CU Boulder: *Algebra* Prelim
August 2017

Juan Moreno
April 2019

These are my solutions to the questions on the CU Boulder *Algebra* preliminary exam from *August 2017* 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. *Assume that G is an infinite nonabelian group whose proper subgroups are finite. Show that every proper normal subgroup of G is contained in the center of G. Explain why $G/Z(G)$ is an infinite simple group whose proper subgroups are finite.*

Proof. Let $N \trianglelefteq G$ be a proper normal subgroup of G. Then G acts on N by conjugation, giving rise to a homomorphism $\varphi : G \to S_n$, where $n = |N|$. The kernel of this map must then also be a normal subgroup. This leaves us two options, either $\ker\varphi$ is finite or $\ker\varphi = G$. In the first case, however, we would have the infinite quotient $G/\ker\varphi$ being isomorphic to a subgroup of the finite group S_n, a contradiction. Hence $\ker\varphi = G$ so that action of G on N by conjugation is trivial, implying N lies in the center of G. The last statement follows mostly from the lattice isomorphism theorem since any normal subgroup of $G/Z(G)$ corresponds to a normal subgroup containing $Z(G)$, but as we have shown, all proper normal subgroups are contained in $Z(G)$. Thus the only normal subgroups of $G/Z(G)$ are the trivial subgroup and the entire group, hence $G/Z(G)$ is simple. Similarly, any proper subgroup of $G/Z(G)$ is isomorphic to the quotient of a proper subgroup of G containing $Z(G)$ by $Z(G)$, which must be finite by assumption. It is infinite since $Z(G)$ is normal in G and since G is nonabelian, it is proper and thus finite, implying $G/Z(G)$ is infinite. □

Problem 2. *Suppose the alternating group A_4 acts transitively on a set X. What are the possible sizes of X.*

Solution. For a group G, define a transitive G-set to be a set X with a transitive action by G. Define an isomorphism of G-sets X and Y to be a bijective map of sets $f : X \to Y$ which preserves the G-action, i.e. $f(g \cdot x) = g \cdot f(x)$ for all $g \in G$. For $x \in X$, let G_x be the stabilizer of x under the G-action. We prove that any transitive G-set X is isomorphic to the set of cosets G/G_x for any $x \in X$. Simply pick any $x \in X$, and define the map $\varphi : G \to X$ by $\varphi(g) = g \cdot x$. Evidently, this map factors through the map $\pi : G \to G/G_x$ since $G_x \cdot x = x$. So we have the following commutative diagram

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ G/G_x \arrow[r, dashed, "\overline{\varphi}"'] & X \end{tikzcd}$$

We claim that the induced map $\overline{\varphi}$ is a G-set isomorphism. To see this, simply note that $|G/G_x| = |X|$ and compute for any $g \in G$, $\overline{\varphi}(g \cdot hG_x) = \overline{\varphi}((gh)G_x) = (gh)G_x \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot (hG_x \cdot x) = g\overline{\varphi}(hG_x)$. This proves the result.

Now consider the case $G = A_4$. By the above, any set X on which A_4 acts transitively, is isomorphic as an A_4-set to some set of cosets of A_4. Since A_4 has subgroups of order $1, 2, 3, 4$, and 12, the possible sizes of sets of cosets and hence sets on which G acts transitively are $12, 6, 4, 3$, and 1.

Problem 3. *Let A be an integral domain containing the field $\mathbb{F}$ as a subring. This makes A a vector space over $\mathbb{F}$. Show that if A is finite dimensional over $\mathbb{F}$ then A is a field. Show that A need not be a field if it is not finite dimensional over $\mathbb{F}$.*

Proof. Assume A is finite dimensional over $\mathbb{F}$. Take any nonzero $r \in A$. Consider the set of powers of r, $\{r^k\}_{k=0}^{\infty}$. If this set is finite, then we must have $r^k = r^{k'}$ for some k, k'. Using the cancellation property of multiplication in integral domains we have that $r^l = 1$ for some l so that r is a unit in A with inverse r^{l-1}. If, on the other hand the set is infinite, by finite dimensionality of A over $\mathbb{F}$, we have that there exists some $n \in \mathbb{N}$ and $c_0, c_1, \ldots, c_n \in \mathbb{F}$ not all zero such that $\sum_{i=0}^{n} c_i r^i = 0$. Notice that if k is the minimal number such that $c_k \neq= 0$ then we may write $\sum_{i=k}^{n} c_i r^i = r^k \sum_{i=0} c_i r^{i-k} = 0$, and since A is an integral domain and $r \neq 0$, we have $\sum_{i=k}^{n} c_i r^{i-k}$. Therefore, we may assume $c_0 \neq 0$. Let $b_i = \frac{c_i}{c_0}$ so that, in particular, $b_0 = 1$. Then

$$\sum_{i=0}^{n} c_i r^i = 0 \implies \sum_{i=0}^{n} b_i r^i = 0 \implies 1 = \sum_{i=1}^{n} (-b_i) r^i.$$

