MATH 4E03/6E03 Galois Theory, Fall 2014
Homework 1 Solution

Total: 18 marks.

(1) Let G be a group acting on a set X. If $x, y \in X$ lie in the same G-orbit, what is the relation between the stabilizers of x and y? (1 mark, no work is needed)

Answer: If $g \cdot x = y$, then $\mathrm{Stab}_G(y) = g\mathrm{Stab}_G(x)g^{-1}$, because for every $k \in \mathrm{Stab}_G(x)$, we have $k \cdot x = x$ and so

$$gkg^{-1} \cdot y = gkg^{-1} \cdot (g \cdot x) = (gkg^{-1}g) \cdot x = (gk) \cdot x = g \cdot x = y,$$

or in other words, $gkg^{-1} \in \mathrm{Stab}_G(y)$. □

(2) Let p be a prime number and G be a group. Show that if the order of G is a power of p, then the *center* of G, defined as

$$Z(G) = \{g \in G \text{ such that } gk = kg \text{ for all } k \in G\},$$

is non-trivial. (3 marks)

(Hint: Consider the conjugate action of G on itself, and decompose G into orbits, which are conjugacy classes in this situation. If $g \in G$ lies in the center, how does its conjugacy class look like?)

Answer: Direct from the definition of the center of G, we know that

$$x \in Z(G) \Leftrightarrow \quad gxg^{-1} = x \text{ or all } g \in G \Leftrightarrow \quad \mathrm{orb}_G(x) = \{x\}. \qquad \text{(1 mark)}$$

In other words, elements in $Z(G)$ are are those with singleton conjugacy classes (orbits). Decompose G into conjugacy classes and count the number of elements on each orbit, we have

$$\#G = \#Z(G) + \sum_{\substack{x \in G \\ \#(Conj-Class(x)) \geq 2}} \#Conj - Class(x). \qquad \text{(1 mark)}$$

Notice that each $\#Conj - Class(x)$, if $\#(Conj - Class(x)) \geq 2$, must be a p-power, because its cardinality divides the order of G which is a p-power. This forces $\#Z(G)$ to be a multiple of p, and so it cannot be 1. (1 mark) □

(3) (Garling, Ex 1.10) Let Σ_n be the permutation group of n elements.

(a) Given a permutation $\sigma \in \Sigma_n$, convince yourself that the following quantity

$$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

is either 1 or -1 (0 marks).

Answer: As explained in class, if we define $X_+ = \{(i, j), \text{ where } 1 \leq i < j \leq n\}$, then

$$\epsilon(\sigma) = (-1)^{\text{the number of pairs in } X_+ \text{ inverted by } \sigma}.$$

(b) Show that the map $\epsilon : \Sigma_n \to \{\pm 1\}$ is a group homomorphism of Σ_n onto the cyclic group $\{\pm 1\}$ of order 2 (2 marks).

Answer: This is to show that $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$. We have

$$\begin{aligned}\epsilon(\sigma\tau) &= \prod_{1\le i<j\le n} \frac{\sigma\tau(i)-\sigma\tau(j)}{i-j} \\ &= \prod_{1\le i<j\le n} \left(\frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}\right)\left(\frac{\tau(i)-\tau(j)}{i-j}\right) \\ &\left(\prod_{1\le i<j\le n} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}\right)\left(\prod_{1\le i<j\le n} \frac{\tau(i)-\tau(j)}{i-j}\right). \qquad \text{(1 mark)}\end{aligned}$$

The second product is $\epsilon(\tau)$. To show that the first product is $\epsilon(\sigma)$, (Comment: Some of you did not show this.) we separate the factors into two subsets: one has order preserved by τ and one has order reversed by τ,

$$\prod_{1\le i<j\le n} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)} = \left(\prod_{\substack{1\le i<j\le n\\ \tau(i)<\tau(j)}} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}\right)\left(\prod_{\substack{1\le i<j\le n\\ \tau(i)>\tau(j)}} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}\right).$$

In the second product, if we replace $\frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}$ by $\frac{\sigma\tau(j)-\sigma\tau(i)}{\tau(j)-\tau(i)}$, which does not change the value, then all pairs are now in the correct order. Since τ is a bijection on the n numbers, we have

$$\prod_{1\le i<j\le n} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)} = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j} = \epsilon(\sigma).$$

(1 mark)

□

(c) Prove that the kernel of ϵ is A_n consisting of all even permutations (2 marks).

