The Steinberg module and the Hecke algebra
Neil P. Strickland
`https://neil-strickland.staff.shef.ac.uk/research/jordan.pdf`
version of 2 May 2012
Errata and addenda by Darij Grinberg

The list below contains corrections and comments to the preprint "The Steinberg module and the Hecke algebra" by Neil P. Strickland. The comments include alternative proofs and additional details (indeed, most of the comments below are of the latter kind, and they are the main reason why this list is so large). I have written this list while I was reading the preprint (over the course of several months[1]); since I am not myself an expert in the subject, my comments are not always particularly learned (I suspect that many of the proofs I am giving below can be drastically simplified), and they are probably full of mistakes of their own. (I have tried to be detailed, partly in order to avoid mistakes.)

I will refer to the results appearing in Strickland's preprint by the numbers under which they appear in it (specifically, in its version of 2 May 2012, available from `https://neil-strickland.staff.shef.ac.uk/research/jordan.pdf`).

Errata and addenda

- **§2:** I think it would be better if you spent a bit of time defining some of your notations:
  - For any nonnegative integer n, you let Σ_n denote the symmetric group of the set $\{1, 2, \ldots, n\}$. (This is not a notation I have seen very often. Most combinatorialists call it either S_n or $\mathfrak{S}_n$ or $\mathcal{S}_n$.)
  - The composition $\alpha\beta$ of two maps $\alpha : Y \to Z$ and $\beta : X \to Y$ is defined as the map $X \to Z$ that sends each $x \in X$ to $\alpha(\beta(x))$. (This might sound obvious, but irritatingly, a lot of people use the opposite convention for the order of multiplication, particularly when permutations are concerned.)
  - If $\alpha : X \to Y$ is a map, then α_* means the map $\mathcal{P}(X) \to \mathcal{P}(Y)$ canonically induced by α (where $\mathcal{P}(Z)$ denotes the powerset of a set Z). This is the map that sends every subset T of X to the subset $\alpha(T)$ of Y.
- **§2:** Do you ever use the notation $L^+(\sigma)$ that you define in the beginning of §2? (I don't know for sure; just asking.)

[1] The preprint packs a whole lot of material into just 15 pages. Partly, I wish it would proceed more slowly and leave less work to the reader; the below comments fill in lots of details that are omitted.

- **Lemma 2.6:** Replace "Σ" by "Σ_n".
- **Lemma 2.6:** The period at the end of the sentence should be outside of the parentheses.
- **Proof of Proposition 2.11:** After "are disjoint, and", add "we have $\sigma = t^n_{m_n}\tau$; thus, Lemma 2.6 (applied to $t^n_{m_n}$ instead of σ) yields

  $$\overline{L}(\sigma) = \overline{L}(\tau)\,\Delta\tau_*^{-1}\overline{L}\left(t^n_{m_n}\right) = \overline{L}(\tau) \sqcup \tau_*^{-1}\overline{L}\left(t^n_{m_n}\right)$$

  and therefore".
- **Proof of Proposition 2.11:** You have not proven the uniqueness that is claimed in Proposition 2.11. This is not a large gap to fill, and becomes obvious later on[2]; but I think it is worth at least briefly mentioning how it is proven.
- **Definition 2.12:** Replace "there is a canonical map" by "there is a canonical homomorphism".
- **Proof of Proposition 2.13:** You are slightly abusing notation here: When you write "$X_n = \bigcup_{m=1}^n t^n_m X_{n-1}$", you are implicitly suggesting that $\widetilde{\Sigma}_{n-1}$ can be embedded into $\widetilde{\Sigma}_n$. This is correct, but is not obvious until Proposition 2.13 is already proven (at which point it is not useful anymore). A-priori, it is plausible that some nontrivial elements of $\widetilde{\Sigma}_{n-1}$ would collapse to the identity upon adding the extra generator s_{n-1} of $\widetilde{\Sigma}_n$ and the extra relations that come with it.

  Fortunately, the proof is easy to fix, by introducing a group homomorphism $\widetilde{\Sigma}_{n-1} \to \widetilde{\Sigma}_n$: Namely, observe that all the generators and the relations appearing in the definition of $\widetilde{\Sigma}_{n-1}$ also appear in the definition of $\widetilde{\Sigma}_n$ (along with one new generator s_{n-1} and some new relation). Thus, there is a group homomorphism $\eta : \widetilde{\Sigma}_{n-1} \to \widetilde{\Sigma}_n$ sending $s_i \mapsto s_i$ for each $i \in \{1, 2, \ldots, n-2\}$. Consider this η. Regard $\widetilde{\Sigma}_n$ as a right $\widetilde{\Sigma}_{n-1}$-set by having $\widetilde{\Sigma}_{n-1}$ act through η (that is, set $xy = x\eta(y)$ for all $x \in \widetilde{\Sigma}_n$ and $y \in \widetilde{\Sigma}_{n-1}$). Then, $X_n = \bigcup_{m=1}^n t^n_m X_{n-1}$ is still correct (where the implied multiplication in $t^n_m X_{n-1} = \{t^n_m x \mid x \in X_{n-1}\}$ is now to be understood as the $\widetilde{\Sigma}_{n-1}$-action on $\widetilde{\Sigma}_n$). All the rest of the proof goes through unchanged, except for one simple modification (namely, "$\widetilde{\Sigma}_n$ is generated by $\widetilde{\Sigma}_{n-1}$ and s_{n-1}" must become "$\widetilde{\Sigma}_n$ is generated by $\eta\left(\widetilde{\Sigma}_{n-1}\right)$ and s_{n-1}").

[2] Namely: In the proof of Proposition 2.13, you show that the map $\epsilon : X_n \to \Sigma_n$ is surjective. Since $|X_n| \leq n! = |\Sigma_n|$, this entails that the map ϵ also is injective. But this means precisely that no two distinct sequences $(m_1, m_2, \ldots, m_n)$ with $1 \leq m_k \leq k$ give rise to one and the same permutation $t^n_{m_n} t^{n-1}_{m_{n-1}} \cdots t^2_{m_2} t^1_{m_1}$. And this is exactly the uniqueness claim of Proposition 2.11.

- **Proof of Lemma 2.14:** Replace "identity permutation" by "identity of $\widetilde{\Sigma}_n$". (The identification between permutations and elements $\widetilde{\Sigma}_n$ cannot yet be used at this point.)
- **Definition 2.15:** Replace "$s_1, \ldots, s_n$" by "$s_1, \ldots, s_{n-1}$" twice in this definition.
- **Definition 2.15:** Replace "$us_is_js_iv = us_js_is_jv$" by "$us_is_js_iv \sim us_js_is_jv$".
- **Definition 2.15:** Replace "Σ" by "Σ_n" twice in this definition (the second time is inside the commutative diagram). Or just define Σ to be an abbreviation for Σ_n ?
- **Definition 2.15:** Please explain that $\sim$ is defined to be the disjoint union of the relations $\sim_r$ over all $r \in \mathbb{N}$. (This is a relation on $\coprod_r W_r = W$.)
- **Definition 2.17:** At the end of condition (c), add "and the word uv is reduced". Otherwise, condition (c) would always hold!
- **Definition 2.17:** I think the justification for the equivalence of the four conditions would be clearer if you replaced "and it follows from Lemma 2.6 that (a) is equivalent to (d)" by "and it follows from Lemma 2.6 (applied to $\sigma\tau^{-1}$ instead of σ) that (b) is equivalent to (d)".
- **Proof of Lemma 2.18:** Replace "the 3-cycle $(i, i+1, i+2)$" by "the transposition $(i, i+2)$".
- **Proof of Theorem 2.16:** I suspect the LaTeX here is slightly broken: You want to start the proof by "*Proof of Theorem 2.16.*" and not by "*Proof.* Proof of Theorem 2.16.".
- **Proof of Theorem 2.16:** Replace "so $u = v$" by "so $u \sim v$".
- **§2:** I suggest adding the following fact to §2 (which is used later, in §9):

  Corollary 2.19. (a) We have $l\left(\sigma^{-1}\rho\right) = n(n-1)/2 - l(\sigma)$ for each $\sigma \in \Sigma_n$.

  (b) We have $l(\sigma\rho) = n(n-1)/2 - l(\sigma)$ for each $\sigma \in \Sigma_n$.

  (c) We have $l\left(\rho\sigma^{-1}\right) = n(n-1)/2 - l(\sigma)$ for each $\sigma \in \Sigma_n$.

  (d) We have $l(\rho\sigma) = n(n-1)/2 - l(\sigma)$ for each $\sigma \in \Sigma_n$.

  [*Proof of Corollary 2.19.* **(c)** Recall the four equivalent conditions (a), (b), (c) and (d) in Definition 2.17. In particular, the two conditions (b) and (d) are equivalent for each $\sigma \in \Sigma_n$ and $\tau \in \Sigma_n$. In other words, for each $\sigma \in \Sigma_n$ and $\tau \in \Sigma_n$, we have the following equivalence:

$$\left(l\left(\sigma\tau^{-1}\right) = l(\sigma) - l(\tau)\right) \iff \left(\overline{L}(\tau) \subseteq \overline{L}(\sigma)\right). \tag{1}$$

Now, fix $\sigma \in \Sigma_n$. Then, $\overline{L}(\sigma) \subseteq \overline{L}(\rho)$ [3]. But the equivalence (1) (applied to ρ and σ instead of σ and ρ) shows that

$$\left(l\left(\rho\sigma^{-1}\right) = l(\rho) - l(\sigma)\right) \iff \left(\overline{L}(\sigma) \subseteq \overline{L}(\rho)\right).$$

Therefore, we have $l\left(\rho\sigma^{-1}\right) = l(\rho) - l(\sigma)$ (since we have $\overline{L}(\sigma) \subseteq \overline{L}(\rho)$). Thus, $l\left(\rho\sigma^{-1}\right) = \underbrace{l(\rho)}_{=n(n-1)/2} - l(\sigma) = n(n-1)/2 - l(\sigma)$. This proves Corollary 2.19 **(c)**.

(d) Let $\sigma \in \Sigma_n$. Corollary 2.19 **(c)** (applied to σ^{-1} instead of σ) shows that $l\left(\rho\left(\sigma^{-1}\right)^{-1}\right) = n(n-1)/2 - l\left(\sigma^{-1}\right)$. Since $\left(\sigma^{-1}\right)^{-1} = \sigma$, this rewrites as

$$l(\rho\sigma) = n(n-1)/2 - \underbrace{l\left(\sigma^{-1}\right)}_{\substack{=l(\sigma) \\ \text{(by Lemma 2.3)}}} = n(n-1)/2 - l(\sigma).$$

This proves Corollary 2.19 **(d)**.

(a) Let $\sigma \in \Sigma_n$. Then, Lemma 2.3 (applied to $\rho\sigma$ instead of σ) shows that $l\left((\rho\sigma)^{-1}\right) = l(\rho\sigma) = n(n-1)/2 - l(\sigma)$ (by Corollary 2.19 **(d)**). Since $(\rho\sigma)^{-1} = \sigma^{-1}\underbrace{\rho^{-1}}_{=\rho} = \sigma^{-1}\rho$, this rewrites as $l\left(\sigma^{-1}\rho\right) = n(n-1)/2 - l(\sigma)$. This proves Corollary 2.19 **(a)**.

(b) Let $\sigma \in \Sigma_n$. Then, Lemma 2.3 (applied to $\sigma\rho$ instead of σ) shows that $l\left((\sigma\rho)^{-1}\right) = l(\sigma\rho)$. Since $(\sigma\rho)^{-1} = \underbrace{\rho^{-1}}_{=\rho}\sigma^{-1} = \rho\sigma^{-1}$, this rewrites as $l\left(\rho\sigma^{-1}\right) = l(\sigma\rho)$. Hence, $l(\sigma\rho) = l\left(\rho\sigma^{-1}\right) = n(n-1)/2 - l(\sigma)$ (by Corollary 2.19 **(c)**). This proves Corollary 2.19 **(b)**. □]

- **§3:** In the definition of T, a whitespace is missing between "$ge_i \in \mathbb{F}_p e_i$" and "for all i".

[3] *Proof.* Let $U \in \overline{L}(\sigma)$. Then, $U \in \overline{L}(\sigma) = \{\{i,j\} \mid (i,j) \in L(\sigma)\} = \{\{u,v\} \mid (u,v) \in L(\sigma)\}$. In other words, $U = \{u,v\}$ for some $(u,v) \in L(\sigma)$. Fix this (u,v). We have $0 < u < v \leq n$ (since $(u,v) \in L(\sigma)$). The definition of ρ yields $\rho(u) = n+1-u$ and $\rho(v) = n+1-v$. Hence, $\rho(u) = n+1-\underbrace{u}_{<v} > n+1-v = \rho(v)$. Thus, $0 < u < v \leq n$ and $\rho(u) > \rho(v)$. In other words, (u,v) is an element (i,j) such that $0 < i < j \leq n$ and $\rho(i) > \rho(j)$. In other words, $(u,v) \in \{(i,j) \mid 0 < i < j \leq n \text{ and } \rho(u) > \rho(v)\}$. This rewrites as $(u,v) \in L(\rho)$ (since $L(\rho) = \{(i,j) \mid 0 < i < j \leq n \text{ and } \rho(u) > \rho(v)\}$ (by the definition of $L(\rho)$)). Now, recall that $U = \{u,v\}$. Hence, $U = \{i,j\}$ for some $(i,j) \in L(\rho)$ (namely, for $(i,j) = (u,v)$). In other words, $U \in \{\{i,j\} \mid (i,j) \in L(\rho)\}$. This rewrites as $U \in \overline{L}(\rho)$ (since $\overline{L}(\rho) = \{\{i,j\} \mid (i,j) \in L(\rho)\}$ (by the definition of $\overline{L}(\rho)$)).

Now, forget that we fixed U. We thus have shown that $U \in \overline{L}(\rho)$ for each $U \in \overline{L}(\sigma)$. In other words, $\overline{L}(\sigma) \subseteq \overline{L}(\rho)$, qed.

- **§3:** Add a period before "With this convention".
- **§3:** After "and $(g.x)_i = \sum_j g_{ij} x_j$", add "for $x = (x_1, x_2, \ldots, x_n)^T$".
- **§4:** Before Example 4.1, it would be good to say the following: "We shall call $\delta(\underline{U}, \underline{V})$ the *Jordan permutation* of the flags $\underline{U}$ and $\underline{V}$.". This way, the words "Jordan permutation" (which are used in Definition 8.2) are actually defined.
- **§4:** It would also be useful to point out explicitly that $\delta(\underline{U}, \underline{U}) = 1$ for each $\underline{U} \in \operatorname{Flag}(W)$. This is very easy to prove (it is a corollary of Lemma 4.5, but it is also pretty easy to check using just the definition); but I think it's worth explicitly stating.
- **Example 4.1:** At the very beginning of this example, add the following sentence: "Set $\underline{E} = \left(E_0 < E_1 < \cdots < E_n = \mathbb{F}_p^n\right) \in \operatorname{Flag}\left(\mathbb{F}_p^n\right)$.".
- **Example 4.1:** At the end of the last formula on page 5 (the formula that defines Q_{ij}), add a period.
- **Example 4.1:** At the end of the first displayed formula on page 6 (the formula that defines C_{ij}), a closing parenthesis is missing.
- **Example 4.2:** Before "Then Q_{15}", add: "Set $U_i = \operatorname{span}\{u_1, \ldots, u_i\}$ and $V_i = E_i$ for each i.". (Otherwise it is not clear how the Q_{ij} are defined.)
- **Lemma 4.5:** It might be better to split the second sentence of this proposition as follows: "Assume that $U_{i-1} = V_{i-1}$. Then, $\sigma(i) = i$ iff $U_i = V_i$." (Otherwise, the order of precedence between the "then" and the "iff" is ambiguous.)
- **Proof of Proposition 4.7:** Replace "$U_i < V_{i+1}$" by "$U_i \leq V_{i+1}$" (unless you really mean to use the symbol $<$ for not-necessarily-proper submodules; but in that case, you would need to replace several $<$'s by other symbols).
- **Proof of Proposition 4.7:** Remove the word "we" in "Of course we also".
- **Proof of Proposition 4.7:** You replace $\dim(U_i \cap V_i)$ by $i-1$ in the long displayed equation. I would suggest explaining why this is allowed: Namely, you argue that $U_i \cap V_i = A = U_{i-1}$, and thus $\dim(U_i \cap V_i) = \dim(U_{i-1}) = i-1$.
- **Proof of Proposition 4.7:** After "Symmetrically, we have $U_{i+1} = U_i + V_i$.", I would add "Hence, $U_{i+1} = V_{i+1}$.".
- **Proof of Proposition 4.7:** Replace "$U_j = V_j$ for all such j" by "$U_j = V_j$ for all $j \geq i+1$" (since the induction starts at $j = i+1$, not at $j = i+2$).

- **Proof of Lemma 5.1:** After the first sentence, add: "Thus, assume that $g_{ii} = 1$ from now on."

- **Proof of Lemma 5.1:** Replace "iff $a_{ij} = 0$" by "iff $g_{ij} = 0$".

- **Proposition 5.2:** You write: "and thus $|Y(\sigma, \underline{V})| = p^{l(\sigma)}$ for any $\underline{V}$". This is correct, but I find it a bit too nontrivial to just state without further explanation. Maybe it's even worth moving this claim into a separate corollary:

  Corollary 5.2a. Let $\sigma \in \Sigma_n$ and $\underline{V} \in \operatorname{Flag}(W)$, where W is an n-dimensional $\mathbb{F}_p$-vector space. Then, $|Y(\sigma, \underline{V})| = p^{l(\sigma)}$.

  [*Proof of Corollary 5.2a.* Pick a basis $(f_1, f_2, \ldots, f_n)$ of W such that each $0 \leq i \leq n$ satisfies $V_i = \operatorname{span}\{f_1, f_2, \ldots, f_i\}$. (Such a basis exists, because we can start with the empty basis of V_0, then extend it to a basis of V_1, then extend it to a basis of V_2, etc..) Let α be the $\mathbb{F}_p$-linear map $\mathbb{F}_p^n \to W$ that sends each e_k to f_k. Then, α is a vector space isomorphism (since it sends the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$ to the basis $(f_1, f_2, \ldots, f_n)$ of W). Moreover, it satisfies $\alpha E_i = V_i$ for each $0 \leq i \leq n$. In other words, $\alpha \underline{E} = \underline{V}$.

  But the naturality of the definition of $\delta(\underline{U}, \underline{V})$ yields an important fact (which is a slight generalization of your Remark 4.3): If W_1 and W_2 are two $\mathbb{F}_p$-vector spaces, and if $\beta : W_1 \to W_2$ is an isomorphism, then:

  (a) any $\underline{P}, \underline{Q} \in \operatorname{Flag}(W_1)$ satisfy $\delta(\beta\underline{P}, \beta\underline{Q}) = \delta(\underline{P}, \underline{Q})$.

  (b) for any $\sigma \in \Sigma_n$ and any $\underline{Q} \in \operatorname{Flag}(W_1)$, the map $\operatorname{Flag}(W_1) \to \operatorname{Flag}(W_2)$, $\underline{P} \mapsto \beta\underline{P}$ maps the subset $Y(\sigma, \underline{Q})$ bijectively onto $Y(\sigma, \beta\underline{Q})$.

  Applying part (b) of this fact to $W_1 = \mathbb{F}_p^n$, $W_2 = W$, $\beta = \alpha$ and $\underline{Q} = \underline{E}$, we see that the map $\operatorname{Flag}\left(\mathbb{F}_p^n\right) \to \operatorname{Flag}(W)$, $\underline{P} \mapsto \alpha\underline{P}$ maps the subset $Y(\sigma, \underline{E})$ bijectively onto $Y(\sigma, \alpha\underline{E})$. Thus, $|Y(\sigma, \alpha\underline{E})| = |Y(\sigma, \underline{E})|$. Since $\alpha\underline{E} = \underline{V}$ and $Y(\sigma, \underline{E}) = Y(\sigma)$, this rewrites as $|Y(\sigma, \underline{V})| = |Y(\sigma)|$.

  But the first sentence of Proposition 5.2 entails $|Y(\sigma)| = |X(\sigma)| = p^{l(\sigma)}$ (by Lemma 5.1). Hence, $|Y(\sigma, \underline{V})| = |Y(\sigma)| = p^{l(\sigma)}$. This proves Corollary 5.2a. □]

- **Proof of Proposition 5.2:** Replace "that $X(\sigma)$ acts freely on $\sigma\underline{E}$" by "that $X(\sigma)$ acts freely on the $X(\sigma)$-orbit of $\sigma\underline{E}$" (just to use more standard terminology).

- **Proof of Proposition 5.2:** Replace "We claim that there is a unique element $v_i \in V_i \cap T_i$ such that $\epsilon_{\sigma(i)}(v_i) = 1$, and moreover that $v_1, \ldots, v_i$ is a basis for V_i over $\mathbb{F}_p$" by "We claim that, for each $i \in \{1, 2, \ldots, n\}$, there is a unique element $v_i \in V_i \cap T_i$ such that $\epsilon_{\sigma(i)}(v_i) = 1$, and moreover that $v_1, \ldots, v_i$ is a basis for V_i over $\mathbb{F}_p$ (if the elements v_j for all $j < i$ are defined similarly)".

- **Proof of Proposition 5.2:** Add a period at the end of the displayed equation that defines S_i.
- **Proof of Proposition 5.2:** The word "leading term" might use a definition. Actually, it is probably best to introduce a number of related notions **before** the proof of Proposition 5.2:
  - For each $i \in \{1, 2, \ldots, n\}$, let $\epsilon_i : \mathbb{F}_p^n \to \mathbb{F}_p$ be the i-th coordinate projection. Thus, for any $x \in \mathbb{F}_p^n$ and $i \in \{1, 2, \ldots, n\}$, the element $\epsilon_i(x) \in \mathbb{F}_p$ is the i-th coordinate of the vector x.
  - The *leading index* of a nonzero vector $x \in \mathbb{F}_p^n$ is defined to be the highest $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$. This leading index is denoted by $\operatorname{lind}(x)$. The definition of the leading index can be rewritten as follows: The *leading index* of a nonzero vector $x = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_p^n$ is the highest $k \in \{1, 2, \ldots, n\}$ satisfying $\lambda_k \neq 0$.
  - The *leading term* of a nonzero vector $x \in \mathbb{F}_p^n$ is defined to be $\epsilon_k(x) e_k$, where $k = \operatorname{lind}(x)$. In other words, the *leading term* of a nonzero vector $x = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_p^n$ is $\lambda_k e_k$, where k is the highest element of $\{1, 2, \ldots, n\}$ satisfying $\lambda_k \neq 0$.

  Here are some basic properties of leading indices:
  - **Lemma 5.2b.** Let $x \in \mathbb{F}_p^n$ is a nonzero vector.

    (a) If $i \in \{1, 2, \ldots, n\}$ is such that $i > \operatorname{lind}(x)$, then $\epsilon_i(x) = 0$.

    (b) We have $\epsilon_{\operatorname{lind}(x)}(x) \neq 0$.

    [*Proof of Lemma 5.2b:* **(a)** Let $i \in \{1, 2, \ldots, n\}$ be such that $i > \operatorname{lind}(x)$. But $\operatorname{lind}(x)$ is the highest $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$ (by the definition of $\operatorname{lind}(x)$). Hence, every $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$ must satisfy $k \leq \operatorname{lind}(x)$. Applying this to $k = i$, we conclude that if $\epsilon_i(x) \neq 0$, then $i \leq \operatorname{lind}(x)$. Hence, we cannot have $\epsilon_i(x) \neq 0$ (since we cannot have $i \leq \operatorname{lind}(x)$ (since we have $i > \operatorname{lind}(x)$)). In other words, we have $\epsilon_i(x) = 0$. This proves Lemma 5.2b **(a)**.

    (b) We know that $\operatorname{lind}(x)$ is the highest $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$ (by the definition of $\operatorname{lind}(x)$). Hence, $\operatorname{lind}(x)$ is a $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$. Thus, $\epsilon_{\operatorname{lind}(x)}(x) \neq 0$. This proves Lemma 5.2b **(b)**. □]
  - **Lemma 5.2c.** Let $(w_s)_{s \in S}$ be a finite family of nonzero vectors in $\mathbb{F}_p^n$. Assume that the leading indices of the w_s (for $s \in S$) are pairwise distinct.

    (a) Each nonzero vector $x \in \mathbb{F}_p \{w_s \mid s \in S\}$ satisfies

    $$\operatorname{lind}(x) \in \{\operatorname{lind}(w_s) \mid s \in S\}.$$

(b) The family $(w_s)_{s\in S}$ is $\mathbb{F}_p$-linearly independent.

(c) Let $(\lambda_s)_{s\in S} \in \mathbb{F}_p^S$ be a family of elements of $\mathbb{F}_p$. Assume that there exists at least one $s \in S$ satisfying $\lambda_s \neq 0$. Set $x = \sum\limits_{s\in S} \lambda_s w_s$. Then, $x \neq 0$ and $\operatorname{lind}(x) \in \{\operatorname{lind}(w_s) \mid s \in S\}$.

[*Proof of Lemma 5.2c:* **(c)** There exists at least one $s \in S$ satisfying $\lambda_s \neq 0$. Among all these $s \in S$ satisfying $\lambda_s \neq 0$, pick one for which $\operatorname{lind}(w_s)$ is maximum, and denote this s by t. Thus, $\lambda_t \neq 0$, and $\operatorname{lind}(w_t)$ is the highest among the $\operatorname{lind}(w_s)$ for all $s \in S$ satisfying $\lambda_s \neq 0$. As a consequence,

$$\text{every } s \in S \text{ satisfying } \lambda_s \neq 0 \text{ satisfies } \operatorname{lind}(w_s) \leq \operatorname{lind}(w_t) \qquad (2)$$

(since $\operatorname{lind}(w_t)$ is the highest among the $\operatorname{lind}(w_s)$ for all $s \in S$ satisfying $\lambda_s \neq 0$).

Moreover, recall that the leading indices of the w_s (for $s \in S$) are pairwise distinct. In other words,

$$\text{every two distinct elements } p \text{ and } q \text{ of } S \text{ satisfy } \operatorname{lind}(w_p) \neq \operatorname{lind}(w_q). \qquad (3)$$

Now,

$$\epsilon_{\operatorname{lind}(w_t)}(\lambda_s w_s) = 0 \qquad \text{for every } s \in S \text{ satisfying } s \neq t \qquad (4)$$

[4]. Furthermore, if $i \in \{1, 2, \ldots, n\}$ is such that $i > \operatorname{lind}(w_t)$, then

$$\epsilon_i(\lambda_s w_s) = 0 \qquad \text{for every } s \in S \qquad (5)$$

[4] *Proof of (4):* Let $s \in S$ be such that $s \neq t$. Then, (3) (applied to $p = s$ and $q = t$) yields $\operatorname{lind}(w_s) \neq \operatorname{lind}(w_t)$.

If $\lambda_s = 0$, then $\epsilon_{\operatorname{lind}(w_t)}\left(\underbrace{\lambda_s}_{=0} w_s\right) = \epsilon_{\operatorname{lind}(w_t)}(0 w_s) = 0$. Hence, if $\lambda_s = 0$, then (4) holds. Thus, for the rest of this proof of (4), we WLOG asume that $\lambda_s \neq 0$. Hence, (2) shows that $\operatorname{lind}(w_s) \leq \operatorname{lind}(w_t)$. Combining this with $\operatorname{lind}(w_s) \neq \operatorname{lind}(w_t)$, we obtain $\operatorname{lind}(w_s) < \operatorname{lind}(w_t)$. Thus, $\operatorname{lind}(w_t) > \operatorname{lind}(w_s)$. Hence, Lemma 5.2b **(a)** (applied to $x = w_s$ and $i = \operatorname{lind}(w_t)$) yields $\epsilon_{\operatorname{lind}(w_t)}(w_s) = 0$. Thus, $\epsilon_{\operatorname{lind}(w_t)}(\lambda_s w_s) = \lambda_s \underbrace{\epsilon_{\operatorname{lind}(w_t)}(w_s)}_{=0} = 0$. This proves (4).

[5]. If $i \in \{1, 2, \ldots, n\}$ is such that $i > \operatorname{lind}(w_t)$, then

$$\epsilon_i \left(\underbrace{x}_{= \sum\limits_{s \in S} \lambda_s w_s} \right) = \epsilon_i \left(\sum_{s \in S} \lambda_s w_s \right) = \sum_{s \in S} \underbrace{\epsilon_i (\lambda_s w_s)}_{\substack{=0 \\ \text{(by (5))}}}$$
$$= \sum_{s \in S} 0 = 0. \qquad (6)$$

But

$$\epsilon_{\operatorname{lind}(w_t)} \left(\underbrace{x}_{= \sum\limits_{s \in S} \lambda_s w_s} \right)$$
$$= \epsilon_{\operatorname{lind}(w_t)} \left(\sum_{s \in S} \lambda_s w_s \right) = \sum_{s \in S} \epsilon_{\operatorname{lind}(w_t)} (\lambda_s w_s)$$
$$= \underbrace{\epsilon_{\operatorname{lind}(w_t)} (\lambda_t w_t)}_{= \lambda_t \epsilon_{\operatorname{lind}(w_t)} (w_t)} + \sum_{\substack{s \in S; \\ s \neq t}} \underbrace{\epsilon_{\operatorname{lind}(w_t)} (\lambda_s w_s)}_{\substack{=0 \\ \text{(by (4))}}}$$

(here, we have split off the addend for $s = t$ from the sum)

$$= \lambda_t \epsilon_{\operatorname{lind}(w_t)} (w_t) + \underbrace{\sum_{\substack{s \in S; \\ s \neq t}} 0}_{=0} = \underbrace{\lambda_t}_{\neq 0} \underbrace{\epsilon_{\operatorname{lind}(w_t)} (w_t)}_{\substack{\neq 0 \\ \text{(by Lemma 5.2b (b), applied} \\ \text{to } x = w_t)}} \neq 0.$$

Hence, $x \neq 0$. It remains to show that $\operatorname{lind}(x) \in \{\operatorname{lind}(w_s) \mid s \in S\}$. But $\operatorname{lind}(w_t)$ is a $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$ (since $\epsilon_{\operatorname{lind}(w_t)}(x) \neq 0$). Moreover, $\operatorname{lind}(w_t)$ is the **highest** such k (because any $i \in \{1, 2, \ldots, n\}$ satisfying $i > \operatorname{lind}(w_t)$ satisfies $\epsilon_i(x) = 0$ (by (6))). Thus, $\operatorname{lind}(w_t)$ is the highest $k \in \{1, 2, \ldots, n\}$ satisfying $\epsilon_k(x) \neq 0$. In other words, $\operatorname{lind}(w_t)$ is the leading index of x (by the definition of the leading index). In other words, $\operatorname{lind}(w_t) = \operatorname{lind}(x)$. Thus,

$$\operatorname{lind}(x) = \operatorname{lind}(w_t) \in \{\operatorname{lind}(w_s) \mid s \in S\}.$$

This completes the proof of Lemma 5.2c **(c)**.

[5] *Proof of (5):* Let $s \in S$. If $\lambda_s = 0$, then $\epsilon_i \left(\underbrace{\lambda_s}_{=0} w_s \right) = \epsilon_i(0 w_s) = 0$. Hence, if $\lambda_s = 0$, then (5) holds. Thus, for the rest of this proof of (5), we WLOG asume that $\lambda_s \neq 0$. Hence, (2) shows that $\operatorname{lind}(w_s) \leq \operatorname{lind}(w_t) < i$ (since $i > \operatorname{lind}(w_t)$). Thus, $i > \operatorname{lind}(w_s)$. Hence, Lemma 5.2b **(a)** (applied to $x = w_s$) yields $\epsilon_i(w_s) = 0$. Thus, $\epsilon_i(\lambda_s w_s) = \lambda_s \underbrace{\epsilon_i(w_s)}_{=0} = 0$. This proves (5).

(b) Let $(\lambda_s)_{s\in S} \in \mathbb{F}_p^S$ be a family of elements of $\mathbb{F}_p$ satisfying $\sum\limits_{s\in S} \lambda_s w_s = 0$. Thus, $0 = \sum\limits_{s\in S} \lambda_s w_s$. Then, no $s \in S$ satisfies $\lambda_s \neq 0$ [6]. In other words, every $s \in S$ satisfies $\lambda_s = 0$.

Now, forget that we fixed $(\lambda_s)_{s\in S}$. We thus have shown that if $(\lambda_s)_{s\in S} \in \mathbb{F}_p^S$ is a family of elements of $\mathbb{F}_p$ satisfying $\sum\limits_{s\in S} \lambda_s w_s = 0$, then every $s \in S$ satisfies $\lambda_s = 0$. In other words, the family $(w_s)_{s\in S}$ is $\mathbb{F}_p$-linearly independent. This proves Lemma 5.2c **(b)**.

(a) Let $x \in \mathbb{F}_p \{w_s \mid s \in S\}$ be a nonzero vector. We must prove that $\operatorname{lind}(x) \in \{\operatorname{lind}(w_s) \mid s \in S\}$.

