, since $5 \nmid 7 - 1$, QR is cyclic.

3.2.3 c

In QR, there are

- $35 - 5 + 1$ elements of order *not* equal to 5,

- $5 - 7 + 1$ elements of order *not* equal to 7.

Since $QR \leq G$, there are *at least* this many such elements in G.

Suppose $n_5 = 21$ or $n_7 = 15$.

- Combining elements of order 5 with elements *not* of order 5 yields at least 31 elements of order *not* 5 with $n_5(5-1) = 21(4) = 84$ elements of order 5, this contributes $31 + 84 > 105$ elements – contradiction.
- Similarly, there are at least 29 elements of order *not* 7, plus $n_7(7-1) = 15(6) = 90$ elements of order 7, yielding $29 + 90 > 105$ elements.

So both $n_5 = 1, n_7 = 1$.

3.2.4 d

If P is normal, then $G = PQR$ with all intersections of the form $AB \bigcap C = \{e\}$, and since P, Q, R are all normal we have $G \cong P \times Q \times R \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{105}$ by characterization of direct products and 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

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

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 $\left|E^\times\right| = q^k - 1$. Noting that $\zeta \in E^\times$ we must have $n = o(\zeta) \;\Big|\; \left|E^\times\right| = q^k - 1$ by Lagrange's theorem.

3.4.2 b

Rephrasing (a), we have

$$\begin{aligned} n \mid q^k - 1 &\iff q^k - 1 \cong 0 \mod n \\ &\iff q^k \cong 1 \mod n \\ &\iff m \coloneqq o(q) \mid k. \end{aligned}$$

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 $q^m - 1 = \left|M^\times\right|$, and $M^\times$ is cyclic, so it contains a cyclic subgroup H of order n.

But then $x \in H \implies p(x) \coloneqq x^n - 1 = 0$, 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 ζ is one such solution, so $\zeta \in H \subset M^\times \subset M$. Since $F[\zeta]$ is the smallest field extension containing ζ, 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

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

We have

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

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

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

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 $b \curvearrowright m \coloneqq bm \in M$ 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 $\left\{ I \trianglelefteq R \;\middle|\; J \bigcap S = \emptyset \right\}$ 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 $S = \left\{ r^k \;\middle|\; k \in \mathbb{N} \right\}$ 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, $\left\{ I \trianglelefteq R \;\middle|\; I \bigcap S = \emptyset \right\}$ 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 $r \in \mathfrak{p}$.

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: ζ 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

$$\begin{aligned} \tau_j : K &\longrightarrow K \\ \zeta &\mapsto \zeta^j \end{aligned}$$

and if we restrict to j such that $\gcd(n, j) = 1$, this yields $\varphi(n)$ maps. Noting that if ζ is a primitive root, then $(n, j) = 1$ implies that that ζ^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

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

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 θ 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 ω_i which exist by the primitive element theorem.

3.8 8

3.8.1 a.

Let $\mathbf{v} \in \Lambda$, so $\mathbf{v} = \sum r_i \mathbf{e}_i$ where $r_i \in \mathbb{Z}$.

Then if $\mathbf{x} = \sum s_i \mathbf{e}_i \in \Lambda$, we have

$$\mathbf{v} \cdot \mathbf{x} = \sum r_i s_i \in \mathbb{Z}$$

since each term is just a product of integers, 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 $\mathbf{v} = [v_1, \cdots, v_n]$.

Note that

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

$$\implies \sum_j (\mathbf{e}_1 \cdot \mathbf{e}_j) v_j = 0 \quad \forall j.$$

Let $\mathbf{w} = \sum v_i \mathbf{e}_i$. Then $\mathbf{e}_k \cdot \mathbf{w} = \sum_j v_j \mathbf{e}_k \cdot \mathbf{e}_j = 0$ for every k, so $\mathbf{w}$ is orthogonal to every $\mathbf{e}_k$, and thus its span.

But $\mathbf{w}$ is in the span of the $\mathbf{e}_i$ by definition, so

$$\mathbf{w} \cdot \mathbf{w} = 0 \implies \mathbf{w} = 0 \implies \{\mathbf{e}_i\} \text{ is linearly dependent,}$$

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.

