Midterm

D. Zack Garza

October 31, 2019

Contents

1 Problem 1

Note that if either $p = 1$ or $q = 1$, G is a p-group, which is a nontrivial center that is always normal. So assume $p \neq 1$ and $q \neq 1$.

We want to show that G has a non-trivial normal subgroup. Noting that $\#G = p^2 q$, we will proceed by showing that either n_p or n_q must be 1.

We immediately note that

$$
\begin{aligned}
n_p &\equiv 1 \mod p \qquad & n_q &\equiv 1 \mod q \\
n_p &\,\Big|\, q & n_q &\,\Big|\, p^2,
\end{aligned}
$$

which forces

$$n_p \in \{1, q\}, \quad n_1 \in \left\{1, p, p^2\right\}.$$

If either $n_p = 1$ or $n_q = 1$, we are done, so suppose $n_p \neq 1$ and $n_1 \neq 1$. This forces $n_p = q$, and we proceed by cases:

1.1 Case 1: $p = q$.

Then $\#G = p^3$ and G is a p-group. But every p-group has a non-trivial center $Z(G) \leq G$, and the center is always a normal subgroup.

1.2 Case 2: $p > q$.

Here, since $n_p \,\Big|\, q$, we must have $n_p < q$. But if $n_p < q < p$ and $n_p = 1 \mod p$, then $n_p = 1$.

1.3 Case 3: $q > p$.

Since $n_p \neq 1$ by assumption, we must have $n_p = q$. Now consider sub-cases for n_q:

- $n_q = p$: If $n_q = p = 1 \mod q$ and $p < q$, this forces $p = 1$.
- $n_q = p^2$: We will reach a contradiction by showing that this forces

  $$\left| P := \bigcup_{S_p \in \mathrm{Syl}(p,G)} S_p \setminus \{e\} \right| + \left| Q := \bigcup_{S_q \in \mathrm{Syl}(q,G)} S_q \setminus \{e\} \right| + |\{e\}| > |G|.$$

  We have

  $$
  \begin{aligned}
  |P| + |Q| + |\{e\}| &= n_p(q-1) + n_q(p^2-1) + 1 \\
  &= p^2(q-1) + q(p^2-1) + 1 \\
  &= p^2(q-1) + 1(p^2-1) + (q-1)(p^2-1) + 1 \qquad \text{(since } q > 1\text{)} \\
  &= (p^2q - p^2) + (p^2-1) + (q-1)(p^2-1) + 1 \\
  &= p^2q + (q-1)(p^2-1) \\
  &\geq p^2q + (2-1)(2^2-1) \qquad \text{(since } p, q \geq 2\text{)} \\
  &= p^2q + 3 \\
  &> p^2q = |G|,
  \end{aligned}
  $$

  which is a contradiction. $\square$

2 Problem 2

We'll use the fact that $H \trianglelefteq N(H)$ for any subgroup H (following directly from the closure axioms for a subgroup), and thus

$$P \trianglelefteq N(P) \quad \text{and} \quad N(P) \trianglelefteq N^2(P).$$

Since it is then clear that $N(P) \subseteq N^2(P)$, it remains to show that $N^2(P) \subseteq N(P)$.

So if we let $x \in N^2(P)$, so x normalizes $N(P)$, we need to show that x normalizes P as well, i.e. $xPx^{-1} = P$.

However, supposing that $|G| = p^k m$ where $(p, m) = 1$, we have

$$P \leq N(P) \leq G \implies p^k \,\Big|\, |N(P)| \,\Big|\, p^k m,$$

so in fact $P \in \mathrm{Syl}(p, N(P))$ since it is a maximal p-subgroup.

Then $P' := xPx^{-1} \in \mathrm{Syl}(p, N(P))$ as well, since all conjugates of Sylow p-subgroups are also Sylow p-subgroups.

But since $P \trianglelefteq N(P)$, there is only *one* Sylow p- subgroup of $N(P)$, namely P. This forces $P = P'$, i.e. $P = xPx^{-1}$, which says that $x \in N(P)$ as desired. $\square$

3 Problem 3

By definition, G is simple iff it has no non-trivial subgroups, so we will show that if $|G| = 148$ then it must contain a normal subgroup.

Noting that $248 = p^2 q$ where $p = 2, q = 37$, we find that (for example) $n_2 \,\Big|\, 37$ but $n \equiv 1 \mod 2$; but the only odd divisor of 7 is 1, forcing $n_2 = 1$. So G has a normal Sylow 2-subgroup and we are done.