Since the left side of the final expression above must be nonzero ($1 \neq 0$ in a nontrivial ring) and the indexing begins at $i = 1$, we may factor out at least one factor of r and write

$$r \sum_{i=0}^{n} (-b_i) r^i = 1,$$

implying r has an inverse in A. □

Problem 4. *You are given that G is a group for which there exists a surjective homomorphism $\alpha : \mathbb{Z}^n \to G$ and an injective homomorphism $\beta : \mathbb{Z}^n \to G$. What are the possible isomorphism classes of G?*

Solution. Since we have a surjective homomorphism from the abelian group $\mathbb{Z}^n$ onto G, we must have that G is abelian. Further, since $\mathbb{Z}^n$ has n generators, and α is determined by the images of these generators, the fact that α is surjective implies that G has at most n generators. By the classification of finitely generated abelian groups, we have that

$$G \cong \mathbb{Z}^k \times \mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_l),$$

for some $k, l \in \mathbb{N}$ such that $k + l \leq n$, and $a_i \in \mathbb{Z}$. Here k is the free rank of G. Now the existence of the injective map β from $\mathbb{Z}^n$ into G, implies that G has a subgroup isomorphic to $\mathbb{Z}^n$, implying that the free rank of G is at least n. It follows that $k = n$ and $l = 0$ so that $G \cong \mathbb{Z}^n$.

Problem 5. *Consider the following three rings*

$$\mathbb{F}_3[x]/(x^2+1), \quad \mathbb{F}_3[x](x^2+2), \quad \text{and } \mathbb{F}_3[x]/(x^2+2x+2),$$

where $\mathbb{F}_3$ is the field with 3 elements.
(a) Show that each of these rings is a product of fields and say which fields are involved.

Solution. Let $p_1(x) = x^2+1, p_2(x) = x^2+2, p_3(x) = x^2+2x+2$ and $K_i = \mathbb{F}_3[x]/(p_i(x))$. Since these polynomials are all of degree 2 it is trivial to check by finding roots that $p_1(x)$ and $p_3(x)$ are irreducible and $p_2(x) = (x+1)(x+2)$. Since $\mathbb{F}_3$ is a field, $\mathbb{F}_3[x]$ is a PID so that both $p_1(x)$ and $p_3(x)$ must be prime hence generate maximal ideals. It follows that K_1 and K_3 are fields. Further, as sets each of these are of the form $\{a + b\bar{x} | a, b \in \mathbb{F}_3\}$, where $\bar{x}$ denotes the image of x in K_i. These are both finite fields of the same order, namely 9. Thus, $K_1 \cong K_3 \cong \mathbb{F}_9$. As for $p_2(x)$, since $2(x+1) + (x+2) = 1$, as ideals we have $(x+1) + (x+2) = \mathbb{F}_3[x]$. Moreover, since $x+1$ and $x+2$ are irreducible in $\mathbb{F}_3[x]$, $(x+1) \bigcap (x+2)$ is notrivial only if $(x+1) = (x+2)$ since this intersection would be generated by a greatest common divisor of $x+1$ and $x+2$. This can only be the case if $x+1$ and $x+2$ differ by a unit in $\mathbb{F}_3[x]$, which is not the case since they are not multiples of one another as can easily be checked. Thus, by the Chinese Remainder Theorem

$$K_2[x] = \mathbb{F}_3[x]/(x^2+2) \cong \mathbb{F}_3[x]/(x+1) \times \mathbb{F}_3[x]/(x+2) \cong \mathbb{F}_3 \times \mathbb{F}_3.$$

(b) For each pair of isomorphic rings in the list, provide an explicit isomorphism.

