CU Boulder: Algebra Prelim
August 2018

Juan Moreno
Summer 2019

These are my solutions to the questions on the CU Boulder Algebra preliminary exam from August 2018 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. *Suppose G is a group of order* 385.
(a) Show that G has exactly one Sylow 11*-subgroup and that it is a normal subgroup.*

Proof. First note that $|G| = 385 = 11 \cdot 35 = 5 \cdot 7 \cdot 11$. By Sylow's Theorem, the number of Sylow 11-subgroups of G is $n_{11} \equiv 1 \text{mod } 11$ and $n_{11} \big| 35$. The only integer satisying these two properties is $n_{11} = 1$ so we have exactly one Sylow 11-subgroup of G and since it is the unique subgroup of its order, it must constitute its own conjugacy class and hence be normal. □

(b) Show that G has exactly one Sylow 7*-subgroup and it is contained in the center of G.*

Proof. As before, the number of Sylow 7-subgroups is constrained by Sylow's Theorem to satify $n_7 \equiv 1 \text{mod} 7$ and $n_7 \big| 55$. The only integer satisfying these conditions is $n_7 = 1$ so G has exactly one Sylow 7-subgroup, call it P_7. Since it is the unique subgroup of order 7, it must be normal so its normalizer is $N_G(P_7) = G$. We then have

$$N_G(P_7)/C_G(P_7) = G/C_G(P_7) \leq \text{Aut}(P_7),$$

where $C_G(P_7)$ is the centralizer of P_7 in G. Since P_7 has prime order, it is necessarily isomorphic to Z_7, the cyclic group of order 7 so $\text{Aut}(P_7) \cong Z_6$. Further, since the order of a subgroup must divide the order of the group, we must have $G/C_G(P_7) = 1$, the trivial subgroup. Thus $C_g(P_7) = G$, implying P_7 lies in the center of G. □

Problem 2. *Let K be a field and let K[[x]] be the ring of formal power series in x over K.*
(a) Show that $\sum_{i=0}^{\infty} a_i x^i$ is a unit if and only if $a_0 \neq 0$.

Proof. If $\sum_{i=0}^{\infty} a_i x^i$ is a unit, then there is some $\sum_{i=0}^{\infty} b_i x^i \in K[[x]]$ such that

$$\Big(\sum_{i=0}^{\infty} a_i x^i\Big)\Big(\sum_{i=0}^{\infty} b_i x^i\Big) = 1 \implies a_0 b_0 = 1.$$

Since K is a field, it has no zero divisors so neither a_0 or b_0 can be zero.

Now suppose $a_0 \neq 0$. Then we can define the coefficients of a power series $\sum_{i=0}^{\infty} b_i x^i$ inductively from those of $\sum_{i=0}^{\infty} a_i x^i$ as

$$b_0 = \frac{1}{a_0}, \quad \text{and} \quad b_k = \frac{-1}{a_0} \sum_{i=0}^{k-1} a_{k-i} b_i, \quad \text{for } k > 0.$$

Then the i-th coefficient of $\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right)$ is $a_0 b_0 = a_0 \frac{1}{a_0} = 1$ for $i = 0$ and 0 for $i > 0$, by construction. Thus $\sum_{i=0}^{\infty} a_i x^i$ is a unit in $F[[x]]$. □

(b) Show that every nonzero proper ideal in $K[[x]]$ is generated by x^k for some $k \geq 1$.

Proof. Let I be such a nonzero proper ideal. Then for any polynomial $p(x) \in I$, $p(x)$ has zero constant term otherwise, by (a), it is a unit and $(p(x)) = F[[x]] \subset I \implies I = F[[x]]$. For any power series $p(x) = \sum_{i=0}^{\infty} a_i x^i$ let $d(p)$ be the smallest positive integer for which $a_{d(p)} \neq 0$. Let $p(x) \in F[[x]]$ be such that $d(p)$ is minimal. Then $p(x) = x^k q(x)$, for some polynomial $q(x)$ with a nonzero constant term. It follows that $(x^k) \subset I$. Further, since we chose $p(x)$ with minimal $d(p)$, for any other nonzero power series $f(x) \in I$, we may write $f(x) = x^k g(x)$ for some $g(x) \in F[[x]]$. Thus $I = (x^k)$. □

Problem 3. *Let G denote the Galois group of $x^5 - 10x + 5$ over $\mathbb{Q}$. View G as a subgroup of S_5.*
(a) Consider any irreducible polynomial $g(x)$ over $\mathbb{Q}$ of prime degree p. Show that the Galois group of $g(x)$ has an element of order p.