■

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

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

Possibly an error – should be the rows of A^{-1} instead of M^{-1}?

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

Since $A \in \mathrm{GL}(n, \mathbb{Z})$ which is a group, $A^{-1}, A^t, A^{-t} \in \mathrm{GL}(n, \mathbb{Z})$ as well.

$$\begin{aligned} \mathbf{v} \in \Lambda^\vee &\implies \mathbf{e}_i \cdot \mathbf{v} = z_i \in \mathbb{Z} \quad \forall i \\ &\implies A^t\mathbf{v} = \mathbf{z} \in \mathbb{Z}^n \\ &\implies \mathbf{v} = A^{-t}\mathbf{z} \coloneqq B\mathbf{z} \in \text{im } B \\ &\implies \text{span } \Lambda^\vee \subseteq \text{im } B, \end{aligned}$$

and

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

■

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

Let $A \in \mathrm{GL}(m, \mathbb{F})$. 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 $A \in \mathrm{GL}(m, \mathbb{F}) \implies A^n \in \mathrm{GL}(m, \mathbb{F})$: 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 $\det : \mathrm{Mat}(m \times m) \longrightarrow \mathbb{F}$ 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 λ_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

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

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

We now claim that $q_A(x)$ has exactly $n \cdot m$ distinct linear factors in $\overline{\mathbb{F}}[x]$, 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

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

  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 $\overline{\mathbb{F}}[x]$ and $\min_A(x) \;\Big|\; q_A(x)$, $\min_A(x) \in \mathbb{F}[x]$ 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 ρ is a ring morphism, we have

$$\begin{aligned}
\rho(q(x)) = \rho(x^{p^d} - x) = \rho(x)^{p^d} - \rho(x) = 0 \in K & \\
&\iff q(x) \in \ker \rho \\
&\iff q(x) \in \langle \pi(x) \rangle \\
&\iff \pi(x) \,\Big|\, q(x) = x^{p^d} - x \quad \text{"to contain is to divide".}
\end{aligned}$$

■

4.2.2 (b)

Some potentially useful facts:

- $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
- $x^{p^d} - x \,\Big|\, x^{p^n} - x \iff d \,\Big|\, n$
- $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \,\Big|\, n$
- $x^{p^n} - x = \prod f_i(x)$ 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 $\varphi_n(x) \coloneqq x^{p^n} - x$; then since $\pi \,\Big|\, \varphi_n$ by assumption, π splits in L. Let $\alpha \in L$ be any root of π; 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 $d \,\Big|\, n$, 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

- Notation: X/G is the set of G-orbits
- Notation: $X^g = \left\{ x \in x \;\middle|\; g \curvearrowright x = x \right\}$
- Burnside's formula: $|G||X/G| = \sum |X^g|$.

4.4.1 a

Letting n be the number of conjugacy classes, what we want to show is that

$$P([g,h] = 1) = \frac{n}{|G|}$$

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

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

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

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

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

We have Burnside's formula:

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

We can rearrange Burnside's formula to obtain

$$|X/G||G| = n|G| = \sum_{g\in G} |X^g|$$

and so

$$\begin{aligned} P([g,h]=1) &= \frac{\left|\left\{(g,h) \;\middle|\; [g,h]=1\right\}\right|}{|G|^2} \\ &= \frac{\sum_{g\in G}|X^g|}{|G|^2} \\ &= \frac{|X/G||G|}{|G|^2} \\ &= \frac{n|G|}{|G|^2} \\ &= \frac{n}{|G|}. \end{aligned}$$

■

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** $\frac{1}{2}|G \setminus Z(G)|$.

Thus

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

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

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.

■

4.5.2 b

Let $n = \operatorname{rank} M$, and let $\mathcal{B} = \{\mathbf{r}_i\}_{i=1}^n \subseteq R$ be a generating set. Let $M' \coloneqq M/\mathrm{Tor}(M)$ 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 $\pi(\mathcal{B}) = \{\mathbf{r}_i + \text{Tor}(M)\}_{i=1}^n$.

