CU Boulder: *Algebra* Prelim
January 2018

Juan Moreno
April 2019

These are my solutions to the questions on the CU Boulder *Algebra* preliminary exam from *January 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. *Let G be the symmetric group S_5 and P a Sylow 5-subgroup of G.*
(i) Show that the normalizer $N_G(P)$ has order 20.

Proof. By Sylow's Theorem, $|\mathrm{Syl}_5(G)| \equiv 1(\mathrm{mod} 5)$ and $|\mathrm{Syl}_5(G)|$ divides $\frac{120}{5} = 24$. Thus $|\mathrm{Syl}_5(G) = 1$ or 6. However, there are 24 5-cycles in S_5 so in fact $|\mathrm{Syl}_5(G)| = 6$. Sylow's Theorem also states that G acts on the set $\mathrm{Syl}_5(G)$ by conjugation. Since 5-cycles constitute an equivalence class in G, this action is transitive. Observing that the stabilizer of P under this action is $N_G(P)$, orbit-stabilizer theorem then implies that

$$|G| = |N_G(P)| \cdot |\mathrm{Syl}_5(G)| \implies |N_G(P)| = \frac{120}{6} = 20.$$

□

(ii) In the special case when P contains the 5-cycle (12345), find a set of generators for $N_G(P)$.

Solution. Clearly $P = \langle (12345) \rangle \leq N_G(P)$. Now $(12345)^4 = (12345)^{-1} = (15432) = ((25)(34))(12345)((25)(34))^{-1}$. It follows that $\sigma = (12345), \tau = (25)(34) \in N_G(P)$ and these elements satisfy the relations

$$\sigma^5 = \tau^2 = 1, \quad \sigma\tau = \tau\sigma^{-1},$$

so that these elements generate a subgroup of $N_G(P)$ isomorphic to the dihedral group D_{20}. Since this group has order 20, we must have $N_G(P) = \langle \sigma, \tau \rangle \cong D_{20}$

Problem 2. *Let G be a group and $Z(G)$ be the center of the group. An automorphism $\alpha \in \mathrm{Aut}(G)$ is said to be central if for all $x \in G$ we have $x^{-1}\alpha(x) \in Z(G)$. Show that the central automorphisms form a normal subgroup N of $\mathrm{Aut}(G)$.*

Proof. The identity automorphism is clearly central. As for inverses, in $\alpha \in \mathrm{Aut}(G)$ is central then for all $x \in G$, $x\alpha(x^{-1}) \in Z(G)$ and since automorphisms must preserve the center, $\alpha^{-1}(x\alpha(x^{-1})) = \alpha^{-1}(x)x^{-1} \in Z(G)$, so that $\alpha^{-1}(x)x^{-1} = x^{-1}(\alpha^{-1}(x)x^{-1})x = x^{-1}\alpha^{-1}(x) \in Z(G)$. So the inverse of a central automorphism is also central. To see that the central automorphisms are closed under composition, take two central automorphisms α, β and compute

$$x^{-1}\alpha \circ \beta(x) = x^{-1}\alpha(\beta(x)) = x^{-1}\beta(x)\beta(x)^{-1}\alpha(\beta(x)).$$

Since both β and α are central, $x^{-1}\beta(x), \beta(x)^{-1}\alpha(\beta(x)) \in Z(G)$. That the central automorphisms are closed under composition then follows from the fact that $Z(G)$, being a subgroup of G, is closed under multiplication. Lastly, to see that this group is indeed normal we simply compute the following for any central α, any $\beta \in \mathrm{Aut}(G)$ and all $x \in G$:

$$x^{-1}(\beta^{-1} \circ \alpha \circ \beta(x)) = \beta^{-1}(\beta(x^{-1}) \cdot \alpha(\beta(x))) = \beta^{-1}(\beta(x)^{-1} \cdot \alpha(\beta(x))).$$

Since α is central, $\beta(x)^{-1} \cdot \alpha(\beta(x)) \in Z(G)$ and since β, being an automorphism of G, preserves the center, we have $\beta^{-1}(\beta(x)^{-1} \cdot \alpha(\beta(x))) \in Z(G)$. Thus $\beta^{-1} \circ \alpha \circ \beta$ is central, implying the subgroup of $\mathrm{Aut}(G)$ of central automorphisms is indeed a normal sugroup.

□

Problem 3. *Let k be a field and R the subring of $k(x)$ generated by $k[x]$ and $1/x$. For a typical nonzero element $p(x) = \sum_{i=-M}^{N} a_i x^i$ of R, define*

$$H(p(x)) = max(\{i \in \mathbb{Z} | a_i \neq 0\}) \quad \text{and} \quad L(p(x)) = min(\{i \in \mathbb{Z} | a_i \neq 0\}).$$

Show that R is a Euclidean domain with Euclidean norm given by $N(p(x)) = H(p(x)) - L(p(x))$ and $N(0) = 0$.