Answer: It is the same as to show that ϵ is equal to the signature homomorphism $s : \Sigma_n/A_n \to \{\pm 1\}$. Since we have shown that ϵ is also a group homomorphism, to prove that the two homomorphisms ϵ and s are equal, it suffices to show that every transposition $\sigma = (a\ b)$ is mapped by ϵ to -1. Notice that a, b are just two random numbers between 1 and n, but recall from (b) that ϵ is an homomorphism, we know that

$$\begin{aligned}\epsilon(\tau\sigma\tau^{-1}) &= \epsilon(\tau)\epsilon(\sigma)\epsilon(\tau)^{-1} \\ &= \epsilon(\tau)\epsilon(\tau)^{-1}\epsilon(\sigma) \qquad \text{(because the codomain } \{\pm 1\} \text{ is an abelian group)} \\ &= \epsilon(\sigma).\end{aligned}$$

Therefore, if we take τ to be the permutation

$$\tau : a \mapsto 1 \text{ and } b \mapsto 2$$

then $\tau\sigma\tau^{-1} = (1\ 2)$. Therefore, it suffices to show that $\epsilon((1\ 2)) = -1$. The affected pairs are those (i, j) with either i or j being 1 or 2, namely

$$(1,2),\ (1,3)\ldots,\ (1,n),\ (2,3),\ \ldots,\ (2,n),$$

which are mapped by $(1\ 2)$ to

$$(2,1),\ (2,3)\ldots,\ (2,n),\ (1,3),\ \ldots,\ (1,n).$$

Only the pair $(2,1)$ has negative order. Therefore, in the product $\epsilon((1\ 2)) = \prod_{1\le i<j\le n} \frac{(1\ 2)(i)-(1\ 2)(j)}{i-j}$, almost all fractions are equal to 1 except when $i=1$, $j=2$, in which case $\epsilon((1\ 2)) = \frac{1-2}{2-1} = -1$. ☐

Comment: Some of you says that an arbitrary transposition $(a\ b)$ has only one pair (a,b) with order swapped. This is wrong. Consider when $n=3$ and the transposition $(1\ 3)$, then all pairs $(1,2)$, $(1,3)$, $(2,3)$ are mapped by $(1\ 3)$ to $(3,2)$, $(3,1)$, $(2,1)$, so all three pairs have order swapped. So if you insist to check the affected pairs by arbitrary transposition (a,b), you should say that the pairs with order swapped are (a,b) and all $(a,c),(c,b)$ with $a<c<b$, but the negative signs produced by (a,c) and (c,b) cancel each other and finally we only have the negative sign coming from the pair (a,b).

(4) Let Σ_4 be the group of permutations of 4 elements. Let $\sigma = (12)(34)$ be a product of transpositions in Σ_4.

(a) Express the Σ_4-stabilizer of σ and find its order. (2 marks)

Answer: The stabilizer of σ are those $\tau \in \Sigma_4$ such that $\tau\sigma\tau^{-1} = \sigma$. We write down this relation explicitly as

$$\tau(12)(34)\tau^{-1} = (\tau(1)\tau(2))(\tau(3)\tau(4)) = (12)(34).$$

Therefore, it suffices to look for the permutations on $\{1,2,3,4\}$ which stabilize $(12)(34)$. We see that

- We can permute the elements within each cycle, i.e., take $\tau_1 = (12) : 1 \leftrightarrow 2$, leaving 3,4 fixed, and $\tau_2 = (34) : 3 \leftrightarrow 4$, leaving 1,2 fixed.
- We can permute the two 2-cycles, i.e., we take $\tau_3 = (13)(24) : 1 \leftrightarrow 3,\ 2 \leftrightarrow 4$.

The stabilizer of σ is hence generated by the group generated by τ_1, τ_2 and τ_3. Using the relations

$$\tau_1\tau_2 = \tau_2\tau_1 \qquad \text{and} \qquad \tau_3\tau_1 = \tau_2\tau_3,$$

we find that this group is equal to

$$\begin{aligned}&\{I,\ \tau_1,\ \tau_2,\ \tau_3,\ \tau_1\tau_2,\ \tau_3\tau_1,\ \tau_3\tau_2,\ \tau_1\tau_2\tau_3\}\\ =&\{I,\ (12),\ (34),\ (13)(24),\ (12)(34),\ (1423),\ (1324),\ (14)(23)\}\end{aligned} \quad \text{(2 marks)}$$

which has order 8. ☐

Note: this is the dihedral group of order 8, represented by generator relations

$$\langle \rho, \tau,\ \text{where}\ \rho^4 = 1,\ \tau^2 = 1,\ \tau\rho\tau = \rho^3 \rangle$$

if we take $\rho = \tau_3\tau_1 = (1423)$ and $\tau = \tau_1 = (12)$.

