Silvain Rideau
1091 Evans
silvain.rideau@berkeley.edu
www.normalesup.org/~srideau/en/teaching

Solutions to homework 7

Due October 23rd

Problem 1 (Action of the dihedral group on the diagonals) **:**
Let $n \geqslant 4$ be an even positive integer. Let us number the vertices of the n-gon by $\mathbb{Z}/n\mathbb{Z}$ (clockwise for example). And let $X = \{\{i,j\} : i \text{ and } j \text{ number opposite vertices}\}$. So X is the set of diagonals of the n-gon. Let $r \in D_{2n}$ be the rotation sending the vertex 0 to the vertex 1 and s be the symmetry that fixes the vertex 0.

1. Let $\sigma \in D_{2n}$ and $\{i,j\} \in X$, show that $\{\sigma(i), \sigma(j)\} \in X$ where the action of D_{2n} on the vertices is the usual one.

   Solution: If i and j are opposite vertices, then $j = i + n/2$. We have to check that for all $\sigma \in D_{2n}$, $\sigma(i + n/2) - \sigma(i) = n/2 mod n$. Because this property is stable under composition, it suffices to prove it for r and s. We have $r(i + n/2) - r(i) = i+1+n/2-(i+1) = n/2$ and $s(i+n/2)-s(i) = -(i+n/2)-(-i) = -n/2 = n/2 \mod n$.

   You don't really need the reduction as one can directly compute $r^k s^l(i + n/2) - r^k s^l(i) = (-1)^l(i + n/2) + k - ((-1)^k i + k) = (-1)^l n/2 = n/2 \mod n$.

2. Show that $\sigma \star \{i,j\} = \{\sigma(i), \sigma(j)\}$ is an action of D_{2n} on X.

   Solution: Let σ_1 and $\sigma_2 \in D_{2n}$, we have:

$$\begin{aligned}
(\sigma_1 \circ \sigma_2) \star \{i,j\} &= \{\sigma_1 \circ \sigma_2(i), \sigma_1 \circ \sigma_2(j)\} \\
&= \{\sigma_1(\sigma_2(i)), \sigma_1(\sigma_2(j))\} \\
&= \sigma_1 \star \{\sigma_2(i), \sigma_2(j)\} \\
&= \sigma_1 \star (\sigma_2 \star \{i,j\})
\end{aligned}$$

   and $\mathrm{id} \star \{i,j\} = \{\mathrm{id}(i), \mathrm{id}(j)\} = \{i,j\}$.

3. Show that this action has a unique orbit.

   Solution: Pick $i, k \in D_{2n}$, then $r^{k-i} \star \{i, i+n/2\} = \{i+k-i, i+n/2+k-i\} = \{k, k+n/2\}$, so the two diagonals $\{i, i+n/2\}$ and $\{k, k+n/2\}$ are in the same orbit. Note that here all the integer are considered modulo n although it is not specified (the same is true in what follows).

4. Show that $\mathrm{Stab}_{D_{2n}}(\{i,j\}) = \{1, r^{n/2}, r^{2i}s, r^{2i+n/2}s\}$.

   Solution: Let $\sigma \in D_{2n}$, σ stabilizes $\{i,j\}$ if and only if $\sigma(i) = i$ or $\sigma(i) = j = i + n/2$. We have $r^k(i) = i + k$ and $i + k = i$ if and only if $k = 0$ and $i + k = i + n/2$ if and only if $k = n/2$. Similarly, $sr^k(i) = -i + k$ and $-i + k = i$ if and only if $k = 2i$ and $-i + k = i + n/2$ if and only if $k = 2i + n/2$. So the stabilizer contains those for elements.

5. Let $n = 4$, show that $\mathrm{Stab}_{D_8}(X) = \{1, r^2, s, r^2 s\}$.

   Solution: We have $\mathrm{Stab}_{D_8}(X) = \bigcap_i \mathrm{Stab}_{D_8}(\{i,j\}) = \bigcap_i \{1, r^2, r^{2i}s, r^{2i+2}s\}$. But if $i = 0, 2$ then $2i = 0 \mod 4$ and $2i + 2 = 2 \mod 4$ and if $i = 1, 3$, $2i = 2 \mod 4$ and $2i + 2 = 0 \mod 4$ so $\{1, r^2, r^{2i}s, r^{2i+2}s\} = \{1, r^2, s, r^2 s\}$ does not depend on i and $\mathrm{Stab}_{D_8}(X) = \{1, r^2, s, r^2 s\}$.