We have $x \in \mathbb{F}_p \{w_s \mid s \in S\}$. Hence, we can write x in the form $x = \sum\limits_{s\in S} \lambda_s w_s$ for some elements λ_s of $\mathbb{F}_p$. Consider these λ_s. There exists at least one $s \in S$ satisfying $\lambda_s \neq 0$ [7]. Thus, Lemma 5.2c **(c)** yields $x \neq 0$ and $\operatorname{lind}(x) \in \{\operatorname{lind}(w_s) \mid s \in S\}$. This proves Lemma 5.2c **(a)**. □]

- **Lemma 5.2d.** If $\mathfrak{W}$ is a vector subspace of $\mathbb{F}_p^n$, then

$$\dim \mathfrak{W} = |\{\operatorname{lind}(x) \mid x \in \mathfrak{W} \setminus \{0\}\}|.$$

[*Proof of Lemma 5.2d (sketched).* Lemma 5.2d is well-known and not hard to prove. We shall only use it on one occasion, which is not central to our argument; thus, I shall only outline the proof.

Define the *energy* of a basis $(w_1, w_2, \ldots, w_k)$ of $\mathfrak{W}$ to be the nonnegative integer $\operatorname{lind}(w_1) + \operatorname{lind}(w_2) + \cdots + \operatorname{lind}(w_k)$. Then, there clearly exists a basis $(w_1, w_2, \ldots, w_k)$ having minimum energy. Fix such a basis[8]. Then, no two among the elements $w_1, w_2, \ldots, w_k$ can have equal leading indices (because if w_i and w_j had equal leading indices for some i and j, then we could replace w_j by some linear combination $\alpha w_i + w_j$ with $\alpha \in \mathbb{F}_p$, and by choosing α and β appropriately we would ensure that $\operatorname{lind}(\alpha w_i + w_j) < \operatorname{lind}(w_j)$, so that the resulting basis would have a smaller energy than $(w_1, w_2, \ldots, w_k)$; but this

[6] *Proof.* Assume the contrary. Thus, there exists at least one $s \in S$ satisfying $\lambda_s \neq 0$. Hence, Lemma 5.2c **(c)** (applied to $x = 0$) yields $0 \neq 0$ and $\operatorname{lind}(0) \in \{\operatorname{lind}(w_s) \mid s \in S\}$. But $0 \neq 0$ is clearly absurd. Hence, we have obtained a contradiction. This shows that our assumption was wrong. Qed.

[7] *Proof.* Assume the contrary. Thus, $\lambda_s = 0$ for all $s \in S$. Now, $x = \sum\limits_{s\in S} \underbrace{\lambda_s}_{=0} w_s = \sum\limits_{s\in S} 0 w_s = 0$. This contradicts the fact that x is nonzero. This contradiction shows that our assumption was wrong, qed.

[8] This argument is not constructive, but we could easily replace it by a constructive argument by induction.

would contradict our choice of $(w_1, w_2, \ldots, w_k)$ as the basis with minimum energy). Hence, the indices of the elements $w_1, w_2, \ldots, w_k$ are distinct. Thus, $|\{\operatorname{lind}(x) \mid x \in \mathfrak{W} \setminus \{0\}\}| \geq k = \dim \mathfrak{W}$. It remains to prove that $\dim \mathfrak{W} \geq |\{\operatorname{lind}(x) \mid x \in \mathfrak{W} \setminus \{0\}\}|$. In order to do so, we assume the contrary. Thus, $|\{\operatorname{lind}(x) \mid x \in \mathfrak{W} \setminus \{0\}\}| > \dim \mathfrak{W} = k$. Hence, there exists some $x \in \mathfrak{W} \setminus \{0\}$ such that $\operatorname{lind}(x)$ equals none of $\operatorname{lind}(w_1), \operatorname{lind}(w_2), \ldots, \operatorname{lind}(w_k)$. Consider the x. The $k+1$ nonzero vectors $w_1, w_2, \ldots, w_k, x$ in $\mathbb{F}_p^n$ have the property that their leading indices are pairwise distinct. Thus, Lemma 5.2c **(b)** shows that they are $\mathbb{F}_p$-linearly independent. Since these $k+1$ vectors all belong to $\mathfrak{W}$, we thus have found $k+1$ linearly independent vectors in $\mathfrak{W}$. But this contradicts the fact that $\dim \mathfrak{W} = k < k+1$. This contradiction completes our proof. □]

- **Proof of Proposition 5.2:** Before the sentence that begins with "The leading terms", I would suggest adding the following text: "For each $j < i$, the leading term of the vector v_j is $e_{\sigma(j)}$ (since $e_j \in V_j \cap T_j \subseteq T_j \subseteq E_{\sigma(j)}$ and $\epsilon_{\sigma(j)}(v_j) = 1$). Hence, the leading terms of the vectors v_j in S_i are precisely the vectors $e_{\sigma(j)}$ with $j < i$ and $\sigma(j) < \sigma(i)$. In other words,".

- **Proof of Proposition 5.2:** Before the sentence that begins with "Using this, we see that $E_{\sigma(i)} = S_i \oplus T_i$", I would add the following: "Now, consider the vectors v_j spanning S_i and the vectors e_m spanning T_i. Altogether, these are $\sigma(i)$ vectors lying in the $\sigma(i)$-dimensional space $E_{\sigma(i)}$. Each of the vectors e_m with $m \leq \sigma(i)$ is the leading term of exactly one of these $\sigma(i)$ vectors (as we have just shown). Thus, each of the numbers $1, 2, \ldots, \sigma(i)$ is the leading index of exactly one of these $\sigma(i)$ vectors. Consequently, the leading indices of these $\sigma(i)$ vectors are pairwise distinct. Lemma 5.2c **(b)** (applied to the family of these $\sigma(i)$ vectors) therefore shows that these $\sigma(i)$ vectors are $\mathbb{F}_p$-.linearly independent. Hence, these $\sigma(i)$ vectors form a basis of $E_{\sigma(i)}$ (because they are $\sigma(i)$ linearly independent vectors lying in the $\sigma(i)$-dimensional space $E_{\sigma(i)}$).".

- **Proof of Proposition 5.2:** You claim that "and thus that $V_i \cap E_{\sigma(i)} = S_i \oplus L_i$ for some (unique) subspace $L_i \leq T_i$". It would be friendlier to the reader to explain why this follows.

  Namely, you are using the following (easy) fact from linear algebra: If $\mathfrak{A}$ and $\mathfrak{B}$ are two subspaces of a vector space $\mathfrak{V}$, and if $\mathfrak{C}$ is a subspace of $\mathfrak{V}$ satisfying $\mathfrak{A} \leq \mathfrak{C} \leq \mathfrak{A} \oplus \mathfrak{B}$, then there is a unique subspace $\mathfrak{D} \leq \mathfrak{B}$ satisfying $\mathfrak{C} = \mathfrak{A} \oplus \mathfrak{D}$. (Namely, this $\mathfrak{D}$ can be constructed as $\mathfrak{D} = \mathfrak{C} \cap \mathfrak{B}$.)

  Applying this fact to $\mathfrak{V} = \mathbb{F}_p^n$, $\mathfrak{A} = S_i$, $\mathfrak{B} = T_i$ and $\mathfrak{C} = V_i \cap E_{\sigma(i)}$ (and renaming $\mathfrak{D}$ as L_i) shows that there is a unique subspace $L_i \leq T_i$ satisfying $V_i \cap E_{\sigma(i)} = S_i \oplus L_i$ (since $S_i \leq V_i \cap E_{\sigma(i)} \leq E_{\sigma(i)} = S_i \oplus T_i$). This is exactly your claim. □

- **Proof of Proposition 5.2:** You claim that "$S_i = V_{i-1} \cap E_{\sigma(i)}$" and write that "This is straightforward". Again, I do not agree that this is straightforward enough to be left to the reader. Let me flesh out this proof; more precisely, let me give one proof of the fact that $S_i = V_{i-1} \cap E_{\sigma(i)}$, and one alternative proof of the existence of v_i that sidesteps this and other confusing points in your proof.

  Proof of $S_i = V_{i-1} \cap E_{\sigma(i)}$: Let $x \in \left(V_{i-1} \cap E_{\sigma(i)}\right) \setminus \{0\}$. Thus, x is nonzero. Also, $x \in \left(V_{i-1} \cap E_{\sigma(i)}\right) \setminus \{0\} \subseteq V_{i-1} \cap E_{\sigma(i)} \subseteq E_{\sigma(i)}$, so that $\operatorname{lind}(x) \in \{1,2,\ldots,\sigma(i)\}$. But we also have

  $$\begin{aligned} x &\in \left(V_{i-1} \cap E_{\sigma(i)}\right) \setminus \{0\} \subseteq V_{i-1} \cap E_{\sigma(i)} \\ &\subseteq V_{i-1} = \mathbb{F}_p\{v_1, v_2, \ldots, v_{i-1}\} = \mathbb{F}_p\{v_j \mid j \in \{1,2,\ldots,i-1\}\}. \end{aligned}$$

  For each $j < i$, the leading term of v_j is $e_{\sigma(j)}$ (since $e_j \in V_j \cap T_j \leq T_j \leq E_{\sigma(j)}$ and $\epsilon_{\sigma(j)}(v_j) = 1$). Thus, for each $j < i$, the leading index of v_j is $\sigma(j)$. Thus, the leading indices of $v_1, v_2, \ldots, v_{i-1}$ are $\sigma(1), \sigma(2), \ldots, \sigma(i-1)$. Therefore, these leading indices are pairwise distinct (since σ is injective). In other words, the family $(v_j)_{j \in \{1,2,\ldots,i-1\}}$ of nonzero vectors in $\mathbb{F}_p^n$ has the property that the leading indices of the v_j (for $j \in \{1,2,\ldots,i-1\}$) are pairwise distinct. Thus, Lemma 5.2c **(c)** (applied to $\{1,2,\ldots,i-1\}$ and $(v_j)_{j \in \{1,2,\ldots,i-1\}}$ instead of S and $(w_s)_{s \in S}$) shows that

  $$\begin{aligned} \operatorname{lind}(x) &\in \left\{\operatorname{lind}(v_j) \mid j \in \{1,2,\ldots,i-1\}\right\} \\ &\qquad \left(\text{since } x \in \mathbb{F}_p\{v_j \mid j \in \{1,2,\ldots,i-1\}\} \text{ is a nonzero vector}\right) \\ &= \left\{ \underbrace{\operatorname{lind}(v_j)}_{\substack{=\sigma(j) \\ (\text{since the leading index of } v_j \text{ is } \sigma(j))}} \mid j < i \right\} = \{\sigma(j) \mid j < i\}. \end{aligned}$$

  Combining this with $\operatorname{lind}(x) \in \{1,2,\ldots,\sigma(i)\}$, we find

  $$\begin{aligned} \operatorname{lind}(x) &\in \{1,2,\ldots,\sigma(i)\} \cap \{\sigma(j) \mid j < i\} \\ &= \{\sigma(j) \mid j < i \text{ and } \sigma(j) < \sigma(i)\}. \end{aligned}$$

  Now, forget that we fixed x. We thus have proven that $\operatorname{lind}(x) \in \{\sigma(j) \mid j < i \text{ and } \sigma(j) < \sigma(i)\}$ for each $x \in \left(V_{i-1} \cap E_{\sigma(i)}\right) \setminus \{0\}$. In other words,

  $$\begin{aligned} &\left\{\operatorname{lind}(x) \mid x \in \left(V_{i-1} \cap E_{\sigma(i)}\right) \setminus \{0\}\right\} \\ &\subseteq \{\sigma(j) \mid j < i \text{ and } \sigma(j) < \sigma(i)\}. \end{aligned} \tag{7}$$

But Lemma 5.2d (applied to $\mathfrak{W} = V_{i-1} \cap E_{\sigma(i)}$) yields

$$\begin{aligned}
\dim\left(V_{i-1} \cap E_{\sigma(i)}\right) &= \left|\left\{\operatorname{lind}(x) \mid x \in \left(V_{i-1} \cap E_{\sigma(i)}\right) \setminus \{0\}\right\}\right| \\
&\leq \left|\{\sigma(j) \mid j < i \text{ and } \sigma(j) < \sigma(i)\}\right| \qquad \text{(because of (7))} \\
&= \left|\{j \mid j < i \text{ and } \sigma(j) < \sigma(i)\}\right| \qquad (8)
\end{aligned}$$

(since the map σ is injective).

But $(v_1, v_2, \ldots, v_{i-1})$ is a basis for V_{j-1} (by the induction hypothesis). Hence, the vectors $v_1, v_2, \ldots, v_{i-1}$ are linearly independent. Thus, the vectors v_j for all $j < i$ satisfying $\sigma(j) < \sigma(i)$ are also linearly independent (since these vectors form a subfamily of the vectors $v_1, v_2, \ldots, v_{i-1}$), and therefore distinct. The definition of S_i yields that the vector space S_i is spanned by these vectors v_j for all $j < i$ satisfying $\sigma(j) < \sigma(i)$. Therefore, these vectors v_j for all $j < i$ satisfying $\sigma(j) < \sigma(i)$ form a basis of S_i (because they are linearly independent). Hence, the dimension of S_i equals the number of these vectors. In other words,

$$\begin{aligned}
\dim(S_i) &= \left|\left\{v_j \mid j < i \text{ and } \sigma(j) < \sigma(i)\right\}\right| \\
&= \left|\{j \mid j < i \text{ and } \sigma(j) < \sigma(i)\}\right| \\
&\qquad \left(\text{since the vectors } v_j \text{ for all } j < i \text{ satisfying } \sigma(j) < \sigma(i) \text{ are distinct}\right) \\
&\geq \dim\left(V_{i-1} \cap E_{\sigma(i)}\right) \qquad (\text{by (8)}). \qquad (9)
\end{aligned}$$

On the other hand, $S_i \leq V_{i-1} \cap E_{\sigma(i)}$ (this follows by combining

$$S_i = \mathbb{F}_p \underbrace{\left\{v_j \mid j < i \text{ and } \sigma(j) < \sigma(i)\right\}}_{\subseteq \left\{v_j \mid j < i\right\}} \subseteq \mathbb{F}_p \left\{v_j \mid j < i\right\} = V_{i-1}$$

with

$$S_i = \mathbb{F}_p \left\{v_j \mid j < i \text{ and } \sigma(j) < \sigma(i)\right\} \subseteq E_{\sigma(i)}$$
$$\left(\begin{array}{c} \text{since each } j < i \text{ satisfying } \sigma(j) < \sigma(i) \text{ satisfies} \\ \operatorname{lind}\left(v_j\right) = \sigma(j) \in \{1, 2, \ldots, \sigma(i)\} \text{ and thus} \\ v_j \in \mathbb{F}_p \left\{e_1, e_2, \ldots, e_{\sigma(i)}\right\} = E_{\sigma(i)} \end{array}\right)$$

). Thus, S_i is a vector subspace of the finite-dimensional vector space $V_{i-1} \cap E_{\sigma(i)}$. Since the dimension of this subspace S_i is at least as high as the dimension of $V_{i-1} \cap E_{\sigma(i)}$ (indeed, this is what (9) says), we conclude that this subspace S_i is the whole $V_{i-1} \cap E_{\sigma(i)}$. In other words, $S_i = V_{i-1} \cap E_{\sigma(i)}$, qed. □

Alternative proof of the existence of an $v_i \in V_i \cap T_i$ such that $\epsilon_{\sigma(i)}(v_i) = 1$ and moreover that $v_1, v_2, \ldots, v_i$ is a basis for V_i over $\mathbb{F}_p$: Let me now show another way to prove that there is an element $v_i \in V_i \cap T_i$ such that $\epsilon_{\sigma(i)}(v_i) = 1$ and moreover that $v_1, v_2, \ldots, v_i$ is a basis for V_i over $\mathbb{F}_p$. This argument will not show the uniqueness of this v_i (but you don't ever use this uniqueness anyway).

I proceed by induction over i (as you do). As in your proof, I define S_i, and show that $S_i \leq V_i \cap E_{\sigma(i)}$ and that $E_{\sigma(i)} = S_i \oplus T_i$.

But $\underline{V} \in Y(\sigma) = Y(\sigma, \underline{E})$. In other words, $\delta(\underline{V}, \underline{E}) = \sigma$ (by the definition of $Y(\sigma, \underline{E})$). By the definition of δ, this yields that $Q_{i,\sigma(i)} \neq 0$, where $Q_{i,j} = \dfrac{V_i \cap E_j}{V_{i-1} \cap E_j + V_i \cap E_{j-1}}$. In other words,

$$\frac{V_i \cap E_{\sigma(i)}}{V_{i-1} \cap E_{\sigma(i)} + V_i \cap E_{\sigma(i)-1}} \neq 0.$$

Hence,

$$V_i \cap E_{\sigma(i)} > V_{i-1} \cap E_{\sigma(i)} + V_i \cap E_{\sigma(i)-1} \geq V_i \cap E_{\sigma(i)-1}. \tag{10}$$

Now, $\epsilon_{\sigma(i)} \mid_{V_i \cap E_{\sigma(i)}} \neq 0$ [9]. Hence, the $\mathbb{F}_p$-linear map $\epsilon_{\sigma(i)} \mid_{V_i \cap E_{\sigma(i)}} : V_i \cap E_{\sigma(i)} \to \mathbb{F}_p$ has rank ≥ 1, and therefore must be surjective (since its target is the 1-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p$). Therefore, there exists some $x \in V_i \cap E_{\sigma(i)}$ satisfying $\left(\epsilon_{\sigma(i)} \mid_{V_i \cap E_{\sigma(i)}}\right)(x) = 1$. Consider this x.

We have $\epsilon_{\sigma(i)}(x) = \left(\epsilon_{\sigma(i)} \mid_{V_i \cap E_{\sigma(i)}}\right)(x) = 1$. Furthermore, $x \in V_i \cap E_{\sigma(i)} \subseteq E_{\sigma(i)} = S_i \oplus T_i$. In other words, there exist $y \in S_i$ and $z \in T_i$ such that $x = y + z$. Consider these y and z. We have $x \in V_i \cap E_{\sigma(i)} \leq V_i$ and $y \in S_i \leq V_i \cap E_{\sigma(i)} \leq V_i$. Now, $x = y + z$, so that $z = x - y \in V_i$ (since $x \in V_i$ and $y \in V_i$, and since V_i is an $\mathbb{F}_p$-vector space). Combining this with $z \in T_i$, we obtain $z \in V_i \cap T_i$.

For each $j < i$, the leading term of v_j is $e_{\sigma(j)}$ (since $e_j \in V_j \cap T_j \leq T_j \leq E_{\sigma(j)}$ and $\epsilon_{\sigma(j)}(v_j) = 1$). Thus, for each $j < i$, the leading index of v_j is $\sigma(j)$. In

[9] *Proof.* Assume the contrary. Thus, $\epsilon_{\sigma(i)} \mid_{V_i \cap E_{\sigma(i)}} = 0$.

Fix $x \in V_i \cap E_{\sigma(i)}$. Then, $x \in V_i \cap E_{\sigma(i)} \subseteq E_{\sigma(i)} = \mathbb{F}_p \left\{e_1, e_2, \ldots, e_{\sigma(i)}\right\}$. Also, $x \in V_i \cap E_{\sigma(i)}$, so that $\epsilon_{\sigma(i)}(x) = \underbrace{\left(\epsilon_{\sigma(i)} \mid_{V_i \cap E_{\sigma(i)}}\right)}_{=0}(x) = 0$. In other words, the $\sigma(i)$-th coordinate of the vector x is 0. Combining this with $x \in \mathbb{F}_p \left\{e_1, e_2, \ldots, e_{\sigma(i)}\right\}$, we conclude $x \in \mathbb{F}_p \left\{e_1, e_2, \ldots, e_{\sigma(i)-1}\right\} = E_{\sigma(i)-1}$. Combining $x \in V_i \cap E_{\sigma(i)} \subseteq V_i$ with $x \in E_{\sigma(i)-1}$, we find $x \in V_i \cap E_{\sigma(i)-1}$.

Now, forget that we fixed x. We thus have proven that $x \in V_i \cap E_{\sigma(i)-1}$ for each $x \in V_i \cap E_{\sigma(i)}$. In other words, $V_i \cap E_{\sigma(i)} \subseteq V_i \cap E_{\sigma(i)-1}$. Hence, $V_i \cap E_{\sigma(i)-1}$ is not a proper subset of $V_i \cap E_{\sigma(i)}$. This contradicts (10). This contradiction shows that our assumption was wrong, qed.

other words, for each $j < i$, we have $\operatorname{lind}\left(v_j\right) = \sigma\left(j\right)$. Thus, every $j < i$ satisfying $\sigma\left(j\right) < \sigma\left(i\right)$ must satisfy

$$\operatorname{lind}\left(v_j\right) = \sigma\left(j\right) \in \left\{1, 2, \ldots, \sigma\left(i\right) - 1\right\} \qquad \left(\text{since } \sigma\left(j\right) < \sigma\left(i\right)\right)$$

and therefore

$$v_j \in \mathbb{F}_p \left\{e_1, e_2, \ldots, e_{\sigma(i)-1}\right\} = E_{\sigma(i)-1}. \tag{11}$$

Now,

$$y \in S_i = \mathbb{F}_p \left\{v_j \mid j < i \text{ and } \sigma\left(j\right) < \sigma\left(i\right)\right\} \subseteq E_{\sigma(i)-1}$$
$$\left(\text{since each } j < i \text{ satisfying } \sigma\left(j\right) < \sigma\left(i\right) \text{ satisfies (11)}\right)$$

and thus $\epsilon_{\sigma(i)}\left(y\right) = 0$. Now,

$$\epsilon_{\sigma(i)}\left(\underbrace{x}_{=y+z}\right) = \epsilon_{\sigma(i)}\left(y+z\right) = \underbrace{\epsilon_{\sigma(i)}\left(y\right)}_{=0} + \epsilon_{\sigma(i)}\left(z\right) = \epsilon_{\sigma(i)}\left(z\right).$$

Comparing this with $\epsilon_{\sigma(i)}\left(x\right) = 1$, we find $\epsilon_{\sigma(i)}\left(z\right) = 1$.

Furthermore, $z \notin V_{i-1}$ [10].

[10] *Proof.* Assume the contrary. Then, $z \in V_{i-1} = \mathbb{F}_p\left\{v_1, v_2, \ldots, v_{i-1}\right\} = \mathbb{F}_p\left\{v_j \mid j \in \left\{1, 2, \ldots, i-1\right\}\right\}$. Also, z is nonzero (since $\epsilon_{\sigma(i)}\left(z\right) = 1 \neq 0$).

For each $j < i$, the leading term of v_j is $e_{\sigma(j)}$ (as we have already seen). Thus, for each $j < i$, the leading index of v_j is $\sigma\left(j\right)$. Thus, the leading indices of $v_1, v_2, \ldots, v_{i-1}$ are $\sigma\left(1\right), \sigma\left(2\right), \ldots, \sigma\left(i-1\right)$. Therefore, these leading indices are pairwise distinct (since σ is injective). In other words, the family $\left(v_j\right)_{j\in\{1,2,\ldots,i-1\}}$ of nonzero vectors in $\mathbb{F}_p^n$ has the property that the leading indices of the v_j (for $j \in \left\{1, 2, \ldots, i-1\right\}$) are pairwise distinct. Thus, Lemma 5.2c **(c)** (applied to $\left\{1, 2, \ldots, i-1\right\}$, $\left(v_j\right)_{j\in\{1,2,\ldots,i-1\}}$ and z instead of S, $\left(w_s\right)_{s\in S}$ and x) shows that

$$\begin{aligned}\operatorname{lind}\left(z\right) &\in \left\{\operatorname{lind}\left(v_j\right) \mid j \in \left\{1, 2, \ldots, i-1\right\}\right\} \\ &\qquad \left(\text{since } z \in \mathbb{F}_p\left\{v_j \mid j \in \left\{1, 2, \ldots, i-1\right\}\right\} \text{ is a nonzero vector}\right) \\ &= \left\{\underbrace{\operatorname{lind}\left(v_j\right)}_{\substack{=\sigma(j) \\ \text{(since the leading index of } v_j \text{ is } \sigma(j))}} \mid j < i\right\} = \left\{\sigma\left(j\right) \mid j < i\right\}.\end{aligned}$$

But $z \in T_i \leq E_{\sigma(i)} = \mathbb{F}_p\left\{e_1, e_2, \ldots, e_{\sigma(i)}\right\}$. Hence, the k-th coordinate of z is 0 for all $k > \sigma\left(i\right)$. But the $\sigma\left(i\right)$-th coordinate of z is $\epsilon_{\sigma(i)}\left(z\right) = 1 \neq 0$. Combining the preceding two sentences, we conclude that the leading index of z is $\sigma\left(i\right)$. In other words, $\operatorname{lind}\left(z\right) = \sigma\left(i\right)$. Hence, $\sigma\left(i\right) = \operatorname{lind}\left(z\right) \in \left\{\sigma\left(j\right) \mid j < i\right\}$, so that $\sigma\left(i\right) = \sigma\left(j\right)$ for some $j < i$. This is absurd, since σ is injective. Thus, we have obtained a contradiction. This completes our proof of the fact that $z \notin V_{i-1}$.

Finally, the list $v_1, v_2, \ldots, v_{i-1}, z$ is a basis for V_i over $\mathbb{F}_p$ [11].

Thus, we have shown that z is an element of $V_i \cap T_i$ such that $\epsilon_{\sigma(i)}(z) = 1$ and moreover that $v_1, v_2, \ldots, v_{i-1}, z$ is a basis for V_i over $\mathbb{F}_p$. Hence, there is an element $v_i \in V_i \cap T_i$ such that $\epsilon_{\sigma(i)}(v_i) = 1$ and moreover that $v_1, v_2, \ldots, v_i$ is a basis for V_i over $\mathbb{F}_p$ (namely, $v_i = z$). This completes our proof. (As I have said, the uniqueness of this v_i is not proven here, but it is not needed in your argument either.) □

- **Proof of Proposition 5.2:** Before the words "Now define g", add the following sentences: "Notice that, for each $i \in \{1, 2, \ldots, n\}$, the leading term of v_i is $e_{\sigma(i)}$ (because $v_i \in T_i \leq E_{\sigma(i)} = \mathbb{F}_p \left\{e_1, e_2, \ldots, e_{\sigma(i)}\right\}$ has its $\sigma(i)$-th coordinate equal to $\epsilon_{\sigma(i)}(v_i) = 1$). Hence, for each $i \in \{1, 2, \ldots, n\}$, the leading term of $v_{\sigma^{-1}(i)}$ is e_i."
- **Proof of Proposition 5.2:** Replace "Now define g" by "Now define an $\mathbb{F}_p$-linear map g".
- **Proof of Proposition 5.2:** Replace "$\mathbb{F}_p \left\{e_{\sigma(k)}, e_{\sigma(k+1)}, \ldots, e_{\sigma(m)}\right\}$" by "$\mathbb{F}_p \left\{e_{\sigma(k)}, e_{\sigma(k+1)}, \ldots, e_{\sigma(n)}\right\}$".
- **Proof of Proposition 5.2:** Replace "so $\sigma^{-1} g \sigma$ is a lower-triangular matrix" by: "so $\sigma^{-1} g \sigma(e_k) \in \mathbb{F}_p \{e_k, e_{k+1}, \ldots, e_n\}$. Hence, $\sigma^{-1} g \sigma$ is a lower-triangular matrix".
- **Proof of Proposition 5.2:** Replace "so $g \in U^{\rho\sigma^{-1}}$" by "so $g \in U^{\rho\sigma^{-1}} = U^{(\sigma\rho)^{-1}}$".

[11] *Proof.* We have $V_{i-1} + \mathbb{F}_p z > V_{i-1}$ (since $z \in \mathbb{F}_p z \subseteq V_{i-1} + \mathbb{F}_p z$ but $z \notin V_{i-1}$). Hence, $\dim\left(V_{i-1} + \mathbb{F}_p z\right) > \dim\left(V_{i-1}\right) = i - 1$. Since $\dim\left(V_{i-1} + \mathbb{F}_p z\right)$ and $i - 1$ are integers, this entails that $\dim\left(V_{i-1} + \mathbb{F}_p z\right) \geq (i-1) + 1 = i = \dim\left(V_i\right)$. Furthermore, $\underbrace{V_{i-1}}_{\leq V_i} + \underbrace{\mathbb{F}_p z}_{\substack{\leq V_i \\ (\text{since } z \in V_i)}} \leq V_i + V_i = V_i$.

Now, it is well-known that if $\mathfrak{U}$ is a subspace of a finite-dimensional vector space $\mathfrak{V}$, and if $\dim \mathfrak{U} \geq \dim \mathfrak{V}$, then $\mathfrak{U} = \mathfrak{V}$. Applying this to $\mathfrak{U} = V_{i-1} + \mathbb{F}_p z$ and $\mathfrak{V} = V_i$, we obtain $V_{i-1} + \mathbb{F}_p z = V_i$ (since $V_{i-1} + \mathbb{F}_p z$ is a subspace of V_i and satisfies $\dim\left(V_{i-1} + \mathbb{F}_p z\right) \geq \dim\left(V_i\right)$). Now,

$$\mathbb{F}_p \{v_1, v_2, \ldots, v_{i-1}, z\} = \underbrace{\mathbb{F}_p \{v_1, v_2, \ldots, v_{i-1}\}}_{\substack{= V_{i-1} \\ (\text{since } (v_1, v_2, \ldots, v_{i-1}) \\ \text{is a basis for } V_{i-1})}} + \mathbb{F}_p z = V_{i-1} + \mathbb{F}_p z = V_i.$$

Hence, the list $(v_1, v_2, \ldots, v_{i-1}, z)$ spans the $\mathbb{F}_p$-vector space V_i. Since the size i of this list equals the dimension of V_i (because $\dim(V_i) = i$), this shows that the list $(v_1, v_2, \ldots, v_{i-1}, z)$ is a basis for V_i. Qed.

- **Proof of Proposition 5.2:** Replace "and $\phi(g) = \underline{V}$" by "and $\phi(g) = g\sigma(\underline{E}) = \underline{V}$".

- **Example 5.3:** Replace "$g = \begin{bmatrix} 1 & 0 & 0 & b & a \\ 0 & 1 & 0 & d & c \\ 0 & 0 & 1 & f & e \\ 0 & 0 & 0 & 1 & g \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$" by "$g = \begin{bmatrix} 1 & 0 & 0 & e & a \\ 0 & 1 & 0 & f & b \\ 0 & 0 & 1 & g & c \\ 0 & 0 & 0 & 1 & d \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$". (Otherwise, the equation after it wouldn't be true.)

- **Example 5.3:** Rename "g" as "h" in the contexts "$g =$", "For such g", "$g\sigma =$" and "$\phi(g)$". (In fact, the notation "g" here clashes with the notation "g" for the $(4,5)$-th entry of the matrix g.)

- **Corollary 5.4:** I think you should define what you mean by "isomorphism" here. Namely, an *isomorphism* from a triple $(V, \underline{U}, \underline{W})$ (where V is an n-dimensional $\mathbb{F}_p$-vector space, and $\underline{U}$ and $\underline{W}$ are two complete flags in V) to a triple $(V', \underline{U'}, \underline{W'})$ (where V' is an n-dimensional $\mathbb{F}_p$-vector space, and $\underline{U'}$ and $\underline{W'}$ are two complete flags in V') means an isomorphism $\phi : V \to V'$ of $\mathbb{F}_p$-vector spaces satisfying $\phi U = U'$ and $\phi W = W'$.

- **Corollary 5.4:** Replace "Σ" by "Σ_n".

- **Corollary 5.4:** Replace "if and only iff" by "if and only if" (or by "iff").

- **Proof of Corollary 5.4:** Replace "a pair as above" by "a triple as above".

- **Proof of Corollary 5.4:** Replace "by $f(a) = \sum\limits_i a_i w_i$" by "by $f(a_1, a_2, \ldots, a_n) = \sum\limits_i a_i w_i$".

- **Proof of Corollary 5.4:** Replace "so $\underline{F} = x\sigma\underline{E}$" by: ". Since the map $X(\sigma) \to Y(\sigma)$, $g \mapsto g\sigma\underline{E}$ is a bijection (by Proposition 5.2), we thus see that $\underline{F} = x\sigma\underline{E}$".

- **Proof of Corollary 5.4:** At the end of this proof, add the following sentence: "Hence, $\left(\mathbb{F}_p^n, \sigma\underline{E}, \underline{E}\right) \simeq \left(\mathbb{F}_p^n, \underline{F}, \underline{E}\right) \simeq (V, \underline{U}, \underline{W})$ (since the map $f : \mathbb{F}_p^n \to V$ is an isomorphism $\left(\mathbb{F}_p^n, \underline{F}, \underline{E}\right) \to (V, \underline{U}, \underline{W})$)."

- **Proof of Corollary 5.5:** After "such bases exist iff $\delta(\underline{U}, \underline{W}) = \sigma$", add "(because the first claim of Corollary 5.4 shows that $\left(\mathbb{F}_p^n, \sigma\underline{E}, \underline{E}\right) \cong (V, \underline{U}, \underline{W})$ holds if and only if $\delta(\underline{U}, \underline{W}) = \delta(\sigma\underline{E}, \underline{E})$; but in light of Example 4.1 this condition rewrites as $\delta(\underline{U}, \underline{W}) = \sigma$)".

- **Proof of Corollary 5.5:** I think the last sentence of this proof would be better off taken out into a separate result:

Lemma 5.5a. Let $\sigma \in \Sigma_n$. Then, $|B^\sigma \cap B| = (p-1)^n p^{l(\sigma^{-1}\rho)}$.

