Qual Solutions Collection

D. Zack Garza

December 26, 2019

Contents

1 Fall 2019

1.1 1

Centralizer:

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

Class equation:

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

Notation:

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

Theorem 1: $\left|h^G\right| = [G : Z(h)]$
Theorem 2: $|\{H^g \ni g \in G\}| = [G : N_G(H)]$

Use the fact that $\bigcup_{g \in G} H^g = \bigcup_{g \in G} gHg^{-1} \subsetneq G$ for any proper $H \leq G$. Proof: By theorem 2,

$$\begin{aligned}
\left| \bigcup_{g \in G} H^g \right| &< |H|[G : N_G(H)] \quad \text{since } e \text{ is in every conjugate} \\
&= |H| \frac{|G|}{|N_G(H)|} \\
&\leq |H| \frac{|G|}{|H|} \\
&= |G|.
\end{aligned}$$

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 can only happen if $Z(g_j) = G$ for every j. But this says that $g_j \in Z(G)$, and so $[g_j] = \{g_j\}$, i.e. each conjugacy class is size one, so every element of g is some g_j, and thus $g \in Z(G)$, so $G \subseteq Z(G)$ and G is abelian.

Todo: Revisit. I don't get it!

1.2 2

pqr Theorem.

1.2.1 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

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

1.2.2 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 $5 \not\Big| 7 - 1$, QR is cyclic.

1.2.3 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 $n_5 = 1, n_7 = 1$.

1.2.4 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).

1.3 3

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

1.3.1 a

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

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

1.3.2 b

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

1.4 4

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

1.4.1 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 $n=o(\zeta) \mid |E^\times| = q^k-1$ by Lagrange's theorem.

1.4.2 b

Rephrasing (a), we have

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

1.4.3 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 $x \in H \implies p(x) \coloneqq x^n-1=0$, and since $p(x)$ has at most n roots in a field. So $H=\{x \in M \ni x^n-1=0\}$, 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!

1.5 5

> One-step submodule test.

1.5.1 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

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

1.5.2 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.

1.5.3 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.

■

1.6 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 $\left\{ I \trianglelefteq R \ni J \bigcap S = \emptyset \right\}$ 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?)

1.6.1 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 $x \in \mathfrak{p}$.

1.6.2 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, $\left\{ I \trianglelefteq R \ni I \bigcap S = \emptyset \right\}$ has a maximal element $\mathfrak{p}$.

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

1.6.3 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 $r \in \mathfrak{p}$.

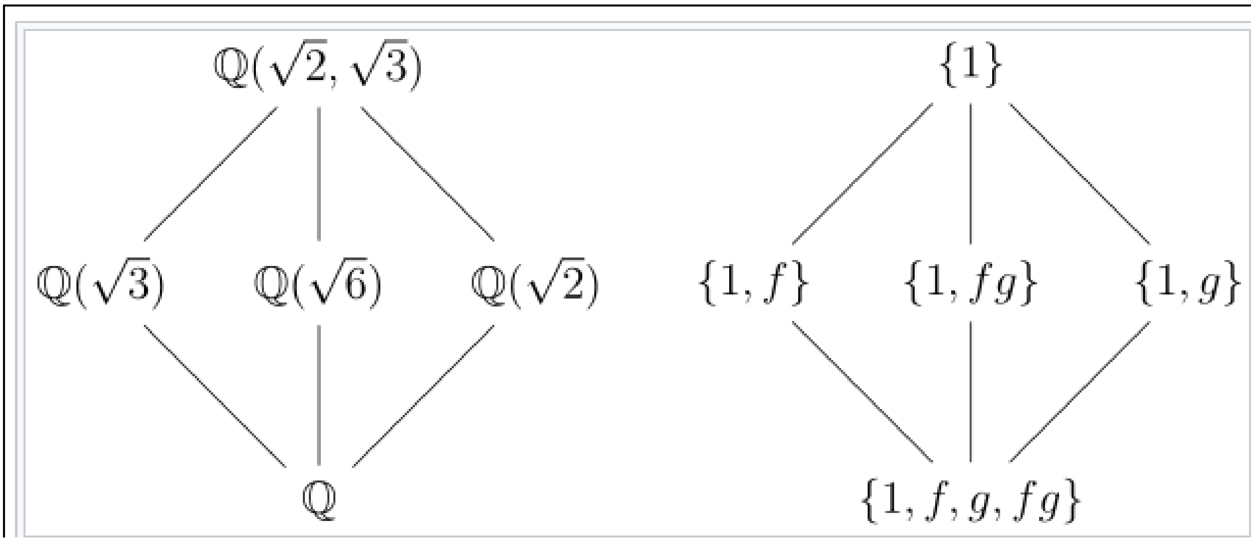
Since $r \notin N$, by (b) there is a maximal ideal $\mathfrak{m}$ that avoids all positive powers of r. Since $\mathfrak{m}$ is prime, we must have $\mathfrak{m} = \mathfrak{p}$. But then $r \notin \mathfrak{p}$, a contradiction.

