Spring 2011
Algebra Qualfying Exam Solutions

Hannah Hoganson, Allechar Serrano

August 5, 2016

1. Let p be prime. Show that an element in the symmetric group S_n has order p if and only if it is a product of commuting $p-$cycles. Show by an explicit example that this need not to be the case if p is not prime.

   Solution: ($\Rightarrow$) Suppose $\sigma \in S_n$ has order p. Then we have that $\sigma^p(a_1) = a_1$. Construct the cycle $C_1 = (a_1 \, \sigma(a_1) \, \dots \, \sigma^k(a_1))$. Since p is the order, we have $k \leqslant p$ and $k|p$, so either $k = 1$ or $k = p$. The case $k = 1$ is trivial. For $k = p$, consider i to be the smallest i that is not in C_1. We have a cycle containing a_i of the form $C_i(a_i \, \sigma(a_i) \, \dots \, \sigma^k(a_i)$. We continue to repeat this process, so any element of order p has its cycle decomposition has product of commutative $p-$cycles.
   ($\Leftarrow$) Suppose $\sigma = (a_{1,1} \dots a_{1,p}) \dots (a_{k,1} \dots a_{k,p})$ where each $a_{i,j}$ is distinct. Since the cycles commute, we have that if

   $$\sigma^l = (a_{1,1} \dots a_{1,p})^l \dots (a_{k,1} \dots a_{k,p})^l = 1$$

   and since the order of each $p-$cycle is p, then $p|l$. Hence, the minimum value for l is p.

   For the example, $\sigma = (1\,2)(3\,4\,5)$ has order 6.

2. Prove that the number of Sylow $p-$subgroups of $GL_2(\mathbb{F}_p)$ is $p+1$.

   Solution: Consider n_p the number of Sylow $p-$subgroups of $GL_2(\mathbb{F}_p)$. Since $|GL_2(\mathbb{F}_p)| = p(p+1)(p-1)^2$, we have that $n_p|(p+1)(p-1)^2$ and $n_p \equiv 1 \bmod p$ so $n_p \in \{1, p+1, (p-1)^2, (p+1)(p-1)^2\}$. The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order p and generates a Sylow $p-$subgroup P.

Its transpose $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ also has order p, so $n_p \neq 1$. If $a, d \neq 0$, we have

$$\frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & ad^{-1} \\ 1 & 1 \end{pmatrix}$$

so every $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is in the normalizer $N_P(G)$. There are $p(p-1)^2$ such elements. Since $n_p = [G : N_P(G)]$, then $n_p \leqslant p+1$ so $n_p = p+1$.

3. Let G be a $p-$group with $|G| > p$. Show that

   (a) G has a nontrivial center;

   Solution: Consider the action of G on itself by conjugation. From the class equation, we have that $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$ where g_i are representatives of the distinct noncentral conjugacy classes. By definition, $C_G(g_i) \neq G$, so p divides $|G : C_G(g_i)|$. Since p divides $|G|$, then p divides $|Z(G)|$. Therefore, the center is nontrivial.

   (b) G has a normal subgroup of every order $p^m < |G|$.

   Solution: Suppose that every group of order p^m for $0 \leqslant m \leqslant n$. Let G be a group of order p^{n+1}. We have that $Z(G)$ is nontrivial. If $Z(G) = G$, then G is abelian. Let $H \leqslant G$ be a subgroup of order p by Cauchy.
   If $Z(G) \neq G$, then $Z(G)$ is a nontrivial proper normal subgroup. Let $H = Z(G)$. Since H and G/H are groups of order p^k for $1 \leqslant k \leqslant n$. Then H has a subgroup of order p^j for all p^j dividing $|H|$. We have the same for G/H. By Fourth Isomorphism theorem, G has a subgroup of order p^j for all $0 \leqslant j \leqslant n+1$.