[*Proof of Lemma 5.5a.* The definition of $X(\sigma^{-1}\rho)$ yields

$$\begin{aligned} X\left(\sigma^{-1}\rho\right) &= U \cap U^{\left(\sigma^{-1}\rho\rho\right)^{-1}} \\ &= U \cap U^{\sigma} \qquad \left(\text{since } \left(\sigma^{-1}\underbrace{\rho\rho}_{=1}\right)^{-1} = \left(\sigma^{-1}\right)^{-1} = \sigma\right) \\ &= U^\sigma \cap U. \end{aligned}$$

But the last sentence of Lemma 5.1 (applied to $\sigma^{-1}\rho$ instead of σ) yields $\left|X\left(\sigma^{-1}\rho\right)\right| = p^{l(\sigma^{-1}\rho)}$.

Consider the short exact sequence

$$1 \longrightarrow U^\sigma \cap U \longrightarrow B^\sigma \cap B \longrightarrow T \longrightarrow 1,$$

where the arrow $U^\sigma \cap U \longrightarrow B^\sigma \cap B$ is the canonical inclusion, and where the arrow $B^\sigma \cap B \longrightarrow T$ is the map that replaces all off-diagonal entries of a matrix $g \in B^\sigma \cap B$ by 0. [12] This short exact sequence shows that

$$\begin{aligned} |B^\sigma \cap B| &= |T| \cdot \left|\underbrace{U^\sigma \cap U}_{=X\left(\sigma^{-1}\rho\right)}\right| = |T| \cdot \underbrace{\left|X\left(\sigma^{-1}\rho\right)\right|}_{=p^{l\left(\sigma^{-1}\rho\right)}} = \underbrace{|T|}_{=(p-1)^n} \cdot p^{l\left(\sigma^{-1}\rho\right)} \qquad (12) \\ &= (p-1)^n \cdot p^{l\left(\sigma^{-1}\rho\right)}. \end{aligned}$$

Thus, Lemma 5.5a is proven. □]

- **Proof of Proposition 6.1:** Before "Moreover, if", add the following sentence: "Thus, $\pi(BgB) = \{\pi(g)\}$ for each $g \in G$.".
- **Proof of Proposition 6.1:** Replace "from which it follows directly that $\pi(\sigma) = \sigma$" by "and the definition of π yields $\pi(\sigma) = \delta(\sigma\underline{E}, \underline{E}) = \sigma$ (by Example 4.1)".
- **Proof of Proposition 6.1:** After "This means that $\pi(B\sigma B) = \{\sigma\}$.", add "Hence, $B\sigma B \subseteq \pi^{-1}\{\sigma\}$.".
- **Proof of Proposition 6.1:** Replace "Conversely, suppose that $\pi(h) = \sigma$." by "Conversely, let $h \in \pi^{-1}\{\sigma\}$. Thus, $h \in G$ and $\pi(h) = \sigma$. Hence, $\sigma = \pi(h) = \delta(h\underline{E}, \underline{E})$, so that $h\underline{E} \in Y(\sigma, \underline{E}) = Y(\sigma)$. Hence,".

[12] This is indeed a short exact sequence, because the matrices $g \in B^\sigma \cap B$ whose diagonal entries all equal 1 are exactly the elements of $U^\sigma \cap U$. It is actually a split extension, since the arrow $B^\sigma \cap B \longrightarrow T$ is split by the canonical inclusion $T \longrightarrow B^\sigma \cap B$.

- **Proof of Proposition 6.1:** Replace "Propsition" by "Proposition".
- **Proof of Proposition 6.1:** After "we find that $b \in B$", add "(since $b\underline{E} = (g\sigma)^{-1} \underbrace{h\underline{E}}_{=g\sigma\underline{E}} = (g\sigma)^{-1} g\sigma\underline{E} = \underline{E}$)".
- **Proof of Proposition 6.1:** After "shows that $h \in B\sigma B$", add "(since $g \in X(\sigma) \leq U \leq B$ and $b \in B$). Hence, we have shown that $\pi^{-1}\{\sigma\} \subseteq B\sigma B$ (since h was assumed to be any element of G satisfying $\pi(h) = \sigma$)".
- **Proof of Proposition 6.1:** Replace "we see that $g\sigma\underline{E} = g'\sigma\underline{E}$" by "and $g\sigma b = h = g'\sigma b'$, we see that $g\sigma \underbrace{\underline{E}}_{=b\underline{E}} = \underbrace{g\sigma b}_{=g'\sigma b'} \underline{E} = g'\sigma \underbrace{b'\underline{E}}_{=\underline{E}} = g'\sigma\underline{E}$".
- **Proof of Corollary 6.2:** The claim "$B = T \times U$" is wrong, or at least seriously misleading (the group B is not a direct product of T and U). I would replace the whole sentence containing it by "Applying (12) to $\rho\sigma^{-1}$ instead of σ, we obtain $\left|B^{\rho\sigma^{-1}} \cap B\right| = |T| \cdot p^{l\left(\left(\rho\sigma^{-1}\right)^{-1}\rho\right)}$. Since $B^{\rho\sigma^{-1}} \cap B = B \cap B^{\rho\sigma^{-1}}$ and $\left(\rho\sigma^{-1}\right)^{-1}\rho = \sigma$, this rewrites as $\left|B \cap B^{\rho\sigma^{-1}}\right| = |T| \cdot p^{l(\sigma)}$.
- **Proof of Corollary 6.2:** After the displayed equation "$|B\sigma B| = p^{l(\sigma)}|B| = |U||T|p^{l(\sigma)}$", add "(since the short exact sequence $1 \longrightarrow U \longrightarrow B \longrightarrow T \longrightarrow 1$ yields $|B| = |U||T|$)".
- **Proof of Corollary 6.3:** Before "We have a bijection", add "Proposition 6.1 (applied to σ^{-1} instead of σ) shows that".
- **Proof of Corollary 6.3:** Replace "given by $\phi(g,b) = g\sigma b$" by "given by $\phi(g,b) = g\sigma^{-1}b$".
- **Proof of Proposition 6.4:** The statement in the first sentence of your proof is worth stating as a separate lemma:

  Lemma 2.6a. Let $\sigma, \tau \in \Sigma_n$. Then, the following two conditions are equivalent:

  Condition $\mathcal{C}_1$: We have $l(\sigma\tau) = l(\sigma) + l(\tau)$.

  Condition $\mathcal{C}_2$: For any $T \subseteq \{1, 2, \ldots, n\}$ with $|T| = 2$, at most one of the two maps $T \xrightarrow{\tau} \tau(T) \xrightarrow{\sigma} \sigma\tau(T)$ is order-reversing.

  [*Proof of Lemma 2.6a.* Let us prove the implications $\mathcal{C}_1 \Longrightarrow \mathcal{C}_2$ and $\mathcal{C}_2 \Longrightarrow \mathcal{C}_1$ separately.

  Proof of the implication $\mathcal{C}_1 \Longrightarrow \mathcal{C}_2$: Assume that Condition $\mathcal{C}_1$ holds. In other words, we have $l(\sigma\tau) = l(\sigma) + l(\tau)$.

Lemma 2.6 shows that $\overline{L}(\sigma\tau) = \overline{L}(\tau)\Delta\tau_*^{-1}\overline{L}(\sigma)$. Also, $l(\sigma) = |L(\sigma)| = \left|\overline{L}(\sigma)\right|$ and similarly $l(\tau) = \left|\overline{L}(\tau)\right|$ and $l(\sigma\tau) = \left|\overline{L}(\sigma\tau)\right|$. Now,

$$\begin{aligned}\left|\overline{L}(\tau)\right| + \underbrace{\left|\tau_*^{-1}\overline{L}(\sigma)\right|}_{\substack{=\left|\overline{L}(\sigma)\right| \\ \text{(since } \tau_* \text{ is a bijection)}}} &= \underbrace{\left|\overline{L}(\tau)\right|}_{=l(\tau)} + \underbrace{\left|\overline{L}(\sigma)\right|}_{=l(\sigma)} = l(\tau) + l(\sigma) = l(\sigma) + l(\tau) \\ &= l(\sigma\tau) = \left|\underbrace{\overline{L}(\sigma\tau)}_{=\overline{L}(\tau)\Delta\tau_*^{-1}\overline{L}(\sigma)}\right| = \left|\overline{L}(\tau)\Delta\tau_*^{-1}\overline{L}(\sigma)\right|.\end{aligned}$$

But a simple and fundamental fact states that if A and B are two finite sets satisfying $|A| + |B| = |A\Delta B|$, then $A \cap B = \varnothing$. Applying this to $A = \overline{L}(\tau)$ and $B = \tau_*^{-1}\overline{L}(\sigma)$, we find that $\overline{L}(\tau) \cap \tau_*^{-1}\overline{L}(\sigma) = \varnothing$ (since $\left|\overline{L}(\tau)\right| + \left|\tau_*^{-1}\overline{L}(\sigma)\right| = \left|\overline{L}(\tau)\Delta\tau_*^{-1}\overline{L}(\sigma)\right|$).

Now, let $T \subseteq \{1, 2, \ldots, n\}$ with $|T| = 2$. We shall show that at most one of the two maps $T \xrightarrow{\tau} \tau(T) \xrightarrow{\sigma} \sigma\tau(T)$ is order-reversing.

Indeed, assume the contrary. Thus, both maps $T \xrightarrow{\tau} \tau(T) \xrightarrow{\sigma} \sigma\tau(T)$ are order-reversing.

One of the characterizations of $\overline{L}(\sigma)$ shows that the two-element subset $\tau(T)$ of $\{1, 2, \ldots, n\}$ belongs to $\overline{L}(\sigma)$ if and only if the map $\sigma : \tau(T) \to \sigma\tau(T)$ is order-reversing. Hence, the two-element subset $\tau(T)$ of $\{1, 2, \ldots, n\}$ belongs to $\overline{L}(\sigma)$ (since the map $\sigma : \tau(T) \to \sigma\tau(T)$ is order-reversing). Thus, $\tau(T) \in \overline{L}(\sigma)$. But $\tau_*(T) = \tau(T) \in \overline{L}(\sigma)$, so that $T \in \tau_*^{-1}\overline{L}(\sigma)$.

One of the characterizations of $\overline{L}(\tau)$ shows that the two-element subset T of $\{1, 2, \ldots, n\}$ belongs to $\overline{L}(\tau)$ if and only if the map $\tau : T \to \tau(T)$ is order-reversing. Hence, the two-element subset T of $\{1, 2, \ldots, n\}$ belongs to $\overline{L}(\tau)$ (since the map $\tau : T \to \tau(T)$ is order-reversing). In other words, $T \in \overline{L}(\tau)$. Combining this with $T \in \tau_*^{-1}\overline{L}(\sigma)$, we obtain $T \in \overline{L}(\tau) \cap \tau_*^{-1}\overline{L}(\sigma) = \varnothing$. In other words, T belongs to the empty set. This is clearly absurd.

Thus, we have obtained a contradiction. Hence, our assumption was wrong. We thus have proven that at most one of the two maps $T \xrightarrow{\tau} \tau(T) \xrightarrow{\sigma} \sigma\tau(T)$ is order-reversing.

Now, forget that we fixed T. We thus have shown that for any $T \subseteq \{1, 2, \ldots, n\}$ with $|T| = 2$, at most one of the two maps $T \xrightarrow{\tau} \tau(T) \xrightarrow{\sigma} \sigma\tau(T)$ is order-reversing. In other words, Condition $\mathcal{C}_2$ holds.

Thus, we have derived Condition $\mathcal{C}_2$ from Condition $\mathcal{C}_1$. In other words, we have proven the implication $\mathcal{C}_1 \Longrightarrow \mathcal{C}_2$.

We omit the proof of the implication $\mathcal{C}_2 \Longrightarrow \mathcal{C}_1$ (since you don't actually use this implication in your arguments, and since this proof is rather easy to obtained by "walking backwards" our above proof of the implication $\mathcal{C}_1 \Longrightarrow \mathcal{C}_2$).

Combining the implications $\mathcal{C}_1 \Longrightarrow \mathcal{C}_2$ and $\mathcal{C}_2 \Longrightarrow \mathcal{C}_1$, we obtain the equivalence $\mathcal{C}_1 \Longleftrightarrow \mathcal{C}_2$. Thus, Lemma 2.6a is proven.]

- **§6:** Let me suggest an alternative way of proving Proposition 6.4 and Proposition 6.5. This alternative way has the advantage that it does not use the finiteness of the field $\mathbb{F}_p$, and so can be directly generalized to an arbitrary field.[13]

  First, let me show a few useful lemmas:

  Lemma 6.4a. Let $\sigma \in \Sigma_n$ and $g = \left(g_{i,j}\right)_{i,j=1}^{n} \in G$.

  (a) If $g \in X\left(\sigma\right)$, then

  $$\left(g_{i,i} = 1 \text{ for all } i \in \left\{1,2,\ldots,n\right\}\right) \tag{13}$$

  and

  $$\left(g_{i,j} = 0 \text{ for any } i,j \in \left\{1,2,\ldots,n\right\} \text{ satisfying } i \neq j \text{ and } \left(i,j\right) \notin L\left(\sigma^{-1}\right)\right). \tag{14}$$

  (b) If (13) and (14) hold, then $g \in X\left(\sigma\right)$.

  [*Proof of Lemma 6.4a.* From the first sentence of Lemma 5.1, we see that $g \in X\left(\sigma\right)$ holds if and only if we have

  $$g_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ \text{arbitrary}, & \text{if } \left(i,j\right) \in L\left(\sigma^{-1}\right); \\ 0, & \text{otherwise} \end{cases}.$$

  In other words, $g \in X\left(\sigma\right)$ holds if and only if (13) and (14) hold. This proves both parts **(a)** and **(b)** of Lemma 6.4a. □]

  Lemma 6.4b. Let $g = \left(g_{i,j}\right)_{i,j=1}^{n} \in G$.

  (a) If $g \in U$, then

  $$\left(g_{i,i} = 1 \text{ for all } i \in \left\{1,2,\ldots,n\right\}\right) \tag{15}$$

  and

  $$\left(g_{i,j} = 0 \text{ for any } i,j \in \left\{1,2,\ldots,n\right\} \text{ satisfying } i > j\right). \tag{16}$$

  (b) If (15) and (16) hold, then $g \in U$.

[13] A few comments on your proofs:

– In the proof of Proposition 6.4, before "We now show that $\phi\left(g,h\right) \in X\left(\sigma\tau\right)$", I would suggest adding "Let $g \in X\left(\sigma\right)$ and $h \in X\left(\tau\right)$.".

– In the proof of Proposition 6.4, "apply Corollary 6.1" should be replaced by "apply Proposition 6.1".

[*Proof of Lemma 6.4b.* Recall that U is the set of all upper-unitriangular $n \times n$-matrices. Hence, $g \in U$ holds if and only if g is upper-unitriangular. By the definition of upper-triangular, this rewrites as follows: $g \in U$ holds if and only if (15) and (16) hold. This proves both parts **(a)** and **(b)** of Lemma 6.4b. □]

Lemma 6.4c. Let $\sigma \in \Sigma_n$. Then, the map $X(\sigma) \times B \to B\sigma B$, $(g, b) \mapsto g\sigma b$ is well-defined and is a bijection.

[*Proof of Lemma 6.4c.* Lemma 6.4c is the first claim of Proposition 6.1, and thus we already have proven it. □]

Lemma 6.4d. Let $\sigma \in \Sigma_n$ and $\tau \in \Sigma_n$ be such that $l(\sigma\tau) = l(\sigma) + l(\tau)$. Then:

(a) We have $\overline{L}(\tau) \cap \tau_*^{-1}\overline{L}(\sigma) = \varnothing$.

(b) We have $X(\sigma) \cap (X(\tau))^{\sigma^{-1}} = 1$.

(c) We have $X(\sigma) \subseteq U^{\rho\tau^{-1}\sigma^{-1}}$.

(d) We have $(X(\tau))^{\sigma^{-1}} \subseteq U$.

(e) We have $X(\sigma) \cdot (X(\tau))^{\sigma^{-1}} \subseteq X(\sigma\tau)$.

(f) We have $B\sigma B\tau B = B\sigma\tau B$.

(g) The map

$$X(\sigma) \times X(\tau) \to X(\sigma\tau), \qquad (g, h) \mapsto gh^{\sigma^{-1}}$$

is well-defined and bijective.

[*Proof of Lemma 6.4d.* **(a)** This was shown in the proof of Claim 1 during the proof of Lemma 2.6a given above.

(b) Let $g \in X(\sigma) \cap U^{\sigma^{-1}}$. Thus, $g \in X(\sigma)$ and $g \in U^{\sigma^{-1}}$. Write the matrix g in the form $g = (g_{i,j})_{i,j=1}^{n}$. Then, $g^{\sigma} = \left(g_{\sigma(i),\sigma(j)}\right)_{i,j=1}^{n}$. But $g \in U^{\sigma^{-1}}$, so that

$$g^{\sigma} \in \left(U^{\sigma^{-1}}\right)^{\sigma} = U^{\sigma^{-1}\sigma} = U^{1} = U.$$

Hence, Lemma 6.4a **(a)** (applied to g^{σ} and $g_{\sigma(i),\sigma(j)}$ instead of g and $g_{i,j}$) yields that

$$\left(g_{\sigma(i),\sigma(i)} = 1 \text{ for all } i \in \{1, 2, \ldots, n\}\right) \qquad (17)$$

and

$$\left(g_{\sigma(i),\sigma(j)} = 0 \text{ for any } i, j \in \{1, 2, \ldots, n\} \text{ satisfying } i > j\right). \qquad (18)$$

On the other hand, $g \in X(\sigma)$. Hence, Lemma 6.4a **(a)** yields that

$$\left(g_{i,i} = 1 \text{ for all } i \in \{1, 2, \ldots, n\}\right) \qquad (19)$$

and

$$\left(g_{i,j} = 0 \text{ for any } i,j \in \{1,2,\ldots,n\} \text{ satisfying } i \neq j \text{ and } (i,j) \notin L\left(\sigma^{-1}\right)\right). \tag{20}$$

Now, let $i,j \in \{1,2,\ldots,n\}$. We shall show that $g_{i,j} = \delta_{i,j}$.

Indeed, assume the contrary. Thus, $g_{i,j} \neq \delta_{i,j}$. Hence, $i \neq j$ [14], so that $\delta_{i,j} = 0$ and thus $g_{i,j} \neq \delta_{i,j} = 0$.

If we had $(i,j) \notin L\left(\sigma^{-1}\right)$, then we would have $g_{i,j} = 0$ (by (20)), which would contradict $g_{i,j} \neq 0$. Thus, we cannot have $(i,j) \notin L\left(\sigma^{-1}\right)$. Hence, we have $(i,j) \in L\left(\sigma^{-1}\right)$. In other words, $i < j$ and $\sigma^{-1}(i) > \sigma^{-1}(j)$ (by the definition of $L\left(\sigma^{-1}\right)$). Thus, (18) (applied to $\left(\sigma^{-1}(i), \sigma^{-1}(j)\right)$ instead of (i,j)) yields

$g_{\sigma\left(\sigma^{-1}(i)\right),\sigma\left(\sigma^{-1}(j)\right)} = 0$. This contradicts $g_{\sigma\left(\sigma^{-1}(i)\right),\sigma\left(\sigma^{-1}(j)\right)} = g_{i,j} \neq 0$. This contradiction shows that our assumption was false. Hence, $g_{i,j} = \delta_{i,j}$ is proven.

Now, forget that we fixed i,j. We thus have shown that $g_{i,j} = \delta_{i,j}$ for all $i,j \in \{1,2,\ldots,n\}$. In other words, $\left(g_{i,j}\right)_{i,j=1}^{n} = \left(\delta_{i,j}\right)_{i,j=1}^{n} = 1$. Hence, $g = \left(g_{i,j}\right)_{i,j=1}^{n} = 1$.

Now, forget that we fixed g. Thus we have proven that $g = 1$ for each $g \in X(\sigma) \cap U^{\sigma^{-1}}$. In other words, $X(\sigma) \cap U^{\sigma^{-1}} = 1$.

But the definition of $X(\tau)$ yields $X(\tau) = U \cap U^{(\tau\rho)^{-1}} \subseteq U$. Thus, $(X(\tau))^{\sigma^{-1}} \subseteq U^{\sigma^{-1}}$, so that $X(\sigma) \cap \underbrace{(X(\tau))^{\sigma^{-1}}}_{\subseteq U^{\sigma^{-1}}} \subseteq X(\sigma) \cap U^{\sigma^{-1}} = 1$. Hence, $X(\sigma) \cap (X(\tau))^{\sigma^{-1}} = 1$. This proves Lemma 6.4d **(b)**.

(c) Let $g \in X(\sigma)$. We shall prove that $g \in U^{\rho\tau^{-1}\sigma^{-1}}$.

Write the matrix g in the form $g = \left(g_{i,j}\right)_{i,j=1}^{n}$.

We have $g \in X(\sigma)$. Hence, Lemma 6.4a **(a)** yields that

$$\left(g_{i,i} = 1 \text{ for all } i \in \{1,2,\ldots,n\}\right) \tag{21}$$

and

$$\left(g_{i,j} = 0 \text{ for any } i,j \in \{1,2,\ldots,n\} \text{ satisfying } i \neq j \text{ and } (i,j) \notin L\left(\sigma^{-1}\right)\right). \tag{22}$$

[14] *Proof.* Assume the contrary. Thus, $i = j$. Hence, $j = i$, so that $g_{i,j} = g_{i,i} = 1$ (by (19)). But from $i = j$, we also obtain $\delta_{i,j} = 1$. Comparing this with $g_{i,j} = 1$, we obtain $g_{i,j} = \delta_{i,j}$. This contradicts $g_{i,j} \neq \delta_{i,j}$. This contradiction shows that our assumption was wrong. Qed.

Let $\eta = \sigma\tau\rho$. Thus, $\eta \in \Sigma_n$, so that η is an injective map. From $\eta = \sigma\tau\rho$, we obtain $\eta^{-1} = (\sigma\tau\rho)^{-1} = \underbrace{\rho^{-1}}_{=\rho} \tau^{-1}\sigma^{-1} = \rho\tau^{-1}\sigma^{-1}$.

Let $i, j \in \{1, 2, \ldots, n\}$ be such that $i > j$. We shall show that $g_{\eta(i),\eta(j)} = 0$.

Indeed, assume the contrary. Thus, $g_{\eta(i),\eta(j)} \neq 0$. From $i > j$, we obtain $i \neq j$ and therefore $\eta(i) \neq \eta(j)$ (since η is injective). If we had $(\eta(i), \eta(j)) \notin L(\sigma^{-1})$, then we would have $g_{\eta(i),\eta(j)} = 0$ (by (22), applied to $\eta(i)$ and $\eta(j)$ instead of i and j), which would contradict $g_{\eta(i),\eta(j)} \neq 0$. Hence, we cannot have $(\eta(i), \eta(j)) \notin L(\sigma^{-1})$. Thus, we must have $(\eta(i), \eta(j)) \in L(\sigma^{-1})$. In other words, $\eta(i) < \eta(j)$ and $\sigma^{-1}(\eta(i)) > \sigma^{-1}(\eta(j))$ (by the definition of $L(\sigma^{-1})$). From $\eta(i) < \eta(j)$, we obtain $\eta(j) > \eta(i)$.

Now, the definition of ρ yields $\rho(i) = n + 1 - \underbrace{i}_{>j} < n + 1 - j = \rho(j)$ (since $\rho(j) = n + 1 - j$ (by the definition of ρ)). But $\eta = \sigma\tau\rho$, so that $\sigma^{-1}\eta = \tau\rho$. Now, $\sigma^{-1}(\eta(i)) = \underbrace{\left(\sigma^{-1}\eta\right)}_{=\tau\rho}(i) = (\tau\rho)(i) = \tau(\rho(i))$ and similarly $\sigma^{-1}(\eta(j)) = \tau(\rho(j))$. Thus, $\tau(\rho(i)) = \sigma^{-1}(\eta(i)) > \sigma^{-1}(\eta(j)) = \tau(\rho(j))$.

Combining $\rho(i) < \rho(j)$ with $\tau(\rho(i)) > \tau(\rho(j))$, we obtain $(\rho(i), \rho(j)) \in L(\tau)$ (by the definition of $L(\tau)$). Thus, $\{\rho(i), \rho(j)\} \in \overline{L}(\tau)$ (by the definition of $\overline{L}(\tau)$).

On the other hand, $\tau(\rho(j)) < \tau(\rho(i))$ (since $\tau(\rho(i)) > \tau(\rho(j))$) and $\sigma(\tau(\rho(j))) = \underbrace{(\sigma\tau\rho)}_{=\eta}(j) = \eta(j) > \underbrace{\eta}_{=\sigma\tau\rho}(i) = (\sigma\tau\rho)(i) = \sigma(\tau(\rho(i)))$. Combining these two inequalities, we obtain $(\tau(\rho(j)), \tau(\rho(i))) \in L(\sigma)$ (by the definition of $L(\sigma)$). Hence, $\{\tau(\rho(j)), \tau(\rho(i))\} \in \overline{L}(\sigma)$ (by the definition of $\overline{L}(\sigma)$).

Now,

$$\begin{aligned} \tau_*(\{\rho(i), \rho(j)\}) &= \tau(\{\rho(i), \rho(j)\}) \qquad \text{(by the definition of } \tau_*) \\ &= \{\tau(\rho(i)), \tau(\rho(j))\} = \{\tau(\rho(j)), \tau(\rho(i))\} \in \overline{L}(\sigma), \end{aligned}$$

so that $\{\rho(i), \rho(j)\} \in \tau_*^{-1}\overline{L}(\sigma)$. Combining this with $\{\rho(i), \rho(j)\} \in \overline{L}(\tau)$, we obtain $\{\rho(i), \rho(j)\} \in \overline{L}(\tau) \cap \tau_*^{-1}\overline{L}(\sigma) = \varnothing$. Thus, $\{\rho(i), \rho(j)\}$ belongs to the empty set. This is clearly absurd. Thus, we have obtained a contradiction. This shows that our assumption was false. Hence, $g_{\eta(i),\eta(j)} = 0$ is proven.

Now, forget that we fixed i, j. We thus have shown that

$$\left(g_{\eta(i),\eta(j)} = 0 \text{ for any } i, j \in \{1, 2, \ldots, n\} \text{ satisfying } i > j\right). \tag{23}$$

Moreover, if $i \in \{1,2,\ldots,n\}$, then $g_{\eta(i),\eta(i)} = 1$ (by (21), applied to $\eta(i)$ instead of i). Thus, we have shown that

$$\left(g_{\eta(i),\eta(i)} = 1 \text{ for all } i \in \{1,2,\ldots,n\}\right). \tag{24}$$

Now, $g^{\eta} = \left(g_{\eta(i),\eta(j)}\right)_{i,j=1}^{n}$ (since $g = \left(g_{i,j}\right)_{i,j=1}^{n}$). Hence, Lemma 6.4b **(b)** (applied to g^{η} and $g_{\eta(i),\eta(j)}$ instead of g and $g_{i,j}$) shows that $g^{\eta} \in U$ (since (24) and (23) hold). Hence, $\left(g^{\eta}\right)^{\eta^{-1}} \in U^{\eta^{-1}}$. Since $\left(g^{\eta}\right)^{\eta^{-1}} = g^{\eta\eta^{-1}} = g^{1} = g$, this rewrites as $g \in U^{\eta^{-1}}$. Since $\eta^{-1} = \rho\tau^{-1}\sigma^{-1}$, this rewrites as $g \in U^{\rho\tau^{-1}\sigma^{-1}}$.

Now, forget that we fixed g. We thus have shown that $g \in U^{\rho\tau^{-1}\sigma^{-1}}$ for each $g \in X(\sigma)$. In other words, $X(\sigma) \subseteq U^{\rho\tau^{-1}\sigma^{-1}}$. This proves Lemma 6.4d **(c)**.

(d) Let $g \in X(\tau)$. We shall prove that $g \in U^{\sigma}$.

Write the matrix g in the form $g = \left(g_{i,j}\right)_{i,j=1}^{n}$.

We have $g \in X(\tau)$. Hence, Lemma 6.4a **(a)** (applied to τ instead of σ) yields that

$$\left(g_{i,i} = 1 \text{ for all } i \in \{1,2,\ldots,n\}\right) \tag{25}$$

and

$$\left(g_{i,j} = 0 \text{ for any } i,j \in \{1,2,\ldots,n\} \text{ satisfying } i \neq j \text{ and } (i,j) \notin L\left(\tau^{-1}\right)\right). \tag{26}$$

Let $\eta = \sigma^{-1}$. Thus, $\eta \in \Sigma_n$. Hence, η is an injective map.

Let $i,j \in \{1,2,\ldots,n\}$ be such that $i > j$. We shall show that $g_{\eta(i),\eta(j)} = 0$.

Indeed, assume the contrary. Thus, $g_{\eta(i),\eta(j)} \neq 0$. From $i > j$, we obtain $i \neq j$ and therefore $\eta(i) \neq \eta(j)$ (since η is injective). If we had $(\eta(i), \eta(j)) \notin L\left(\tau^{-1}\right)$, then we would have $g_{\eta(i),\eta(j)} = 0$ (by (26), applied to $\eta(i)$ and $\eta(j)$ instead of i and j), which would contradict $g_{\eta(i),\eta(j)} \neq 0$. Hence, we cannot have $(\eta(i), \eta(j)) \notin L\left(\tau^{-1}\right)$. Thus, we must have $(\eta(i), \eta(j)) \in L\left(\tau^{-1}\right)$. In other words, $\eta(i) < \eta(j)$ and $\tau^{-1}(\eta(i)) > \tau^{-1}(\eta(j))$ (by the definition of $L\left(\tau^{-1}\right)$). From $\eta(i) < \eta(j)$, we obtain $\eta(j) > \eta(i)$.

Set $x = \tau^{-1}(\eta(j))$ and $y = \tau^{-1}(\eta(i))$. Then, x, y are elements of $\{1,2,\ldots,n\}$. Furthermore, $y = \tau^{-1}(\eta(i)) > \tau^{-1}(\eta(j)) = x$, so that $x < y$. Besides, from $x = \tau^{-1}(\eta(j))$, we obtain $\tau(x) = \eta(j)$. From $y = \tau^{-1}(\eta(i))$, we obtain $\tau(y) = \eta(i)$. Thus, $\tau(y) = \eta(i) < \eta(j) = \tau(x)$, so that $\tau(x) > \tau(y)$.

From $x < y$ and $\tau(x) > \tau(y)$, we obtain $(x,y) \in L(\tau)$ (by the definition of $L(\tau)$). Thus, $\{x,y\} \in \overline{L}(\tau)$ (by the definition of $\overline{L}(\tau)$).

On the other hand, the elements $\eta(i), \eta(j) \in \{1, 2, \ldots, n\}$ satisfy $\eta(i) < \eta(j)$ and $\sigma(\eta(i)) > \sigma(\eta(j))$ (since $\sigma\left(\underbrace{\eta}_{=\sigma^{-1}}(i)\right) = \sigma\left(\sigma^{-1}(i)\right) = i > j = \sigma\left(\underbrace{\sigma^{-1}}_{=\eta}(j)\right) = \sigma(\eta(j))$). In other words, $(\eta(i), \eta(j)) \in L(\sigma)$ (by the definition of $L(\sigma)$). Hence, $\{\eta(i), \eta(j)\} \in \overline{L}(\sigma)$ (by the definition of $\overline{L}(\sigma)$).

But

$$\begin{aligned} \tau_*(\{x, y\}) &= \tau(\{x, y\}) \qquad \text{(by the definition of } \tau_*\text{)} \\ &= \left\{\underbrace{\tau(x)}_{=\eta(j)}, \underbrace{\tau(y)}_{=\eta(i)}\right\} = \{\eta(j), \eta(i)\} = \{\eta(i), \eta(j)\} \in \overline{L}(\sigma), \end{aligned}$$

so that $\{x, y\} \in \tau_*^{-1}\overline{L}(\sigma)$. Combining this with $\{x, y\} \in \overline{L}(\tau)$, we obtain $\{x, y\} \in \overline{L}(\tau) \cap \tau_*^{-1}\overline{L}(\sigma) = \varnothing$. Thus, $\{x, y\}$ belongs to the empty set. This is clearly absurd. Thus, we have obtained a contradiction. This shows that our assumption was false. Hence, $g_{\eta(i),\eta(j)} = 0$ is proven.

Now, forget that we fixed i, j. We thus have shown that

$$\left(g_{\eta(i),\eta(j)} = 0 \text{ for any } i, j \in \{1, 2, \ldots, n\} \text{ satisfying } i > j\right). \qquad (27)$$

Moreover, if $i \in \{1, 2, \ldots, n\}$, then $g_{\eta(i),\eta(i)} = 1$ (by (25), applied to $\eta(i)$ instead of i). Thus, we have shown that

$$\left(g_{\eta(i),\eta(i)} = 1 \text{ for all } i \in \{1, 2, \ldots, n\}\right). \qquad (28)$$

Now, $g^\eta = \left(g_{\eta(i),\eta(j)}\right)_{i,j=1}^n$ (since $g = \left(g_{i,j}\right)_{i,j=1}^n$). Hence, Lemma 6.4b **(b)** (applied to g^η and $g_{\eta(i),\eta(j)}$ instead of g and $g_{i,j}$) shows that $g^\eta \in U$ (since (28) and (27) hold). Hence, $(g^\eta)^\sigma \in U^\sigma$. Since

$$\begin{aligned} (g^\eta)^\sigma &= g^{\eta\sigma} = g^1 \qquad \left(\text{since } \underbrace{\eta}_{=\sigma^{-1}}\sigma = \sigma^{-1}\sigma = 1\right) \\ &= g, \end{aligned}$$

this rewrites as $g \in U^\sigma$.