Proof. Since $g(x)$ is irreducible, the degree p field extension $F[x]/(g(x))$ isomorphic to a field contained in the splitting field of g and containing F. Thus the Galois group must have a subgroup of order p and since p is prime this subgroup must be generated by some element of order p. □

(b) Show that G contains a 5-cycle.

Proof. By part (a), G contains an element of order 5. The only such elements in S_5 are 5-cycles. If this is not immediately clear, recall that any permutation in S_n can be written as the product of disjoint cycles and that the order of any such element is the least common multiple of the lengths of each cycle. Since no integers ≥ 1 have 5 as a least common multiple, the result follows. □

(c) Show that G contains a 2-cycle.

Proof. We use Sturm's Theorem to determine the number of real roots this polynomial. First note that the polynomial is surely positive for $x > 2$ and negative for $x < -2$. So it suffices to look for roots in the interval $(-2, 2)$. Let $f_0(x) = x^5 - 10x + 5$, and $f_1(x) = f_0'(x) = 5x^4 - 10$. The remaining terms of the Sturm sequence are then

$$f_2(x) = 8x - 5, \quad f_3(x) = \frac{37835}{4096}.$$

The Sturm sequence at -2 is then

$$f_0(-2) = -7, \quad f_1(-2) = 70, \quad f_2(-2) = -21, \quad f_3(-2) = \frac{37835}{4096},$$

while the Sturm sequence at 2 is

$$f_0(2) = 17, \quad f_1(2) = 70, \quad f_2(2) = 11, \quad f_3(2) = \frac{37835}{4096}.$$

The sequence changes sign 3 times in the first sequence and 0 times in the second so that $f(x)$ must have exactly 3 real roots. The remaining 2 roots must then be complex conjugates so that the restriction of complex conjugation in $\mathbb{C}$ to the splitting field of this polynomial (viewed as a subfield of $\mathbb{C}$) is then an automorphism of order 2 which fixes $\mathbb{Q}$. This automorphism corresponds to a 2-cycle when the Galois group is viewed as a subgroup of S_5. □

(d) Use the previous results to prove that $G \cong S_5$.

Proof. We know that S_5 is generated by any combination of a 5-cycle and a 2-cycle so because G contains at least one of each, it must be all of S_5. □

Problem 4. *(a) Prove that there are exactly two distinct automorphisms of the ring $\mathbb{F}_5 \times \mathbb{F}_{25}$.*