4. For the matrix $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$, find:

   (a) the rational canonical form over $\mathbb{Q}$;

   Solution: The characteristic polynomial is $p_A(x) = (x-1)^2(x-2)$ and the minimal polynomial is $m_A(x) = (x-1)(x-2)$ hence the invariant factors are $(x-1)(x-2) = x^2 - 3x + 2$ and $x - 1$.

The corresponding companion matrices are $\begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$ and 1. Therefore, the rational canonical form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$$

(b) the Jordan canonical form over $\mathbb{C}$.

Solution: Since the minimal polynomial is $m_A(x) = (x-1)(x-2)$, then all Jordan blocks have size 1. Therefore, the Jordan form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

5. Prove that the ring $\mathbb{Z}[i]$ is a Euclidean domain.

   Solution: Let $\alpha = a + bi$ and $\beta = c + di \neq 0$ be Gaussian integers. Then in $\mathbb{Q}[i]$, we have that $\frac{\alpha}{\beta} = r + si$ where $r = \frac{ac+bd}{c^2+d^2}$, $s = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$. Let $p \in \mathbb{Z}$ be the integer closest to the rational r and let q be the integer closest to the rational s so that both $|r-p|$ and $|s-q|$ are at most $\frac{1}{2}$. Then $\alpha = (p+qi)\beta + \gamma$ for some $\gamma \in \mathbb{Z}[i]$ with $N(\gamma) \leqslant \frac{1}{2}N(\beta)$. Let $\theta = (r-p) + (s-q)i$, set $\gamma = \beta\theta$. Then $\gamma = \alpha - (p+qi)\beta$ so $\gamma \in \mathbb{Z}[i]$ and $\alpha = (p+qi)\beta + \gamma$. Since $N(\theta) = (r-p)^2 + (s-q)^2$ is at most $\frac{1}{2}$. Therefore, $N(\gamma) = N(\theta)N(\beta) \leqslant \frac{1}{2}N(\beta)$.

6. Let G be a finite abelian group and H a subgroup of G. Show that G has a subgroup isomorphic with G/H.

   Solution: Since G is a finite abelian group, we have that $G \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k}$ where $d_1, \ldots, d_k$ are the invariant factors $d_1 > 1$ and $d_i | d_{i+1}$. Since $H \leqslant G$, $H \cong (H \cap \mathbb{Z}_{d_1}) \oplus \cdots (H \cap \oplus \mathbb{Z}_{d_k})$. Since every subgroup of a cyclic group is cyclic, we have $H_i := H \cap \mathbb{Z}_{d_i} \cong \mathbb{Z}_{n_i}$ where $H_i \leqslant \mathbb{Z}_{d_i}$ so by Lagrange $\frac{d_i}{n_i} = l_i \in \mathbb{Z}$. Since $\mathbb{Z}_{d_i}$ is cyclic, $\mathbb{Z}_{d_i}$ has a unique subgroup $N_i \cong \mathbb{Z}_{l_i}$. Thus, G has a subgroup $N \cong N_1 \oplus \cdots N_k \cong \mathbb{Z}_{l_1} \oplus \cdots \oplus \mathbb{Z}_{l_k} \cong N$ so G/H is isomorphic to a subgroup N of G.

7. Let m, n be positive integers and d their greatest common divisor. Show that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$

   Solution: $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is cyclic since $a \otimes b = b(a \otimes 1) = ab(1 \otimes 1)$ with $1 \otimes 1$ as generator. There exist integers a, b such that $am + bn = d$

so $d(1 \otimes 1) = (am + bn)(1 \otimes 1) = am \otimes bn = 0$, so the order of the cyclic group divides d. Consider $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ defined by $(a \bmod m, b \bmod n) \longmapsto ab \bmod d$. It is $\mathbb{Z}-$linear and the induced map $\varphi' : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ maps $1 \otimes 1 \longmapsto \overline{1}$ an element of order d. Thus $1 \otimes 1$ has order at least d, hence the cyclic group has order at least d, so the order is exactly d. Then φ' is an isomorphism.