Now, forget that we fixed g. We thus have shown that $g \in U^{\sigma}$ for each $g \in X(\tau)$. In other words, $X(\tau) \subseteq U^{\sigma}$. Hence, $(X(\tau))^{\sigma^{-1}} \subseteq (U^{\sigma})^{\sigma^{-1}} = U^{\sigma\sigma^{-1}} = U^{1} = U$. This proves Lemma 6.4d **(d)**.

(e) The definition of $X(\sigma\tau)$ yields $X(\sigma\tau) = U \cap U^{(\sigma\tau\rho)^{-1}}$. Hence, $X(\sigma\tau)$ is the intersection of two subgroups of G (namely, of the subgroup U and of the subgroup $U^{(\sigma\tau\rho)^{-1}}$). Thus, $X(\sigma\tau)$ is itself a subgroup of G. Therefore, $X(\sigma\tau) \cdot X(\sigma\tau) \subseteq X(\sigma\tau)$.

Now, $(\sigma\tau\rho)^{-1} = \underbrace{\rho^{-1}}_{=\rho}\tau^{-1}\sigma^{-1} = \rho\tau^{-1}\sigma^{-1}$, so that $U^{(\sigma\tau\rho)^{-1}} = U^{\rho\tau^{-1}\sigma^{-1}}$.

The definition of $X(\sigma)$ yields $X(\sigma) = U \cap U^{(\sigma\rho)^{-1}} \subseteq U$. But Lemma 6.4d **(c)** yields $X(\sigma) \subseteq U^{\rho\tau^{-1}\sigma^{-1}} = U^{(\sigma\tau\rho)^{-1}}$. Combining $X(\sigma) \subseteq U$ with $X(\sigma) \subseteq U^{(\sigma\tau\rho)^{-1}}$, we obtain $X(\sigma) \subseteq U \cap U^{(\sigma\tau\rho)^{-1}} = X(\sigma\tau)$.

On the other hand, the definition of $X(\tau)$ yields $X(\tau) = U \cap U^{(\tau\rho)^{-1}} \subseteq U^{(\tau\rho)^{-1}}$. Hence, $(X(\tau))^{\sigma^{-1}} \subseteq \left(U^{(\tau\rho)^{-1}}\right)^{\sigma^{-1}} = U^{(\tau\rho)^{-1}\sigma^{-1}} = U^{(\sigma\tau\rho)^{-1}}$ (since $(\tau\rho)^{-1}\sigma^{-1} = (\sigma\tau\rho)^{-1}$). Combining $(X(\tau))^{\sigma^{-1}} \subseteq U$ (which follows from Lemma 6.4d **(d)**) with $(X(\tau))^{\sigma^{-1}} \subseteq U^{(\sigma\tau\rho)^{-1}}$, we obtain $(X(\tau))^{\sigma^{-1}} \subseteq U \cap U^{(\sigma\tau\rho)^{-1}} = X(\sigma\tau)$.

Now,

$$\underbrace{X(\sigma)}_{\subseteq X(\sigma\tau)} \cdot \underbrace{(X(\tau))^{\sigma^{-1}}}_{\subseteq X(\sigma\tau)} \subseteq X(\sigma\tau) \cdot X(\sigma\tau) \subseteq X(\sigma\tau).$$

This proves Lemma 6.4d **(e)**.

(f) Let $r \in B\sigma B\tau B$. Then, $r \in B\sigma B\tau B = B\sigma(B\tau B)$. In other words, there exist $c \in B$ and $p \in B\tau B$ such that $r = c\sigma p$. Consider these c and p.

Lemma 6.4c (applied to τ instead of σ) yields that the map $X(\tau) \times B \to B\tau B$, $(g, b) \mapsto g\tau b$ is well-defined and is a bijection. Hence, the element $p \in B\tau B$ is an image under this map. In other words, there exists some $(g, b) \in X(\tau) \times B$ such that $p = g\tau b$. Consider this (g, b).

From $(g, b) \in X(\tau) \times B$, we obtain $g \in X(\tau)$ and $b \in B$. From $g \in X(\tau)$, we obtain $g^{\sigma^{-1}} \in (X(\tau))^{\sigma^{-1}} \subseteq U$ (by Lemma 6.4c **(d)**), so that $g^{\sigma^{-1}} \in U \subseteq B$. Since $g^{\sigma^{-1}} = \underbrace{\left(\sigma^{-1}\right)^{-1}}_{=\sigma} g\sigma^{-1} = \sigma g\sigma^{-1}$, this rewrites as $\sigma g\sigma^{-1} \in B$.

Now, $\sigma g \underbrace{\sigma^{-1}\sigma}_{=1} \tau b = \sigma \underbrace{g\tau b}_{=p} = \sigma p$, so that $\sigma p = \underbrace{\sigma g\sigma^{-1}}_{\in B} \sigma\tau \underbrace{b}_{\in B} \in B\sigma\tau B$. Now,

$$r = \underbrace{c}_{\in B} \underbrace{\sigma p}_{\in B\sigma\tau B} \in \underbrace{BB}_{\substack{\subseteq B \\ \text{(since } B \text{ is a group)}}} \sigma\tau B \subseteq B\sigma\tau B.$$

Now, forget that we fixed r. We thus have proven that $r \in B\sigma\tau B$ for each $r \in B\sigma B\tau B$. In other words, $B\sigma B\tau B \subseteq B\sigma\tau B$. Combining this with the inclusion

$$B \underbrace{\sigma}_{=\sigma 1} \tau B = B\sigma \underbrace{1}_{\in B} \tau B \subseteq B\sigma B\tau B,$$

we obtain $B\sigma B\tau B = B\sigma\tau B$. This proves Lemma 6.4d **(f)**.

(g) For every $(g,h) \in X(\sigma) \times X(\tau)$, we have

$$\underbrace{g}_{\substack{\in X(\sigma) \\ (\text{since } (g,h)\in X(\sigma)\times X(\tau))}} \underbrace{h^{\sigma^{-1}}}_{\substack{\in (X(\tau))^{\sigma^{-1}} \\ (\text{since } h\in X(\tau) \\ (\text{since } (g,h)\in X(\sigma)\times X(\tau)))}} \in X(\sigma) \cdot (X(\tau))^{\sigma^{-1}} \subseteq X(\sigma\tau)$$

(by Lemma 6.4d **(e)**). Thus, the map

$$X(\sigma) \times X(\tau) \to X(\sigma\tau), \qquad (g,h) \mapsto gh^{\sigma^{-1}}$$

is well-defined. It remains to prove that this map is bijective. In order to do so, we denote this map by Φ. Thus, $\Phi(g,h) = gh^{\sigma^{-1}}$ for each $(g,h) \in X(\sigma) \times X(\tau)$. Our goal is to prove that Φ is bijective.

Let us first prove that Φ is surjective. Indeed, let $k \in X(\sigma\tau)$. Then, $k \in X(\sigma\tau) = U \cap U^{(\sigma\tau\rho)^{-1}}$ (by the definition of $X(\sigma\tau)$), so that $k \in U \cap U^{(\sigma\tau\rho)^{-1}} \subseteq U \subseteq B$. Hence, $k\sigma = \underbrace{k}_{\in B} \sigma \underbrace{1}_{\in B} \in B\sigma B$.

Lemma 6.4c yields that the map $X(\sigma) \times B \to B\sigma B$, $(g,b) \mapsto g\sigma b$ is well-defined and is a bijection. Hence, the element $k\sigma \in B\sigma B$ is an image under this map. In other words, there exists some $(u,d) \in X(\sigma) \times B$ such that $k\sigma = u\sigma d$. Consider this (u,d). From $(u,d) \in X(\sigma) \times B$, we obtain $u \in X(\sigma)$ and $d \in B$.

We have $d\tau = \underbrace{d}_{\in B} \tau \underbrace{1}_{\in B} \in B\tau B$.

Lemma 6.4c (applied to τ instead of σ) yields that the map $X(\tau) \times B \to B\tau B$, $(g,b) \mapsto g\tau b$ is well-defined and is a bijection. Hence, the element $d\tau \in B\tau B$ is an image under this map. In other words, there exists some $(h,c) \in X(\tau) \times B$ such that $d\tau = h\tau c$. Consider this (h,c). From $(h,c) \in X(\tau) \times B$, we obtain $h \in X(\tau)$ and $c \in B$.

We have $(u,h) \in X(\sigma) \times X(\tau)$ (since $u \in X(\sigma)$ and $h \in X(\tau)$). Thus, the definition of Φ yields $\Phi(u,h) = u \underbrace{h^{\sigma^{-1}}}_{=\left(\sigma^{-1}\right)^{-1} h\sigma^{-1}} = u \underbrace{\left(\sigma^{-1}\right)^{-1}}_{=\sigma} h\sigma^{-1} = u\sigma h\sigma^{-1}$, so that

$$\Phi(u,h)\,\sigma = u\sigma h. \tag{29}$$

We have

$$\underbrace{k\sigma}_{=u\sigma d}\underbrace{\tau 1}_{=\tau} = u\sigma \underbrace{d\tau}_{=h\tau c} = \underbrace{u\sigma h}_{\substack{=\Phi(u,h)\sigma \\ \text{(by (29))}}} \tau c = \Phi\left(u,h\right)\sigma\tau c.$$

Notice that $(k,1) \in X\left(\sigma\tau\right) \times B$ (since $k \in X\left(\sigma\tau\right)$ and $1 \in B$) and $\left(\Phi\left(u,h\right),c\right) \in X\left(\sigma\tau\right) \times B$ (since $\Phi\left(u,h\right) \in X\left(\sigma\tau\right)$ and $c \in B$).

But Lemma 6.4c (applied to $\sigma\tau$ instead of σ) yields that the map $X\left(\sigma\tau\right) \times B \to B\sigma\tau B$, $(g,b) \mapsto g\sigma\tau b$ is well-defined and is a bijection. In particular, this map is bijective, thus injective. In other words, if (g_1,b_1) and (g_2,b_2) are two elements of $X\left(\sigma\tau\right) \times B$ satisfying $g_1\sigma\tau b_1 = g_2\sigma\tau b_2$, then we have $(g_1,b_1) = (g_2,b_2)$. Applying this to $(g_1,b_1) = (k,1)$ and $(g_2,b_2) = \left(\Phi\left(u,h\right),c\right)$, we obtain $(k,1) = \left(\Phi\left(u,h\right),c\right)$ (since $(k,1) \in X\left(\sigma\tau\right) \times B$ and $\left(\Phi\left(u,h\right),c\right) \in X\left(\sigma\tau\right) \times B$ and $k\sigma\tau 1 = \Phi\left(u,h\right)\sigma\tau c$). In other words, $k = \Phi\left(u,h\right)$ and $1 = c$. Hence, $k = \Phi\left(u,h\right) \in \Phi\left(X\left(\sigma\right) \times X\left(\tau\right)\right)$.

Now, forget that we fixed k. We thus have shown that every $k \in X\left(\sigma\tau\right)$ satisfies $k \in \Phi\left(X\left(\sigma\right) \times X\left(\tau\right)\right)$. In other words, $X\left(\sigma\tau\right) \subseteq \Phi\left(X\left(\sigma\right) \times X\left(\tau\right)\right)$. In other words, the map Φ is surjective. (This proof was a more detailed paraphrase of an argument that you included in your proof of Proposition 6.4.)

Let us now show that the map Φ is injective. Indeed, let (g_1,h_1) and (g_2,h_2) be two elements of $X\left(\sigma\right) \times X\left(\tau\right)$ satisfying $\Phi\left(g_1,h_1\right) = \Phi\left(g_2,h_2\right)$. We shall show that $(g_1,h_1) = (g_2,h_2)$.

We have $(g_1,h_1) \in X\left(\sigma\right) \times X\left(\tau\right)$. In other words, $g_1 \in X\left(\sigma\right)$ and $h_1 \in X\left(\tau\right)$.

We have $(g_2,h_2) \in X\left(\sigma\right) \times X\left(\tau\right)$. In other words, $g_2 \in X\left(\sigma\right)$ and $h_2 \in X\left(\tau\right)$.

The definition of Φ yields $\Phi\left(g_1,h_1\right) = g_1\left(h_1\right)^{\sigma^{-1}}$. The definition of Φ yields $\Phi\left(g_2,h_2\right) = g_2\left(h_2\right)^{\sigma^{-1}}$. Now,

$$g_1\left(h_1\right)^{\sigma^{-1}} = \Phi\left(g_1,h_1\right) = \Phi\left(g_2,h_2\right) = g_2\left(h_2\right)^{\sigma^{-1}}.$$

Multiplying both sides of this equality by g_2^{-1} from the left and by $\left(\left(h_1\right)^{\sigma^{-1}}\right)^{-1}$ from the right, we obtain

$$g_2^{-1}g_1 = \left(h_2\right)^{\sigma^{-1}}\left(\left(h_1\right)^{\sigma^{-1}}\right)^{-1} = \left(h_2h_1^{-1}\right)^{\sigma^{-1}}$$

(since the map $G \to G$, $x \mapsto x^{\sigma^{-1}}$ is a group automorphism).

But the definition of $X\left(\sigma\right)$ yields $X\left(\sigma\right) = U \cap U^{(\sigma\rho)^{-1}}$. Hence, $X\left(\sigma\right)$ is the intersection of two subgroups of G (namely, of the subgroup U and of the subgroup $U^{(\sigma\rho)^{-1}}$). Thus, $X(\sigma)$ is itself a subgroup of G. The same argument (applied to τ instead of σ) shows that $X(\tau)$ is a subgroup of G.

From $g_2 \in X(\sigma)$ and $g_1 \in X(\sigma)$, we obtain $g_2^{-1}g_1 \in X(\sigma)$ (since $X(\sigma)$ is a subgroup of G).

From $h_2 \in X(\tau)$ and $h_1 \in X(\tau)$, we obtain $h_2h_1^{-1} \in X(\tau)$ (since $X(\tau)$ is a subgroup of G), so that $\left(h_2h_1^{-1}\right)^{\sigma^{-1}} \in (X(\tau))^{\sigma^{-1}}$.

Combining $g_2^{-1}g_1 \in X(\sigma)$ with $g_2^{-1}g_1 = \left(h_2h_1^{-1}\right)^{\sigma^{-1}} \in (X(\tau))^{\sigma^{-1}}$, we obtain $g_2^{-1}g_1 \in X(\sigma) \cap (X(\tau))^{\sigma^{-1}} = 1$ (by Lemma 6.4d **(b)**). In other words, $g_2^{-1}g_1 = 1$. Thus, $g_1 = g_2$.

Comparing $g_2^{-1}g_1 = 1$ with $g_2^{-1}g_1 = \left(h_2h_1^{-1}\right)^{\sigma^{-1}}$, we obtain $1 = \left(h_2h_1^{-1}\right)^{\sigma^{-1}} = \underbrace{\left(\sigma^{-1}\right)^{-1}}_{=\sigma} h_2h_1^{-1}\sigma^{-1} = \sigma h_2h_1^{-1}\sigma^{-1}$. Multiplying both sides of this equality by σ from the right, we obtain $\sigma = \sigma h_2h_1^{-1}$. Cancelling σ from this equality, we find $1 = h_2h_1^{-1}$. Thus, $h_1 = h_2$.

Now, $\left(\underbrace{g_1}_{=g_2}, \underbrace{h_1}_{=h_2}\right) = (g_2, h_2)$.

Let us now forget that we fixed (g_1, h_1) and (g_2, h_2). We thus have shown that if (g_1, h_1) and (g_2, h_2) are two elements of $X(\sigma) \times X(\tau)$ satisfying $\Phi(g_1, h_1) = \Phi(g_2, h_2)$, then $(g_1, h_1) = (g_2, h_2)$. In other words, the map Φ is injective. Since we also know that Φ is surjective, we therefore conclude that the map Φ is bijective. In other words, the map

$$X(\sigma) \times X(\tau) \to X(\sigma\tau), \qquad (g, h) \mapsto gh^{\sigma^{-1}}$$

is bijective (since this map is Φ). This proves Lemma 6.4d **(g)**. □]

Now, your Proposition 6.4 is precisely Lemma 6.4d **(g)**, whereas your Proposition 6.5 is exactly Lemma 6.4d **(f)**. Hence, both Proposition 6.4 and Proposition 6.5 are proven.

- **Definition 7.1:** Remove the comma in "preserves the sets,".
- **Definition 7.1:** After "it is the largest subgroup of Σ_n that preserves these sets", I would add "(actually, it is the set of all permutations $\sigma \in \Sigma_n$ that preserve these sets)". (This is a more concrete description of Σ_I, and you use it in the proof of Proposition 7.3 below.)

  I would also suggest replacing the word "sets" by "intervals" whenever you are talking about these sets.

- **Definition 7.2:** At the beginning of this definition, I would add the following sentences: "Let I be a subset of $\{1, 2, \ldots, n-1\}$. Set $I^c = \{0, 1, \ldots, n\} \setminus I$. Again, write this set I^c as $\{i_0, i_1, \ldots, i_r\}$ with $0 = i_0 < i_1 < \cdots < i_r = n$.".

- **Definition 7.2:** Replace "write P_i for $P\{i\}$ and P_{ij} for $P\{i, j\}$" by "write P_i for $P_{\{i\}}$ and P_{ij} for $P_{\{i,j\}}$".

- **Definition 7.2:** Replace "This gives a functor from n-dimensional vector spaces to sets" by "This gives a functor from the category (n-dimensional vector spaces, isomorphisms) to the category (sets, bijections)". (If you try to apply a linear map that is not an isomorphism to a flag, then the resulting flag might have different dimensions.)

- **Definition 7.2:** After "We let P_I denote the stabilizer of this flag", add "in G".

- **Proof of Proposition 7.3:** For the sake of clarity, I would replace the two sentences

  "Let σ be the permutation such that $g \in B\sigma B$. Recall from Section 6 that this is characterised by characterised by $Q_{i,\sigma(i)} \neq 0$, where

  $$Q_{ij} = \left(U_i \cap E_j\right) / \left(\left(U_{i-1} \cap E_j\right) + \left(U_i \cap E_{j-1}\right)\right).$$

  "

  by

  "Let $\sigma = \delta\left(g\underline{E}, \underline{E}\right)$. Then, $\sigma \in \Sigma_n$. If we define the map $\pi : G \to \Sigma_n$ as in the proof of Proposition 6.1, then $\pi(g) = \delta\left(g\underline{E}, \underline{E}\right) = \sigma$, so that $g \in \pi^{-1}\{\sigma\} = B\sigma B$ (as was proven in the proof of Proposition 6.1). Hence, it suffices to show that $\sigma \in \Sigma_I$ (because then, it will follow that $g \in B \underbrace{\sigma}_{\in \Sigma_I} B \subseteq B\Sigma_I B$, so that $P_I \subseteq B\Sigma_I B$ and therefore $P_I = B\Sigma_I B$). We have $\sigma = \delta\left(g\underline{E}, \underline{E}\right)$; in other words, each $i \in \{1, 2, \ldots, n\}$ satisfies $Q_{i,\sigma(i)} \neq 0$, where

  $$Q_{ij} = \left(U_i \cap E_j\right) / \left(\left(U_{i-1} \cap E_j\right) + \left(U_i \cap E_{j-1}\right)\right).$$

  ".

- **Proof of Proposition 7.3:** After "$U_a \leq U_{i-1}$", add "(since $a \leq i-1$)".

- **Proof of Lemma 7.4:** Replace "the element $g = \sigma g \sigma^{-1}$" by "the element $b = \sigma g \sigma^{-1}$".

- **Proof of Lemma 7.4:** Replace "$b\left(e_{\sigma(k)}\right) = e_{\sigma(k+1)}$" by "$b\left(e_{\sigma(k)}\right) = \underbrace{b}_{=\sigma g \sigma^{-1}} \sigma\left(e_k\right) = \sigma g \underbrace{\sigma^{-1}\sigma}_{=1}\left(e_k\right) = \sigma \underbrace{g\left(e_k\right)}_{=e_k + e_{k+1}} = \sigma\left(e_k + e_{k+1}\right) = e_{\sigma(k)} + e_{\sigma(k+1)}$".

- **Proof of Proposition 7.5:** After "Put $I = \{i \mid s_i \in P\}$", add ". Hence, $\Sigma_I \leq P$ and thus $P_I = B\Sigma_I B \leq P$, ".

- **Proof of Proposition 7.5:** Replace the sentence "Suppose that $g \in P$, and put $\sigma = \pi(g)$." by the following: "Thus, it remains to show that $P \leq P_I$. Let $g \in P$; our goal is to prove that $g \in P_I$. Define the map $\pi : G \to \Sigma_n$ as in the proof of Proposition 6.1. Set $\sigma = \pi(g)$. We showed in the proof of Proposition 6.1 that $\pi^{-1}\{\sigma\} = B\sigma B$. Now, from $\sigma = \pi(g)$, we obtain $g \in \pi^{-1}\{\sigma\} = B\sigma B$, so that $BgB = B\sigma B$.".

- **Proof of Proposition 7.5:** Before "If $l(\sigma) = 0$", add the following sentences: "Thus, it suffices to prove that $\sigma \in P_I$. Now, let us forget how σ was defined. Our goal is to show that $\sigma \in P_I$ for every $\sigma \in \Sigma_n$ satisfying $\sigma \in P$. We shall do this by induction over $l(\sigma)$:".

- **Proof of Proposition 7.5:** Replace "Now suppose that $l(\sigma) > 1$" by "Now suppose that $l(\sigma) > 0$". Also, remove the preceding sentence ("If $l(\sigma) = 1$ then $\sigma = s_i$ for some i and $\sigma \in P$ so $i \in I$ so $\sigma \in P_I$") completely (it is unnecessary and complicates the structure of the proof).

- **Proof of Proposition 7.5:** Replace "so $s_k \in P_I$" by "so $s_k \in \Sigma_I \subseteq B\Sigma_I B = P_I$".

- **Proof of Proposition 7.5:** Replace "so we can assume by induction that" by "so the induction hypothesis yields".

- **Proof of Proposition 7.5:** Remove "and thus that $g \in P_I$".

- **Proof of Proposition 7.5:** I would notice that your proof of Proposition 7.5 proves a slightly slonger claim:

  Proposition 7.5a. Let P be a subgroup of G such that $P \geq B$. Let $I = \{i \mid s_i \in P\}$. Then, $P = P_I$.

  Furthermore, let me state another fact (that will be used later):

  Lemma 7.5b. Let $I \subseteq \{1, 2, \ldots, n-1\}$. Then, $I = \{i \mid s_i \in P_I\}$.

  [*Proof of Lemma 7.5b.* Define a subset J of $\{1, 2, \ldots, n-1\}$ by $J = \{i \mid s_i \in P_I\}$. Then, $J = \{i \mid s_i \in P_I\} \supseteq I$ (since every $i \in I$ satisfies $s_i \in \Sigma_I \subseteq B\Sigma_I B = P_I$).

  Now, let $j \in J$. We are going to prove that $j \in I$.

  Indeed, assume the contrary. Hence, $j \notin I$, so that $j \in I^c$. Hence, E_j is one of the entries of the obvious flag $\underline{E} \in \operatorname{Flag}_I\left(\mathbb{F}_p^n\right)$. Therefore, the group P_I fixes the subspace E_j (since the group P_I fixes the obvious flag $\underline{E} \in \operatorname{Flag}_I\left(\mathbb{F}_p^n\right)$). In other words, $pE_j \subseteq E_j$ for each $p \in P_I$.

But $j \in J = \{i \mid s_i \in P_I\}$. In other words, $s_j \in P_I$. But we have $pE_j \subseteq E_j$ for each $p \in P_I$. Applying this to $p = s_j$, we conclude that $s_jE_j \subseteq E_j$ (since $s_j \in P_I$). Now, $s_je_j = e_{j+1}$, so that $e_{j+1} = s_j \underbrace{e_j}_{\in E_j} \in s_jE_j \subseteq E_j$. This contradicts the (obvious) fact that $e_{j+1} \notin E_j$. This contradiction proves that our assumption was false. Hence, we have $j \in I$.

Now, forget that we fixed j. We thus have shown that $j \in I$ for each $j \in J$. In other words, $J \subseteq I$. Combining this with $J \supseteq I$, we obtain $J = I$. Hence, $I = J = \{i \mid s_i \in P_I\}$. This proves Lemma 7.5b. □]

- **Proposition 7.7:** Add "Let $V = \mathbb{F}_p^n$." at the beginning of the theorem. (Otherwise, $\operatorname{Flag}_I(V)$ and $\operatorname{Flag}_J(V)$ wouldn't canonically be G-sets.)

- **Proof of Proposition 7.7:** Again, I'd prefer some more details:

  1. You claim that "the orbits of B in V are precisely the sets $E_k \setminus E_{k-1}$". In order for this claim to be fully correct, you should set $E_{-1} = \varnothing$, and allow k to range over $\{0, 1, \ldots, n\}$ (rather than $\{1, 2, \ldots, n\}$ only). (Otherwise, you are missing the orbit $\{0\} = E_0 \setminus E_{-1}$.)

  Let me also prove this claim:

  [*Proof of the fact that the orbits of B in V are precisely the sets $E_k \setminus E_{k-1}$:* For every $k \in \{1, 2, \ldots, n\}$, we have
  $$E_k \setminus E_{k-1} = Be_k \tag{30}$$
  [15].

[15] *Proof of (30):* Let $k \in \{1, 2, \ldots, n\}$. Hence, the vector e_k is well-defined.

Let $b \in B$. Then, $bE_k = E_k$ and $bE_{k-1} = E_{k-1}$ (by the definition of B). But the element b of G is invertible (since G is a group), thus a bijection. Hence, $b(E_k \setminus E_{k-1}) = \underbrace{bE_k}_{=E_k} \setminus \underbrace{bE_{k-1}}_{=E_{k-1}} = E_k \setminus E_{k-1}$.

Now, $e_k \in E_k \setminus E_{k-1}$ (since $e_k \in E_k$ and $e_k \notin E_{k-1}$), and thus $b \underbrace{e_k}_{\in E_k \setminus E_{k-1}} \in b(E_k \setminus E_{k-1}) = E_k \setminus E_{k-1}$.

Now, forget that we fixed b. We thus have shown that $be_k \in E_k \setminus E_{k-1}$ for each $b \in B$. In other words, $Be_k \subseteq E_k \setminus E_{k-1}$.

On the other hand, fix $\zeta \in E_k \setminus E_{k-1}$. Thus, $\zeta \in E_k$ and $\zeta \notin E_{k-1}$. The last $n-k$ coordinates of ζ are zero (since $\zeta \in E_k$), but the last $n-k+1$ coordinates of ζ are not all zero (since $\zeta \notin E_{k-1}$). Hence, the k-th coordinate of ζ must be nonzero.

Let $c \in \mathbb{F}_p^{n \times n}$ be the $n \times n$-matrix whose k-th column is ζ whereas all its other columns are the corresponding columns of the identity matrix (i.e., for each $i \neq k$, the i-th column of c shall be e_i). Then, the k-th column of c is the vector ζ, whose last $n-k$ coordinates are zero. Thus, the last $n-k$ entries of the k-th column of c are zero. Moreover, the k-th column of c is the vector ζ, whose k-th coordinate is nonzero. Hence, the k-th entry of the k-th column of c is nonzero. Now, the matrix c is upper-triangular (since the last $n-k$ entries of the k-th column of c are zero, while all other columns are the corresponding columns of the identity

Every set of the form $E_k \setminus E_{k-1}$ (with $k \in \{0, 1, \ldots, n\}$) is an orbit of B in V [16]. The union of these orbits $E_k \setminus E_{k-1}$ is the whole space $\mathbb{F}_p^n$ (because this union is $\bigcup_{k=0}^{n} (E_k \setminus E_{k-1}) = \underbrace{E_n}_{=\mathbb{F}_p^n} \setminus \underbrace{E_{-1}}_{=\varnothing} = \mathbb{F}_p^n \setminus \varnothing = \mathbb{F}_p^n$). Hence, these orbits $E_k \setminus E_{k-1}$ are **all** the orbits of B in V. This is exactly what we wanted to prove. $\square$]

2. You claim that "the spaces E_k are the only B-invariant subspace of V". This claim has a little typo in it ("subspace" should be "subspaces"), and again needs a proof.

[*Proof of the fact that the subspaces E_k (for $k \in \{0, 1, \ldots, n\}$) are the only B-invariant subspaces of V:* For each $k \in \{0, 1, \ldots, n\}$, the subspace E_k is a B-invariant subspace of V (because every $b \in B$ satisfies $bE_k = E_k$). Conversely, every B-invariant subspace of V has the form E_k for some $k \in \{0, 1, \ldots, n\}$ [17]. Hence, the subspaces E_k (for $k \in \{0, 1, \ldots, n\}$) are the

matrix) and its diagonal entries are nonzero (since the k-th entry of the k-th column of c is nonzero, while all other columns are the corresponding columns of the identity matrix). Thus, the matrix c is an invertible upper-triangular matrix. In other words, $c \in B$. Now, $ce_k = (\text{the } k\text{-th column of } c) = \zeta$, so that $\zeta = \underbrace{c}_{\in B} e_k \in Be_k$.

Now, forget that we fixed ζ. We thus have proven that $\zeta \in Be_k$ for each $\zeta \in E_k \setminus E_{k-1}$. In other words, $E_k \setminus E_{k-1} \subseteq Be_k$. Combining this with $Be_k \subseteq E_k \setminus E_{k-1}$, we obtain $E_k \setminus E_{k-1} = Be_k$. This proves (30).

[16] *Proof.* Let $k \in \{0, 1, \ldots, n\}$. We must show that the set $E_k \setminus E_{k-1}$ is an orbit of B in V.

If $k = 0$, then this is fairly clear (indeed, if $k = 0$, then $\underbrace{E_k}_{=E_0 = \{0\}} \setminus \underbrace{E_{k-1}}_{=E_{-1} = \varnothing} = \{0\} \setminus \varnothing = \{0\} = B0$, which is clearly an orbit of B in V). Thus, we WLOG assume that $k \neq 0$. Hence, $k \in \{1, 2, \ldots, n\}$ (since $k \in \{1, 2, \ldots, n\}$). Hence, (30) shows that $E_k \setminus E_{k-1} = Be_k$. Thus, $E_k \setminus E_{k-1}$ is an orbit of B in V (since Be_k is an orbit of B in V). Qed.

[17] *Proof.* Let Q be a B-invariant subspace of V. We must show that Q has the form E_k for some $k \in \{0, 1, \ldots, n\}$.

We have $Q \subseteq V = \mathbb{F}_p^n = E_n$. Hence, there exists some $k \in \{-1, 0, \ldots, n\}$ such that $Q \subseteq E_k$ (namely, $k = n$). Let ℓ be the **largest** such k. Thus, $Q \subseteq E_\ell$.

We have $0 \in Q$ (since Q is a subspace of V) but $0 \notin \varnothing$. If we had $E_\ell = \varnothing$, then we would have $0 \in Q \subseteq E_\ell = \varnothing$, which would contradict $0 \notin \varnothing$. Hence, we cannot have $E_\ell = \varnothing$. Thus, we have $E_\ell \neq \varnothing = E_{-1}$. Consequently, $\ell \neq -1$. Hence, $\ell \geq 0$, so that $\ell \in \{0, 1, \ldots, n\}$ and therefore $\ell - 1 \in \{-1, 0, \ldots, n\}$.

But ℓ is the **largest** $k \in \{-1, 0, \ldots, n\}$ such that $Q \subseteq E_k$ (by the definition of ℓ). Thus, every $k \in \{-1, 0, \ldots, n\}$ satisfying $k < \ell$ satisfies $Q \not\subseteq E_k$. Applying this to $k = \ell - 1$, we obtain $Q \not\subseteq E_{\ell-1}$ (since $\ell - 1 < \ell$). Thus, there exists some $q \in Q$ such that $q \notin E_{\ell-1}$. Consider this q. Combining $q \in Q \subseteq E_\ell$ with $q \notin E_{\ell-1}$, we obtain $q \in E_\ell \setminus E_{\ell-1} = Be_\ell$ (by (30)). In other words, there exists some $b \in B$ such that $q = be_\ell$. Consider this b. Since B is a group, we have $Bb = B$ (since $b \in B$). Now, $B \underbrace{q}_{=be_\ell} = \underbrace{Bb}_{=B} e_\ell = Be_\ell = E_\ell \setminus E_{\ell-1}$. Thus, $E_\ell \setminus E_{\ell-1} = B \underbrace{q}_{\in Q} \subseteq BQ \subseteq Q$ (since the subspace Q is B-invariant).

Now, let $r \in E_\ell$. We will show that $r \in Q$. In fact, if $r \in E_\ell \setminus E_{\ell-1}$, then this is obvious (because if $r \in E_{\ell-1}$, then $r \in E_\ell \setminus E_{\ell-1} \subseteq Q$). Thus, we WLOG assume that we don't have only B-invariant subspaces of V. This completes the proof. $\square$]

- **Proof of Proposition 7.7:** Replace "the point $\underline{E}_I \in \operatorname{Flag}_I(V)$" by "the point $\underline{E} \in \operatorname{Flag}_I(V)$".
- **Proof of Proposition 7.7:** Replace "any map" by "any G-equivariant map".
- **Proof of Proposition 7.7:** You write that "It is also clear that $P_I \leq P_J$ iff $I \subseteq J$". Maybe it is worth giving a proof of this:

  [*Proof of the fact that $P_I \leq P_J$ iff $I \subseteq J$:* We want to show that $P_I \leq P_J$ iff $I \subseteq J$. One direction of this equivalence is clear (namely: if $I \subseteq J$, then $P_I \leq P_J$). It remains to prove the other. In other words, it remains to prove that if $P_I \leq P_J$, then $I \subseteq J$. So let us assume that $P_I \leq P_J$. We must show that $I \subseteq J$.

