CU Boulder: *Algebra* Prelim
January 2008

Juan Moreno
April 2019

These are my solutions to the questions on the CU Boulder *Algebra* preliminary exam from *January 2008* found here. I worked on these solutions over the summer of 2019 in preparation for the preliminary exam in the Fall 2019. Please send any questions, comments, or corrections to juan.moreno-1@boulder.edu.

Problem 1. *Let G be a nonabelian finite simple group, and let p be a prime divisor of its order $|G|$. Show that if the number of Sylow p-subgroups of G is n, then $|G|$ divides $n!$.*

Proof. If p is a prime divisor of $|G|$ then $\mathrm{Syl}_p(G) \neq \emptyset$ and G acts on this set of Sylow p-subgroups by conjugation. This gives rise to a homomorphism $G \to S_n$, where $n = |\mathrm{Syl}_p(G)|$. Since G is simple and the kernel of a homomorphism is a normal subgroup, either this homomorphism is injective, in which case G can be viewed as a subgroup of S_n and the result follows from Lagrange's Theorem, otherwise the kernel of this homomorphism is all of G. We show that the latter case cannot be.

In this latter case, we have for all $g \in G$, $gPg^{-1} = P, \forall P \in \mathrm{Syl}_p(G)$, implying every Sylow p-subgroup is normal in G. Since we have already established the set of such subgroups is nonempty and 1 is not a prime, we must have that $|G| = p^\alpha$ for some positive integer α. The class equation for G then reads

$$|G| = p^\alpha = |Z(G)| + \sum_{\mathcal{O} \in \mathcal{C}} |\mathcal{O}|,$$

where $Z(G)$ is the center of G and $\mathcal{C}$ is the set of conjugacy classes of order > 1. Since $p | p^\alpha$, we must have that p divides the right side of the class equation. By the Orbit-Stabilizer Theorem, the order of the orbits $\mathcal{O}$ must divide $|G| = p^\alpha$ and since these orders are greater that 1, we have that p divides the sum on the right side of the class equation. It follows that p must also divide $|Z(G)|$ so that the center of G is a nontrivial subgroup. Since the center of a group is always normal, if we are to reconcile this with the fact that G is simple, we must have that $Z(G) = G$, implying G must be abelian. $\square$

Problem 2. *Let G be a finite solvable group. Show that*
(a) G has a nontrivial abelian normal subgroup of prime power order.

Proof. Let H be a minimal nontrivial normal subgroup of G. Then H must also be solvable, so its derived series must eventually trivialize. Note that $H' = [H, H] \leq H$ is a characteristic subgroup of H, and since $H \trianglelefteq G$, we have that $H' \trianglelefteq G$. Thus $H' = 1$, implying H is abelian. Now consider, for any prime p dividing $|H|$, $H_p = \langle x \in H | x^p = 1\rangle$. This is a characteristic subgroup of H since any automorphism preserves order. Further, by Cauchy's theorem, this subgroup is nontrivial. Thus, by minimality of H, $H_p = H$. It follows that H is a nontrivial abelian normal subgroup of G of prime power order. $\square$

(b) every maximal proper subgroup of G has prime power index in G

Proof. Note that the result holds for the trivial group $G = 1$ and the only group of order 2, Z_2. Proceeding by induction on the order of G, let $H \leq G$ be maximal. Suppose first that H contains a minimal nontrivial abelian normal subgroup of prime power order as in part (a), N. Then $H/N \leq G/N$ is maximal (lattice isomorphism) and G/N is a solvable group of order strictly less than $|G|$ so that the induction hypthesis implies the index of H/N in G/N is a prime power. It follows that the index of H in G is a prime power. Now suppose H does not contain any such minimal subgroup. Then for any such minimal subgroup, N,

NH is a subgroup of G containing H so that by maximality of H and the fact that H does not contain N, $NH = G$. THus

$$|NH| = \frac{|N||H|}{|N \bigcap H|} = |G|$$

$$\implies \frac{|G|}{|H|} = \frac{|N|}{|N \bigcap H|},$$

and $\frac{|N|}{|N \bigcap H|}$ is a prime power. □

Problem 3. *Let R be a UFD such that any ideal generated by two elements of R is principal. Prove that R is a PID.*

Proof. Let I be any ideal of R and let $a \in I$ be an element with a minimal number of irreducible factors. Such an element always exists since in a UFD every element can be expressed as a finite product of irreducibles unique up to multiplication by a unit and the number of such irreducible factors is unique. If $b \in I \setminus (a)$, then $(a, b) = (d) \subset I$, where d is a greatest common divisor of a and b. However this contradicts the minimality of the number of irreducible factors of a so that in fact any $b \in I$ is contained in (a). Thus $I = (a)$. □