8. For a ring R define its nilradical $\mathfrak{n}(R) = \{x \in R : x^n = 0 \text{ for some } n \in \mathbb{Z}\}$.

   (a) If R is commutative, prove that $\mathfrak{n}(R)$ is an ideal of R.
   Solution: Consider $x, y \in \mathfrak{n}(R)$, so we have $x^n = y^m = 0$. So

$$\begin{aligned}(x+y)^{n+m} &= \sum_{k=0}^{n+m} x^k y^{n+m-k} \\ &= \sum_{k=0}^{n-1} x^k \underbrace{y^{n+m-k}}_{=0} + \sum_{k=n}^{n+m} \underbrace{x^k}_{=0} y^{n+m-k} \\ &= 0\end{aligned}$$

   so $x+y \in \mathfrak{n}(R)$. We have that $0 \in \mathfrak{n}(R)$ and $(-x)^n = (-1)^n x^n = 0$ so $-x \in \mathfrak{n}(R)$. Then $\mathfrak{n}(R)$ is an additive subgroup of R. Since R is commutative, let $r \in R$ and $(rx)^n = r^n x^n = (xr)^n = 0$. Hence $\mathfrak{n}(R)$ is an ideal.

   (b) Is the nilradical an ideal even if R is noncommutative?
   Solution: Consider $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Since $x^2 = y^2 = 0$ then x, y are in the nilradical of the noncommutative ring of matrices. We have that $x + y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $(x+y)^2 = I$, which is a unit, and it's not nilpotent.

9. What is the Galois group of $x^4 - 5$ over:

   (a) $\mathbb{Q}$
   Solution: The splitting field of $x^4 - 5$ is $\mathbb{Q}(i, \sqrt[4]{5})$. The automorphisms are given by $\tau : i \longmapsto -i, \sqrt[4]{5} \longmapsto \sqrt[4]{5}$ and $\sigma : i \longmapsto i, \sqrt[4]{5} \longmapsto i\sqrt[4]{5}$. We have that $|\tau| = 2, |\sigma| = 4$, and $\sigma\tau = \tau\sigma^{-1}$. Hence $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{5})/\mathbb{Q}) = D_4$.

(b) $\mathbb{Q}(\sqrt{5})$

Solution: $\mathbb{Q}(\sqrt{5})$ is fixed by $\langle \tau, \sigma^2 \rangle$, hence the Galois group is isomorphic to the Klein group, $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) $\mathbb{Q}(i)$

Solution: Since σ fixes i, we have that the Galois group of $x^4 - 5$ over $\mathbb{Q}(i)$ is $\langle \sigma \rangle$, so it is isomorphic to $\mathbb{Z}_4$.

10. Show that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$, and determine the Galois group.

    Solution: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of the separable polynomial $(x^2-2)(x^2-3)$ and hence it's Galois over $\mathbb{Q}$. This extension has degree 4 since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Since the automorphisms permute the roots of each irreducible factor, they are $\tau : \sqrt{2} \longmapsto -\sqrt{2}, \sqrt{3} \longmapsto \sqrt{3}$ and $\sigma : \sqrt{2} \longmapsto \sqrt{2}, \sqrt{3} \longmapsto -\sqrt{3}$. Hence $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

11. Show that the polynomial $x^2 + y^2 - 1 = 0$ is irreducible in $\mathbb{Q}[x, y]$. Is it irreducible in $\mathbb{C}[x, y]$?

    Solution: $x^2 + y^2 - 1 \in \mathbb{Q}[x, y] = \mathbb{Q}[x][y]$. Since $\mathbb{Q}[y]$ is a UFD and $y + 1 \in \mathbb{Q}[y]$ is irreducible, hence prime. So $x^2 + (y+1)(y-1)$ is irreducible by Eisenstein.
    Suppose $x^2 + y^2 - 1$ is reducible on $\mathbb{C}[x, y]$, then $x^2 + y^2 - 1 = f(x, y)g(x, y)$ and $\deg f, \deg g = 1$. So the circle $x^2 + y^2 - 1 = 0$ would be a union of two lines, a contradiction.