1.7 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 $F^{\times}$.
$\phi(p^k) = p^{k-1}(p-1)$

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, $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = \phi(n)$ for the totient function.

We can now define maps

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

and if we restrict to j such that $\gcd(n, j) = 1$, this yields $\phi(n)$ 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

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

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 $\phi(20) = 8$, 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.

1.8 8

1.8.1 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.

1.8.2 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.

$\blacksquare$

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.

$\blacksquare$

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.

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

and

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

$\blacksquare$

1.8.3 c.

?

2 Spring 2019

2.1 1

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

Since A^n is diagonalizable (and $\mathbb{C}$ is algebraically closed), we can write $\min_{A^n}(x)$ as a product of **distinct** linear factors:

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

where λ_i are the **distinct** eigenvalues of A^n.

Moreover $A \in \mathrm{GL}(n, \mathbb{C}) \implies A^n \in \mathrm{GL}(n, \mathbb{C})$, so $\lambda_i \neq 0$ for any i.

This implies that there are no roots with multiplicity, since x^k is not a factor of $\mu_{A^n}(x)$, meaning that the k terms in the product correspond to exactly k **distinct** factors.

We can now construct a polynomial that annihilates A, namely

$$q_A(x) := \min_{A^n}(x^n) = \prod_{i=1}^{k} (x^n - \lambda_i),$$

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.

But then $\min_A(x)$ must have distinct linear factors, so A is diagonalizable.

■

2.2 2

2.2.1 (a)

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

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

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 satisfies $q(x) = x^{p^d} - x$.

Now letting $x \in \mathbb{F}^p$ be arbitray, since f is a group homomorphism, we have

$$\begin{aligned}
\rho(q(x)) = q(\rho(x)) = \rho(x)^{p^d} - \rho(x) = 0 \in K& \\
\implies q(x) &\in \ker \rho \\
\implies q(x) &\in \langle \pi(x) \rangle \\
\implies \pi(x) &\,\Big|\, q(x) = x^{p^d} - x.
\end{aligned}$$

■

2.2.2 (b)

Some potentially useful facts:

- $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x$
- $x^{p^d} - x \,\Big|\, x^{p^n} - x \iff d \,\Big|\, n$
- $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \,\Big|\, n$
- $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.

Let $\phi_n(x) = x^{p^n} - x$ and $\phi_d(x) = x^{p^d} - x$.

Let γ be an irreducible degree n polynomial over $\mathbb{F}_p$, then $L := \mathbb{F}[x]/\left\langle \gamma \right\rangle \cong \mathbb{GF}(p^n)$.

Note that by (a), $\pi(x) \,\Big|\, \phi_d(x)$ and $\gamma(x) \,\Big|\, \phi_n(x)$.

Then **(claim)** $\phi_n(x)$ splits in L. Since $\pi(x) \,\Big|\, \phi_n(x)$, $\pi(x)$ also splits in L.

Let $\alpha \in L$ be a root of $\pi(x)$. Since $\pi(x)$ is irreducible, $\deg \min(\alpha, \mathbb{F}_p) = d$.

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

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

so d divides n.

■

Proof of converse: If $d \,\Big|\, n$, use the fact 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. Proof of that fact:

2.3 3

- Sylow theorems:
- $n_p \cong 1 \mod p$
- $n_p \,\Big|\, m$.

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

■

2.4 4

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

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

What are the fixed points? $X^g = \left\{h \in G \ni hgh^{-1} = g\right\}$, 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

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

$\blacksquare$

2.4.2 b

Class equation:

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

where $Z(x) = \{g \in G \ni [g,x]=1\}$.

2.4.3 c

Todo: revisit.

As shown in part 1,

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

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

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

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

2.5 5

2.5.1 a

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

However, since $\mathbf{r} \in \text{Tor}(M)$, 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.

■

2.5.2 b

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

2.5.3 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 $m_2m_1 - m_1m_2 = 0$ 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 $\mathrm{Tor}(M) = \{0_R\}$.

$\blacksquare$

2.6 6

2.6.1 a

Define the set of proper ideals

$$S = \{J \ni I \subseteq J < R\},$$

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.

2.6.2 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

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

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 $x \in J(R)$.

2.6.3 c

- $\mathfrak{N}(R) = \{x \in R \ni x^n = 0 \text{ for some } n\}$.
- $J(R) = \mathrm{Spec}_{\max}(R) = \bigcap\limits_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$.

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

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

2.7 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

2.7.1 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 $\mathbf{p}_i := \mathbf{e}_1 - \mathbf{e}_{i+1}$ 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

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

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

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

2.7.2 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 $\dim E_{\lambda=0} = \dim \{\mathbf{e}_i - \mathbf{e}_j \ni i \neq j\} = p-1$, 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

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

2.8 8

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

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

2.8.1 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 $\phi(8) = \phi(2^3) = 2^2(1) = 4$.

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

2.8.2 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.

2.8.3 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 $x^2 + 1$.