4 Problem 4

Let $\tau := (t_1, t_2)$ denote the transposition and $\sigma = (s_1, s_2 \cdots, s_p)$ denote the p-cycle, and let $S = \langle \sigma, \tau \rangle$. We would like to show that $S = S_p$, and since $S \subseteq S_p$ is clear, we just need to show that $S_p \subseteq S$.

We first note that because p is prime, σ^k is a p-cycle for every $1 \leq k \leq p$, and $\langle \sigma \rangle = \langle \sigma^k \rangle$ for any such k.

Then note that $t_1 = s_i$ for some i and $t_2 = s_j$ for some j, so we can take $k = j - i$ to get a cycle σ^k that sends t_1 to t_2. So without loss of generality, we can replace σ with

$$\sigma = (t_1, t_2, \cdots)$$

But now, we can relabel all of the elements of S_p simultaneously (i.e. replace $\langle \sigma, \tau \rangle$ with another subgroup in the same conjugacy class) in such a way that t_1 becomes 1 and t_2 becomes 2. We can then assume wlog that

$$\tau = (1,2), \quad \sigma = (1,2,\cdots,p)$$

We can then get all adjacent transpositions: noting that

$$\begin{aligned}
\sigma^{-1}\tau\sigma &= (2,3) \\
\sigma^{-2}\tau\sigma^2 &= (3,4) \\
&\cdots \\
\sigma^{-k}\tau\sigma^k &= (k+1 \mod p,\ k+2 \mod p) \quad \forall 1 \leq k \leq p,
\end{aligned}$$

where we use the fact that for any $\gamma \in S_p$, we have $\gamma\tau\gamma = (\gamma(1),\ \gamma(2))$.

But this also gives us all transpositions of the form $(1,j)$ for each $2 \leq j \leq p$:

$$\begin{aligned}
(2,3)^{-1}(1,2)(2,3) &= (1,3) \\
(3,4)^{-1}(1,3)(3,4) &= (1,4) \\
&\cdots \\
(j-1,j)^{-1}(1,j-1)(j-1,j) &= (1,j) \quad \forall 1 \leq j \leq p.
\end{aligned}$$

Thus we have $J \coloneqq \langle \{(1,j) \mid 2 \leq j \leq p\} \rangle \subseteq S$.

But now if $\gamma = (g_1, g_2, \cdots, g_k) \in S_p$ is an arbitrary cycle, we can write

$$\gamma = (g_1, g_2, \cdots, g_k) = (1, g_1)(1, g_2), \cdots (1, g_k),$$

so $\gamma \in J$. Then writing any arbitrary permutation as a product of disjoint cycles, we find that $S_p \subseteq J \subseteq S$, and so $S_p \subseteq S$ as desired. $\square$

5 Problem 5

Since G is a p-group, it has a nontrivial center. Since p is prime and $Z(G)$ is a subgroup, this forces $\#Z(G) \in \{p, p^2\}$, where p^3 is ruled out because this would make G abelian.

Supposing that $\#Z(G) = p^2$,we would have $[G : Z(G)] = p$, and since $Z(G) \trianglelefteq G$, we can take the quotient and $\#\left(G/Z(G)\right) = p$. But this means $G/Z(G)$ is cyclic, which implies that G is abelian, a contradiction.

So we must have $\#Z(G) = p$, and $\#\left(G/Z(G)\right) = p^2$.

But any group of p^2 is abelian, and we can characterize $G' \coloneqq [G, G]$ in the following way:

$G' \leq G$ is the unique subgroup of G such that if $N \trianglelefteq G$ and G/N is abelian, then $N \leq G'$.

We can thus conclude that $G' \leq Z(G)$. It can not be the case that $G' = \{e\}$, since this would make G abelian. This forces $G' = Z(G)$ as desired. $\square$

6 Problem 6

Writing $f(x) = x^3 - 3x - 3 = \sum a_i x_i \in \mathbb{Q}[x]$, we can conclude that f is irreducible over $\mathbb{Q}$ by Eisenstein with the prime $p = 3$, since $p \,\Big|\, a_0 = -3, a_1 = 3, a_2 = 0$, but $p^2 \nmid a_3 = 1$.

We can check that $f(0) < 0$ and $f(10) > 0$, so f has at least one real root. By the 1st derivative test, we can find that f is increasing on $(-\infty, -1)$ and less than zero, decreasing on $(-1, 1)$ and less than zero, and increasing on $(1, \infty)$, where it it attains its root. This root has multiplicity one, since $\gcd(f, f') = 1$, which means that f has *exactly* one real root r_0, and thus a complex conjugate pair of roots $r_1, \overline{r}_1$ as well.