Proof. First we note that R is an integral domain since it is a subring of the field $k(x)$. It remains to show that the Division algorithm holds for any two $p(x), q(x) \in R$ with $q(x) \neq 0$. Suppose first that $L(p(x)), L(q(x)) \geq 0$. Then in fact $p(x), q(x) \in k[x]$ and using the standard division algorithm we may write

$$p(x) = q(x) \cdot b(x) + r(x),$$

for some $b(x), r(x) \in k[x]$ with either $r(x) = 0$ or $\deg(r(x)) < \deg(q(x))$. Note that in this case $\deg(r(x)) = H((r(x))$. □

Problem 4. *Let F be a field of arbitrary characteristic. Show that any two elements of order 2 in the special linear group $SL_2(F)$ are conjugate in $GL_2(F)$. Find a necessary and sufficient condition on F for $SL_2(F)$ to have a unique element of order 2.*

Solution. Let $A \in SL_2(F)$ be an element of order 2. Then A satisfies the equation $p(A) = 0$, where $p(x) = x^2 - 1$. Now recall that the conjugacy class of a matrix is completely determined by a list of invariant factors $a_0(x), a_1(x), ..., a_n(x)$ such that $a_i(x)$ divides $a_{i+1}(x)$ for all $i = 0, ..., n-1$, and the product $\prod_{i=0}^{n} a_i(x)$ is the characteristic polynomial of the matrix, $c_A(x)$. Since in this case $c_A(x)$ is of degree 2, there are only two possible lists of invariant factors, namely $L1 = \{c_A(x)\}$ or $L2 = \{x - a, x - a\}$, for some $a \in F$ such that $(x-a)^2 = c_A(x)$. The $L2$ case implies the only root of $c_A(x)$, that is, the unique eigenvalue of A must be $a \in F$. Since $A \in SL_2(F)$ $\det A = a^2 = 1$ so either $a = 1$ or $a = -1$. If $a = 1$ then A is simply the identity matrix, which we do not actually consider an element of order 2. If $a = -1$, the rational canonical form of A is then $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Note that this matrix is still the identity if $\text{char} F = 2$. Now consider the $L1$ case. Let $c_A(x) = x^2 + bx + c$. The rational canonical form of A is then $\begin{pmatrix} 0 & -c \\ 1 & -b \end{pmatrix}$. Since $\det A = 1$, we must have $c = 1$, but then

$$\begin{pmatrix} 0 & -1 \\ 1 & -b \end{pmatrix}^2 = \begin{pmatrix} -1 & b \\ -b & b^2 - 1 \end{pmatrix}.$$

The only way this matrix could equal the 2×2 identity is if $\text{char} F = 2$ and $b = 0$. The rational canonical form is then $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus, if $\text{char} F \neq 2$ the unique rational canonical form representing matrices of order 2 and determinant 1 in $GL_2(F)$ is $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and if $\text{char} F = 2$ the representing matrix is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
Since the rational canonical forms derived above are examples of matrices in $SL_2(F)$ of order 2, there is a unique such matrix in $SL_2(F)$ if and only if these matrices constitute their own conjugacy class, i.e. if and only if these matrices are in the center of $GL_2(F)$. Suppose first that $\text{char} F \neq 2$. Then the matrix in question is scalar and hence lies in the center of $GL_2(F)$ so it must be the unique element of $SL_2(F)$ of order 2. Now if $\text{char} F = 2$ then we find that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

so the matrix in question does not lie in the center. Thus, a necessary and sufficient condition for $SL_2(F)$ to have a unique element of order 2 is for $\text{char} F \neq 2$.

Problem 5. *Let p be a prime, $\mathbb{F}_p$ be the field with p elements, and let t be an indeterminate. Let $F = \mathbb{F}_p(t)$ be the field of fractions of the polynomial ring $\mathbb{F}_p[t]$.*
(i) Show that $g(x) = x^p - x + t$ is separable over F.

Proof. The derivative of g is $D_x(g(x)) = -1$. This polynomial has no roots, hence $g(x)$ is relatively prime to its derivative so it must be separable. □

(ii) Show that if α is a root of g then $\alpha + 1$ is also a root. Deduce that the roots of g are precisely those of the form $\alpha + b$ for $b \in \mathbb{F}_p$.

Proof. If α is a root of g then

$$(\alpha+1)^p - (\alpha+1) + t = \alpha^p + 1 - (\alpha+1) + t = \alpha^p - \alpha + t = g(\alpha) = 0.$$

Thus $\alpha + 1$ is also a root of g. Replacing α with $\alpha + 1$ and repeating the above computation $p - 1$ times shows that $\alpha, \alpha + 1, ..., \alpha + (p-1)$ are all roots of g. Since g is a degree p polynomial, it can have at most p roots, therefore there are all the roots of g.