  Lemma 7.5b yields $I = \{i \mid s_i \in P_I\} \subseteq \{i \mid s_i \in P_J\}$ (since $P_I \leq P_J$).

  But Lemma 7.5b (applied to J instead of I) yields $J = \{i \mid s_i \in P_J\}$. Hence, $I \subseteq \{i \mid s_i \in P_J\} = J$. Thus, $I \subseteq J$ is proven. This completes our proof. $\square$]

- **§7:** I think it is worthwhile stating three additional facts as consequences of the proof of Proposition 7.7:

  Proposition 7.7a. Let $V = \mathbb{F}_p^n$. Let $I \subseteq \{1, 2, \ldots, n-1\}$. Then, $\operatorname{Flag}_I(V) \cong G/P_I$ as G-sets.

  [*Proof of Proposition 7.7a.* In the proof of Proposition 7.7, we have shown that G acts transitivitely on $\operatorname{Flag}_I(V)$. Thus, for any $\underline{X} \in \operatorname{Flag}_I(V)$, we have $\operatorname{Flag}_I(V) \cong G/G_{\underline{X}}$ as G-sets, where $G_{\underline{X}}$ denotes the stabilizer of $\underline{X}$. Applying this to $\underline{X} = \underline{E}$ (where $\underline{E}$ is the "obvious flag" defined in Definition 7.2), we conclude that $\operatorname{Flag}_I(V) \cong G/G_{\underline{E}}$ as G-sets. But the stabilizer of $\underline{E}$ is P_I (by the definition of P_I). In other words, $G_{\underline{E}} = P_I$. Hence, $\operatorname{Flag}_I(V) \cong G/\underbrace{G_{\underline{E}}}_{=P_I} = G/P_I$ as G-sets. This proves Proposition 7.7a. $\square$]

$r \in E_\ell \setminus E_{\ell-1}$. In other words, we have $r \notin E_\ell \setminus E_{\ell-1}$. Combining $r \in E_\ell$ with $r \notin E_\ell \setminus E_{\ell-1}$, we obtain $r \in E_\ell \setminus (E_\ell \setminus E_{\ell-1}) \subseteq E_{\ell-1}$.

If we had $r - q \in E_{\ell-1}$, then we would have $q = \underbrace{r}_{\in E_{\ell-1}} - \underbrace{(r-q)}_{\in E_{\ell-1}} \in E_{\ell-1} - E_{\ell-1} \subseteq E_{\ell-1}$ (since $E_{\ell-1}$ is a vector space), which would contradict $q \notin E_{\ell-1}$. Hence, we do not have $r - q \in E_{\ell-1}$. In other words, we have $r - q \notin E_{\ell-1}$. But $\underbrace{r}_{\in E_\ell \setminus E_{\ell-1} \subseteq E_\ell} - \underbrace{q}_{\in E_\ell} \in E_\ell - E_\ell \subseteq E_\ell$ (since E_ℓ is a vector space). Combining this with $r - q \notin E_{\ell-1}$, we obtain $r - q \in E_\ell \setminus E_{\ell-1} \subseteq Q$. Now, $r = \underbrace{q}_{\in Q} + \underbrace{(r-q)}_{\in Q} \in Q + Q \subseteq Q$ (since Q is a vector space). Hence, we have proven that $r \in Q$.

Now, forget that we fixed r. We thus have shown that $r \in Q$ for each $r \in E_\ell$. In other words, $E_\ell \subseteq Q$. Combining this with $Q \subseteq E_\ell$, we obtain $Q = E_\ell$. Thus, $Q = E_k$ for some $k \in \{0, 1, \ldots, n\}$ (namely, $k = \ell$). In other words, Q has the form E_k for some $k \in \{0, 1, \ldots, n\}$. Qed.

Proposition 7.7b. Let $V = \mathbb{F}_p^n$. Let $I \subseteq \{1, 2, \ldots, n-1\}$. For any $g \in G$, we shall use the notation $\overline{g}$ for the coset gP_I of g in G/P_I.

(a) There is precisely one B-fixed point in G/P_I. This B-fixed point is $\overline{1}$, and will be called the *basepoint* of G/P_I. We have

$$\left(G/P_I\right)^B = \left\{\overline{1}\right\}. \tag{31}$$

(b) Let $i \in \{1, 2, \ldots, n-1\}$. Then, $\left(G/P_I\right)^{P_i} = \begin{cases} \left\{\overline{1}\right\}, & \text{if } i \in I; \\ \varnothing, & \text{otherwise} \end{cases}$.

[*Proof of Proposition 7.7b.* Proposition 7.7a yields $\operatorname{Flag}_I(V) \cong G/P_I$ as G-sets.

We have the following general fact about group actions: If $\mathfrak{A}$ is a subgroup of a group $\mathfrak{G}$, and if $\mathfrak{X}$ is a $\mathfrak{G}$-set, then

$$\mathfrak{X}^{\mathfrak{A}} \cong \operatorname{Map}_{\mathfrak{G}}\left(\mathfrak{G}/\mathfrak{A}, \mathfrak{X}\right) \tag{32}$$

as sets[18].

(a) In the proof of Proposition 7.7, we have seen that the point $\underline{E} \in \operatorname{Flag}_I(V)$ is the unique B-fixed point in $\operatorname{Flag}_I(V)$. In other words, $\left(\operatorname{Flag}_I(V)\right)^B = \{\underline{E}\}$. But $\operatorname{Flag}_I(V) \cong G/P_I$ as G-sets. Hence, $\left(\operatorname{Flag}_I(V)\right)^B \cong \left(G/P_I\right)^B$ as sets. Thus, $\left(G/P_I\right)^B \cong \left(\operatorname{Flag}_I(V)\right)^B = \{\underline{E}\}$ as sets. Hence, $\left(G/P_I\right)^B$ is a 1-element set (since $\{\underline{E}\}$ is a 1-element set).

For every $b \in B$, we have $b\overline{1} = \overline{b1} = \overline{b} = \overline{1}$ in G/P_I (since $b \in B \leq P_I$). Therefore, $\overline{1} \in \left(G/P_I\right)^B$. Therefore, $\left(G/P_I\right)^B = \left\{\overline{1}\right\}$ (since $\left(G/P_I\right)^B$ is a 1-element set). In other words, the set of all B-fixed points in G/P_I is $\left\{\overline{1}\right\}$. In other words, there is precisely one B-fixed point in G/P_I, and this B-fixed point is $\overline{1}$. This completes the proof of Proposition 7.7b **(a)**.

(b) Applying (32) to $\mathfrak{G} = G$, $\mathfrak{A} = P_i$ and $\mathfrak{X} = G/P_I$, we conclude that $\left(G/P_I\right)^{P_i} \cong \operatorname{Map}_G\left(G/P_i, G/P_I\right)$ as sets. But recall that $\operatorname{Flag}_I(V) \cong G/P_I$ as G-sets. Also, Proposition 7.7a (applied to $\{i\}$ instead of I) yields $\operatorname{Flag}_{\{i\}}(V) \cong$

[18] This is easy to prove. (In fact, for each $g \in \mathfrak{G}$, let $\overline{g}$ denote the coset $g\mathfrak{A}$ of g in $\mathfrak{G}/\mathfrak{A}$. Then, the map $\operatorname{Map}_{\mathfrak{G}}\left(\mathfrak{G}/\mathfrak{A}, \mathfrak{X}\right) \to \mathfrak{X}^{\mathfrak{A}}$ sending each $f \in \operatorname{Map}_{\mathfrak{G}}\left(\mathfrak{G}/\mathfrak{A}, \mathfrak{X}\right)$ to $f\left(\overline{1}\right) \in \mathfrak{X}^{\mathfrak{A}}$ is a bijection. Indeed, its inverse map sends each $u \in \mathfrak{X}^{\mathfrak{A}}$ to the G-map $\mathfrak{G}/\mathfrak{A} \to \mathfrak{X}$, $\overline{g} \mapsto gu$.)

$G/P_{\{i\}} = G/P_i$ as G-sets. Hence,

$$(G/P_I)^{P_i} \cong \operatorname{Map}_G\left(\underbrace{G/P_i}_{\substack{\cong \operatorname{Flag}_{\{i\}}(V) \\ = \operatorname{Flag}_i(V)}}, \underbrace{G/P_I}_{\cong \operatorname{Flag}_I(V)}\right) \cong \operatorname{Map}_G\left(\operatorname{Flag}_i(V), \operatorname{Flag}_I(V)\right)$$
$$= \begin{cases} (\text{a singleton}), & \text{if } \{i\} \subseteq I; \\ \varnothing, & \text{otherwise} \end{cases}$$
$$\left(\begin{array}{c}\text{by Proposition 7.7 (applied to } \{i\} \text{ and } I \\ \text{instead of } I \text{ and } J)\end{array}\right)$$
$$= \begin{cases} (\text{a singleton}), & \text{if } i \in I; \\ \varnothing, & \text{otherwise} \end{cases}.$$

Therefore, if $i \notin I$, then $(G/P_I)^{P_i} \cong \varnothing$ and thus $(G/P_I)^{P_i} = \varnothing$. Hence, Proposition 7.7b **(b)** is proven in the case when $i \notin I$. We thus WLOG assume that we don't have $i \notin I$. Hence, we have $i \in I$. We must show that $(G/P_I)^{P_i} = \{\overline{1}\}$.

Now, $(G/P_I)^{P_i} \cong \begin{cases} (\text{a singleton}), & \text{if } i \in I; \\ \varnothing, & \text{otherwise} \end{cases} = (\text{a singleton})$ (since $i \in I$).

Hence, $(G/P_I)^{P_i}$ is a 1-element set.

But $i \in I$, so that $\{i\} \subseteq I$ and thus $P_{\{i\}} \subseteq P_I$. Therefore, every $p \in P_i$ satisfies $p\overline{1} = \overline{p1} = \overline{p} = \overline{1}$ in G/P_I (since $p \in P_i = P_{\{i\}} \subseteq P_I$). In other words, $\overline{1} \in (G/P_I)^{P_i}$. Since $(G/P_I)^{P_i}$ is a 1-element set, we can therefore conclude that $(G/P_I)^{P_i} = \{\overline{1}\}$. This completes the proof of Proposition 7.7b **(b)**.]

Proposition 7.7c. Let $V = \mathbb{F}_p^n$. Let X be a parabolic G-set. For each $y \in X^B$, set $I_y = \left\{i \in \{1, 2, \ldots, n-1\} \mid y \in X^{P_i}\right\}$. For each $y \in X$, let G_y denote the stabilizer of y in G.

(a) If $y \in X^B$, then $P_{I_y} = G_y$.

(b) Let $y_1 \in X^B$, $y_2 \in X^B$, $q_1 \in G$ and $q_2 \in G$ be such that $q_1 y_1 = q_2 y_2$. Then, $y_1 = y_2$ and $q_1 G_{y_1} = q_2 G_{y_1}$.

[*Proof of Proposition 7.7c.* **(a)** Let $y \in X^B$. Then, $B \subseteq G_y$ (since $y \in X^B$), so that $G_y \geq B$. Thus, G_y is a subgroup of G such that $G_y \geq B$.

Let $I = \left\{i \mid s_i \in G_y\right\}$. Hence, Proposition 7.5a (applied to $P = G_y$) shows that $G_y = P_I$.

Now, let $j \in I_y$. Then, $j \in I_y = \left\{i \in \{1, 2, \ldots, n-1\} \mid y \in X^{P_i}\right\}$. In other words, j is an element of $\{1, 2, \ldots, n-1\}$ and satisfies $y \in X^{P_j}$. But $P_j =$

$P_{\{j\}} = B\Sigma_{\{j\}}B$ (by Proposition 7.3, applied to $\{j\}$ instead of I). Now, $s_j = \underbrace{1}_{\in B} \underbrace{s_j}_{\in \Sigma_{\{j\}}} \underbrace{1}_{\in B} \in B\Sigma_{\{j\}}B = P_j$.

From $y \in X^{P_j}$, we conclude that $py = y$ for each $p \in P_j$. Applying this to $p = s_j$, we obtain $s_j y = y$ (since $s_j \in P_j$). In other words, $s_j \in G_y$. In other words, $j \in \left\{i \mid s_i \in G_y\right\}$. This rewrites as $j \in I$ (since $I = \left\{i \mid s_i \in G_y\right\}$).

Now, forget that we fixed j. We thus have proven that $j \in I$ for each $j \in I_y$. In other words, $I_y \subseteq I$.

On the other hand, let $k \in I$. Thus, $k \in I = \left\{i \mid s_i \in G_y\right\}$. In other words, k is an element of $\{1, 2, \ldots, n-1\}$ and satisfies $s_k \in G_y$. In other words, $s_k y = y$.

But $P_k = P_{\{k\}} = B\Sigma_{\{k\}}B$ (by Proposition 7.3, applied to $\{k\}$ instead of I). The definition of $\Sigma_{\{k\}}$ yields $\Sigma_{\{k\}} = \langle s_k \rangle = \{1, s_k\}$. Hence, $gy = y$ for each $g \in \Sigma_{\{k\}}$ (since $1y = y$ and $s_k y = y$). In other words, $y \in X^{\Sigma_{\{k\}}}$.

Now, let $p \in P_k$. Then, $p \in P_k = B\Sigma_{\{k\}}B$. In other words, there exist $b_1 \in B$, $g \in \Sigma_{\{k\}}$ and $b_2 \in B$ such that $p = b_1 g b_2$. Consider these b_1, g and b_2. Now,

$$\underbrace{p}_{=b_1 g b_2} y = b_1 g \underbrace{b_2 y}_{\substack{=y \\ (\text{since } y \in X^B)}} = b_1 \underbrace{gy}_{\substack{=y \\ (\text{since } y \in X^{\Sigma_{\{k\}}})}} = b_1 y = y$$

(since $y \in X^B$).

Now, forget that we fixed p. We thus have proven that $py = y$ for each $p \in P_k$. In other words, $y \in X^{P_k}$. Hence, k is an element of $\{1, 2, \ldots, n-1\}$ and satisfies $y \in X^{P_k}$. In other words, $k \in \left\{i \in \{1, 2, \ldots, n-1\} \mid y \in X^{P_i}\right\}$. In other words, $k \in I_y$ (since $I_y = \left\{i \in \{1, 2, \ldots, n-1\} \mid y \in X^{P_i}\right\}$).

Now, forget that we fixed k. We thus have proven that $k \in I_y$ for each $k \in I$. In other words, $I \subseteq I_y$. Combining this with $I_y \subseteq I$, we obtain $I_y = I$. Hence, $P_{I_y} = P_I = G_y$. This proves Proposition 7.7c **(a)**.

(b) Let $Y = Gy_1$ be the G-orbit of y_1. Then, Y is a G-subset of X^B. Moreover, $Y \cong G/G_{y_1}$ as G-sets (by the orbit-stabilizer theorem). Proposition 7.7c **(a)** (applied to $y = y_1$) yields $P_{I_{y_1}} = G_{y_1}$. But Proposition 7.7b **(a)** (applied to $I = I_{y_1}$) yields $\left(G/P_{I_{y_1}}\right)^B = \left\{\overline{1}\right\}$. Hence, $\left|\left(G/P_{I_{y_1}}\right)^B\right| = \left|\left\{\overline{1}\right\}\right| = 1$.

We have $Y \cong G/\underbrace{G_{y_1}}_{=P_{I_{y_1}}} = G/P_{I_{y_1}}$ as G-sets, and thus $Y^B \cong \left(G/P_{I_{y_1}}\right)^B$ as sets. Hence, $\left|Y^B\right| = \left|\left(G/P_{I_{y_1}}\right)^B\right| = 1$.

Both y_1 and y_2 are B-fixed points (since $y_1 \in X^B$ and $y_2 \in X^B$). We have $q_1 y_1 = q_2 y_2$. Multiplying both sides of this equality by q_2^{-1}, we obtain $q_2^{-1} q_1 y_1 = \underbrace{q_2^{-1} q_2}_{=1} y_2 = y_2$, so that $y_2 = \underbrace{q_2^{-1} q_1}_{\in G} y_1 \in G y_1 = Y$.

We have $y_1 \in Y$ (since Y is the G-orbit of y_1). Thus, $y_1 \in Y^B$ (since y_1 is a B-fixed point). We also have $y_2 \in Y$. Thus, $y_2 \in Y^B$ (since y_2 is a B-fixed point).

But Y^B is a 1-element set (since $\left|Y^B\right| = 1$). Thus, any two elements of Y^B are identical. Applying this to the two elements y_1 and y_2 of Y^B, we conclude that y_1 and y_2 are identical (since $y_1 \in Y^B$ and $y_2 \in Y^B$). In other words, $y_1 = y_2$.

Now, $q_2^{-1} q_1 y_1 = y_2 = y_1$. In other words, $q_2^{-1} q_1 \in G_{y_1}$. In other words, $q_1 G_{y_1} = q_2 G_{y_1}$. This completes the proof of Proposition 7.7c **(b)**. $\square$]

- **Definition 7.8:** Replace "the category of finite sets Y equipped with a list $(Y_1, \ldots, Y_{n-1})$ of subsets." by "the category whose objects are finite sets Y equipped with a list $(Y_1, \ldots, Y_{n-1})$ of subsets. Such an object will be denoted $(Y; Y_1, \ldots, Y_{n-1})$. Morphisms $(Y; Y_1, \ldots, Y_{n-1}) \to (Z; Z_1, \ldots, Z_{n-1})$ in $\mathcal{P}'$ shall be maps $Y \to Z$ mapping each Y_i into Z_i."

- **Proof of Proposition 7.9:** Replace "Consider an object $Y \in \mathcal{P}'$." by "Consider an object $(Y; Y_1, \ldots, Y_{n-1}) \in \mathcal{P}'$ (abbreviated as Y).".

- **Proof of Proposition 7.9:** Replace "Now consider a morphism $f : Y \to Z$ in $\mathcal{P}'$" by "Now consider a morphism $f : (Y; Y_1, \ldots, Y_{n-1}) \to (Z; Z_1, \ldots, Z_{n-1})$ in $\mathcal{P}'$".

- **Proof of Proposition 7.9:** You write: "so there is a unique G-map $G/P_{I_y} \to G/P_{I_{f(y)}}$". The uniqueness of this G-map might need a proof[19].

[19] *Proof.* We have $I_y \subseteq I_{f(y)}$. Thus, $P_{I_y} \subseteq P_{I_{f(y)}}$ (because if two subsets I and J of $\{1, 2, \ldots, n-1\}$ satisfy $I \subseteq J$, then they also satisfy $P_I \subseteq P_J$). Hence, there clearly exists a G-map $G/P_{I_y} \to G/P_{I_{f(y)}}$ (namely, the map that sends any coset gP_{I_y} of P_{I_y} to the coset $gP_{I_{f(y)}}$ of $P_{I_{f(y)}}$). It remains to prove that there exists **at most one** G-map $G/P_{I_y} \to G/P_{I_{f(y)}}$.

Let $V = \mathbb{F}_p^n$. If I is any subset of $\{1, 2, \ldots, n-1\}$, then we have $\operatorname{Flag}_I(V) \cong G/P_I$ as G-sets (because G acts transitively on the G-set $\operatorname{Flag}_I(V)$, and the stabilizer of the element $\underline{E} \in \operatorname{Flag}_I(V)$ is P_I). In other words, if I is a subset of $\{1, 2, \ldots, n-1\}$, then $G/P_I \cong \operatorname{Flag}_I(V)$ as G-sets. Thus, if I and J are two subsets of $\{1, 2, \ldots, n-1\}$, then

$$\operatorname{Map}_G\left(\underbrace{G/P_I}_{\cong \operatorname{Flag}_I(V)}, \underbrace{G/P_J}_{\cong \operatorname{Flag}_J(V)}\right) \cong \operatorname{Map}_G\left(\operatorname{Flag}_I(V), \operatorname{Flag}_J(V)\right) = \begin{cases} \text{a singleton}, & \text{if } I \subseteq J \\ \varnothing, & \text{otherwise} \end{cases}$$

(by Proposition 7.7). Hence, if I and J are two subsets of $\{1, 2, \ldots, n-1\}$, then the set $\operatorname{Map}_G(G/P_I, G/P_J)$ has at most one element. In other words, if I and J are two subsets

- **Proof of Proposition 7.9:** Replace “this gives us a functor $\mathcal{P}' \to \mathcal{P}$” by “this gives us a functor $F' : \mathcal{P}' \to \mathcal{P}$”.

- **Proof of Proposition 7.9:** You write: “Note that

$$(G/P_I)^{P_i} = \operatorname{Map}_G\left(\operatorname{Flag}_i(V), \operatorname{Flag}_I(V)\right) = \begin{cases} 1 & \text{if } i \in I \\ \varnothing & \text{otherwise.} \end{cases}$$

Using this we see that $FF' = 1_{\mathcal{P}'}$.”.

I would suggest replacing this by the following (more detailed) argument: “Let $Y \in \mathcal{P}'$ be an object. Then, $F'Y = \coprod_{y\in Y} G/P_{I_y}$, so that

$$\left(F'Y\right)^B = \left(\coprod_{y\in Y} G/P_{I_y}\right)^B \cong \coprod_{y\in Y} \underbrace{\left(G/P_{I_y}\right)^B}_{\substack{=\left\{\overline{1}\right\} \\ \text{(by (31), applied to } I=I_y\text{)}}} = \coprod_{y\in Y} \left\{\overline{1}\right\}.$$

Hence, there exists a bijection $Y \to \left(F'Y\right)^B$ that sends each $y \in Y$ to the element $\overline{1}$ of G/P_{I_y}. Denote this bijection by η_Y.

We have $FF'Y = \left(F'Y\right)^B$ as sets (by the definition of the functor F). Thus, the bijection $\eta_Y : Y \to \left(F'Y\right)^B$ is a bijection $Y \to FF'Y$.

This bijection η_Y is an isomorphism in the category $\mathcal{P}'$ [20].

Now, forget that we fixed Y. Thus, for each object $Y \in \mathcal{P}'$, we have constructed an isomorphism $\eta_Y : Y \to FF'Y$ in the category $\mathcal{P}'$. It is straightforward to see that this isomorphism η_Y is functorial in Y. Thus, we have

of $\{1, 2, \ldots, n-1\}$, then there exists **at most one** G-map $G/P_I \to G/P_J$. Applying this to $I = I_y$ and $J = I_{f(y)}$, we conclude that there exists **at most one** G-map $G/P_{I_y} \to G/P_{I_{f(y)}}$. This concludes our proof.

[20] *Proof.* Fix $j \in \{1, 2, \ldots, n-1\}$.

For each $y \in Y$, we have $I_y = \{i \in \{1, 2, \ldots, n-1\} \mid y \in Y_i\}$ (by the definition of I_y). Hence, for each $y \in Y$ and $i \in \{1, 2, \ldots, n-1\}$, we have the following logical equivalence:

$$\left(i \in I_y\right) \iff \left(y \in Y_i\right).$$

Applying this to $i = j$, we conclude that for each $y \in Y$, we have the following logical equivalence:

$$\left(j \in I_y\right) \iff \left(y \in Y_j\right). \tag{33}$$

For every $y \in Y$, we have

$$\begin{aligned} \left(G/P_{I_y}\right)^{P_j} &= \begin{cases} \left\{\overline{1}\right\}, & \text{if } j \in I_y; \\ \varnothing, & \text{otherwise} \end{cases} && \text{(by Proposition 7.7b \textbf{(b)}, applied to } j \text{ instead of } i\text{)} \\ &= \begin{cases} \left\{\overline{1}\right\}, & \text{if } y \in Y_j; \\ \varnothing, & \text{otherwise} \end{cases} && (34) \end{aligned}$$

(because of the equivalence (33)).

defined a natural isomorphism $\eta : 1_{\mathcal{P}'} \to FF'$. Therefore, $FF' \cong 1_{\mathcal{P}'}$ as functors.".

- **Proof of Proposition 7.9:** After "The only B-fixed point in G/P_I is the basepoint", I would add "(by Proposition 7.7b **(a)**)".

- **Proof of Proposition 7.9:** After "and the basepoint is fixed by P_i iff $i \in I$", I would add "(by Proposition 7.7b **(b)**)".

- **Proof of Proposition 7.9:** Replace "$X = F'FX$" by "$X \cong F'FX$ by a functorial isomorphism (i.e., we have $1_{\mathcal{P}} \cong F'F$)".

  More importantly, I believe that this claim should be proven. Here is my proof:

  [*Proof of the functorial isomorphism $1_{\mathcal{P}} \cong F'F$:* Let $X \in \mathcal{P}$ be an object. Then, $FX = \left(X^B; X^{P_1}, \ldots, X^{P_{n-1}}\right)$ (by the definition of the functor F). Hence, the definition of the functor F' shows that $F'FX = \coprod_{y \in X^B} G/P_{I_y}$, where we set $I_y = \left\{i \in \{1, 2, \ldots, n-1\} \mid y \in X^{P_i}\right\}$ for each $y \in X^B$. We shall now define a map $\varepsilon_X : F'FX \to X$ as follows:

  Let $p \in F'FX$. Then, $p \in F'FX = \coprod_{y \in X^B} G/P_{I_y}$. In other words, $p \in G/P_{I_y}$ for some $y \in X^B$. Consider this y. Write p in the form $p = \overline{q}$ for some $q \in G$ (where $\overline{q}$ denotes the coset qP_{I_y} of q in G/P_{I_y}). Then, the element qy

From $F'Y = \coprod_{y \in Y} G/P_{I_y}$, we obtain

$$\left(F'Y\right)^{P_j} = \left(\coprod_{y \in Y} G/P_{I_y}\right)^{P_j} \cong \coprod_{y \in Y} \underbrace{\left(G/P_{I_y}\right)^{P_j}}_{\substack{= \begin{cases} \left\{\overline{1}\right\}, & \text{if } y \in Y_j; \\ \varnothing, & \text{otherwise} \end{cases} \\ \text{(by (34))}}} = \coprod_{y \in Y} \begin{cases} \left\{\overline{1}\right\}, & \text{if } y \in Y_j; \\ \varnothing, & \text{otherwise} \end{cases}$$

$$= \coprod_{y \in Y_j} \left\{\overline{1}\right\} = \eta_Y\left(Y_j\right)$$

(because the definition of η_Y yields $\eta_Y\left(Y_j\right) = \coprod_{y \in Y_j} \left\{\overline{1}\right\}$).

Now, forget that we fixed j. We thus have proven that

$$\left(F'Y\right)^{P_j} = \eta_Y\left(Y_j\right)$$

for each $j \in \{1, 2, \ldots, n-1\}$. Hence, we have $\eta_Y\left(Y_j\right) \subseteq \left(F'Y\right)^{P_j}$ and $\left(\eta_Y\right)^{-1}\left(\left(F'Y\right)^{P_j}\right) \subseteq Y_j$ for each $j \in \{1, 2, \ldots, n-1\}$.

Recall that $Y = \left(Y; Y_1, \ldots, Y_{n-1}\right)$ and $FF'Y = \left(\left(F'Y\right)^B; \left(F'Y\right)^{P_1}, \ldots, \left(F'Y\right)^{P_{n-1}}\right)$ (by the definition of F). Hence, the bijection $\eta_Y : Y \to FF'Y$ is a morphism in $\mathcal{P}'$ (since $\eta_Y\left(Y_j\right) \subseteq \left(F'Y\right)^{P_j}$ for each $j \in \{1, 2, \ldots, n-1\}$), and its inverse $\left(\eta_Y\right)^{-1} : FF'Y \to Y$ is also a morphism in $\mathcal{P}'$ (since $\left(\eta_Y\right)^{-1}\left(\left(F'Y\right)^{P_j}\right) \subseteq Y_j$ for each $j \in \{1, 2, \ldots, n-1\}$). Thus, η_Y is an isomorphism in the category $\mathcal{P}'$. Qed.

of X does not depend on the choice of q [21]. Hence, we can define $\varepsilon_X(p)$ to be the element qy of X. Thus, a map $\varepsilon_X : F'FX \to X$ is defined.

This map $\varepsilon_X : F'FX \to X$ is G-equivariant[22]. Moreover, this map ε_X is injective[23] and surjective[24]. Hence, the map ε_X is bijective, and thus is a

[21] *Proof.* Let q_1 and q_2 be two elements $q \in G$ satisfying $p = \overline{q}$. We must prove that $q_1 y = q_2 y$.

We know that q_1 is an element $q \in G$ satisfying $p = \overline{q}$. In other words, q_1 is an element of G and satisfies $p = \overline{q_1}$. Similarly, q_2 is an element of G and satisfies $p = \overline{q_2}$. From $\overline{q_1} = p = \overline{q_2}$, we conclude that $q_1 P_{I_y} = q_2 P_{I_y}$. In other words, $q_1 = q_2 h$ for some $h \in P_{I_y}$.

Let G_y denote the stabilizer of y in G. Then, Proposition 7.7c **(a)** yields $P_{I_y} = G_y$. Therefore, $h \in P_{I_y} = G_y$. In other words, $hy = y$.

Now, $\underbrace{q_1}_{=q_2 h} y = q_2 \underbrace{hy}_{=y} = q_2 y$. This completes our proof.

[22] *Proof.* Let $p \in FF'X$ and $g \in G$. We must show that $\varepsilon_X(gp) = g\varepsilon_X(p)$.

Indeed, we have $p \in F'FX = \coprod_{y \in X^B} G/P_{I_y}$. In other words, $p \in G/P_{I_y}$ for some $y \in X^B$. Consider this y. Write p in the form $p = \overline{q}$ for some $q \in G$ (where $\overline{q}$ denotes the coset qP_{I_y} of q in G/P_{I_y}). Then, $\varepsilon_X(p) = qy$ (by the definition of ε_X). On the other hand, $gp \in G/P_{I_y}$ (since $p \in G/P_{I_y}$) and $g \underbrace{p}_{=\overline{q}} = g\overline{q} = \overline{gq}$ with $gq \in G$. Hence, the definition of ε_X yields

$$\varepsilon_X(gp) = g \underbrace{qy}_{=\varepsilon_X(p)} = g\varepsilon_X(p).$$

Now, forgot that we fixed p and g. We thus have shown that $\varepsilon_X(gp) = g\varepsilon_X(p)$ for each $p \in FF'X$ and $g \in G$. In other words, the map $\varepsilon_X : F'FX \to X$ is G-equivariant. Qed.

[23] *Proof.* Let $p_1 \in F'FX$ and $p_2 \in F'FX$ be such that $\varepsilon_X(p_1) = \varepsilon_X(p_2)$. We shall show that $p_1 = p_2$.

For each $y \in X$, let G_y denote the stabilizer of y in G.

We have $p_1 \in F'FX = \coprod_{y \in X^B} G/P_{I_y}$. In other words, $p_1 \in G/P_{I_y}$ for some $y \in X^B$. Denote this y by y_1. Thus, $y_1 \in X^B$ and $p_1 \in G/P_{I_{y_1}}$. Write p_1 in the form $p_1 = \overline{q_1}^{/I_{y_1}}$ for some $q_1 \in G$ (where $\overline{q_1}^{/I_{y_1}}$ denotes the coset $q_1 P_{I_{y_1}}$ of q_1 in $G/P_{I_{y_1}}$). Then, $\varepsilon_X(p_1) = q_1 y_1$ (by the definition of ε_X).

We have $p_2 \in F'FX = \coprod_{y \in X^B} G/P_{I_y}$. In other words, $p_2 \in G/P_{I_y}$ for some $y \in X^B$. Denote this y by y_2. Thus, $y_2 \in X^B$ and $p_2 \in G/P_{I_{y_2}}$. Write p_2 in the form $p_2 = \overline{q_2}^{/I_{y_2}}$ for some $q_2 \in G$ (where $\overline{q_2}^{/I_{y_2}}$ denotes the coset $q_2 P_{I_{y_2}}$ of q_2 in $G/P_{I_{y_2}}$). Then, $\varepsilon_X(p_2) = q_2 y_2$ (by the definition of ε_X).

Now, $q_1 y_1 = \varepsilon_X(p_1) = \varepsilon_X(p_2) = q_2 y_2$. Hence, Proposition 7.7c **(b)** shows that $y_1 = y_2$ and $q_1 G_{y_1} = q_2 G_{y_1}$.

On the other hand, Proposition 7.7c **(a)** (applied to $y = y_1$) shows that $P_{I_{y_1}} = G_{y_1}$. Thus, the equality $q_1 G_{y_1} = q_2 G_{y_1}$ rewrites as $q_1 P_{I_{y_1}} = q_2 P_{I_{y_1}}$.

The definition of $\overline{q_1}^{/I_{y_1}}$ yields $\overline{q_1}^{/I_{y_1}} = q_1 P_{I_{y_1}} = q_2 P_{I_{y_1}} = q_2 P_{I_{y_2}}$ (since $y_1 = y_2$). Hence, $p_1 = \overline{q_1}^{/I_{y_1}} = q_2 P_{I_{y_2}}$.