Letting $\mathbf{x} \in M'$ be arbitrary, we can write $\mathbf{x} = \mathbf{m} + \text{Tor}(M)$ 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

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

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 $x \in \text{Tor}M$, 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 $\text{Tor}(M) = \{0_R\}$.

■

4.6 6

4.6.1 a

Define the set of proper ideals

$$S = \left\{ J \;\middle|\; I \subseteq J < R \right\},$$

which is a poset under set inclusion.

Given a chain $J_1 \subseteq \cdots$, there is an upper bound $J \coloneqq \bigcup J_i$, 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 $\mathfrak{m} = R$.

$\impliedby$

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

$$M' \coloneqq \left\{ rx + m \;\middle|\; r \in R,\ m \in M \right\}.$$

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

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

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

$$\begin{aligned}(1-x)x = x - x^2 = x - x = 0 \\ \implies u(1-x)x = x = 0 \\ \implies x = 0.\end{aligned}$$

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

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

so it suffices to find the eigenvalues of B.

The vector $\mathbf{v}_1 = \sum \mathbf{e}_i$ (the vector of all 1's) is an eigenvector with eigenvalue $\lambda = p$ and $\dim E_{\lambda=p} = 1$.

Similarly, any vector of the form $\mathbf{p}_i \coloneqq \mathbf{e}_1 - \mathbf{e}_{i+1}$ where $i \neq j$ is also an eigenvector with eigenvalues $\lambda = 0$. This supplies the remaining $p - 1$ possibilities. Note that this also supplies $p - 1$ linearly independent vectors that span the corresponding eigenspace, so $\dim E_{\lambda=0} = p - 1$.

So

$$\begin{aligned}\text{Spec } (B) = \{(\lambda_1 = p, m_1 = 1), (\lambda_2 = 0, m_2 = p-1)\} \\ \implies \text{Spec } (A) = \{(\lambda_1 = p-1, m_1 = 1), (\lambda_2 = -1, m_2 = p-1)\} \\ \implies \chi_{A,\mathbb{Q}}(x) = (x - (p-1))(x - (-1))^{p-1}\end{aligned}$$

and geometric multiplicities are preserved, so

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

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 $-1 = p-1$, $\chi_{A,\mathbb{F}_p}(x) = (x+1)^p$, and the Jordan blocks may merge.

But a computation shows that $(A+I)^2 = pA = 0 \in M_p(\mathbb{F}_p)$ and $(A+I) \neq 0$, so $\min_{A,\mathbb{F}_p}(x) = (x+1)^2$.

So the largest Jordan block corresponding to $\lambda = 0$ is of size 2, and we can check that $\dim E_{\lambda=0} = \dim \left\{ \mathbf{e}_i - \mathbf{e}_j \;\middle|\; i \neq j \right\} = p-1$, so there are $p-1$ Jordan blocks for $\lambda = 0$.

Thus

$$JCF_{\mathbb{F}_p}(A) = J^2_{\lambda=-1} \oplus (p-2)J^1_{\lambda=-1} = \left[\begin{array}{cc|c|c|c|c} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

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

- Galois theory.
- $\deg \Phi_n(x) = \varphi(n)$
- $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$

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

4.8.1 a

Note that ζ is a primitive 8th root of unity, so we are looking for the degree of Φ_8, the 8th cyclotomic polynomial, which is $\varphi(8) = \varphi(2^3) = 2^2(1) = 4$.

So $[K : \mathbb{Q}] = 4$.

4.8.2 b

We have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/(8)^\times \cong \mathbb{Z}/(4)$, which is exactly one subgroup of index 2. Thus there is exactly **one** intermediate field of degree 2.

4.8.3 c

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

We can use the fact that $K = \mathbb{Q}(i, \sqrt{2})$ and thus $L = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2})$.

Proof: $\zeta_8^2 = i$, and $\zeta_8 = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$ so $\zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}$.

We can also use the fact that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$, and so $L = \mathbb{Q}(i, \sqrt[4]{2})$.

But then

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

Here we use the fact that the minimal polynomial of i over any subfield of $\mathbb{R}$ is always $x^2 + 1$.