(b) How many elements are there in the Σ_4-orbit of σ? (1 marks)

Answer: $24/8 = 3$. ☐

(5) (Garling, Ex 3.9) Suppose that R is an infinite ring (i.e., $\#R = \infty$) such that R/I is finite for each non-trivial ideal I. Show that R is an integral domain. (3 marks)

Answer: Suppose that R is not an integral domain, so that there are non-zero elements a and b in R with $ab = 0$. Consider the map

$$\phi : R \to R,\ \phi(x) = ax. \qquad \text{(1 mark)}$$

If we regard R as a group under addition, then ϕ is a group homomorphism. The image is the ideal (a). By Isomorphism Theorem (of Groups), we have

$$R/\ker\phi \cong (a). \qquad \text{(1 mark)}$$

Now $\ker \phi$ cannot be a trivial subgroup, because $(b) \subseteq \ker \phi$. Therefore by the given condition, $R/\ker \phi$ is finite, and the ideal (a) should also be finite because it is isomorphic to $R/\ker \phi$. However, with the condition that $\#(R/(a))$ is finite, this implies that R is a finite ring because $\#R = \#(a) \times \#(R/(a))$. We arrive at a contradiction. (1 mark) □

Comment: Some of you gave the following alternative solution, of which I only sketch the idea. Given $a, b \neq 0$ but $ab = 0$. Since $R/(a) = \{r_i + (a),\, i = 1 \ldots, n\}$ is finite, then every element in R is of the form $r_i + sa$, but then it forces $(b) = \{r_i b,\, i = 1 \ldots, n\}$ to be finite.

(6) (Garling, Ex 3.4) Let R be a ring. Suppose that $a, b \in R$ for which $(a, b) = R$. Show that $(a^m, b^n) = R$ for every positive integers m, n. (2 marks)

Answer: Let $N = m + n$. The given condition $(a, b) = R$ implies that $as + bt = 1$ for some $s, t \in R$. Taking N-th power, we obtain

$$1 = (as + bt)^N = \sum_{k=0}^{N} C^N_{N-k} (as)^{N-k} (bt)^k.$$

(1 mark)
Look at each term $(as)^{N-k}(bt)^k$ above. If $k \leq n$, then $N - k \geq m$ and the term is a multiple of a^m. If $k \geq n$, then the term is a multiple of b^n. The above equality implies that there exists S and T, both in R, such that $a^m S + b^n T = 1$, which is equivalent to say that $(a^m, b^n) = R$. (1 mark) □

(7) Let R be a ring and I be an ideal of R. Prove that

(a) $I[X] = \{\text{polynomials in } R[X] \text{ with coefficients in } I\}$ is an ideal of $R[X]$, and

(b) $R[X]/I[X]$ is isomorphic to $(R/I)[X]$ as a ring.

(2 marks)

Answer: To show that $I[X]$ is an ideal, first notice that is clearly ad additive subgroup. If $p(X) = \sum_i a_i X^i \in R[X]$ and $q(X) = \sum_j b_j X^j \in I[X]$, then $p(X)q(X) = \sum_k c_k X^k$ where $c_k = \sum_j a_{k-j} b_j$. Clearly $c_k \in I$ since I is an ideal and each $b_j \in I$. Therefore $I[X]$ is an ideal of $R[X]$. (1 mark)

If we denote

$$R \to R/I,\ a \mapsto \bar{a} = a + I$$

the natural surjective homomorphism, then we define

$$\phi : R[X] \to (R/I)[X],\ \phi\left(\sum_i a_i X^i\right) = \sum_i \bar{a}_i X^i.$$

Then we show that

- ϕ is a ring homomorphism, since

$$\begin{aligned}
&\phi\left(\sum_i a_i X^i + \sum_i b_i X^i\right) = \phi\left(\sum_i (a_i + b_i) X^i\right) \\
&= \sum_i \overline{(a_i + b_i)} X^i = \sum_i (\bar{a}_i + \bar{b}_i) X^i \qquad \text{(since } a \mapsto \bar{a} \text{ is a ring homomorphism)} \\
&= \sum_i \bar{a}_i X^i + \sum_i \bar{b}_i X^i = \phi(\sum_i a_i X^i) + \phi(\sum_i b_i X^i).
\end{aligned}$$

and

$$\phi\left(\sum_i a_iX^i\sum_j b_jX^j\right)=\phi\left(\sum_k(\sum_{i+j=k}a_ib_j)X^k\right)$$
$$=\sum_k\overline{(\sum_{i+j=k}a_ib_j)}X^k=\sum_k(\sum_{i+j=k}\bar{a}_i\bar{b}_j)X^k \qquad \text{(since } a\mapsto\bar{a} \text{ is a ring homomorphism)}$$
$$=\sum_i\bar{a}_iX^i\sum_j\bar{b}_jX^j=\phi(\sum_i a_iX^i)\phi(\sum_j b_jX^j).$$

and $\phi(1_{R[X]})=\phi(1_R)=1_{R/I}=1_{(R/I)[X]}$. (It is fine if you just state that ϕ is a ring homomorphism without showing it.)

