Math250aHw5

Trustin Nguyen

October 24, 2023

Exercise 1: Let R be a PID, and $0 \neq p$, $0 \neq q$ prime elements of R (which might be equal or distinct).

- What is the length of a composition series for $R/(p^n)$?

    Proof. We consider the chain of inclusions:

    $$\{0\} \subseteq R/p \subseteq R/(p^2) \subseteq \cdots \subseteq R/(p^{n-1}) \subseteq R/(p^n)$$

    We first show that R/p has no proper submodule. Using the definition of a submodule that $RN \subseteq N$, we consider the homomorphism

    $$\varphi : R \to M$$
    $$\varphi(1) = m$$

    in which we notice that 1 generates R, which will uniquely determine our homomorphism. So the image of the homomorphism will yield the submodules of M. Then because this is a module homomorphism,

    $$a\varphi(1) = am$$

    the kernel of φ would be $am \in (p)$. That means that $p \mid am$, and since p is prime, $p \mid a$ or $p \mid m$. If $p \mid m$, that means that φ was the 0 map. If $p \mid a$, then the kernel would be ideals of R generated by p or in other words, $\ker \varphi = (p)$. Considering either case, by the isomorphism theorem, we have that $R/\ker \varphi$ is isomorphic to either $\{0\}$ or R/p. So there is no proper submodule. Notice that this generalizes for when we want to prove that R/p^i is maximal in R/p^{i+1}. Consider the homomorphism:

    $$\varphi : R \to R/p^{i+1}$$
    $$\varphi(1) = m + (p^{i+1})$$

    So we have

    $$a\varphi(1) = am + (p^{i+1})$$

    By unique factorization, we know that the kernel is of the form (p^k) for some $k \leqslant i + 1$. This is because if there are j factors of p in m, then there are at least $i + 1 - j$ factors of p in a if $am \in \ker \varphi$. So to get the maximal submodule, we quotient by the smallest kernel that does not give us back the same module which is (p^i). So therefore, the maximal submodule of R/p^j is R/p^{j-1} thereby showing that this is a composition series. By Jordan Holder, we know that all other composition series are the same. So the length is $n + 1$. □

- What is the length of a composition series for $R/(p^n q^m)$?

Proof. Consider the chain of inclusions:

$$\{0\} \subseteq R/p \subseteq R/p^2 \subseteq \cdots \subseteq R/p^n \subseteq R/p^n q \subseteq R/p^n q^2 \subseteq \cdots \subseteq R/p^n q^m$$

We know that $\{0\}$ is maximal in R/p as proved in part (a). We know that the first part of the chain is a composition series. To show that the second part is, consider again the action of R on our submodule:

$$a\varphi(1) = am + (p^n q^m)$$

this time starting at $R/p^n q^m$ and working down to lower powers of n, m. Then the smallest kernel we can quotient by would be obtained by either removing a power of p or of q to get either $(p^{n-1} q^m)$ or $(p^n q^{m-1})$. By the Jordan Holder, it tells us that it does not matter. So we continue this process, which tells us that the chain of inclusions above is a composition series. The length of the composition series is $n + m + 1$ which we say is unique by Jordan Holder. $\qquad\square$

- Let R be a PID, and $0 \neq p$ a prime element of R. Compute $\mathrm{Hom}_R(R/(p^n), R/(q^m))$.

  Answer. Consider the fact that every homomorphism is uniquely determined by what 1 maps to. Then we must have:

  $$\varphi(1 + (p^n)) = r + (q^m)$$

  and therefore,
  $$p^n \varphi(1 + (p^n)) = p^n r + (q^m) = 0$$
  so we conclude that $p^n r \in (q^m)$ and therefore:

  $$p^n r = a q^m$$

  We will proceed by cases, and the following claims use unique factorization:

  – If $q^m \mid p^n$, then we have that any mapping of $1 + (p^n)$ will create a module homomorphism. We can check this:

  $$\begin{aligned}
  \varphi(a_1 + (p^n) + a_2 + (p^n)) &= \varphi(a_1 + a_2 + (p^n)) \\
  &= r(a_1 + a_2) + (p^n) \\
  &= ra_1 + ra_2 + (p^n) \\
  &= \varphi(a_1 + p^n) + \varphi(a_2 + (p^n))
  \end{aligned}$$

  And
  $$a \cdot \varphi(b + (p^n)) = a(br + (p^n)) = abr + (p^n) = \varphi(ab + (p^n))$$
  So the number of homomorphisms in this case would be $|R/(q^m)|$ each represented by what 1 maps to in $R/(q^m)$.

  – Otherwise, we could get that $q \mid p$ but $m > n$. In this case, $q^{m-n} \mid r$. So our homomorphisms look like:

  $$1 + (p^n) \mapsto a q^{m-n} + (q^m)$$

  Consider $R/(q^{m-n})$. We observe that the representatives of our homomorphism above denoted a are the elements of this. So there are $|R/(q^{m-n})|$ such homomorphisms and theses are represented by elements of $R/(q^{m-n})$.

  – If $q \nmid p$, then $q^m \mid r$. But that would mean that every homomorphism would be the 0 map.

  So we have calculated $\mathrm{Hom}_R(R/(p^n), R/q^m)$ in three different cases.

- Show that if $H \leqslant G$ and $K \leqslant G$ are any subgroups of a group, then the double cosets HgK and $Hg'K$ are either equal or disjoint, generalizing the fact about ordinary cosets, the case when H is just the identity.