This means that complex conjugation is a nontrivial element τ of the Galois group $G \leq S_3$, and thus G contains a 2-cycle.

The Galois group must be a transitive subgroup of S_3, which restricts the possibilities to S_3, A_3.

Since A_3 only contains 3-cycles, this possibility is ruled out. Thus the Galois group must be S_3. $\square$

7 Problem 7

Definition: A field F is *perfect* if every irreducible polynomial $f(x) \in F[x]$ is separable in $\overline{F}[x]$.

Note that since F is a finite field, p must be a prime.

7.1 $\implies$:

Suppose all irreducible polynomials in $F[x]$ are separable. Then let $a \in K$ be arbitrary, we will show that there exists some $\beta \in K$ such that $\beta^p = a$.

Given such an a, define the polynomial

$$f(x) = x^p - a \in F[x].$$

Note that f is *not* separable, since $f'(x) = px^{p-1} = 0$ since $\operatorname{char}(F) = p$, which means (by assumption) that f must be *reducible*.

Thus we can write $f(x) = g(x)h(x)$ where $g \in F[x]$ is some irreducible factor that divides f.

Noting that if $\beta \in \overline{F}$ is a any root of f, then

$$f(\beta) = 0 \implies \beta^p = a \implies f(x) = x^p - a = x^p - \beta^p = (x - \beta)^p,$$

and so β is necessarily a multiple root.

Moreover, since $g \,\Big|\, f$, we must have $g(x) = (x - \beta)^\ell$ for some $1 \leq \ell \leq p$.

But then we can expand g using the binomial formula:

$$g(x) = (x - \beta)^\ell = \sum_{k=1}^{\ell} \binom{\ell}{k} x^{\ell-k}(-\beta)^k = x^\ell + \cdots + (-\beta)^\ell \in F[x].$$

But since every coefficient must be in F, we must have $\beta^\ell \in F$. We know that $\beta^p = a \in F$ as well, but since p is prime, $\gcd(p, \ell) = 1$.

We can thus find $s, t \in \mathbb{Z}$ such that $ps + t\ell = 1$. But then

$$\beta = \beta^1 = \beta^{ps+t\ell} = \beta^{st}\beta^{t\ell} = (\beta^\ell)^s(\beta^p)^t,$$

where since $\beta^\ell, \beta^p \in F$, the entire RHS is in F, and thus the LHS $\beta \in F$ as well.

But then $\alpha = \beta^p$ where $\beta \in F$, which is exactly what we wanted to show.

7.2 $\Longleftarrow$:

Suppose every element in F admits a pth root in F, and suppose $f \in F[x]$ is an irreducible polynomial which is *not* separable, so it has a repeated root in $\overline{F}$.

Supposing that $\gcd(f, f') = g(x)$ for any polynomial $g(x)$, this would imply that $g \mathrel{\Big|} f$. But f was assumed irreducible, so the only possibility is that in fact $g = f$.

But if $\gcd(f, f') = f$, since $\deg f' < f$, we can not have $f \mathrel{\Big|} f'$ unless f' is identically zero.

If we thus write

$$\begin{aligned} f(x) &= \sum_{k=0}^{n} c_k x^k, \\ f'(x) &= \sum_{k=1}^{n} k c_k x^{k-1} \\ &\equiv 0, \end{aligned}$$

then for each k we must have $c_k = 0$ or $k = 0$ in F, i.e. $c_k = 0$ or $p \mathrel{\Big|} k$.

Thus the only possible nonzero terms in f must come from coefficients of x^{kp} for each k such that $1 \leq kp \leq n$, i.e.

$$f(x) = c_0 + c_p x^p + c_{2p} x^{2p} + \cdots$$

But this says we can write $f(x) := g(x^p)$, where

$$g(x) = c_0 + c_p x + c_{2p} x^2 + \cdots$$

and furthermore, we can now use the assumption that F is perfect to write $c_i = b_i^p$ for each i, yielding

$$g(x) = b_0^p + b_p^p x^2 + b_{2p}^p x^2 + \cdots$$

.

and thus

$$\begin{aligned} f(x) &= g(x^p) \\ &= b_0^p + b_p^p x^p + b_{2p}^p x^{2p} + \cdots \\ &= (b_0 + b_p x + b_{2p} x^2)^p \\ &\coloneqq (j(x))^p \,, \end{aligned}$$

from which it follows that $j \mid f$ in $F[x]$. But since f was irreducible, this is a contradiction, and so f could not have had a repeated root. Thus every irreducible polynomial is separable, which is what we wanted to show. $\square$

8 Problem 8

Let $f(x) \in F[x]$ be irreducible, then since $p(x) \coloneqq \gcd(f, f')$ must divide f and f is irreducible, the only possibilities are $p(x) = 1$ or $p(x) = f(x)$.