To exhibit an explicit isomorphism between the fields K_1 and K_3, let α denote the image of x under the projection $\mathbb{F}_3[x] \to K_1$ and β the image of x under the projection $\mathbb{F}_3[x] \to K_2$. Then $\alpha^2 = 2$ and $\beta^2 = \beta + 1 \implies (\beta+1)^2 = \beta^2 + 2\beta + 1 = 2$. We can then define a map $\varphi : K_1 \to K_3$ by requiring it restrict to the identity on $\mathbb{F}_3$ and map $\alpha \mapsto \beta+1$. To see that this is a field homomorphism, take any $a+b\alpha, c+d\alpha \in K_1$ and compute

$$\varphi((a+b\alpha)(c+d\alpha)) = \varphi((ac+2bd)+(ad+bc)\alpha) = (ac+2bd)+(ad+bc)(\beta+1),$$

and

$$\varphi(a+b\alpha)\varphi(c+d\alpha) = (a+b(\beta+1))(c+d(\beta+1)) = (ac+bd(\beta+1)^2)+(ad+bc)(\beta+1) = (ac+2bd)+(ad+bc)(\beta+1).$$

The additive property of φ follows simply from its definition, so φ is indeed a field homomorphism. It is also evidently nontrivial and so it must be an isomorphism onto its image. Since these fields have the same cardinality, we have that φ is an explicit isomorphism between the two fields K_1 and K_3.

Problem 6. *Let $p \geq 5$ be a prime number and let L be the splitting field of $x^p - 1$ over $\mathbb{Q}$.*
(a) Find explicit generators for the Galois group $Gal(L/\mathbb{Q})$ and explain why your answer is correct. What is the structure of this group?

Solution. We view $\mathbb{Q}$ as a subfield of $\mathbb{C}$ as usual. Then $\alpha_k = e^{2\pi ki/p}, k = 0,1,...,p-1$ are the roots of $p(x) = x^2 - 1$ in $\mathbb{C}$. Notice that if $\alpha_k \in \mathbb{Q}$ then $2\pi k/p = \pi l$ for some $l \in \mathbb{Z}$, implying $2k/p \in \mathbb{Z}$, however, this cannot be unless $k = 0$ since $k < p$ and p is an odd prime. Thus, the only root of $p(x)$ in $\mathbb{Q}$ is $\alpha_0 = 1$. Moreover, note that $\alpha_k = \alpha_1^k$ for all $k = 0,1,...,p-1$. Hence $L = \mathbb{Q}(\alpha_1) \cong \mathbb{Q}[x]/(q(x))$ where $q(x) = \frac{x^p-1}{x-1}$. We now have that $[L:\mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| = p-1$ and that this Galois group must act transitively on the roots of $q(x)$ since it is irreducible and L is its splitting field. Let $\sigma_k : L \to L$ be the automorphism which fixes $\mathbb{Q}$ and maps $\alpha_1 \mapsto \alpha_k$, for $k = 1,2,...,p-1$. We can quickly investigate how these automorphisms relate

$$\sigma_l \circ \sigma_k(\alpha_1) = \sigma_l(\alpha_k) = \sigma_l(\alpha_1^k) = \sigma_l(\alpha_1)^k = \alpha_l^k = \alpha_1^{lk} = \alpha_{lk} = \sigma_{lk}(\alpha_1).$$

It follows that $\mathrm{Gal}(L/\mathbb{Q}) \cong Z_{p-1}$ and is generated by any σ_k such that k is a generator of $\mathbb{Z}_p^\times$.

(b) Use (a) to find explicit generators for a subfield K of L such that $[L:K] = 2$ and explain why your answer is correct.

Solution. In part (a) we found that the Galois group of K over $\mathbb{Q}$ is cyclic of order $p-1$. By the fundamental theorem of Galois Theory, to find a subfield of L of index 2 is equivalent to finding a subgroup of the Galois group of order 2. Such a subgroup can be found simply by noting that the automorphism of complex conjugation on $\mathbb{C}$ restricts to the identity on $\mathbb{Q}$ and the nontrivial automorphism $\sigma_{p-1} : \alpha_1 \mapsto \alpha_{p-1}$ of L. Since complex conjugation is a transformation of order 2, σ_{p-1} has order 2 in $\mathrm{Gal}(L/\mathbb{Q})$ and so we have found a subgroup of order 2, $\langle \sigma_{p-1} \rangle$. To find its corresponding fixed field, note that the elements

$$\theta_1 = \alpha_1 + \sigma_{p-1}\alpha_1 = 2\mathrm{Re}(\alpha_1),$$

$$\theta_2 = \alpha_2 + \sigma_{p-1}\alpha_2 = 2\mathrm{Re}(\alpha_2),$$

$$\vdots$$

$$\theta_{\frac{p-1}{2}} = \alpha_{\frac{p-1}{2}} + \sigma_{p-1}\alpha_{\frac{p-1}{2}} = 2\mathrm{Re}(\alpha_{\frac{p-1}{2}}),$$

are each distinct and fixed by σ_{p-1}. Moreover, since $\mathrm{Re}(\alpha_k) = \cos(2\pi k/p)$