The definition of $\overline{q_2}^{/I_{y_2}}$ yields $\overline{q_2}^{/I_{y_2}} = q_2 P_{I_{y_2}}$. Hence, $p_2 = \overline{q_2}^{/I_{y_2}} = q_2 P_{I_{y_2}}$. Comparing this with $p_1 = q_2 P_{I_{y_2}}$, we obtain $p_1 = p_2$.

Now, let us forget that we fixed p_1 and p_2. We thus have proven that if $p_1 \in F'FX$ and $p_2 \in F'FX$ are such that $\varepsilon_X(p_1) = \varepsilon_X(p_2)$, then $p_1 = p_2$. In other words, the map ε_X is injective. Qed.

[24] *Proof.* Let $x \in X$.

Let $Y = Gx$ be the G-orbit of x. Then, $Y \cong G/G_x$ (by the orbit-stabilizer theorem). However,

G-set isomorphism (since it is G-equivariant).

Now, forget that we fixed X. Thus, for each object $X \in \mathcal{P}$, we have constructed a G-set isomorphism $\varepsilon_X : F'FX \to X$. Moreover, this isomorphism

X is a parabolic G-set; thus, the stabilizer of every element of X is parabolic. In other words, for every $\xi \in X$, the subgroup G_ξ of G is parabolic. Applying this to $\xi = x$, we conclude that the subgroup G_x of G is parabolic. In other words, G_x contains a conjugate of B (by the definition of "parabolic"). In other words, there exists some $q \in G$ such that $G_x \supseteq qBq^{-1}$. Consider this q.

Set $z = q^{-1}x$. Clearly, $z = \underbrace{q^{-1}}_{\in G} x \in Gx = Y$.

Recall that $G_{rx} = rG_xr^{-1}$ for each $r \in G$. Applying this to $r = q^{-1}$, we obtain $G_{q^{-1}x} = q^{-1} \underbrace{G_x}_{\supseteq qBq^{-1}} \underbrace{\left(q^{-1}\right)^{-1}}_{=q} \supseteq \underbrace{q^{-1}q}_{=1} B \underbrace{q^{-1}q}_{=1} = B$. Since $z = q^{-1}x$, we obtain $G_z = G_{q^{-1}x} \supseteq B$. Hence, $B \subseteq G_z$. In other words, $z \in Y^B$ (since $z \in Y$). Thus, G/P_{I_z} is a component of the disjoint union $\coprod_{y \in X^B} G/P_{I_y}$.

Let $\overline{q}$ denote the coset qP_{I_z} of q in G/P_{I_z}. We have $\overline{q} \in G/P_{I_z} \subseteq \coprod_{y \in X^B} G/P_{I_y}$ (since G/P_{I_z} is a component of the disjoint union $\coprod_{y \in X^B} G/P_{I_y}$). Thus, $\overline{q} \in \coprod_{y \in X^B} G/P_{I_y} = FF'X$. Therefore, $\varepsilon_X(\overline{q})$ is well-defined. Moreover, the definition of ε_X shows that $\varepsilon_X(\overline{q}) = qz$ (since $\overline{q} \in G/P_{I_z}$ and since $\overline{q} = \overline{q}$). Thus, $\varepsilon_X(\overline{q}) = q \underbrace{z}_{=q^{-1}x} = \underbrace{qq^{-1}}_{=1} x = x$, so taht $x = \varepsilon_X\left(\underbrace{\overline{q}}_{\in F'FX}\right) \in \varepsilon_X(F'FX)$.

Now, forget that we fixed x. We thus have shown that $x \in \varepsilon_X(F'FX)$ for each $x \in X$. In other words, $X \subseteq \varepsilon_X(F'FX)$. In other words, the map ε_X is surjective. Qed.

ε_X is functorial in X [25]. Hence, we have defined a natural isomorphism $\varepsilon : F'F \to 1_{\mathcal{P}}$. Therefore, $1_{\mathcal{P}} \cong F'F$ as functors.]

- **§8:** I would begin this section with the following introduction:

  "We consider the localization $\mathbb{Z}_{(p)}$ of the ring $\mathbb{Z}$ at its prime ideal $(p) = p\mathbb{Z}$. Explicitly, $\mathbb{Z}_{(p)}$ is the subring

  $$\left\{ \frac{a}{b} \mid (a,b) \in \mathbb{Z} \times \mathbb{Z} \text{ and } \gcd(b,p) = 1 \right\}$$

  of $\mathbb{Q}$.

  Lemma 8.0a. Let V be an n-dimensional $\mathbb{F}_p$-vector space. Then:

  (a) We have $|\operatorname{Flag}(V)| = \sum\limits_{\sigma \in \Sigma_n} p^{l(\sigma)}$.

[25] *Proof.* Let Y and Z be two objects of $\mathcal{P}$, and let $f : Y \to Z$ be a G-equivariant map. We must prove that the diagram

$$\begin{tikzcd} F'FY \arrow[r, "\varepsilon_Y"] \arrow[d, "F'Ff"'] & Y \arrow[d, "f"] \\ F'FZ \arrow[r, "\varepsilon_Z"'] & Z \end{tikzcd} \qquad (35)$$

is commutative.

Let $p \in F'FY$. Then, $FY = \left(Y^B; Y^{P_1}, \ldots, Y^{P_{n-1}}\right)$ (by the definition of the functor F). Hence, the definition of the functor F' shows that $F'FY = \coprod_{y \in Y^B} G/P_{I_y}$, where we set $I_y = \left\{i \in \{1,2,\ldots,n-1\} \mid y \in Y^{P_i}\right\}$ for each $y \in Y^B$.

We have $p \in F'FY = \coprod_{y \in Y^B} G/P_{I_y}$. In other words, $p \in G/P_{I_y}$ for some $y \in Y^B$. Consider this y. Write p in the form $p = \overline{q}$ for some $q \in G$ (where $\overline{q}$ denotes the coset qP_{I_y} of q in G/P_{I_y}). Then, $\varepsilon_Y(p) = qy$ (by the definition of ε_Y).

The definition of the action of the functor F on the morphism $f : Y \to Z$ shows that $Ff : Y^B \to Z^B$ is the restriction of the map $f : Y \to Z$ to the B-fixed points. Thus, $(Ff)(y) = f(y)$.

On the other hand, the definition of the action of the functor F' on the morphism $Ff : FY \to FZ$ yields $(F'Ff)(\overline{q}) = \overline{q} \in G/P_{I_{(Ff)(y)}} = G/P_{I_{f(y)}}$ (since $(Ff)(y) = f(y)$). Hence, the definition of ε_Z yields $\varepsilon_Z((F'Ff)(\overline{q})) = qf(y)$. Hence,

$$\left(\varepsilon_Z \circ (F'Ff)\right)\left(\underbrace{p}_{=\overline{q}}\right) = \left(\varepsilon_Z \circ (F'Ff)\right)(\overline{q}) = \varepsilon_Z\left((F'Ff)(\overline{q})\right) = qf(y).$$

Comparing this with

$$(f \circ \varepsilon_Y)(p) = f\left(\underbrace{\varepsilon_Y(p)}_{=qy}\right) = f(qy) = qf(y) \qquad \text{(since the map } f \text{ is } G\text{-equivariant)},$$

we obtain $(\varepsilon_Z \circ (F'Ff))(p) = (f \circ \varepsilon_Y)(p)$.

Now, let us forget that we fixed p. We thus have proven that $(\varepsilon_Z \circ (F'Ff))(p) = (f \circ \varepsilon_Y)(p)$ for each $p \in F'FY$. In other words, $\varepsilon_Z \circ (F'Ff) = f \circ \varepsilon_Y$. In other words, the diagram (35) is commutative. This completes the proof.

(b) We have $\left|\operatorname{Flag}(V)\right| \equiv 1 \bmod p$ and $\left|\operatorname{Flag}(V)\right|^{-1} \in \mathbb{Z}_{(p)}$.

[*Proof of Lemma 8.0a.* Fix some $\underline{W} \in \operatorname{Flag}(V)$. (Such a $\underline{W}$ clearly exists.) For each $\sigma \in \Sigma_n$, there is a subset $Y(\sigma, \underline{W}) \subset \operatorname{Flag}(V)$ defined by $Y(\sigma, \underline{W}) = \{\underline{U} \in \operatorname{Flag}(V) \mid \delta(\underline{U}, \underline{W}) = \sigma\}$. (Here, $\delta(\underline{U}, \underline{W})$ is the Jordan permutation, defined as in §4.)

Clearly, $\operatorname{Flag}(V)$ is the union of its disjoint subsets $\{\underline{U} \in \operatorname{Flag}(V) \mid \delta(\underline{U}, \underline{W}) = \sigma\}$ for all $\sigma \in \Sigma_n$ (because for each $\underline{U} \in \operatorname{Flag}(V)$, there is exactly one $\sigma \in \Sigma_n$ satisfying $\delta(\underline{U}, \underline{W}) = \sigma$). Hence,

$$\begin{aligned}\left|\operatorname{Flag}(V)\right| &= \sum_{\sigma \in \Sigma_n} \left| \underbrace{\{\underline{U} \in \operatorname{Flag}(V) \mid \delta(\underline{U}, \underline{W}) = \sigma\}}_{=Y(\sigma,\underline{W})} \right| = \sum_{\sigma \in \Sigma_n} \underbrace{\left|Y(\sigma, \underline{W})\right|}_{\substack{=p^{l(\sigma)} \\ \text{(by Corollary 5.2a, applied} \\ \text{to } V \text{ and } \underline{W} \text{ instead of } W \text{ and } \underline{V})}} \\ &= \sum_{\sigma \in \Sigma_n} p^{l(\sigma)}.\end{aligned}$$

This proves Lemma 8.0a **(a)**.

(b) Lemma 8.0a **(a)** yields

$$\begin{aligned}\left|\operatorname{Flag}(V)\right| = \sum_{\sigma \in \Sigma_n} p^{l(\sigma)} &= \underbrace{p^{l(\mathrm{id})}}_{=p^0=1} + \sum_{\substack{\sigma \in \Sigma_n; \\ \sigma \neq \mathrm{id}}} \underbrace{p^{l(\sigma)}}_{\substack{\equiv 0 \bmod p \\ \text{(since } l(\sigma) \geq 1 \\ \text{(since } \sigma \neq \mathrm{id}\text{))}}} \\ &\equiv 1 + \underbrace{\sum_{\substack{\sigma \in \Sigma_n; \\ \sigma \neq \mathrm{id}}} 0}_{=0} = 1 \bmod p.\end{aligned}$$

Hence, $\left|\operatorname{Flag}(V)\right|$ is coprime to p. Thus, $\left|\operatorname{Flag}(V)\right|^{-1} \in \mathbb{Z}_{(p)}$. This proves Lemma 8.0a **(b)**. □]"

You use Lemma 8.0a **(b)** implicitly in Definition 8.5.

- **Definition 8.1:** Replace "ring" by "$\mathbb{Z}_{(p)}$-algebra".
- **Definition 8.1:** Replace "$\mathbb{Z}[\mathrm{Flag}]$" by "$\mathbb{Z}_{(p)}[\mathrm{Flag}]$".
- **§8, between Definition 8.1 and Definition 8.2:** You write: "this construction gives an equivalence $[\mathcal{V}, \{\text{sets}\}] = \{G - \text{sets}\}$".

  This argument is non-constructive[26] and (in my opinion) overkill. It ap-

[26] Namely, it seems to use

- either the fact that every category is equivalent to its skeleton,
- or the fact that any functor that is essentially surjective, full and faithful must be an equivalence of categories.

As far as I know, none of these two facts has a constructive proof.

pears to me that you are not actually using the full power of this equivalence either; instead, you seem to only use the natural $\mathbb{Z}_{(p)}$-algebra isomorphism

$$\begin{aligned}\mathcal{H} = \operatorname{End}_{\mathcal{VA}}\left(\mathbb{Z}_{(p)}\left[\mathrm{Flag}\right]\right) &\cong \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\mathrm{Flag}\left(\mathbb{F}_p^n\right)\right]\right)\\ &\cong \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[G/B\right]\right),\end{aligned}$$

which has an elementary and constructive proof. Namely, this isomorphism follows from Proposition 8.1b further below.

Before I state this proposition, let me state a simple fact from category theory:

Proposition 8.1a. Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. Let $C \in \mathcal{C}$ be an object. Let $F : \mathcal{C} \to \mathcal{D}$ is a functor. Let $\mathcal{E}_F(C)$ denote the subset

$$\left\{f \in \operatorname{End}_{\mathcal{D}}(F(C)) \mid f \circ F(k) = F(k) \circ f \text{ for each } k \in \operatorname{End}_{\mathcal{C}} C\right\}$$

of $\operatorname{End}_{\mathcal{D}}(F(C))$.

(a) The subset $\mathcal{E}_F(C)$ is a submonoid of $\operatorname{End}_{\mathcal{D}}(F(C))$. Moreover, there is a canonical monoid homomorphism $\varepsilon : \operatorname{End}_{[\mathcal{C},\mathcal{D}]} F \to \mathcal{E}_F(C)$ that sends each natural transformation $\alpha : F \Longrightarrow F$ to its component $\alpha_C : F(C) \to F(C)$.

(b) Consider this ε. Assume that each two objects of $\mathcal{C}$ are isomorphic. Then, ε is a monoid isomorphism.

[*Proof of Proposition 8.1a.* **(a)** This is a simple exercise in category theory.

(b) The map ε is injective[27]. We shall now show that ε is surjective.

[27] *Proof.* Let α and β be two elements of $\operatorname{End}_{[\mathcal{C},\mathcal{D}]} F$ such that $\varepsilon(\alpha) = \varepsilon(\beta)$. We shall show that $\alpha = \beta$.

Let $A \in \mathcal{C}$ be any object. Then, the objects A and C of $\mathcal{C}$ are isomorphic (since each two objects of $\mathcal{C}$ are isomorphic). In other words, there exists an isomorphism $j : A \to C$ in $\mathcal{C}$. Consider this j. Thus, the morphism j^{-1} exists (since j is an isomorphism).

Recall that $\alpha \in \operatorname{End}_{[\mathcal{C},\mathcal{D}]} F$. In other words, α is a natural transformation from F to F. Thus, the diagram

$$\begin{tikzcd} F(A) \arrow[r, "\alpha_A"] \arrow[d, "F(j)"'] & F(A) \arrow[d, "F(j)"] \\ F(C) \arrow[r, "\alpha_C"'] & F(C) \end{tikzcd}$$

is commutative. In other words, we have $\alpha_A \circ F(j) = F(j) \circ \alpha_C$. But F is a functor; thus, $F\left(j^{-1}\right) = (F(j))^{-1}$. The definition of ε yields $\varepsilon(\alpha) = \alpha_C$. Thus,

$$F(j) \circ \underbrace{\varepsilon(\alpha)}_{=\alpha_C} \circ \underbrace{F\left(j^{-1}\right)}_{=(F(j))^{-1}} = \underbrace{F(j) \circ \alpha_C}_{=\alpha_A \circ F(j)} \circ (F(j))^{-1} = \alpha_A \circ \underbrace{F(j) \circ (F(j))^{-1}}_{=\mathrm{id}} = \alpha_A.$$

Hence, $\alpha_A = F(j) \circ \varepsilon(\alpha) \circ F\left(j^{-1}\right)$. The same argument (applied to β instead of α) shows that

Indeed, fix any $\rho \in \mathcal{E}_F(C)$. Let $A \in \mathcal{C}$ be any object. We are going to construct a morphism $\alpha_A : F(C) \to F(C)$ in $\mathcal{D}$.

We have

$$\rho \in \mathcal{E}_F(C) = \{f \in \operatorname{End}_{\mathcal{D}}(F(C)) \mid f \circ F(k) = F(k) \circ f \text{ for each } k \in \operatorname{End}_{\mathcal{C}} C\}$$

(by the definition of $\mathcal{E}_F(C)$). In other words, ρ is an element of $\operatorname{End}_{\mathcal{D}}(F(C))$ and satisfies

$$(\rho \circ F(k) = F(k) \circ \rho \text{ for each } k \in \operatorname{End}_{\mathcal{C}} C). \tag{36}$$

The objects A and C of $\mathcal{C}$ are isomorphic (since each two objects of $\mathcal{C}$ are isomorphic). In other words, there exists an isomorphism $j : C \to A$ in $\mathcal{C}$. Consider this j. Thus, the morphism j^{-1} exists (since j is an isomorphism).

Now, define a morphism $\alpha_A : F(C) \to F(C)$ in $\mathcal{D}$ by $\alpha_A = F(j) \circ \rho \circ F\left(j^{-1}\right)$. This morphism α_A is independent on the choice of j [28].

Now, forget that we fixed A. Thus, for each $A \in \mathcal{C}$, we have defined a morphism $\alpha_A : F(C) \to F(C)$ in $\mathcal{D}$. This morphism α_A satisfies

$$\alpha_A = F(j) \circ \rho \circ F\left(j^{-1}\right) \qquad \text{for every isomorphism } j : C \to A \text{ in } \mathcal{C} \tag{37}$$

(by the definition of α_A).

If A and B are two objects in $\mathcal{C}$, and if $f : A \to B$ is a morphism in $\mathcal{C}$, then the diagram

$$\begin{tikzcd} F(A) \arrow[r, "\alpha_A"] \arrow[d, "F(f)"'] & F(A) \arrow[d, "F(f)"] \\ F(B) \arrow[r, "\alpha_B"'] & F(B) \end{tikzcd} \tag{38}$$

$\beta_A = F(j) \circ \varepsilon(\beta) \circ F\left(j^{-1}\right)$.

Now,

$$\alpha_A = F(j) \circ \underbrace{\varepsilon(\alpha)}_{=\varepsilon(\beta)} \circ F\left(j^{-1}\right) = F(j) \circ \varepsilon(\beta) \circ F\left(j^{-1}\right) = \beta_A.$$

Now, forget that we fixed A. We thus have proven that $\alpha_A = \beta_A$ for each object $A \in \mathcal{C}$. In other words, $\alpha = \beta$.

Now, forget that we fixed α and β. We thus have shown that if α and β are two elements of $\operatorname{End}_{[\mathcal{C},\mathcal{D}]} F$ such that $\varepsilon(\alpha) = \varepsilon(\beta)$, then $\alpha = \beta$. In other words, the map ε is injective. Qed.

[28] *Proof.* Let j_1 and j_2 be two isomorphisms $j : C \to A$ in $\mathcal{C}$. We will prove that $F(j_1) \circ \rho \circ F\left(j_1^{-1}\right) = F(j_2) \circ \rho \circ F\left(j_2^{-1}\right)$.

We recall that j_1 and j_2 are two isomorphisms $C \to A$ in $\mathcal{C}$. Thus, $j_1^{-1} \circ j_2 : C \to C$ is an isomorphism in $\mathcal{C}$ as well. In particular, $j_1^{-1} \circ j_2 \in \operatorname{End}_{\mathcal{C}} C$. Thus, (36) (applied to $k = j_1^{-1} \circ j_2$) yields $\rho \circ F\left(j_1^{-1} \circ j_2\right) = F\left(j_1^{-1} \circ j_2\right) \circ \rho$. But F is a functor; thus, $F\left(j_1^{-1} \circ j_2\right) =$

is commutative[29]. Therefore, the morphisms α_A (defined for all objects $A \in \mathcal{C}$) can be assembled to a natural transformation $\alpha : F \Longrightarrow F$. Consider this α. We have $\alpha \in \operatorname{End}_{[\mathcal{C},\mathcal{D}]} F$ (since α is a natural transformation $F \Longrightarrow F$). Moreover, the definition of ε shows that $\varepsilon(\alpha) = \alpha_C$.

But $\operatorname{id} : C \to C$ is an isomorphism in $\mathcal{C}$. Hence, (37) (applied to $A = C$ and

$(F(j_1))^{-1} \circ F(j_2)$. But

$$\begin{aligned}
& F(j_1) \circ \rho \circ \underbrace{F\left(j_1^{-1}\right)}_{\substack{=(F(j_1))^{-1} \\ \text{(since } F \text{ is a functor)}}} \\
&= F(j_1) \circ \rho \circ (F(j_1))^{-1} \\
&= F(j_1) \circ \rho \circ \underbrace{(F(j_1))^{-1} \circ F(j_2)}_{=F\left(j_1^{-1} \circ j_2\right)} \circ \underbrace{(F(j_2))^{-1}}_{\substack{=F\left(j_2^{-1}\right) \\ \text{(since } F \text{ is a functor)}}} \\
&\qquad \left(\text{since } F(j_1) \circ \rho \circ (F(j_1))^{-1} \circ \underbrace{F(j_2) \circ (F(j_2))^{-1}}_{=\operatorname{id}} = F(j_1) \circ \rho \circ (F(j_1))^{-1}\right) \\
&= F(j_1) \circ \underbrace{\rho \circ F\left(j_1^{-1} \circ j_2\right)}_{=F\left(j_1^{-1} \circ j_2\right) \circ \rho} \circ F\left(j_2^{-1}\right) \\
&= \underbrace{F(j_1) \circ F\left(j_1^{-1} \circ j_2\right)}_{\substack{=F\left(j_1 \circ j_1^{-1} \circ j_2\right) \\ \text{(since } F \text{ is a functor)}}} \circ \rho \circ F\left(j_2^{-1}\right) \\
&= F\left(\underbrace{j_1 \circ j_1^{-1}}_{=\operatorname{id}} \circ j_2\right) \circ \rho \circ F\left(j_2^{-1}\right) = F(j_2) \circ \rho \circ F\left(j_2^{-1}\right).
\end{aligned}$$

Now, forget that we fixed j_1 and j_2. We thus have shown that if j_1 and j_2 are two isomorphisms $j : C \to A$ in $\mathcal{C}$, then $F(j_1) \circ \rho \circ F\left(j_1^{-1}\right) = F(j_2) \circ \rho \circ F\left(j_2^{-1}\right)$. In other words, the morphism $F(j) \circ \rho \circ F\left(j^{-1}\right)$ is independent on the choice on j. In other words, the morphism α_A is independent on the choice of j (since $\alpha_A = F(j) \circ \rho \circ F\left(j^{-1}\right)$). Qed.

[29] *Proof.* Let A and B be two objects in $\mathcal{C}$. Let $f : A \to B$ be a morphism in $\mathcal{C}$.

The objects A and C of $\mathcal{C}$ are isomorphic (since each two objects of $\mathcal{C}$ are isomorphic). In other words, there exists an isomorphism $j : C \to A$ in $\mathcal{C}$. Consider this j. Thus, (37) yields $\alpha_A = F(j) \circ \rho \circ F\left(j^{-1}\right)$.

The objects B and C of $\mathcal{C}$ are isomorphic (since each two objects of $\mathcal{C}$ are isomorphic). In other words, there exists an isomorphism $i : C \to B$ in $\mathcal{C}$. Consider this i. Thus, (37) (applied to B and i instead of A and j) yields $\alpha_B = F(i) \circ \rho \circ F\left(i^{-1}\right)$.

Since $i : C \to B$ is an isomorphism, its inverse $i^{-1} : B \to C$ is well-defined and an isomorphism as well. The composition $i^{-1} \circ f \circ j : C \to C$ is thus an endomorphism of C in $\mathcal{C}$. In other words, $i^{-1} \circ f \circ j \in \operatorname{End}_{\mathcal{C}} C$. Hence, (36) (applied to $k = i^{-1} \circ f \circ j$) yields $\rho \circ F\left(i^{-1} \circ f \circ j\right) = F\left(i^{-1} \circ f \circ j\right) \circ \rho$. But F is a functor; thus, $F\left(i^{-1} \circ f \circ j\right) = (F(i))^{-1} \circ$

$j = \operatorname{id}$) yields

$$\alpha_C = F(\operatorname{id}) \circ \rho \circ F\left(\underbrace{\operatorname{id}^{-1}}_{=\operatorname{id}}\right) = \underbrace{F(\operatorname{id})}_{\substack{=\operatorname{id} \\ \text{(since } F \text{ is a functor)}}} \circ \rho \circ \underbrace{F(\operatorname{id})}_{\substack{=\operatorname{id} \\ \text{(since } F \text{ is a functor)}}} = \rho.$$

Comparing this with $\varepsilon(\alpha) = \alpha_C$, we obtain $\rho = \varepsilon\left(\underbrace{\alpha}_{\in \operatorname{End}_{[\mathcal{C},\mathcal{D}]} F}\right) \in \varepsilon\left(\operatorname{End}_{[\mathcal{C},\mathcal{D}]} F\right)$.

Now, forget that we fixed ρ. We thus have shown that $\rho \in \varepsilon\left(\operatorname{End}_{[\mathcal{C},\mathcal{D}]} F\right)$ for each $\rho \in \mathcal{E}_F(C)$. In other words, $\mathcal{E}_F(C) \subseteq \varepsilon\left(\operatorname{End}_{[\mathcal{C},\mathcal{D}]} F\right)$. In other words, the map ε is surjective.

So we know that the map ε is both injective and surjective. Thus, ε is bijective. Furthermore, ε is a monoid homomorphism. Thus, ε is a bijective monoid homomorphism. Therefore, ε is a monoid isomorphism. This proves Proposition 8.1a **(b)**. □]

Proposition 8.1b. We have

$$\mathcal{H} = \operatorname{End}_{\mathcal{VA}}\left(\mathbb{Z}_{(p)}[\operatorname{Flag}]\right) \cong \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \cong \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}[G/B]\right)$$

as $\mathbb{Z}_{(p)}$-algebras. More precisely, the following holds:

$F(f) \circ F(j)$. Now,

$$\underbrace{\alpha_B}_{=F(i)\circ\rho\circ F(i^{-1})} \circ F(f) \circ F(j) = F(i) \circ \rho \circ \underbrace{F\left(i^{-1}\right) \circ F(f) \circ F(j)}_{=F(i^{-1}\circ f\circ j)} = F(i) \circ \underbrace{\rho \circ F\left(i^{-1} \circ f \circ j\right)}_{=F(i^{-1}\circ f\circ j)\circ\rho}$$
$$= F(i) \circ \underbrace{F\left(i^{-1} \circ f \circ j\right)}_{=(F(i))^{-1}\circ F(f)\circ F(j)} \circ \rho = \underbrace{F(i) \circ (F(i))^{-1}}_{=\operatorname{id}} \circ F(f) \circ F(j) \circ \rho$$
$$= F(f) \circ F(j) \circ \rho,$$

so that

$$\underbrace{\alpha_B \circ F(f) \circ F(j)}_{=F(f)\circ F(j)\circ\rho} \circ F\left(j^{-1}\right) = F(f) \circ \underbrace{F(j) \circ \rho \circ F\left(j^{-1}\right)}_{=\alpha_A} = F(f) \circ \alpha_A.$$

Comparing this with

$$\alpha_B \circ F(f) \circ F(j) \circ \underbrace{F\left(j^{-1}\right)}_{\substack{=(F(j))^{-1} \\ \text{(since } F \text{ is a functor)}}} = \alpha_B \circ F(f) \circ \underbrace{F(j) \circ (F(j))^{-1}}_{=\operatorname{id}} = \alpha_B \circ F(f),$$

we obtain $F(f) \circ \alpha_A = \alpha_B \circ F(f)$. In other words, the diagram (38) is commutative. Qed.

(a) Recall the definition of $\mathcal{E}_F(C)$ in Proposition 8.1a (where $\mathcal{C}$ and $\mathcal{D}$ are two categories, $C \in \mathcal{C}$ is an object, and $F : \mathcal{C} \to \mathcal{D}$ is a functor). Applying this to $\mathcal{C} = \mathcal{V}$, $\mathcal{D} = \mathcal{A}$, $C = \mathbb{F}_p^n$ and $F = \mathbb{Z}_{(p)}[\text{Flag}]$, we obtain a set $\mathcal{E}_{\mathbb{Z}_{(p)}[\text{Flag}]}\left(\mathbb{F}_p^n\right)$. Proposition 8.1a **(a)** (applied to $\mathcal{C} = \mathcal{V}$, $\mathcal{D} = \mathcal{A}$, $C = \mathbb{F}_p^n$ and $F = \mathbb{Z}_{(p)}[\text{Flag}]$) shows that this set $\mathcal{E}_{\mathbb{Z}_{(p)}[\text{Flag}]}\left(\mathbb{F}_p^n\right)$ is a submonoid of $\operatorname{End}_{\mathcal{A}}\left(\left(\mathbb{Z}_{(p)}[\text{Flag}]\right)\left(\mathbb{F}_p^n\right)\right)$, and that there is a monoid homomorphism $\varepsilon : \operatorname{End}_{[\mathcal{V},\mathcal{A}]}\left(\mathbb{Z}_{(p)}[\text{Flag}]\right) \to \mathcal{E}_{\mathbb{Z}_{(p)}[\text{Flag}]}\left(\mathbb{F}_p^n\right)$. Consider this ε. Then, ε is a $\mathbb{Z}_{(p)}$-algebra isomorphism $\operatorname{End}_{\mathcal{V}\mathcal{A}}\left(\mathbb{Z}_{(p)}[\text{Flag}]\right) \to \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right)$. Thus,

$$\operatorname{End}_{\mathcal{V}\mathcal{A}}\left(\mathbb{Z}_{(p)}[\text{Flag}]\right) \cong \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right)$$

as $\mathbb{Z}_{(p)}$-algebras.

(b) Consider the complete flag $\underline{E} = \left(E_0 < E_1 < \cdots < E_n = \mathbb{F}_p^n\right) \in \text{Flag}\left(\mathbb{F}_p^n\right)$ defined in §4.

There is a natural isomorphism $G/B \to \text{Flag}\left(\mathbb{F}_p^n\right)$ of G-sets, which sends each coset $hB \in G/B$ of B to the complete flag $h\underline{E} \in \text{Flag}\left(\mathbb{F}_p^n\right)$. The inverse of this isomorphism is an isomorphism $\text{Flag}\left(\mathbb{F}_p^n\right) \to G/B$ of G-sets. This isomorphism gives rise to a $\mathbb{Z}_{(p)}$-module isomorphism $\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right] \to \mathbb{Z}_{(p)}[G/B]$ and thus to a $\mathbb{Z}_{(p)}$-algebra isomorphism $\operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \to \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}[G/B]\right)$. Thus,

$$\operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \cong \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}[G/B]\right)$$

as $\mathbb{Z}_{(p)}$-algebras.

[*Proof of Proposition 8.1b.* **(a)** Recall that $\mathcal{V}$ is the category whose objects are n-dimensional vector spaces over $\mathbb{F}_p$, and whose morphisms are the isomorphisms between these vector spaces. In particular, the endomorphisms of $\mathbb{F}_p^n$ in $\mathcal{V}$ are the vector space isomorphisms $\mathbb{F}_p^n \to \mathbb{F}_p^n$. In other words,

$$\begin{aligned}\operatorname{End}_{\mathcal{V}}\left(\mathbb{F}_p^n\right) &= \left(\text{the set of the vector space isomorphisms } \mathbb{F}_p^n \to \mathbb{F}_p^n\right)\\ &= \left(\text{the set of the vector space automorphisms of } \mathbb{F}_p^n\right)\\ &= \operatorname{GL}_n\left(\mathbb{F}_p\right) = G.\end{aligned}$$

Let F be the functor $\mathbb{Z}_{(p)}[\text{Flag}] : \mathcal{V} \to \mathcal{A}$. Hence, $F\left(\mathbb{F}_p^n\right) = \left(\mathbb{Z}_{(p)}[\text{Flag}]\right)\left(\mathbb{F}_p^n\right) = \mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$. This $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$ is a $\mathbb{Z}_{(p)}[G]$-module, because the set $\text{Flag}\left(\mathbb{F}_p^n\right)$ is a G-set. The action of G on $\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$ has the property that

$$F(k) = \left(\text{the action of } k \text{ on } \mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \tag{39}$$

for each $k \in G$ [30].

Now, it is easy to see that

$$\mathcal{E}_F\left(\mathbb{F}_p^n\right) = \text{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \tag{40}$$

[31].

Each two objects of $\mathcal{V}$ are isomorphic (since the objects of $\mathcal{V}$ are n-dimensional $\mathbb{F}_p$-vector spaces, and since any two such vector spaces are isomorphic). Hence, Proposition 8.1a **(b)** (applied to $\mathcal{C} = \mathcal{V}$, $\mathcal{D} = \mathcal{A}$, $C = \mathbb{F}_p^n$ and $F = \mathbb{Z}_{(p)}[\text{Flag}]$) shows that ε is a monoid isomorphism. Therefore, the map

[30] *Proof of (39):* Let $k \in G$. Then, $k \in G = \text{End}_{\mathcal{V}}\left(\mathbb{F}_p^n\right)$. Hence, $F(k)$ is a well-defined endomorphism of $F\left(\mathbb{F}_p^n\right) = \mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$. Moreover,

$$\underbrace{F}_{=\mathbb{Z}_{(p)}[\text{Flag}]}(k) = \left(\mathbb{Z}_{(p)}[\text{Flag}]\right)(k) = \mathbb{Z}_{(p)}[\text{Flag}(k)].$$

Now, fix $\underline{X} \in \text{Flag}\left(\mathbb{F}_p^n\right)$. Then, $(\text{Flag}(k))(\underline{X}) = k\underline{X}$ (where the $k\underline{X}$ on the right hand side means the image of $\underline{X}$ under the action of $k \in G$ on $\text{Flag}\left(\mathbb{F}_p^n\right)$). Now,

$$\underbrace{(F(k))}_{=\mathbb{Z}_{(p)}[\text{Flag}(k)]}(\underline{X}) = \left(\mathbb{Z}_{(p)}[\text{Flag}(k)]\right)(\underline{X}) = (\text{Flag}(k))(\underline{X}) = k\underline{X}.$$

Now, forget that we fixed $\underline{X}$. We thus have shown that $(F(k))(\underline{X}) = k\underline{X}$ for each $\underline{X} \in \text{Flag}\left(\mathbb{F}_p^n\right)$. In other words,

$$\begin{aligned} F(k) &= \left(\text{the endomorphism of } \mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right] \text{ that sends each } \underline{X} \in \text{Flag}\left(\mathbb{F}_p^n\right) \text{ to } k\underline{X}\right) \\ &= \left(\text{the action of } k \text{ on } \mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \end{aligned}$$

(since the action of k on $\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$ is defined as the endomorphism of $\mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$ that sends each $\underline{X} \in \text{Flag}\left(\mathbb{F}_p^n\right)$ to $k\underline{X}$). This proves (39).