Proof. Let $\mathbb{F}_5$ and $\mathbb{F}_{25}$ denote the subfields $\mathbb{F}_5 \times \{0\}$ and $\{0\} \times \mathbb{F}_{25}$ of $\mathbb{F}_5 \times \mathbb{F}_{25}$. We use the fact that automorphisms preserve annihilators. Note that $\text{Ann}(\mathbb{F}_5) = \mathbb{F}_{25}$ and $\text{Ann}(\mathbb{F}_{25}) = \mathbb{F}_5$. Now let φ be an automorphism of $\mathbb{F}_5 \times \mathbb{F}_{25}$ and suppose $\varphi(\mathbb{F}_{25})$ is not contained in $\mathbb{F}_{25}$. Let $(r,s) \in \varphi(\mathbb{F}_{25})$ with r and s nonzero. Then for any $(a,b) \in \mathbb{F}_5 \times \mathbb{F}_{25}$ with either $a \neq 0$ or $b \neq 0$, $(a,b) \cdot (r,s) \neq 0$ since each $\mathbb{F}_5$ and $\mathbb{F}_{25}$ are integral domains. Thus $\text{Ann}(\varphi(\mathbb{F}_{25})) = \{(0,0)\}$, a set with cardinality strictly less than $\text{Ann}(\mathbb{F}_{25})$, a contradiction. It follows that $\varphi(\mathbb{F}_{25}) = \mathbb{F}_{25}$, which implies, by order considerations, $\varphi(\mathbb{F}_5) = \mathbb{F}_5$. Thus $\varphi = \sigma \times \tau$, where $\sigma \in \text{Aut}(\mathbb{F}_5) = \{id_{\mathbb{F}_5}\}$, and $\tau \in \text{Aut}(\mathbb{F}_{25}) = \{id_{\mathbb{F}_{25}}, \tau_5\}$, where τ_5 is the Frobenius automorphism $x \overset{\tau_5}{\longmapsto} x^5$ of order 2. The only automorphisms of this ring are thus $\varphi_0 = id_{\mathbb{F}_5} \times id_{\mathbb{F}_{25}}$ and $\varphi_1 = id_{\mathbb{F}_5} \times \tau_5$. □

(b) Let $f(x) = x^3 + 3$. Prove that there are exactly two distinct isomorphisms

$$\rho : \mathbb{F}_5[x]/(f(x)) \to \mathbb{F}_5 \times \mathbb{F}_{25}.$$

Proof. First note that $3^3 + 3 \equiv 0(\text{mod}5)$ so that f factors in $\mathbb{F}_5$ as $x^3 + 3 = (x-3)(x^2 + 3x + 4)$. It can be easily checked that $x^2 + 3x + 4$ is irreducible over $\mathbb{F}_5$ by checking that it has no zeros. Using the Chinese Remainder Theorem, we then have an isomorphism

$$\phi : \mathbb{F}_5[x]/(f(x)) \to \Big(\mathbb{F}_5[x]/(x-3)\Big) \times \Big(\mathbb{F}_5[x]/(x^2+3x+4)\Big)$$

mapping $p(x) \mapsto (p(x)(\text{mod}(x-3)), p(x)(\text{mod}(x^2+3x+4)))$. We identify this ring canonically with $\mathbb{F}_5 \times \mathbb{F}_{25}$ since clearly $\mathbb{F}_5 = \mathbb{F}_5/(x-a)$ for any $a \in \mathbb{F}_5$, and $\mathbb{F}_{25}$ is the unique extension of $\mathbb{F}_5$ of degree 2. The two distinct isomorphisms $\mathbb{F}_5[x]/(f(x)) \to \mathbb{F}_5 \times \mathbb{F}_{25}$ are $\phi \circ \varphi_0 = \phi$ and $\phi \circ \varphi_1$. □

Problem 5. *Let $G = Z_{p^2}$, the cyclic group of order p^2, where p is an odd prime. Classify all semi-direct products $G \rtimes G$ up to isomorphism.*

Proof. Such groups are completely determined by an automorphism $\psi : G \to \text{Aut}(G)$. The automorphism group of Z_{p^2} is cyclic of order $\varphi(p^2) = p(p-1)$, where φ is the Euler Phi function. Note that since the image $\psi(G)$ must be a subgroup of $\text{Aut}(G)$ of order dividing p^2, the only possibilities are $|\psi(G)| = 1$ or p. Now since $(p, p-1) = 1$, we have the existence of a Sylow p-subgroup $P_p \in \text{Syl}_p(G)$ of order p. By Sylow's Theorem, the number of such subgroups must satisfy $n_p \equiv 1(\text{mod}p)$ and $n_p|(p-1)$. Since $p-1 < p$, and p is prime, the only option is $n_p = 1$. Thus P_p is the unique Sylow p-subgroup of G and hence is the only possible non-trivial image of ψ.