- Its kernel is $I[X]$, since if $\sum_i \bar{a}_iX^i=0$, then each coefficient $\bar{a}_i=a_i+I=0$, which means that $a_i\in I$ and so $\sum_i a_iX^i\in I[X]$.
- ϕ is surjective, i.e. image$(\phi)=(R/I)[X]$, since each coefficient $\bar{a}_i\in R/I$ is coming from an $a_i\in R$.

Therefore, by the Isomorphism Theorem (for ring homomorphisms) (1 mark for applying Isomorphism Theorem), we have $R[X]/I[X]\cong(R/I)[X]$ as a ring. □

Answer to some Suggested Problems (no need to hand in):

(1) (Garling, Ex 3.3) Show that an integral domain with a finite number of elements is always a field.

Answer: Let a be an non-zero element in R. We want to show it is invertible. Define a map

$$\phi: R\to R,\ \phi(x)=ax.$$

This map is a group homomorphism, if we regard R as a group under addition. This map is injective, because if $\phi(x)=\phi(y)$, then $ax=ay$ and $a(x-y)=0$. Since R is an integral domain and $a\neq 0$, this forces $x-y=0$ and so $x=y$. Now the map is then automatically bijectively, because R is a finite set. In particular, it is surjective, hence $1\in R$ is in the image of ϕ, which means that there is an $x\in R$ such that $\phi(x)=ax=1$. The last statement means that a is invertible. □

(2) Let Σ_X be the group consisting of bijective maps of a set X to itself. Define an action of Σ_X on the cartesian product

$$X\times X=\{(x,y),\text{ where } x,y\in X\}$$

by $\sigma\cdot(x,y)=(\sigma(x),\sigma(y))$. What are the Σ_X-orbits of $X\times X$?

Answer: If $\#X=1$, then $\#(X\times X)=1$ and there is only one orbit. If $\#X\geq 2$, then there are two orbits: one consists of pairs with equal coordinates

$$\Delta(X)=\{(x,x),\text{ where } x\in X\};$$

another consists of pairs with different coordinates

$$X\times X-\Delta(X)=\{(x,y),\text{ where } x,y\in X\text{ and } x\neq y\}.$$

It is clear that $\Delta(X)$ forms an orbit: for every two elements (x,x) and (y,y), any function σ which maps x to y certainly translates (x,x) to $(\sigma(x),\sigma(x))=(y,y)$. Now for every two pairs $(x,y),(z,w)\in X\times X-\Delta(X)$, we have $x\neq y$ and $z\neq w$. We can always find a bijective map of the form $\sigma=\begin{pmatrix}\cdots & x & \cdots & y & \cdots\\ \cdots & z & \cdots & w & \cdots\end{pmatrix}$ such that $\sigma(x)=z$ and $\sigma(y)=w$. □

(3) (Just for fun) Find a formula for the size of a conjugacy class of Σ_n. (Hint: First find the order of the stabilizer of an element in the given orbit.)

Answer: (This question also appears in Dummit-Foote Sec.4.3, Q.33) Given $\sigma \in \Sigma_n$, we define a map $m_\sigma : \mathbb{N} \to \mathbb{N}_0$ defined by the condition: there are $m_\sigma(j)$ many j-cycles in the decomposition of σ into disjoint cycles. We look for the symmetry of such a σ, using the idea similar to the question concerning Σ_4 above.

- We can cyclicly permute the elements in each j-cycle, which generate a subgroup isomorphic to $\mathbb{Z}_j$ the cyclic group of order j. Since there are $m_\sigma(j)$ many j-cycles, their product generates the direct product subgroup $\underbrace{(\mathbb{Z}_j \times \cdots \times \mathbb{Z}_j)}_{m_\sigma(j)\text{-times}}$.
- We can permute each pair of j-cycles, altogether such action generates the permutation group $\Sigma_{m_\sigma(j)}$.

Hence the stabilizer is isomorphic to the product

$$\prod_{j\in\mathbb{N}} \underbrace{(\mathbb{Z}_j \times \cdots \times \mathbb{Z}_j)}_{m_\sigma(j)\text{-times}} \rtimes \Sigma_{m_\sigma(j)},$$

where the semi-direct product of $\Sigma_{m_\sigma(j)}$ on the $m_\sigma(j)$ pieces of $\mathbb{Z}_j$ is given by the action mentioned above. Its order is given by

$$\prod_{j\in\mathbb{N}} j^{m_\sigma(j)}(m_\sigma(j))!.$$

Notice that this is a finite product, because $m_\sigma(j) = 0$ if j is large enough. Therefore, the size of the stabilizer is given by

$$\frac{n!}{\prod_{j\in\mathbb{N}} j^{m_\sigma(j)}(m_\sigma(j))!}.$$

$\square$