□

(iii) Show that g has no roots in F.

Proof. If $a \in \mathbb{F}_p$ were a root, then the set of roots of g is $\{a + b | b \in \mathbb{F}_p\} = \mathbb{F}_p$. To see this simply take $\alpha = a + (-a) = 1$ and proceed as in part b. We then have that g factors in $F[x]$ as

$$g(x) = (x-1)(x-2)\cdots(x-(p-1)).$$

However, the constant term of g would then be $\prod_{b \in \mathbb{F}_p} b \neq t$, a contradiction. □

(iv) Find the Galois group of g over F.

Solution. By part (ii), g splits in $F(\alpha) \cong F[x]/(g(x))$ where α is any root of g. Part (iii) shows that $F(\alpha) \neq F$ so that $[F(\alpha) : F] = p$. It follows that this must be the splitting field of g. Since g is separable, so is $F(\alpha)$ hence $|\mathrm{Gal}(F(\alpha)/F)| = [F(\alpha) : F] = p$. Since p is a prime, the only group of order p is the cyclic group of order p, thus $\mathrm{Gal}(F(\alpha)/F) \cong Z_p$.

Problem 6. *Let $f(x)$ be a monic polynomial of degree $n > 0$ over a field K and let $\Delta(f)$ denote its discriminant. Let $g(x) = f(x^2)$. You may assume without proof that $\Delta(g) = \Delta(f)^2(-4)^n f(0)$.*
(i) Let $f(x) = x^2 + 3x + 1$ so that $g(x) = x^4 + 3x^2 + 1$. Show that g is irreducible over $\mathbb{Q}$.

Proof. Viewing $\mathbb{Q}$ as a subfield of $\mathbb{C}$, we know that the roots of $f(x)$ are

$$r_{\pm} = \frac{-3 \pm \sqrt{5}}{2}.$$

We then have that $g(\sqrt{r_\pm}) = f(r_\pm) = 0$ so that $\sqrt{r_\pm}$ are both roots of g in $\mathbb{C}$. Further, since $g(-x) = g(x)$, we have that $-\sqrt{r_\pm}$ are also roots of g in $\mathbb{C}$. This accounts for 4 roots of g in $\mathbb{C}$ and since g has degree 4, these must be all of its roots. Since none of these roots lie in $\mathbb{Q}$, g does not factor over $\mathbb{Q}$ into a product of 4 degree 1 polynomial or a product of a degree 1 polynomial and a degree 3 polynomial. The only possibilities left are either g is the product of two irreducible quadratics or g is irreducible. That the former case does not hold and can be checked simply looking at pairwise products of the factors $\{(x - \sqrt{r_\pm}), (x + \sqrt{r_\pm})\}$:

$$(x - \sqrt{r_\pm})(x + \sqrt{r_\pm}) = x^2 - r_\pm \notin \mathbb{Q}[x],$$
$$(x - \sqrt{r_+})(x + \sqrt{r_-}) = x^2 + (\sqrt{r_-} - \sqrt{r_+})x - \sqrt{r_+ r_-} \notin \mathbb{Q}[x],$$
$$(x - \sqrt{r_+})(x - \sqrt{r_-}) = x^2 - (\sqrt{r_+} + \sqrt{r_-})x + \sqrt{r_+ r_-} \notin \mathbb{Q}[x].$$

□

(ii) To which familiar group is the Galois group of g over $\mathbb{Q}$ isomorphic?

Solution. The Galois group of g must be a subgroup of S_4 since it permutes the roots of g. Further, since $\Delta(g) = \Delta(f)^2(-4)^2 = 25 \cdot 16 \in \mathbb{Q}$, its discriminant must be fixed by the Galois group and so this group must in fact lie in A_4. Let $\alpha_1 = \sqrt{r_+}, \alpha_2 = -\sqrt{r_+}, \alpha_3 = \sqrt{r_-}, \alpha_4 = -\sqrt{r_-}$ and consider the following elements of K

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = 0$$
$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\sqrt{r_+} + \sqrt{r_-})^2 = 1$$
$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = -(\sqrt{r_+} - \sqrt{r_-})^2 = -1.$$

These elements, as defined, are permuted by the $\mathrm{Gal}(K/\mathbb{Q})$. We view this group as a subgroup of S_4 via the action on the α_i. The stabilizer of the θ_i is the Klein 4-group $V = \{1, (12)(34), (13)(24), (14)(23)\}$. Since g is irreducible, $[K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})|$ is at least 4. Thus, $\mathrm{Gal}(K/\mathbb{Q}) = V$.