6. Let $n > 4$, show that $\mathrm{Stab}_{D_{2n}}(X) = \{1, r^{n/2}\}$.

   Solution: If $n > 4$, then 0, $0 + n/2$, 2 and $2 + n/2$ are distinct (even modulo n) and hence $\mathrm{Stab}_{D_{2n}}(X) = \bigcap_i \mathrm{Stab}_{D_{2n}}(\{i,j\}) = \bigcap_i \{1, r^{n/2}, r^{2i}s, r^{2i+n/2}s\} = \{1, r^{n/2}\}$.

Problem 2 :
Let K be a field. We define $K[[X]] = \{\sum_{i \in \mathbb{Z}_{\geqslant 0}} a_i X^i : a_i \in K\}$ the set of formal power series with coefficients in K. The main difference with polynomials is that we now allow infinitely many coefficients to be non zero. We define addition as follows $\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i$ and multiplication as follows $(\sum_i a_i X^i) \cdot (\sum_i b_i X^i) = \sum_k (\sum_{i=0}^k a_i b_{k-i}) X^k$.

1. Show that $(K[[X]], +, \cdot)$ is a commutative ring.

   Solution: The computations to show that these are rings are the same that for polynomials, but let us redo them to check that the infinite sum does not get in the way. We have to prove that $(K[[X]], +)$ is an Abelian group:

   - Associativity: $(\sum_i a_i X^i + \sum_i b_i X^i) + \sum_i c_i X^i = \sum_i (a_i + b_i) X^i + \sum_i c_i X^i = \sum_i (a_i + b_i + c_i) X^i = \sum_i a_i X^i + \sum_i (b_i + c_i) X^i = \sum_i a_i X^i + (\sum_i b_i X^i + \sum_i c_i X^i)$;
   - Commutativity: $\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i = \sum_i (b_i + a_i) X^i = \sum_i b_i X^i + \sum_i a_i X^i$;
   - Additive identity: $\sum_i a_i X^i + \sum_i 0 X^i = \sum_i (a_i + 0) X^i = \sum_i a_i X^i$;
   - Additive inverse: $\sum_i a_i X_i + \sum_i (-a_i) X_i = \sum_i (a_i - a_i) X^i = \sum_i 0 X^i$.

   Actually, as a group $(K[[X]], +)$ is just $K^{\mathbb{Z}_{\geqslant 0}}$ and we have seen multiple times that coordinate wise operation on a product of groups yields a group. Now let us consider the multiplication:

   - Associativity:

$$
\begin{array}{rcl}
((\sum_i a_i X^i) \cdot (\sum_i b_i X^i)) \cdot (\sum_i c_i X^i) & = & (\sum_k (\sum_{i=0}^k a_i b_{k-i}) X^k) \cdot (\sum_i c_i X^i) \\
& = & \sum_l (\sum_{k=0}^l (\sum_{i=0}^k a_i b_{k-i}) c_{l-k}) X^l \\
& = & \sum_l (\sum_{k=0}^l \sum_{i=0}^k a_i b_{k-i} c_{l-k}) X^l \\
& = & \sum_l (\sum_{i=0}^l \sum_{k=i}^l a_i b_{k-i} c_{l-k}) X^l \\
& = & \sum_l (\sum_{i=0}^l a_i (\sum_{k=i}^l b_{k-i} c_{l-k})) X^l \\
& = & \sum_l (\sum_{i=0}^l a_i (\sum_{k=0}^{l-i} b_k c_{l-i-k})) X^l \\
& = & (\sum_i a_i X^i) \cdot (\sum_j (\sum_{k=0}^j b_k c_{j-k}) X^j) \\
& = & (\sum_i a_i X^i) \cdot ((\sum_i b_i X^i) \cdot (\sum_i c_i X^i))
\end{array}
$$