Problem 4. *Let A be an $n \times n$ matrix over $\mathbb{C}$ such that $\mathrm{Tr}(A^k) = 0$ for all $k > 0$. Show that $A^n = 0$.*

Solution. Let $c_A(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ be the characteristic polynomial of A. Then $c_A(A) = 0$ implying

$$\mathrm{Tr}(c_A(A)) = \mathrm{Tr}(A^n + a_{n-1}A^{n-1} + ... + a_1 A + a_0)$$

$$= \mathrm{Tr}(A^n) + a_{n-1}\mathrm{Tr}(A^{n-1}) + ... + a_1 \mathrm{Tr}(A) + a_0 \mathrm{Tr}(I)$$

$$= a_0 \cdot n = 0$$

$$\implies a_0 = 0.$$

Thus $c_A(x) = xc_1(x) = x(x^{n-1} + a_{n-1}x^{n-2} + ... + a_2 x + a_1)$, implying either $A = 0$ or A satisfies $c_1(A) = 0$. Proceeding as before, we get that $a_0 = a_1 = ... = a_{n-1} = 0$ so that $c_A(x) = x^n$, implying $A^n = 0$.

Problem 5. *Find the splitting field of $x^4 + x^3 + 1$ over the 32-element field.*

Solution. First note that since this polynomial lies in $\mathbb{F}_2[x] \subset \mathbb{F}_{32}[x]$, it suffices to find the splitting field of this polynomial over $\mathbb{F}_2$, say K, and then compute the composite $K\mathbb{F}_{32}$. Now our polynomial $f(x) = x^4 + x^3 + 1$ is irreducible over $\mathbb{F}_2$ since it has no roots in this field and the only possible irreducible factor is $x^2 + x + 1$ which does not square to f. Thus $\mathbb{F}_2[x]/(f) \cong \mathbb{F}_{2^4}$ is the splitting field of f over $\mathbb{F}_2$. Then $\mathbb{F}_{2^4}\mathbb{F}_{2^5} = \mathbb{F}_{2^{20}}$ is the splitting field of f over $\mathbb{F}_{32}$.

Problem 6. *True of false? Justify your answer.*
(i) Every field extension of degree 2 is Galois.
<u>Claim:</u> False

Proof. If char$F \neq 2$ then any degree 2 extension of F is of the form $F(\sqrt{D})$ for some $D \in F$. This is the splitting field of the irreducible polynomial $x^2 - D \in F[x]$ hence is a Galois extension. However, if char$F = 2$ we have the following counterexample. Consider $x^2 - t \in \mathbb{F}_2(t)[x]$. Since $(x + \sqrt{t})^2 = x^2 - t$, this polynomial is not separable and so it's degree 2 splitting field is not Galois. □

(ii) Every algebraically closed field is infinite.
<u>Claim:</u> True

Proof. (iii) If K is a finite field then it is a finite extension of its prime subfield F. The prime subfield of K must be $\mathbb{F}_p$ for some prime p otherwise, $\text{char}F = 0$ and the prime subfield will be infinite, contradicting that K is finite. Thus, $K \cong \mathbb{F}_{p^n}$ for some n. This field is not algebraically closed since, for example $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{2n}}$ is a degree 2 Galois extension so that $\mathbb{F}_{p^{2n}}$ is the splitting field of some irreducible polynomial in $\mathbb{F}_{p^n}[x]$.

□

(iii) If $\alpha = \sqrt[5]{2+i} + \sqrt[5]{2-i}$, then $Gal(\mathbb{Q}[\alpha]/\mathbb{Q}) \cong S_5$.
<u>Claim:</u> False

Proof. Consider the following diagram of field extensions. Since $Q(\sqrt[5]{2+i}, \sqrt[5]{2-i})$ is the composite of the left and right fields in the diagram which are each of degree 5 over $\mathbb{Q}(i)$, we have that $[\mathbb{Q}(\sqrt[5]{2+i}, \sqrt[5]{2-i}) : \mathbb{Q}(i)]$ is at most 25. It follows that $[\mathbb{Q}(\sqrt[5]{2+i}, \sqrt[5]{2-i}) : \mathbb{Q}]$ is at most 50. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is at most 50 so that the order of the Galois group of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is strictly less than $|S_5|$.

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[5]{2+5}, \sqrt[5]{2-i}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[5]{2+i}) \arrow[dr, dash, "5"'] & \mathbb{Q}(\alpha) \arrow[d, dash] & \mathbb{Q}(\sqrt[5]{2-i}) \arrow[dl, dash, "5"] \\
& \mathbb{Q}(i) \arrow[d, dash, "2"'] & \\
& \mathbb{Q} &
\end{tikzcd}$$

□