Let $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ be copies of Z_{p^2} with generators a and b, respectively. Let $\sigma \in \text{Aut}(G_1)$ be a generator of the unique Sylow p-subgroup of $\text{Aut}(G_1)$. We then have a homomorphism $\psi : G_2 \to \text{Aut}(G_1)$ mapping $b \mapsto \sigma$ and can form the semi-direct product

$$G_1 \rtimes_\psi G_2 = \langle a, b \big| a^{p^2} = b^{p^2} = 1, ab = b\sigma(a) \rangle.$$

Note that since $\langle \sigma \rangle \leq \text{Aut}(G_1)$ is a cyclic group of prime order, any nonidentity element generates the entire group. It follows that $\psi_i : G_2 \to G_1$ mapping $b \mapsto \sigma^i$ is a homomorphism for any $i \in \{1, 2, ..., p-1\}$. In fact, by our observations in the preceding paragraph, these are the only non-trivial homomorphisms in $\text{Hom}(G_2, G_1)$. We claim all that these homomorphisms ψ_i give rise to the same semi-direct product. To see this, note that $\sigma(a) = a^k$ for some $k \in \{2, ..., p-1\}$. Then $\sigma^i(a) = a^{k^i}$. Now let $y = b^i$ in $G_1 \rtimes_\psi G_2$ above. Since $i < p$ and p is prime, $(i, p^2) = 1$, then

$$y^{p^2} = 1, \quad \text{and} \quad ay = ab^i = b\sigma(a)b^{i-1} = ba^k b^{i-1} = b^2 a^{k^2} b^{i-2} = \ldots = b^i a^{k^i} = y\sigma^i(a).$$

Thus

$$G_1 \rtimes_\psi G_2 = \langle a, y | a^{p^2} = y^{p^2} = 1, ay = y\sigma^i(a) \rangle \cong G_1 \rtimes_{\psi_i} G_2, \quad \text{for all } i.$$

The only isomorphism classes of semi-direct products of Z_{p^2} with itself are $Z_{p^2} \times Z_{p^2}$, and $Z_{p^2} \rtimes_\psi Z_{p^2}$. □

Problem 6. *Consider the conjugacy classes of $GL_2(\mathbb{F}_5)$. How many such conjugacy classes contain matrices whose eigenvalues lie in $\mathbb{F}_5$.*

Solution. The eigenvalues of a matrix are the roots of its characteristic polynomial. The characteristic polynomial of any $A \in GL_2(\mathbb{F}_5)$ is a degree 2 polynomial in $\mathbb{F}_5[x]$. The reducible polynomials of degree 2 in $\mathbb{F}_5[x]$ are (excluding those with zero as a root, since a matrix with zero eigenvalue is not invertible)

#	*Roots*	*Polynomial*
1	$1, 1$	$x^2 + 3x + 1$
2	$1, 2$	$(x+4)(x+3) = x^2 + 2x + 2$
3	$1, 3$	$(x+4)(x+2) = x^2 + x + 3$
4	$1, 4$	$(x+4)(x+1) = x^2 + 4$
5	$2, 2$	$(x+3)(x+3) = x^2 + x + 4$
6	$2, 3$	$(x+3)(x+2) = x^2 + 1$
7	$2, 4$	$(x+3)(x+1) = x^2 + 4x + 3$
8	$3, 3$	$(x+2)^2 = x^2 + 4x + 4$
9	$3, 4$	$(x+2)(x+1) = x^2 + 3x + 2$
10	$4, 4$	$(x+1)^2 = x^2 + 2x + 1$

Recall that the conjugacy class of a matrix is determined by a list of invariant factors. Since the product of the invariant factors is the characteristic polynomial, the list of invariant factors for a matrix in $GL_2(\mathbb{F}_5)$ consists of at most 2 polynomials. Further one of these polynomials must divide the other. It follows that the characteristic polynomials corresponding to #2, 3, 4, 6, 7, and 9 have only one possible list of invariant factors, while the characteristic polynomials corresponding to # 1, 5, 8,and 10 have two possible lists. That gives us 14 conjugacy classes of matrices whose eigenvalues lie in $\mathbb{F}_5$.