[31] *Proof of (40):* Recall that $F\left(\mathbb{F}_p^n\right) = \mathbb{Z}_{(p)}\left[\text{Flag}\left(\mathbb{F}_p^n\right)\right]$. Also, $\text{End}_{\mathcal{A}}\left(F\left(\mathbb{F}_p^n\right)\right) = \text{End}_{\mathbb{Z}_{(p)}}\left(F\left(\mathbb{F}_p^n\right)\right)$ (because the morphisms in the category $\mathcal{A}$ are just the $\mathbb{Z}_{(p)}$-linear maps).

ε is bijective. Moreover, ε is a $\mathbb{Z}_{(p)}$-algebra homomorphism (this follows di-

Hence,

$$\operatorname{End}_{\mathcal{A}}\left(F\left(\mathbb{F}_p^n\right)\right) = \operatorname{End}_{\mathbb{Z}_{(p)}}\left(\underbrace{F\left(\mathbb{F}_p^n\right)}_{=\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]}\right) = \operatorname{End}_{\mathbb{Z}_{(p)}}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right).$$

For each $f \in \operatorname{End}_{\mathbb{Z}_{(p)}}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right)$, we have the following chain of equivalences:

$$\begin{aligned}
&\left(f \circ F(k) = F(k) \circ f \text{ for each } k \in \underbrace{\operatorname{End}_{\mathcal{V}}\left(\mathbb{F}_p^n\right)}_{=G}\right) \\
\iff& \left(f \circ F(k) = F(k) \circ f \text{ for each } k \in G\right) \\
\iff& \left(f \text{ commutes with } \underbrace{F(k)}_{\substack{=\left(\text{the action of } k \text{ on } \mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \\ \text{(by (39))}}} \text{ for each } k \in G\right) \\
\iff& \left(f \text{ commutes with the action of } k \text{ on } \mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right] \text{ for each } k \in G\right) \\
\iff& \left(f \text{ is } G\text{-equivariant}\right) \\
\iff& \left(f \text{ is a } \mathbb{Z}_{(p)}[G]\text{-linear map}\right) \qquad \left(\text{since } f \text{ is a } \mathbb{Z}_{(p)}\text{-linear map}\right) \\
\iff& \left(f \in \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right)\right). \qquad (41)
\end{aligned}$$

Now, the definition of $\mathcal{E}_F\left(\mathbb{F}_p^n\right)$ yields

$$\begin{aligned}
\mathcal{E}_F\left(\mathbb{F}_p^n\right) &= \left\{ f \in \underbrace{\operatorname{End}_{\mathcal{A}}\left(F\left(\mathbb{F}_p^n\right)\right)}_{=\operatorname{End}_{\mathbb{Z}_{(p)}}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right)} \mid f \circ F(k) = F(k) \circ f \text{ for each } k \in \operatorname{End}_{\mathcal{V}}\left(\mathbb{F}_p^n\right) \right\} \\
&= \left\{ f \in \operatorname{End}_{\mathbb{Z}_{(p)}}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \mid \underbrace{f \circ F(k) = F(k) \circ f \text{ for each } k \in \operatorname{End}_{\mathcal{V}}\left(\mathbb{F}_p^n\right)}_{\substack{\iff \left(f \in \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right)\right) \\ \text{(by (41))}}} \right\} \\
&= \left\{ f \in \operatorname{End}_{\mathbb{Z}_{(p)}}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \mid f \in \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \right\} \\
&= \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right)
\end{aligned}$$

(since $\operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \subseteq \operatorname{End}_{\mathbb{Z}_{(p)}}\left(\mathbb{Z}_{(p)}\left[\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right]\right)$). This proves (40).

rectly from the definition of the $\mathbb{Z}_{(p)}$-algebra structure on $\operatorname{End}_{[\mathcal{V},\mathcal{A}]}\left(\mathbb{Z}_{(p)}[\mathrm{Flag}]\right)$). Hence, the map ε is a $\mathbb{Z}_{(p)}$-algebra isomorphism $\operatorname{End}_{[\mathcal{V},\mathcal{A}]}\left(\mathbb{Z}_{(p)}[\mathrm{Flag}]\right) \to \mathcal{E}_{\mathbb{Z}_{(p)}[\mathrm{Flag}]}\left(\mathbb{F}_p^n\right)$ (since ε is a $\mathbb{Z}_{(p)}$-algebra homomorphism and is bijective). Since $[\mathcal{V},\mathcal{A}] = \mathcal{V}\mathcal{A}$ and

$$\begin{aligned}\mathcal{E}_{\mathbb{Z}_{(p)}[\mathrm{Flag}]}\left(\mathbb{F}_p^n\right) &= \mathcal{E}_F\left(\mathbb{F}_p^n\right) \qquad \left(\text{since } \mathbb{Z}_{(p)}[\mathrm{Flag}] = F\right) \\ &= \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\mathrm{Flag}\left(\mathbb{F}_p^n\right)\right]\right) \qquad (\text{by } (40)),\end{aligned}$$

this rewrites as follows: The map ε is a $\mathbb{Z}_{(p)}$-algebra isomorphism $\operatorname{End}_{\mathcal{V}\mathcal{A}}\left(\mathbb{Z}_{(p)}[\mathrm{Flag}]\right) \to \operatorname{End}_{\mathbb{Z}_{(p)}[G]}\left(\mathbb{Z}_{(p)}\left[\mathrm{Flag}\left(\mathbb{F}_p^n\right)\right]\right)$. This proves Proposition 8.1b **(a)**.

(b) The orbit $G\underline{E}$ of $\underline{E} \in \mathrm{Flag}\left(\mathbb{F}_p^n\right)$ is the whole G-set $\mathrm{Flag}\left(\mathbb{F}_p^n\right)$ (since the G-set $\mathrm{Flag}\left(\mathbb{F}_p^n\right)$ is transitive). Thus, $\mathrm{Flag}\left(\mathbb{F}_p^n\right) = G\underline{E}$. But the orbit-stabilizer theorem shows that $G\underline{E} \cong G/G_{\underline{E}}$ as G-sets, where $G_{\underline{E}}$ denotes the stabilizer of $\underline{E}$ in G. However, the stabilizer of $\underline{E}$ in G is B (this is essentially the definition of B). In other words, $G_{\underline{E}} = B$. Altogether, we thus have $\mathrm{Flag}\left(\mathbb{F}_p^n\right) = G\underline{E} \cong G/\underbrace{G_{\underline{E}}}_{=B} = G/B$ as G-sets. This isomorphism is natural. Hence, there is a natural isomorphism $G/B \to \mathrm{Flag}\left(\mathbb{F}_p^n\right)$ of G-sets. This isomorphism sends each coset $hB \in G/B$ of B to the complete flag $h\underline{E} \in \mathrm{Flag}\left(\mathbb{F}_p^n\right)$ (because of how it is constructed). The remaining statements of Proposition 8.1b **(b)** follow from this immediately.]

- **§8:** Replace "Note that $\mathbb{Z}_{(p)}[X]$ has an obvious inner product" by "Note that $\mathbb{Z}_{(p)}[X]$ (for any set X) has an obvious inner product". (This is to disambiguate the meaning of X; you have previously used X for functors as well.)

- **§8:** Replace "Given $f : \mathbb{Z}_{(p)}[X] \to \mathbb{Z}_{(p)}[Y]$ we let $f^t : \mathbb{Z}_{(p)}[Y] \to \mathbb{Z}_{(p)}[X]$" by "Given a $\mathbb{Z}_{(p)}$-linear map $f : \mathbb{Z}_{(p)}[X] \to \mathbb{Z}_{(p)}[Y]$ we let $f^t : \mathbb{Z}_{(p)}[Y] \to \mathbb{Z}_{(p)}[X]$".

- **§8:** When you write "if f comes from a map $f : X \to Y$", you are slightly abusing notation (you are using the same notation for the map $f : X \to Y$ and the $\mathbb{Z}_{(p)}$-linear map $\mathbb{Z}_{(p)}[X] \to \mathbb{Z}_{(p)}[Y]$ induced by it); it might be good to explicitly point this out. Better yet, I suggest replacing the whole sentence ("In particular, if f comes from a map $f : X \to Y$ then $f^t[y] = \sum\limits_{f(x)=y}[x]$.") by the following paragraphs:

"Notice that if $f : \mathbb{Z}_{(p)}[X] \to \mathbb{Z}_{(p)}[Y]$ and $g : \mathbb{Z}_{(p)}[Y] \to \mathbb{Z}_{(p)}[Z]$ are two $\mathbb{Z}_{(p)}$-linear maps, then

$$(g \circ f)^t = f^t \circ g^t. \tag{42}$$

To each map $f : X \to Y$ between two sets X and Y corresponds a $\mathbb{Z}_{(p)}$-linear map $\mathbb{Z}_{(p)}[f] : \mathbb{Z}_{(p)}[X] \to \mathbb{Z}_{(p)}[Y]$ defined by

$$\left(\left(\mathbb{Z}_{(p)}[f]\right)[x] = [f(x)] \qquad \text{for every } x \in X\right).$$

The adjoint $\left(\mathbb{Z}_{(p)}[f]\right)^t$ of this map $\mathbb{Z}_{(p)}[f]$ is given by

$$\left(\mathbb{Z}_{(p)}[f]\right)^t [y] = \sum_{\substack{x \in X;\\ f(x)=y}} [x] \qquad \text{for each } y \in Y. \tag{43}$$

We shall often (by abuse of notation) denote the $\mathbb{Z}_{(p)}$-linear map $\mathbb{Z}_{(p)}[f]$ by f again. (This is a natural thing to do, because if we regard X and Y as subsets of $\mathbb{Z}_{(p)}[X]$ and $\mathbb{Z}_{(p)}[Y]$ in the obvious way, then the original map $f : X \to Y$ becomes a restriction of the map $\mathbb{Z}_{(p)}[f] : \mathbb{Z}_{(p)}[X] \to \mathbb{Z}_{(p)}[Y]$.) Thus, the equality (43) rewrites as

$$f^t [y] = \sum_{\substack{x \in X;\\ f(x)=y}} [x] \qquad \text{for each } y \in Y. \tag{44}$$

Next, let us state two basic facts about adjoints:

Lemma 8.1d. Let X and Y be two sets. Let $f : X \to Y$ be a bijection. Then, $\left(\mathbb{Z}_{(p)}[f]\right)^t = \mathbb{Z}_{(p)}\left[f^{-1}\right]$. (Relying on our abuse of notation, we can rewrite this as $f^t = f^{-1}$.)

[*Proof of Lemma 8.1d.* Let $y \in Y$. Recall that f is a bijection. Hence, there exists exactly one $x \in X$ satisfying $f(x) = y$ (namely, $x = f^{-1}(y)$). Thus, $\sum\limits_{\substack{x \in X;\\ f(x)=y}} = \sum\limits_{x \in \left\{f^{-1}(y)\right\}}$ (an equality of summation signs). Now, (43) yields

$$\left(\mathbb{Z}_{(p)}[f]\right)^t [y] = \underbrace{\sum_{\substack{x \in X;\\ f(x)=y}}}_{= \sum_{x \in \left\{f^{-1}(y)\right\}}} [x] = \sum_{x \in \left\{f^{-1}(y)\right\}} [x] = \left[f^{-1}(y)\right].$$

Comparing this with $\left(\mathbb{Z}_{(p)}\left[f^{-1}\right]\right)[y] = \left[f^{-1}(y)\right]$, we obtain $\left(\mathbb{Z}_{(p)}[f]\right)^t [y] = \left(\mathbb{Z}_{(p)}\left[f^{-1}\right]\right)[y]$.

Now, forget that we fixed y. We thus have proven that $\left(\mathbb{Z}_{(p)}[f]\right)^t[y] = \left(\mathbb{Z}_{(p)}\left[f^{-1}\right]\right)[y]$ for each $y \in Y$. In other words, the two maps $\left(\mathbb{Z}_{(p)}[f]\right)^t$ and $\mathbb{Z}_{(p)}\left[f^{-1}\right]$ are equal to each other on each of the elements of the basis $([y])_{y\in Y}$ of the $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}[Y]$. Since these two maps are $\mathbb{Z}_{(p)}$-linear, we can therefore conclude that they are equal. In other words, $\left(\mathbb{Z}_{(p)}[f]\right)^t = \mathbb{Z}_{(p)}\left[f^{-1}\right]$. This proves Lemma 8.1d. □]

Lemma 8.1e. Let P and Q be two functors from $\mathcal{V}$ to $\mathcal{F}$. Let $\alpha : P \Longrightarrow Q$ be a natural transformation.

(a) Define a family $\beta = (\beta_V)_{V\in\mathcal{V}}$ of morphisms $\beta_V : \mathbb{Z}_{(p)}[P(V)] \to \mathbb{Z}_{(p)}[Q(V)]$ by

$$\left(\beta_V = \mathbb{Z}_{(p)}[\alpha_V] \qquad \text{for each } V \in \mathcal{V}\right).$$

Then, β is a natural transformation $\mathbb{Z}_{(p)}[P] \Longrightarrow \mathbb{Z}_{(p)}[Q]$.

(b) Define a family $\gamma = (\gamma_V)_{V\in\mathcal{V}}$ of morphisms $\gamma_V : \mathbb{Z}_{(p)}[Q(V)] \to \mathbb{Z}_{(p)}[P(V)]$ by

$$\left(\gamma_V = (\beta_V)^t \qquad \text{for each } V \in \mathcal{V}\right).$$

Then, γ is a natural transformation $\mathbb{Z}_{(p)}[Q] \Longrightarrow \mathbb{Z}_{(p)}[P]$.

[*Proof of Lemma 8.1e.* **(a)** This is straightforward to prove.

(b) We need to prove that if V and W are two objects of $\mathcal{V}$, and if $g : V \to W$ is a morphism of $\mathcal{V}$, then the diagram

$$\begin{tikzcd} \mathbb{Z}_{(p)}[Q(V)] \arrow[r, "\gamma_V"] \arrow[d, "\mathbb{Z}_{(p)}[Q(g)]"'] & \mathbb{Z}_{(p)}[P(V)] \arrow[d, "\mathbb{Z}_{(p)}[P(g)]"] \\ \mathbb{Z}_{(p)}[Q(W)] \arrow[r, "\gamma_W"'] & \mathbb{Z}_{(p)}[P(W)] \end{tikzcd} \qquad (45)$$

is commutative.

So let V and W be two objects of $\mathcal{V}$, and let $g : V \to W$ be a morphism of $\mathcal{V}$. We must prove that the diagram (45) is commutative.

The morphisms of $\mathcal{V}$ are isomorphisms of $\mathbb{F}_p$ -vector spaces (by the definition of $\mathcal{V}$). Thus, each morphism of $\mathcal{V}$ is an isomorphism. In particular, g is an isomorphism (since g is a morphism of $\mathcal{V}$). Since P is a functor, this shows that $P(g)$ is an isomorphism and that $(P(g))^{-1} = P\left(g^{-1}\right)$.

The map $P(g)$ is an isomorphism in $\mathcal{F}$. In other words, $P(g)$ is a bijection. Hence, Lemma 8.1d (applied to $X = P(V)$, $Y = P(W)$ and $f = g$) shows that

$$\left(\mathbb{Z}_{(p)}\left[P\left(g\right)\right]\right)^{t}=\mathbb{Z}_{(p)}\left[\underbrace{\left(P\left(g\right)\right)^{-1}}_{=P\left(g^{-1}\right)}\right]=\mathbb{Z}_{(p)}\left[P\left(g^{-1}\right)\right].$$

Hence,

$$\left(\underbrace{\mathbb{Z}_{(p)}\left[P\left(g^{-1}\right)\right]}_{=\left(\mathbb{Z}_{(p)}\left[P(g)\right]\right)^{t}}\right)^{t}=\left(\left(\mathbb{Z}_{(p)}\left[P\left(g\right)\right]\right)^{t}\right)^{t}=\mathbb{Z}_{(p)}\left[P\left(g\right)\right]$$

(since the adjoint of the adjoint of a linear map is the original map). The same argument (applied to Q instead of P) shows that $\left(\mathbb{Z}_{(p)}\left[Q\left(g^{-1}\right)\right]\right)^{t}=\mathbb{Z}_{(p)}\left[Q\left(g\right)\right]$.

But the definition of γ_V shows that

$$\gamma_V=\left(\underbrace{\beta_V}_{=\mathbb{Z}_{(p)}\left[\alpha_V\right]}\right)^{t}=\left(\mathbb{Z}_{(p)}\left[\alpha_V\right]\right)^{t}.$$

The same argument (applied to W instead of V) shows that $\gamma_W=\left(\mathbb{Z}_{(p)}\left[\alpha_W\right]\right)^{t}$.

But α is a natural transformation. Hence, the diagram

$$\begin{tikzcd}
P\left(W\right) \arrow[r, "\alpha_W"] \arrow[d, "P\left(g^{-1}\right)"'] & Q\left(W\right) \arrow[d, "Q\left(g^{-1}\right)"] \\
P\left(V\right) \arrow[r, "\alpha_V"'] & Q\left(V\right)
\end{tikzcd}$$

is commutative. In other words, we have $Q\left(g^{-1}\right)\circ\alpha_W=\alpha_V\circ P\left(g^{-1}\right)$.

But

$$\begin{aligned}
&\left(\underbrace{\mathbb{Z}_{(p)}\left[Q\left(g^{-1}\right)\right]\circ\mathbb{Z}_{(p)}\left[\alpha_W\right]}_{=\mathbb{Z}_{(p)}\left[Q\left(g^{-1}\right)\circ\alpha_W\right]}\right)^t \\
&=\left(\mathbb{Z}_{(p)}\left[\underbrace{Q\left(g^{-1}\right)\circ\alpha_W}_{=\alpha_V\circ P\left(g^{-1}\right)}\right]\right)^t \\
&=\left(\underbrace{\mathbb{Z}_{(p)}\left[\alpha_V\circ P\left(g^{-1}\right)\right]}_{=\mathbb{Z}_{(p)}\left[\alpha_V\right]\circ\mathbb{Z}_{(p)}\left[P\left(g^{-1}\right)\right]}\right)^t \\
&=\left(\mathbb{Z}_{(p)}\left[\alpha_V\right]\circ\mathbb{Z}_{(p)}\left[P\left(g^{-1}\right)\right]\right)^t=\underbrace{\left(\mathbb{Z}_{(p)}\left[P\left(g^{-1}\right)\right]\right)^t}_{=\mathbb{Z}_{(p)}\left[P(g)\right]}\circ\underbrace{\left(\mathbb{Z}_{(p)}\left[\alpha_V\right]\right)^t}_{=\gamma_V} \\
&\qquad\left(\begin{array}{c}\text{by (42) (applied to } P\left(W\right), P\left(V\right), Q\left(V\right), \mathbb{Z}_{(p)}\left[P\left(g^{-1}\right)\right] \\ \text{and } \mathbb{Z}_{(p)}\left[\alpha_V\right] \text{ instead of } X, Y, Z, f \text{ and } g\text{)}\end{array}\right) \\
&=\mathbb{Z}_{(p)}\left[P\left(g\right)\right]\circ\gamma_V.
\end{aligned}$$

Hence,

$$\begin{aligned}
&\mathbb{Z}_{(p)}\left[P\left(g\right)\right]\circ\gamma_V \\
&=\left(\mathbb{Z}_{(p)}\left[Q\left(g^{-1}\right)\right]\circ\mathbb{Z}_{(p)}\left[\alpha_W\right]\right)^t=\underbrace{\left(\mathbb{Z}_{(p)}\left[\alpha_W\right]\right)^t}_{=\gamma_W}\circ\underbrace{\left(\mathbb{Z}_{(p)}\left[Q\left(g^{-1}\right)\right]\right)^t}_{=\mathbb{Z}_{(p)}\left[Q(g)\right]} \\
&\qquad\left(\begin{array}{c}\text{by (42) (applied to } P\left(W\right), Q\left(W\right), Q\left(V\right), \mathbb{Z}_{(p)}\left[\alpha_W\right] \\ \text{and } \mathbb{Z}_{(p)}\left[Q\left(g^{-1}\right)\right] \text{ instead of } X, Y, Z, f \text{ and } g\text{)}\end{array}\right) \\
&=\gamma_W\circ\mathbb{Z}_{(p)}\left[Q\left(g\right)\right].
\end{aligned}$$

In other words, the diagram (45) is commutative. This is precisely what we wanted to prove. Hence, Lemma 8.1e **(b)** is proven. □]

The natural transformations β and γ defined in Lemma 8.1e will be denoted by $\mathbb{Z}_{(p)}\left[\alpha\right]$ and $\left(\mathbb{Z}_{(p)}\left[\alpha\right]\right)^t$, respectively. By abuse of notation, we shall often denote these natural transformations β and γ by α and α^t, respectively. Notice that this abuse of notation is compatible with composition of functors, because of the following remark:

Remark 8.1f. **(a)** For every functor $P : \mathcal{V} \to \mathcal{F}$, we have $\mathbb{Z}_{(p)}\left[\mathrm{id}_P\right] = \mathrm{id}_{\mathbb{Z}_{(p)}\left[P\right]}$.

(b) Let P, Q and R be three functors from $\mathcal{V}$ to $\mathcal{F}$. Let $\alpha_1 : P \Longrightarrow Q$ and $\alpha_2 : Q \Longrightarrow R$ be two natural transformations. Then, $\mathbb{Z}_{(p)}[\alpha_2] \circ \mathbb{Z}_{(p)}[\alpha_1] = \mathbb{Z}_{(p)}[\alpha_2 \circ \alpha_1]$.

[*Proof of Remark 8.1f.* These are straightforward computations. □]"

The purpose of Lemma 8.1e is to explain the meaning of "$\pi_1 \pi_0^t$" in Definition 8.2.

- **Definition 8.2:** I suggest adding the sentence "Let $\sigma \in \Sigma_n$." at the beginning of this definition.

- **Definition 8.2:** For the sake of completeness, I suggest actually defining the projection maps π_0 and π_1: Namely, the natural transformation $\pi_0 : Z(\sigma) \to \operatorname{Flag}$ (or, rather, its component $(\pi_0)_V : (Z(\sigma))(V) \to \operatorname{Flag}(V)$ for a given $V \in \mathcal{V}$) sends each $(\underline{U}, \underline{W}) \in (Z(\sigma))(V)$ to $\underline{U}$, whereas the natural transformation $\pi_1 : Z(\sigma) \to \operatorname{Flag}$ (or, rather, its component $(\pi_1)_V : (Z(\sigma))(V) \to \operatorname{Flag}(V)$ for a given $V \in \mathcal{V}$) sends each $(\underline{U}, \underline{W}) \in (Z(\sigma))(V)$ to $\underline{W}$.

- **Definition 8.2:** After "that $T_\sigma^t = T_{\sigma^{-1}}$", add "(since $\delta(\underline{U}, \underline{W}) = \delta(\underline{W}, \underline{U})^{-1}$ for all $\underline{U}, \underline{W} \in \operatorname{Flag}(V)$).

- **Proof of Proposition 8.3:** After "Consider an element $f : \mathbb{Z}_{(p)}[\operatorname{Flag}] \to \mathbb{Z}_{(p)}[\operatorname{Flag}]$", add "of $\mathcal{H}$".

- **Proof of Proposition 8.3:** I would replace "well-defined numbers n_σ" by "well-defined numbers $n_\sigma \in \mathbb{Z}_{(p)}$" (in order to avoid creating the false impression that they must necessarily be integers).

- **Proposition 8.4:** Replace "Let $\underline{U}$ be a flag, let F be the set of flags $\underline{W}$ such that $W_j = U_j$ for all $j \neq i$, and put $a = \sum_{\underline{W} \in F} [\underline{W}]$." by: "Let $V \in \mathcal{V}$. Let $\underline{U} \in \operatorname{Flag}(V)$. Let F be the set of all $\underline{W} \in \operatorname{Flag}(V)$ satisfying $W_j = U_j$ for all $j \neq i$. Set $a = \sum_{\underline{W} \in F} [\underline{W}] \in \mathbb{Z}_{(p)}[\operatorname{Flag}(V)]$."

- **Proof of Proposition 8.4:** I would suggest replacing the "$\sum_{\underline{W}}$" sign by an "$\sum_{\underline{W} \in F}$" sign (seeing that you otherwise always use "$\sum_{\underline{W} \in F}$" signs).

- **Proof of Proposition 8.4:** Replace "so $T_i(a) = pa$" by "so $T_i(a) = \left(\underbrace{|F|}_{=p+1} - 1\right) a = pa$, thus $(T_i - p)\, a = 0$".

- **Proof of Proposition 8.4:** Replace “It follows that $(T_i - p)(T_i + 1)[\underline{W}] = (T_i - p)(a) = 0$ as claimed” by “From $(T_i + 1)[\underline{U}] = \underbrace{T_i[\underline{U}]}_{=a-[\underline{U}]} + [\underline{U}] = a$, it follows that $(T_i - p)(T_i + 1)[\underline{U}] = (T_i - p)(a) = 0$ as claimed”. (The claim of Proposition 8.4 does not involve $\underline{W}$!)
- **Definition 8.5:** Replace “We define” by “For each $V \in \mathcal{V}$, we define a $\mathbb{Z}_{(p)}$-linear map”.
- **Definition 8.5:** Replace “We also define a map” by “We also define a $\mathbb{Z}_{(p)}$-linear map”.
- **Definition 8.5:** Replace “$\sum\limits_{\sigma} p^{l(\sigma)}$” by “$\sum\limits_{\sigma} n_\sigma p^{l(\sigma)}$ whenever $n_\sigma \in \mathbb{Z}_{(p)}$”.
- **Proof of Proposition 8.6:** Replace “so $\widehat{e}[\underline{U}] = x$ for all $\underline{W}$” by “so $\widehat{e}[\underline{U}] = x$ for all $\underline{U}$”.
- **Proof of Proposition 8.6:** Replace “$|\mathrm{Flag}|^{-1}$” by “$|\mathrm{Flag}(V)|^{-1}$”.
- **Proof of Proposition 8.6:** I’d suggest more detail once again: Replace “Next, we have

$$\widehat{e}T_\sigma[\underline{U}] = \sum_{\delta(\underline{U},\underline{W})=\sigma} \widehat{e}[\underline{W}] = \left|\left\{\underline{W} \mid \delta(\underline{W},\underline{U}) = \sigma^{-1}\right\}\right| x = p^{l(\sigma^{-1})} x = p^{l(\sigma)} \widehat{e}[\underline{W}].$$

(using Proposition 5.2 and the fact that $l(\sigma^{-1}) = l(\sigma)$)” by “Next, observe that each $\sigma \in \Sigma_n$ satisfies

$$\begin{aligned} &\left\{ \underline{W} \mid \underbrace{\delta(\underline{U},\underline{W})}_{=\delta(\underline{W},\underline{U})^{-1}} = \sigma \right\} \\ &= \left\{ \underline{W} \mid \underbrace{\delta(\underline{W},\underline{U})^{-1} = \sigma}_{\iff (\delta(\underline{W},\underline{U}) = \sigma^{-1})} \right\} = \left\{ \underline{W} \mid \delta(\underline{W},\underline{U}) = \sigma^{-1} \right\} \\ &= Y\left(\sigma^{-1}, \underline{U}\right) \qquad \text{(using the notation from §5)} \end{aligned}$$

and therefore

$$\begin{aligned} \left| \underbrace{\{\underline{W} \mid \delta(\underline{U},\underline{W}) = \sigma\}}_{=Y(\sigma^{-1},\underline{U})} \right| &= \left| Y\left(\sigma^{-1}, \underline{U}\right) \right| = p^{l(\sigma^{-1})} \\ &\qquad \left(\begin{array}{c} \text{by Corollary 5.2a, applied to } \sigma^{-1}, V \text{ and } \underline{U} \\ \text{instead of } \sigma, W \text{ and } \underline{V} \end{array} \right) \\ &= p^{l(\sigma)} \qquad \left(\text{since } l\left(\sigma^{-1}\right) = l(\sigma)\right) \end{aligned}$$

and thus

$$\begin{aligned}\widehat{e}T_{\sigma}\left[\underline{U}\right] &= \sum_{\delta(\underline{U},\underline{W})=\sigma} \underbrace{\widehat{e}\left[\underline{W}\right]}_{=x} \qquad \left(\text{since } T_{\sigma}\left[\underline{U}\right] = \sum_{\delta(\underline{U},\underline{W})=\sigma} \left[\underline{W}\right]\right) \\ &= \sum_{\delta(\underline{U},\underline{W})=\sigma} x = \underbrace{\left|\left\{\underline{W} \mid \delta\left(\underline{U},\underline{W}\right)=\sigma\right\}\right|}_{=p^{l(\sigma)}} x = p^{l(\sigma)} \underbrace{x}_{=\widehat{e}[\underline{U}]} = p^{l(\sigma)}\widehat{e}\left[\underline{U}\right]\end{aligned}$$

". (Notice that I replaced the "$\widehat{e}\left[\underline{W}\right]$." at the end of the long equation by an "$\widehat{e}\left[\underline{U}\right]$", as I think this is what you meant.)

- **Proof of Proposition 8.6:** After "we deduce that $\widehat{\xi}$ is a ring map", I suggest adding "(in fact, we compare $\widehat{e}ab = \widehat{e}\left(ab\right) = \widehat{\xi}\left(ab\right)\widehat{e}$ with $\underbrace{\widehat{e}a}_{=\widehat{\xi}(a)\widehat{e}} b = \widehat{\xi}\left(a\right) \underbrace{\widehat{e}b}_{=\widehat{\xi}(b)\widehat{e}} = \widehat{\xi}\left(a\right)\widehat{\xi}\left(b\right)\widehat{e}$, and thus we find $\widehat{\xi}\left(ab\right)\widehat{e} = \widehat{\xi}\left(a\right)\widehat{\xi}\left(b\right)\widehat{e}$, which leads to $\widehat{\xi}\left(ab\right) = \widehat{\xi}\left(a\right)\widehat{\xi}\left(b\right)$ because $\widehat{e}$ is a nonzero vector in a free $\mathbb{Z}_{(p)}$-module)".
- **Proof of Proposition 8.6:** Replace "$a\widehat{e} = \xi\left(a^{t}\right)\widehat{e}$" by "$a\widehat{e} = \widehat{\xi}\left(a^{t}\right)\widehat{e}$".
- **Proof of Lemma 8.7:** I would replace the last sentence of this proof by the following (more detailed) argument:

  "Since every $\underline{U} \in \operatorname{Flag}\left(\mathbb{F}_p^n\right)$ satisfies the chain of equivalences

  $$\begin{aligned}\left(\delta\left(\underline{E},\underline{U}\right) = \sigma^{-1}\right) &\iff \left(\underbrace{\delta\left(\underline{E},\underline{U}\right)^{-1}}_{=\delta(\underline{U},\underline{E})} = \sigma\right) \iff \left(\delta\left(\underline{U},\underline{E}\right) = \sigma\right) \\ &\iff \left(\underline{U} \in \underbrace{Y\left(\sigma,\underline{E}\right)}_{=Y(\sigma)}\right) \qquad \left(\text{by the definition of } Y\left(\sigma,\underline{E}\right)\right) \\ &\iff \left(\underline{U} \in Y\left(\sigma\right)\right),\end{aligned}$$

  this rewrites as $T_{\sigma^{-1}}\left[\underline{E}\right] = \sum_{\underline{U}\in Y(\sigma)} \left[\underline{U}\right]$. But Proposition 5.2 shows that the map $g \mapsto g\sigma\underline{E}$ gives a bijection $X\left(\sigma\right) \to Y\left(\sigma\right)$. Hence, $\sum_{\underline{U}\in Y(\sigma)} \left[\underline{U}\right] = \sum_{g\in X(\sigma)} \left[g\sigma\underline{E}\right]$. Hence,

  $$T_{\sigma^{-1}}\left[\underline{E}\right] = \sum_{\underline{U}\in Y(\sigma)} \left[\underline{U}\right] = \sum_{g\in X(\sigma)} \left[g\sigma\underline{E}\right] = \sum_{x\in X(\sigma)} \left[x\sigma\underline{E}\right], \tag{46}$$

  as required.".

- **§8:** Between Lemma 8.7 and Corollary 8.8, you write: "note that $\operatorname{Base}(V)$ is canonically the same as $\operatorname{Iso}\left(\mathbb{F}_p^n, V\right)$". I suggest adding "(in fact, there is a canonical bijection $\operatorname{Iso}\left(\mathbb{F}_p^n, V\right) \to \operatorname{Base}(V)$ sending each $\phi \in \operatorname{Iso}\left(\mathbb{F}_p^n, V\right)$ to $(\phi e_1, \phi e_2, \ldots, \phi e_n) \in \operatorname{Base}(V)$)" after this.