   - Distributivity:

$$
\begin{array}{rcl}
((\sum_i a_i X^i) + (\sum_i b_i X^i)) \cdot (\sum_i c_i X^i) & = & (\sum_i (a_i + b_i) X^i) \cdot (\sum_i c_i X^i) \\
& = & \sum_k (\sum_{i=0}^k (a_i + b_i) c_{k-i}) X^k \\
& = & \sum_k (\sum_{i=0}^k (a_i c_{k-i} + b_i c_{k-i})) X^k \\
& = & \sum_k (\sum_{i=0}^k (a_i c_{k-i}) + \sum_{i=0}^k (b_i c_{k-i})) X^k \\
& = & \sum_k (\sum_{i=0}^k a_i c_{k-i}) X^k + \sum_k (\sum_{i=0}^k b_i c_{k-i}) X^k \\
& = & (\sum_i a_i X^i) \cdot (\sum_i c_i X^i) + (\sum_i b_i X^i) \cdot (\sum_i c_i X^i)
\end{array}
$$

   - Commutativity: $(\sum_i a_i X^i) \cdot (\sum_i b_i X^i) = \sum_k (\sum_{i=0}^k a_i b_{k-i}) X^k = \sum_k (\sum_{i=0}^k b_{k-i} a_i) X^k = \sum_k (\sum_{j=0}^k b_j a_{k-j}) X^k = (\sum_i b_i X^i) \cdot (\sum_i a_i X^i)$.
   - Multiplicative identity: let $\delta_i = 1$ if $i = 0$ and 0 otherwise, we have $(\sum_i a_i X^i) \cdot (\sum_i \delta_i X^i) = \sum_k (\sum_{i=0}^k a_i \delta_{k-i}) X^k = \sum_k (\sum_{i=0}^{k-1} a_i \cdot 0 + a_k \cdot 1) X^k = \sum_k a_k X^k$;

2. Show that $S = \sum_i s_i X^i$ is a unit if and only if $s_0 \neq 0$.

 Solution: Assume that S is a unit. There exists $T = \sum_i t_i X^i$ such that $\sum_k (\sum_{i=0}^k s_i t_{k-i}) X^k = ST = 1$. The constant coefficient of the series on the left is $\sum_{i=0}^0 s_i t_{k-i} = s_0 t_0$ which must be equal to 1, so s_0 is a unit in K and $s_0 \neq 0$.

 Conversely, assume that $s_0 \neq 0$. We are looking for $T = \sum_i t_i X^i$ such that $1 = ST = \sum_k (\sum_{i=0}^k s_i t_{k-i}) X^k$, i.e. $s_0 t_0 = 1$ and for all $k > 0$, $\sum_{i=0}^k s_i t_{k-i} = 0$. We define t_k by induction on k: $t_0 = s_0^{-1}$ and $t_{k+1} = -s_0^{-1} \sum_{i=0}^k s_{k+1-i} t_i$. It is easy to check that this (the unique) solution to the above equations.

3. Show that $K[[X]]/(X)$ is isomorphic to K.

 Solution: Let $f(\sum_i a_i X^i) = a_0 \in K$. It is easy to check that f is a ring homomorphism. Its kernel is the set of series whose constant coefficient is 0. One can check that $\sum_{i>0} a_i X^i = X \cdot \sum_i a_{i+1} X^i$, so series whose constant coefficient is 0 are all multiple of X. Conversely, $X \sum_i a_i X^i = \sum_{i>0} a_{i-1} X^i$ so multiples of X have constant coefficient 0. It follows that the kernel of f is exactly (X). Moreover, $f(aX^0 + \sum_{i>0} a_i X^i) = a$ so f is surjective. By the first isomorphism theorem, we get that $K[[X]]/(X) \cong K$.

4. Show that every non zero ideal in $K[[X]]$ is of the form (X^n) for some $n \in \mathbb{Z}_{\geqslant 0}$.

 Solution: Let I be an ideal. Let $n \in \mathbb{Z}_{\geqslant 0}$ be the smallest integer such that $X^n \in I$. Then $(X^n) \subseteq I$. Conversely, pick $S = \sum_i s_i X^i \in I$. Let i_0 be minimal such that $s_i \neq 0$. Then $S = \sum_{i \geqslant i_0} s_i X^i = X^{i_0} \sum_i s_{i+i_0} X^i$. Note that $s_{i_0} \neq 0$ so $S^\star = \sum_i s_{i+i_0} X^i$ has non zero constant coefficient and therefore is a unit. So $X^{i_0} = (S^\star)^{-a} S \in I$ and, by minimality $i_0 \geqslant n$. It follows that $S = X^n X^{i_0 - n} S^\star \in (X^n)$ and hence $I = (X^n)$.