Title

D. Zack Garza

December 24, 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 $n_p \Bigm| m$ 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 $5 \not\Bigm| 7 - 1$, 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 $n = o(\zeta) \,\Big|\, |E^\times| = q^k - 1$ by Lagrange's theorem.

1.4.2 b

Rephrasing (a), we have

$$\begin{aligned} n \,\Big|\, q^k - 1 &\iff q^k - 1 \cong 0 \mod n \\ &\iff q^k \cong 1 \mod n \\ &\iff m := o(q) \,\Big|\, k. \end{aligned}$$

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 $x \in H \implies p(x) := x^n - 1 = 0$, 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.

$\blacksquare$

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 $r \in \mathfrak{p}$.

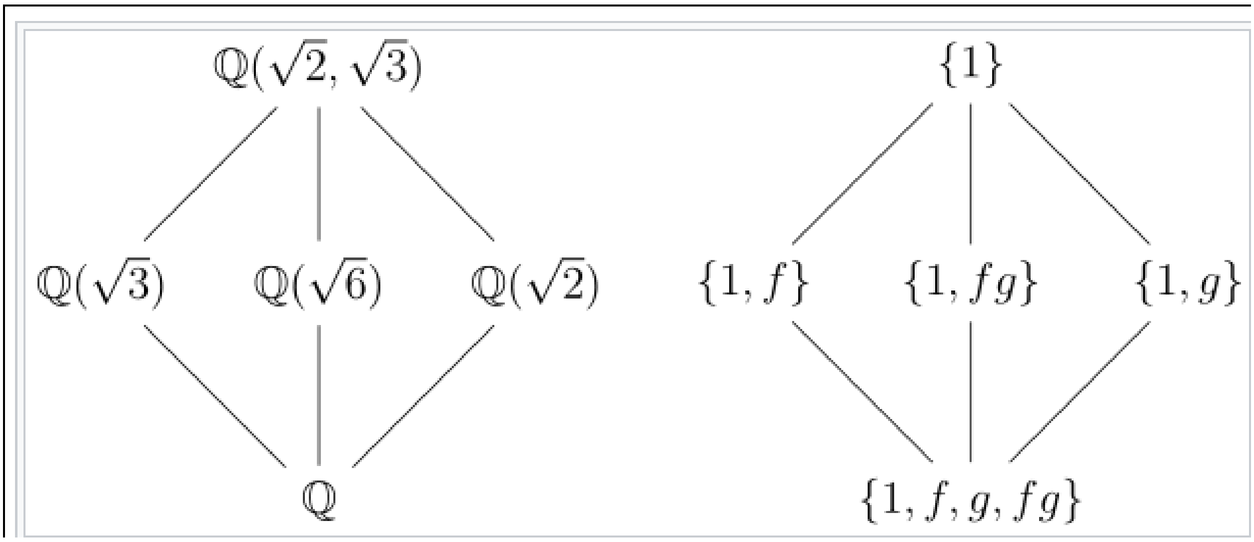
Since $r \notin N$, by (b) there is a maximal ideal $\mathfrak{m}$ that avoids all positive powers of r. Since $\mathfrak{m}$ is prime, we must have $\mathfrak{m} = \mathfrak{p}$. But then $r \notin \mathfrak{p}$, a contradiction.

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 $1 \le k \le n$.

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 $H \le K^\times$, 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.

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

and

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

$\blacksquare$

1.8.3 c.

?