If $p(x) = 1$, then f is separable, so every root is distinct and f itself is of the form $f(x^{p^e})$ where each $e = 0$.

Otherwise, $p(x) = f(x)$, which forces $f'(x) = 0$ in $K[x]$. If we write

$$\begin{aligned} f(x) &= \sum_{k=0}^{n} a_k a^k \\ f'(x) &= \sum_{k=1}^{n} k a_k a^{k-1} \end{aligned}$$
$$,$$

then $f'(x) \equiv 0$ forces either $a_k = 0$, or $k = 0$ in F (so $p \mid k$).

We can thus rewrite f by leaving out all terms where $a_k = 0$ to obtain

$$f(x) = a_p x^p + a_{2p} x^{2p} + \cdots$$

and we thus define

$$g(x) \coloneqq a_p x + a_{2p} x^2 + \cdots$$

and we recover $f(x) = g(x^p)$. Moreover, g is irreducible; otherwise if $h(x) \mid g(x)$ then $h(x^p) \mid g(x^p) = f$, where f was assumed irreducible. If g is separable we are done; otherwise g fulfills the same hypotheses of that applied to f, so we can inductively continue this process to write $g(x) = g_1(x^p)$, and thus $f(x) = g(x^p) = g_1(x^{p^2})$, and so on.

To see that every root of f has multiplicity p^e, note that if $f(\alpha) = 0$ then $g(\alpha^{p^e}) = 0$. But g is separable, so $(x - \alpha^{p^e}) \mid g(x)$ in $K[x]$ and thus $(x^{p^e} - \alpha^{p^e}) \mid g(x^{p^e}) = f$ in $\overline{K}[x]$ where $\overline{K}$ is an algebraic closure of K. But then $x^{p^e} - \alpha^{p^e} = (x-\alpha)^{p^e} \mathrel{\Big|} f(x)$, which precisely says that α is a root of multiplicity p^e.

9 Problem 9

Let $x = [\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}]$.

Noting that

$$\zeta(\zeta + \zeta^{-1}) = \zeta^2 + 1,$$

if we let

$$f(x) = x^2 - (\zeta + \zeta^{-1})x + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[x],$$

then $f(\zeta) = 0$.

Since $\mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{R}$, $\mathbb{Q}(\zeta)$ is a proper extension over this field, so if $d \coloneqq [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$ then $d > 1$. The fact that ζ is a root of f shows that $d \leq 2$, so $d = 2$. We also know that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.

We thus have

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})][\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] \quad \Longrightarrow \quad \phi(n) = 2x,$$

and so $x = \frac{\phi(n)}{2}$ as desired. $\square$

10 Problem 10

Suppose K/F is a finite, normal, Galois extension.

10.1 Part 1

We have $F \leq E \leq K$. Suppose that

- K/F is cyclic, so $\mathrm{Gal}(K/F)$ is a cyclic group,
- E/F is normal

We then want to show that

1. E/F is cyclic, i.e. $\mathrm{Gal}(E/F)$ is cyclic, and
2. K/E is cyclic, i.e. $\mathrm{Gal}(K/E)$ is cyclic.

By the fundamental theorem of Galois theory, E/F is normal if and only if

a. $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$, and
b. $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Since $\mathrm{Gal}(K/F)$ is a cyclic group and every subgroup of a cyclic group is itself cyclic, (a) lets us conclude that (1) holds.

Similarly, since $\mathrm{Gal}(K/F)$ is a cyclic group and every *quotient* of a cyclic group is cyclic, (b) lets us conclude (2).

10.2 Part 2

By the Galois correspondence, all intermediate fields will correspond to subgroups of $\mathrm{Gal}(K/F)$. Since this group is cyclic, we are reduced to analyzing the subgroup lattice of a generic cyclic group.

But if $G = \langle x \mid x^n = e \rangle$ where $\#G = n$, then there is one and *only* one subgroup of index d and order $\frac{n}{d}$ for every d dividing n, given by $H_d \coloneqq \langle x^d \rangle$.

So we have $[G : H_d] = d$, so H_d corresponds to a field E_d/F of degree d where $F \leq E_d \leq K$. This can be done for every d dividing n, and since K/F is a Galois extension, $n = |\mathrm{Gal}(K/F)| = [K : F]$, and this can be done for every divisor of $[K : F]$ as desired. $\square$