    Proof. We have cases:

    - If $gK = g'K$, then we indeed have $HgK = Hg'K$.

    - If $gK \cap gK = \emptyset$, then we have two more cases. If $h_i gK \cap h_j g'K = \emptyset$ for all $h_i, h_j \in H$, then indeed, we have $HgK \cap Hg'K = \emptyset$.

    - Now if we have that one intersection is nonempty:

    $$h_i gK = h_j g'K$$

    then suppose we have some arbitrary element $h \in H$. Then we take hh_i^{-1} and conclude that:
    $$hgK = hh_i^{-1}h_j g'K$$

    so we have $hgK \subseteq Hg'K$. Do that for all $h \in H$ and take the union of the hgK's. We will have: $HgK \subseteq Hg'K$. By symmetry, we can do a similar argument and conclude that $HgK \supseteq Hg'K$, so we conclude $HgK = Hg'K$.

    so the intersection is either $\emptyset$ or they are equal. $\square$

Exercise 2: Let F be a field, and let $G = GL_n(F)$. The subgroup $B < G$ or upper triangular invertible matrices is called a *Borel* subgroup of G, so that G acts on the vector space F^n. The subgroup $W < G$ of permutation matrices (a single entry in each row and column, all entries equal to 1) is called the *Weyl group* of G.

A *transvection* ae_{ij} with $i \neq j$ is an element of G that has 1's on the diagonal and a single off-diagonal entry at position i, j. It is called an upper triangular transvection if it lies in B, that is, $i < j$. Prove that G is the disjoint union of sets BwB for $w \in W$ by showing:

- Show that $|W| = n!$ and acts as the symmetric group of permutations of the standard basis
    $$\{(1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)\}$$

    for F^n.

    Proof. Consider the i-th row and j-th column of the Weyl matrix which has the entry 1. The action of this on a vector takes the i-th row value and places it in the j-th row. So we can denote a Weyl matrix by 1_{ij} which denotes the action $i \mapsto j$ as representative of sending the i-th entry of a vector to the j-th row. Since none of the i's are equal and none of the j's are equal, we have that the set of 1_{ij}'s form a bijection from $[n]$ to $[n]$. This is because the mapping is both injective and surjective. This is just the number of permutations. Since the action of a matrix uniquely determines the matrix, we have that $|W| = n!$.

    By the action we have shown, it is also a permutation of the standard basis of F^n. $\square$

- If $g \in G$ then there is a product of upper triangular transvections p such that for $i = 1, \ldots, n$ there is a row of pg with the (i, j) entry equal to 0 for all $j < i$.

    Proof. Notice that a transvection multiplication on the left ae_{ij} is a row operation of taking a times the j-th row and adding it to the i-th row. Say that two rows have the same length if their i-th column is non-zero and all columns k for $k < i$ are 0. Suppose that two rows have the same length with the first non-empty entry being a, b respectively. Then we can take $\frac{a}{b}$ times the second row and subtract that our from the first row. So we have two rows of unequal length. We repeat

the process to show that the matrix can be arranged to be upper triangular up to permutation. □

- With p as above, there is an element $w \in W$ such that $wpg = b \in B$ and thus

$$g = p^{-1}w^{-1}b \in BwB$$

This is called the Bruhat decomposition of G with respect to B. One can show that if $w \neq w'$, then $BwB \neq Bw'B$, so the decomposition has $n!$ parts. (The case $n = 2$ is done in Lang on page 539).

Proof. We know that pg is upper triangular if we can permute the rows. Notice that the action of a weyl matrix on a vector as we said before, if the i, j-th row and column contain 1, then it sends the j-th row to the i-row. So we can say that the action of this weyl matrix on a matrix sends the $j-$th row to the $i - $ th row or in other words, permutes the rows. We can permute the rows of our matrix pg somehow to get an upper triangular matrix. We note that p is upper triangular so that means that p^{-1} is upper triangular. So

$$g = p^{-1}w^{-1}b \in BwB$$

Suppose that we have $w \in BwB$. If $w \in Bw'B$, then

$$w = bw'b'$$

or

$$b^{-1} = w'b'w^{-1}$$

If we look at $w'w^{-1}$, that is not the identity matrix because $w \neq w'$. And we notice that

$$b^{-1} = w'\left(d + \begin{bmatrix} 0 & * & \dots & * \\ & 0 & \dots & * \\ & & \ddots & * \\ & & & 0 \end{bmatrix}\right)w^{-1}$$

for some diagonal matrix d. Now we see that $w'dw^{-1}$ has non-zero entries in the same entries where $w'w^{-1}$ has non-zero entries. If we take the second matrix:

$$w'\left(\begin{bmatrix} 0 & * & \dots & * \\ & 0 & \dots & * \\ & & \ddots & * \\ & & & 0 \end{bmatrix}\right)w^{-1}$$

and add it to the first, we will essentially be replacing some of the 0's in $w'dw^{-1}$ with non zero entries, as we know the action of $w'b'w^{-1}$ is just the permutation of rows and columns. So the entries do not interact with each other in any way. Now since $w'w^{-1} \neq \mathrm{id}$, we know that $w'dw^{-1}$ is not upper triangular. So we have that the cosets BwB and $Bw'B$ are not equal. So they are disjoint for $w \neq w'$. □