- **§8:** Between Lemma 8.7 and Corollary 8.8, replace "gives a map $g^* : \operatorname{Base} \to \operatorname{Base}$" by "gives a natural transformation $g^* : \operatorname{Base} \to \operatorname{Base}$ (whose V-component for any given $V \in \mathcal{V}$ is the map

$$\operatorname{Iso}\left(\mathbb{F}_p^n, V\right) \to \operatorname{Iso}\left(\mathbb{F}_p^n, V\right), \qquad \phi \mapsto \phi \circ g,$$

interpreted as a map $\operatorname{Base}(V) \to \operatorname{Base}(V)$ via the canonical bijection $\operatorname{Iso}\left(\mathbb{F}_p^n, V\right) \to \operatorname{Base}(V)$)".

- **§8:** Just before Corollary 8.8, I would add the following two lemmas:

Lemma 8.7a. Let $\mathbf{e} \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$ be the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$. Let $g \in G$.

(a) We have $g^*\mathbf{e} = (ge_1, ge_2, \ldots, ge_n)$.

(b) We have $\pi(g^*\mathbf{e}) = g\underline{E}$.

[*Proof of Lemma 8.7a.* **(a)** Set $V = \mathbb{F}_p^n$. Recall that the V-component of the natural transformation $g^* : \operatorname{Base} \to \operatorname{Base}$ is the map

$$\operatorname{Iso}\left(\mathbb{F}_p^n, V\right) \to \operatorname{Iso}\left(\mathbb{F}_p^n, V\right), \qquad \phi \mapsto \phi \circ g,$$

interpreted as a map $\operatorname{Base}(V) \to \operatorname{Base}(V)$ via the canonical bijection $\operatorname{Iso}\left(\mathbb{F}_p^n, V\right) \to \operatorname{Base}(V)$ (because this is how g^* was defined). In other words, every $\mathbf{b} \in \operatorname{Base}(V)$ satisfies $g^*\mathbf{b} = \alpha\left(\alpha^{-1}(\mathbf{b}) \circ g\right)$, where α is the canonical bijection $\operatorname{Iso}\left(\mathbb{F}_p^n, V\right) \to \operatorname{Base}(V)$. Consider this α. Notice that $\operatorname{id}_{\mathbb{F}_p^n} \in \operatorname{Iso}\left(\mathbb{F}_p^n, \underbrace{\mathbb{F}_p^n}_{=V}\right) = \operatorname{Iso}\left(\mathbb{F}_p^n, V\right)$. The definition of α shows that

$$\alpha\left(\operatorname{id}_{\mathbb{F}_p^n}\right) = (\operatorname{id} e_1, \operatorname{id} e_2, \ldots, \operatorname{id} e_n) = (e_1, e_2, \ldots, e_n) = \mathbf{e}.$$

Hence, $\alpha^{-1}(\mathbf{e}) = \operatorname{id}_{\mathbb{F}_p^n}$. Now, recall that every $\mathbf{b} \in \operatorname{Base}(V)$ satisfies $g^*\mathbf{b} = \alpha\left(\alpha^{-1}(\mathbf{b}) \circ g\right)$. Applying this to $\mathbf{b} = \mathbf{e}$, we obtain

$$g^*\mathbf{e} = \alpha\left(\underbrace{\alpha^{-1}(\mathbf{e})}_{=\operatorname{id}_{\mathbb{F}_p^n}} \circ g\right) = \alpha(g) = (ge_1, ge_2, \ldots, ge_n).$$

This proves Lemma 8.7a **(a)**.

(b) We have $g^*\mathbf{e} = (ge_1, ge_2, \ldots, ge_n)$ (by Lemma 8.7a **(a)**). Applying the natural transformation π to both sides of this equality, we obtain

$$\pi(g^*\mathbf{e}) = \pi(ge_1, ge_2, \ldots, ge_n) = g\underbrace{\pi(e_1, e_2, \ldots, e_n)}_{=\underline{E}} = g\underline{E}.$$

This proves Lemma 8.7a **(b)**. □]

Lemma 8.7b. Let $Y \in \mathcal{VA}$ be a functor. Let X be the functor $\mathbb{Z}_{(p)}[\text{Base}] \in \mathcal{VA}$. Let $\alpha : X \Longrightarrow Y$ and $\beta : X \Longrightarrow Y$ be two natural transformations. Let $\mathbf{e} \in \text{Base}\left(\mathbb{F}_p^n\right)$ be the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$. Assume that $\alpha[\mathbf{e}] = \beta[\mathbf{e}]$ in $Y\left(\mathbb{F}_p^n\right)$. Then, $\alpha = \beta$.

[*Proof of Lemma 8.7b.* Fix $V \in \mathcal{V}$. Let $u \in X(V)$. We are going to show that $\alpha(u) = \beta(u)$. Notice that $([\mathbf{u}])_{\mathbf{u} \in \text{Base}(V)}$ is a basis of the $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}[\text{Base}(V)] = \underbrace{\left(\mathbb{Z}_{(p)}[\text{Base}]\right)}_{=X}(V) = X(V)$.

The V-components of α and β are morphisms in the category $\mathcal{A}$. In other words, the V-components of α and β are $\mathbb{Z}_{(p)}$-linear maps. Hence, both $\alpha(u)$ and $\beta(u)$ depend $\mathbb{Z}_{(p)}$-linearly on u. Hence, the equation $\alpha(u) = \beta(u)$ (which we want to prove) is linear in u. Thus, for the proof of this equation, we can WLOG assume that u belongs to the basis $([\mathbf{u}])_{\mathbf{u} \in \text{Base}(V)}$ of the $\mathbb{Z}_{(p)}$-module $X(V)$. Assume this.

We have assumed that u belongs to the basis $([\mathbf{u}])_{\mathbf{u} \in \text{Base}(V)}$ of the $\mathbb{Z}_{(p)}$-module $X(V)$. In other words, $u = [\mathbf{u}]$ for some $\mathbf{u} \in \text{Base}(V)$. Consider this $\mathbf{u}$.

We have $\mathbf{u} \in \text{Base}(V)$. Thus, $\mathbf{u}$ is a basis of the n-dimensional $\mathbb{F}_p$-vector space V. Write $\mathbf{u}$ in the form $(u_1, u_2, \ldots, u_n)$.

Let ϕ be the $\mathbb{F}_p$-linear map $\mathbb{F}_p^n \to V$ that sends the basis vectors $e_1, e_2, \ldots, e_n$ of $\mathbb{F}_p^n$ to $u_1, u_2, \ldots, u_n$, respectively. Then, the $\mathbb{F}_p$-linear map ϕ sends the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$ to the basis $(u_1, u_2, \ldots, u_n)$ of V. Hence, ϕ is an isomorphism of vector spaces. In other words, ϕ is a morphism in the category $\mathcal{V}$.

Now, the morphism $\text{Base}\,\phi : \text{Base}\left(\mathbb{F}_p^n\right) \to \text{Base}(V)$ (induced by the morphism $\phi : \mathbb{F}_p^n \to V$) satisfies

$$\begin{aligned}
(\text{Base}\,\phi)(\mathbf{e}) &= (\text{Base}\,\phi)(e_1, e_2, \ldots, e_n) && (\text{since } \mathbf{e} = (e_1, e_2, \ldots, e_n)) \\
&= (u_1, u_2, \ldots, u_n) && \left(\begin{array}{c}\text{since } \phi \text{ sends the basis vectors} \\ e_1, e_2, \ldots, e_n \text{ to } u_1, u_2, \ldots, u_n\end{array}\right) \\
&= \mathbf{u}.
\end{aligned}$$

But the morphism $X(\phi) : X\left(\mathbb{F}_p^n\right) \to X(V)$ satisfies

$$\left(\underbrace{X}_{=\left(\mathbb{Z}_{(p)}[\text{Base}]\right)} (\phi)\right)[\mathbf{e}] = \left(\left(\mathbb{Z}_{(p)}[\text{Base}]\right)(\phi)\right)[\mathbf{e}] = \left[\underbrace{(\text{Base}\,\phi)(\mathbf{e})}_{=\mathbf{u}}\right] = [\mathbf{u}] = u. \tag{47}$$

But $\alpha : X \Longrightarrow Y$ is a natural transformation. Hence, the diagram

$$\begin{tikzcd} X\left(\mathbb{F}_p^n\right) \arrow[r, "\alpha_{\mathbb{F}_p^n}"] \arrow[d, "X(\phi)"'] & Y\left(\mathbb{F}_p^n\right) \arrow[d, "Y(\phi)"] \\ X(V) \arrow[r, "\alpha_V"'] & Y(V) \end{tikzcd}$$

is commutative (since $\phi : \mathbb{F}_p^n \to V$ is a morphism in the category $\mathcal{V}$). In other words, we have $Y(\phi) \circ \alpha_{\mathbb{F}_p^n} = \alpha_V \circ X(\phi)$. Hence,

$$\underbrace{\left(Y(\phi) \circ \alpha_{\mathbb{F}_p^n}\right)}_{=\alpha_V \circ X(\phi)}[\mathbf{e}] = (\alpha_V \circ X(\phi))[\mathbf{e}] = \alpha_V\left(\underbrace{(X(\phi))[\mathbf{e}]}_{=u}\right) = \alpha_V(u) = \alpha(u).$$

Hence,

$$\alpha(u) = \left(Y(\phi) \circ \alpha_{\mathbb{F}_p^n}\right)[\mathbf{e}] = (Y(\phi))\left(\underbrace{\alpha_{\mathbb{F}_p^n}[\mathbf{e}]}_{=\alpha[\mathbf{e}]}\right) = (Y(\phi))(\alpha[\mathbf{e}]).$$

The same argument (applied to β instead of α) shows that $\beta(u) = (Y(\phi))(\beta[\mathbf{e}])$. Comparing this with $\alpha(u) = (Y(\phi))\left(\underbrace{\alpha[\mathbf{e}]}_{=\beta[\mathbf{e}]}\right) = (Y(\phi))(\beta[\mathbf{e}])$, we obtain $\alpha(u) = \beta(u)$. Thus, $\alpha(u) = \beta(u)$ is proven.

Now, forget that we fixed u. We thus have shown that $\alpha(u) = \beta(u)$ for each $u \in X(V)$. In other words, the V-component of α equals the V-component of β.

Now, forget that we fixed V. We thus have proven that the V-component of α equals the V-component of β for each $V \in \mathcal{V}$. In other words, $\alpha = \beta$. This proves Lemma 8.7b. □]

- **Corollary 8.8:** The map π should be defined! I guess you want to define it as follows: "Let π : Base → Flag be the natural transformation whose V-component (for any given $V \in \mathcal{V}$) is the map Base $(V) \to$ Flag (V) sending each basis $(v_1, v_2, \ldots, v_n) \in \operatorname{Base}(V)$ to the flag

$$(0 = \operatorname{span}\{\} < \operatorname{span}\{v_1\} < \operatorname{span}\{v_1, v_2\} < \cdots < \operatorname{span}\{v_1, v_2, \ldots, v_n\} = V) \\ \in \operatorname{Flag}(V).$$

" (At least, this is the definition you give later, in Definition 9.1.)

- **Proof of Corollary 8.8:** I would replace the proof by the following (clearer) argument:

  [*Proof of Corollary 8.8.* First of all, the diagram makes sense, since all its arrows are well-defined natural transformations. It thus remains to prove that it commutes. In other words, it remains to prove that $T_\sigma^t \circ \pi = \pi \circ \left(\sum\limits_{x \in X(\sigma)} (x\sigma)^* \right)$.

  Let $\mathbf{e} \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$ be the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$. Then, $\pi(\mathbf{e}) = \underline{E}$.

  Now, the natural transformation $\pi : \mathbb{Z}_{(p)}[\mathrm{Base}] \to \mathbb{Z}_{(p)}[\mathrm{Flag}]$ satisfies $\pi[\mathbf{e}] = \left[\underbrace{\pi(\mathbf{e})}_{=\underline{E}} \right] = [\underline{E}]$. Hence,

$$\left(T_\sigma^t \circ \pi\right)[\mathbf{e}] = \underbrace{T_\sigma^t}_{=T_{\sigma^{-1}}} \left(\underbrace{\pi[\mathbf{e}]}_{=[\underline{E}]} \right) = T_{\sigma^{-1}}[\underline{E}] = \sum_{x \in X(\sigma)} [x\sigma\underline{E}]$$

  (by (46)). Comparing this with

$$\left(\pi \circ \left(\sum_{x \in X(\sigma)} (x\sigma)^* \right)\right)[\mathbf{e}] = \pi \underbrace{\left(\left(\sum_{x \in X(\sigma)} (x\sigma)^* \right)[\mathbf{e}] \right)}_{= \sum\limits_{x \in X(\sigma)} (x\sigma)^*[\mathbf{e}]} = \pi \left(\sum_{x \in X(\sigma)} (x\sigma)^*[\mathbf{e}] \right)$$

$$= \pi \left(\sum_{x \in X(\sigma)} (x\sigma)^*[\mathbf{e}] \right) = \sum_{x \in X(\sigma)} \underbrace{\pi\left((x\sigma)^*[\mathbf{e}]\right)}_{=\left[\pi\left((x\sigma)^*\mathbf{e}\right)\right]}$$

$$= \sum_{x \in X(\sigma)} \left[\underbrace{\pi\left((x\sigma)^*\mathbf{e}\right)}_{\substack{=x\sigma\underline{E} \\ \text{(by Lemma 8.7a (b)} \\ \text{(applied to } g=x\sigma))}} \right] = \sum_{x \in X(\sigma)} [x\sigma\underline{E}],$$

we obtain

$$\left(T_\sigma^t \circ \pi\right)[\mathbf{e}] = \left(\pi \circ \left(\sum_{x \in X(\sigma)} (x\sigma)^*\right)\right)[\mathbf{e}].$$

Hence, Lemma 8.7b (applied to $Y = \mathbb{Z}_{(p)}[\text{Flag}]$, $X = \mathbb{Z}_{(p)}[\text{Base}]$, $\alpha = T_\sigma^t \circ \pi$ and $\beta = \pi \circ \left(\sum\limits_{x \in X(\sigma)} (x\sigma)^*\right)$) yields that $T_\sigma^t \circ \pi = \pi \circ \left(\sum\limits_{x \in X(\sigma)} (x\sigma)^*\right)$. This completes the proof of Corollary 8.8. □]

- **Proof of Corollary 8.9:** After "The right hand side is $\sum\limits_{z \in X(\sigma\tau)} [gz\sigma\tau B]$", add "(by Lemma 8.7, applied to $\sigma\tau$ instead of σ)".
- **Corollary 8.10:** The notion of a "reduced word for σ" should be explained. (It means a reduced word $w \in W$ such that $\pi(w) = \sigma$, where π is the map $W \to \Sigma$ introduced in §2.)
- **Proof of Proposition 8.11:** Replace "Now consider T_i^2" by "Now fix $i \in \{1, 2, \ldots, n-1\}$ and consider T_i^2".
- **Proof of Proposition 8.11:** After "so $|A| = p + 1$", add "(because the elements of A are in bijection with the nonzero proper subspaces of the 2-dimensional $\mathbb{F}_p$-vector space U_{i+1}/U_{i-1}, and because the number of the latter subspaces is $p + 1$)".
- **Proof of Proposition 8.11:** Replace "Put

  $$\phi(W) = (0 = U_0 < \cdots < U_{i-1} < W < U_{i+1} < \cdots < U_n = V)$$

  " by "For each $W \in A$, put

  $$\phi(W) = (0 = U_0 < \cdots < U_{i-1} < W < U_{i+1} < \cdots < U_n = V) \in \text{Flag}(V).$$

  ".
- **Proof of Proposition 8.11:** Replace "One checks that the flags with $\delta(\underline{W}, \underline{U}) = s_i$ are" by "Proposition 4.7 shows that the flags $\underline{W}$ with $\delta(\underline{U}, \underline{W}) = s_i$ are". (I have made three changes here. The replacement of "$\delta(\underline{W}, \underline{U})$" by "$\delta(\underline{U}, \underline{W})$" is due to the fact that the explicit formula for T_i shows $T_i[\underline{U}] = \sum\limits_{\delta(\underline{U},\underline{W})=s_i} [\underline{W}]$ rather than $T_i[\underline{U}] = \sum\limits_{\delta(\underline{W},\underline{U})=s_i} [\underline{W}]$, even though both formulas are equivalent upon a closer look.
- **Proof of Proposition 8.11:** I would replace "It follows that $T_i[\underline{U}] = \sum\limits_{W \neq U_i} [\phi(W)]$" by "It follows that $\sum\limits_{\delta(\underline{U},\underline{W})=s_i} [\underline{W}] = \sum\limits_{W \neq U_i} [\phi(W)]$. Hence, $T_i[\underline{U}] = T_{s_i}[\underline{U}] = \sum\limits_{\delta(\underline{U},\underline{W})=s_i} [\underline{W}] = \sum\limits_{W \neq U_i} [\phi(W)]$".

- **Proof of Proposition 8.11:** Replace "as claimed." by "and thus the first relation $T_i^2 = p + (p-1) T_i$ holds. (Alternatively, this also follows from Proposition 8.4.)".

- **Proof of Proposition 8.11:** Replace "Now let $\mathcal{H}'$ be generated" by "Now let $\mathcal{H}'$ be the $\mathbb{Z}_{(p)}$-algebra generated".

- **Proof of Proposition 8.11:** After "subject only to the relations in the statement of the proposition", add "(with the T_k replaced by T'_k)".

- **Proof of Proposition 8.11:** Replace "and the T_i generate" by "and the T_i generate $\mathcal{H}$".

- **Proof of Proposition 8.11:** Replace "ring map θ" by "$\mathbb{Z}_{(p)}$-algebra map θ".

- **Proof of Proposition 8.11:** You write: "any reduced word $u = s_{i_1} \cdots s_{i_r}$ such that $\pi(u) = \sigma$". Here, π denotes the map $\pi : W \to \Sigma$ from §2, not the natural transformation $\pi : \text{Base} \to \text{Flag}$ from Corollary 8.8. I think this should be explained.

- **Proof of Proposition 8.11:** After "This is well-defined", add "(i.e., independent of the choice of u)".

- **Proof of Proposition 8.11:** Replace "Define a map ϕ" by "Define a $\mathbb{Z}_{(p)}$-linear map ϕ".

- **Proof of Proposition 8.11:** Replace "To see this, consider an element $T'_\sigma \in A$" by "To see this, it suffices to check that $T'_\sigma T'_i \in A$ for each $\sigma \in \Sigma_n$ (since the $\mathbb{Z}_{(p)}$-module A is spanned by the $\phi(T_\sigma) = T'_\sigma$ for $\sigma \in \Sigma_n$). Choose any $\sigma \in \Sigma_n$".

- **Proof of Proposition 8.11:** Replace "If $\sigma(i) > \sigma(i+1)$" by "If $\sigma(i) < \sigma(i+1)$".

- **Proof of Proposition 8.11:** Replace "We choose any reduced word" by "In this case, we choose any reduced word".

- **Proof of Proposition 8.11:** Before the long equation that begins with "$T'_\sigma T'_i = T'_\tau \left(T'_i\right)^2$", I would add "$T'_\sigma = T'_\tau T'_i$ and thus".

- **Proof of Proposition 8.11:** I would replace "$pT'_\tau + (p-1) T'_{\tau s_i} \in A$" by "$pT'_\tau + (p-1) \underbrace{T'_\tau T'_i}_{=T'_\sigma} = pT'_\tau + (p-1) T'_\sigma \in A$".

- **Proof of Proposition 8.11:** I would replace "$1 \in A$" by "$1 = T'_{\text{id}} \in A$".

- **Proof of Proposition 8.11:** Replace "injectve" by "injective".

- **§9:** I suggest using the LaTeX syntax `\operatorname{St}` instead of `\text{St}` in order to achieve the "St" subscripts. Otherwise, these subscripts are italicized whenever they appear inside propositions (because text in propositions is italicized).

- **§9:** At the very beginning of §9, I would add the following lemma (which is tacitly used in the definition of ω):

  Lemma 9.0a. We have $\left|G/U\right| \equiv (-1)^n \mod p$ and thus $\left|G/U\right|^{-1} \in \mathbb{Z}_{(p)}$.

  [*Proof of Lemma 9.0a.* Lemma 8.0a **(b)** (applied to $V = \mathbb{F}_p^n$) yields $\left|\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right| \equiv 1 \mod p$ and $\left|\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right|^{-1} \in \mathbb{Z}_{(p)}$.

  Proposition 8.1b **(b)** shows that there is a natural isomorphism $G/B \to \operatorname{Flag}\left(\mathbb{F}_p^n\right)$ of G-sets. Hence, $\left|G/B\right| = \left|\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right| \equiv 1 \mod p$.

  But from $\left|G/U\right| = \left|G\right| / \left|U\right|$ and $\left|G/B\right| = \left|G\right| / \left|B\right|$, we obtain

  $$\begin{aligned} \frac{\left|G/U\right|}{\left|G/B\right|} &= \frac{\left|G\right| / \left|U\right|}{\left|G\right| / \left|B\right|} = \frac{\left|B\right|}{\left|U\right|} = \frac{(p-1)^n p^{n(n-1)/2}}{p^{n(n-1)/2}} \\ &\qquad \left(\text{since } \left|B\right| = (p-1)^n p^{n(n-1)/2} \text{ and } \left|U\right| = p^{n(n-1)/2}\right) \\ &= (p-1)^n . \end{aligned} \tag{48}$$

  Thus,

  $$\left|G/U\right| = \Bigg(\underbrace{p-1}_{\equiv -1 \mod p}\Bigg)^n \cdot \underbrace{\left|G/B\right|}_{\equiv 1 \mod p} \equiv (-1)^n \mod p.$$

  Thus, $\left|G/U\right|$ is coprime to p (since $(-1)^n$ is coprime to p). Hence, $\left|G/U\right|^{-1} \in \mathbb{Z}_{(p)}$. This proves Lemma 9.0a. □]

- **§9:** I believe some more work is needed in order to justify the claim that "$\operatorname{End}\left(\mathbb{Z}_{(p)}\left[\text{Base}\right]\right) = \mathbb{Z}_{(p)}\left[G\right]^{\text{op}}$" (again, an isomorphism, not a literal equality). Here is how I would prove this claim:

  Lemma 9.0b. Let $\tau : G \to \operatorname{Base}\left(\mathbb{F}_p^n\right)$ be the map sending each $g \in G$ to the basis $(ge_1, ge_2, \ldots, ge_n) \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$. This map τ is well-defined and bijective.

  [*Proof of Lemma 9.0b.* If $g \in G$, then $(ge_1, ge_2, \ldots, ge_n) \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$ [32]. Hence, the map τ is well-defined. It remains to prove that this map τ is bijective.

[32] *Proof.* Let $g \in G$. Hence, g is an automorphism of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. But $(e_1, e_2, \ldots, e_n)$ is a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. Thus, the image of this basis $(e_1, e_2, \ldots, e_n)$ under g must also be a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$ (since g is an automorphism of the $\mathbb{F}_p$-vector

The map τ is injective[33] and surjective[34]. Hence, the map τ is bijective. This completes the proof of Lemma 9.0b. $\square$]

Lemma 9.0c. Recall that for every $g \in G$, we have defined a natural transformation $g^* : \operatorname{Base} \Longrightarrow \operatorname{Base}$, and thus we also obtain a natural transformation $\mathbb{Z}_{(p)}[g^*] : \mathbb{Z}_{(p)}[\operatorname{Base}] \Longrightarrow \mathbb{Z}_{(p)}[\operatorname{Base}]$. The latter natural transformation is an element of the ring $\operatorname{End}\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)$. (By abuse of notation, we can denote this natural transformation $\mathbb{Z}_{(p)}[g^*] : \mathbb{Z}_{(p)}[\operatorname{Base}] \Longrightarrow \mathbb{Z}_{(p)}[\operatorname{Base}]$ by g^* again; but we shall not do so in this lemma, because this would risk confusing it with the natural transformation $g^* : \operatorname{Base} \Longrightarrow \operatorname{Base}$.)

Let $\gamma : \mathbb{Z}_{(p)}[G] \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)$ be the $\mathbb{Z}_{(p)}$-linear map that sends each each $[g] \in G$ to $\mathbb{Z}_{(p)}[g^*] \in \operatorname{End}\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)$. (This is well-defined, since the family $([g])_{g \in G}$ is a basis of the $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}[G]$.)

space $\mathbb{F}_p^n$). In other words, $(ge_1, ge_2, \ldots, ge_n)$ must be a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$ (since the image of the basis $(e_1, e_2, \ldots, e_n)$ under g is $(ge_1, ge_2, \ldots, ge_n)$). In other words, $(ge_1, ge_2, \ldots, ge_n) \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$. Qed.

[33] *Proof.* Let $g \in G$ and $h \in G$ be such that $\tau(g) = \tau(h)$. We shall show that $g = h$.

The definition of τ yields $\tau(g) = (ge_1, ge_2, \ldots, ge_n)$ and $\tau(h) = (he_1, he_2, \ldots, he_n)$. Thus, $(ge_1, ge_2, \ldots, ge_n) = \tau(g) = \tau(h) = (he_1, he_2, \ldots, he_n)$. In other words, $ge_i = he_i$ for each $i \in \{1, 2, \ldots, n\}$. But g and h are elements of $G = \operatorname{GL}_n(\mathbb{F}_p)$. Thus, g and h are $\mathbb{F}_p$-linear maps. These two $\mathbb{F}_p$-linear maps are equal to each other on each entry of the basis $(e_1, e_2, \ldots, e_n)$ of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$ (since $ge_i = he_i$ for each $i \in \{1, 2, \ldots, n\}$). Hence, these two maps must be identical. In other words, $g = h$.

Now, forget that we fixed g and h. We thus have shown that if $g \in G$ and $h \in G$ are such that $\tau(g) = \tau(h)$, then $g = h$. In other words, the map τ is injective. Qed.

[34] *Proof.* Let $b \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$. Thus, b is a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. Hence, b is a list of $\dim\left(\mathbb{F}_p^n\right) = n$ elements of $\mathbb{F}_p^n$. Write b in the form $(b_1, b_2, \ldots, b_n)$. (This is possible, since b is a list of n elements of $\mathbb{F}_p^n$). Thus, $(b_1, b_2, \ldots, b_n)$ is a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$ (since $(b_1, b_2, \ldots, b_n) = b \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$).

Let $g : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be the unique $\mathbb{F}_p$-linear map that sends each e_i (with $i \in \{1, 2, \ldots, n\}$) to b_i. (This is well-defined, since $(e_1, e_2, \ldots, e_n)$ is a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$.) Then, $ge_i = b_i$ for each $i \in \{1, 2, \ldots, n\}$. Hence, the map g sends the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$ to the list $(b_1, b_2, \ldots, b_n)$. Therefore, the map g sends a basis of $\mathbb{F}_p^n$ to a basis of $\mathbb{F}_p^n$ (since both lists $(e_1, e_2, \ldots, e_n)$ and $(b_1, b_2, \ldots, b_n)$ are bases of $\mathbb{F}_p^n$). Thus, g is an isomorphism of $\mathbb{F}_p$-vector spaces between $\mathbb{F}_p^n$ and $\mathbb{F}_p^n$. In other words, g is an automorphism of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. Thus, $g \in \operatorname{Aut}\left(\mathbb{F}_p^n\right) = \operatorname{GL}_n(\mathbb{F}_p) = G$. The definition of τ yields $\tau(g) = (ge_1, ge_2, \ldots, ge_n) = (b_1, b_2, \ldots, b_n)$ (since $ge_i = b_i$ for each $i \in \{1, 2, \ldots, n\}$). Thus, $\tau(g) = (b_1, b_2, \ldots, b_n) = b$. Hence, $b = \tau\left(\underbrace{g}_{\in G}\right) \in \tau(G)$.

Now, forget that we fixed b. We thus have proven that $b \in \tau(G)$ for each $b \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$. In other words, $\operatorname{Base}\left(\mathbb{F}_p^n\right) \subseteq \tau(G)$. In other words, the map τ is surjective. Qed.

This map γ is a $\mathbb{Z}_{(p)}$-algebra isomorphism $\mathbb{Z}_{(p)}[G]^{\operatorname{op}} \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)$. Thus, $\operatorname{End}\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right) \cong \mathbb{Z}_{(p)}[G]^{\operatorname{op}}$ as $\mathbb{Z}_{(p)}$-algebras.

[*Proof of Lemma 9.0c.* Consider the map $\tau : G \to \operatorname{Base}\left(\mathbb{F}_p^n\right)$ defined in Lemma 9.0b. Lemma 9.0b shows that this map τ is well-defined and bijective. Hence, τ is an isomorphism of sets. Thus, it induces an isomorphism $\mathbb{Z}_{(p)}[\tau] : \mathbb{Z}_{(p)}[G] \to \mathbb{Z}_{(p)}\left[\operatorname{Base}\left(\mathbb{F}_p^n\right)\right]$ of $\mathbb{Z}_{(p)}$-modules.

Let $\mathbf{e} \in \operatorname{Base}\left(\mathbb{F}_p^n\right)$ be the basis $(e_1, e_2, \ldots, e_n)$ of $\mathbb{F}_p^n$. Then,

$$g^*\mathbf{e} = \tau(g) \qquad \text{for every } g \in G \tag{49}$$

[35].

For every $u \in \mathbb{Z}_{(p)}[G]$, the element $\gamma(u) \in \operatorname{End}\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)$ can be applied to the element $[\mathbf{e}] \in \mathbb{Z}_{(p)}\left[\operatorname{Base}\left(\mathbb{F}_p^n\right)\right] = \left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)\left(\mathbb{F}_p^n\right)$, and the result is a new element $\gamma(u) \cdot [\mathbf{e}]$ of $\left(\mathbb{Z}_{(p)}[\operatorname{Base}]\right)\left(\mathbb{F}_p^n\right) = \mathbb{Z}_{(p)}\left[\operatorname{Base}\left(\mathbb{F}_p^n\right)\right]$. We have

$$\gamma(u) \cdot [\mathbf{e}] = \left(\mathbb{Z}_{(p)}[\tau]\right)(u) \qquad \text{for every } u \in \mathbb{Z}_{(p)}[G] \tag{50}$$

[36].

[35] *Proof of (49):* Let $g \in G$. Then, $\tau(g) = (ge_1, ge_2, \ldots, ge_n)$ (by the definition of τ). Comparing this with $g^*\mathbf{e} = (ge_1, ge_2, \ldots, ge_n)$ (by Lemma 8.7a **(a)**), we obtain $g^*\mathbf{e} = \tau(g)$. This proves (49).

[36] *Proof of (50):* Let $u \in \mathbb{Z}_{(p)}[G]$. We must prove the equality (50).

Both $\gamma(u)$ and $\left(\mathbb{Z}_{(p)}[\tau]\right)(u)$ depend $\mathbb{Z}_{(p)}$-linearly on u. Hence, the equality (50) is $\mathbb{Z}_{(p)}$-linear in u. Thus, for the proof of this equality, we can WLOG assume that u belongs to the basis $([g])_{g \in G}$ of the $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}[G]$. Assume this. Hence, $u = [g]$ for some $g \in G$. Consider this g.

Now, $\gamma\left(\underbrace{u}_{=[g]}\right) = \gamma([g]) = \mathbb{Z}_{(p)}[g^*]$ (by the definition of γ). Hence, $\underbrace{\gamma(u)}_{=\mathbb{Z}_{(p)}[g^*]} \cdot [\mathbf{e}] = \left(\mathbb{Z}_{(p)}[g^*]\right)[\mathbf{e}] = \left[\underbrace{g^*\mathbf{e}}_{\substack{=\tau(g) \\ \text{(by (49))}}}\right] = [\tau(g)]$.

On the other hand, $\left(\mathbb{Z}_{(p)}[\tau]\right)\left(\underbrace{u}_{=[g]}\right) = \left(\mathbb{Z}_{(p)}[\tau]\right)([g]) = [\tau(g)]$ (by the definition of $\mathbb{Z}_{(p)}[\tau]$). Comparing this with $\gamma(u) \cdot [\mathbf{e}] = [\tau(g)]$, we obtain $\gamma(u) \cdot [\mathbf{e}] = \left(\mathbb{Z}_{(p)}[\tau]\right)(u)$. This proves (50).

The map γ is injective[37] and surjective[38]. Hence, the map γ is bijective. Also, γ is a $\mathbb{Z}_{(p)}$-linear map $\mathbb{Z}_{(p)}[G] \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\text{Base}]\right)$. In other words, γ is a $\mathbb{Z}_{(p)}$-linear map $\mathbb{Z}_{(p)}[G]^{\text{op}} \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\text{Base}]\right)$ (since $\mathbb{Z}_{(p)}[G]^{\text{op}} = \mathbb{Z}_{(p)}[G]$ as a $\mathbb{Z}_{(p)}$-module).

We have $\gamma(1) = \operatorname{id}_{\mathbb{Z}_{(p)}[\text{Base}]}$ [39]. Also, recall that any $g \in G$ and $h \in G$ satisfy

$$(gh)^* = h^* g^*. \tag{51}$$

[37] *Proof.* Let $u \in \operatorname{Ker}\gamma$. Thus, $u \in \mathbb{Z}_{(p)}[G]$ and $\gamma(u) = 0$. But (50) yields $\gamma(u) \cdot [\mathbf{e}] = \left(\mathbb{Z}_{(p)}[\tau]\right)(u)$. Hence, $\left(\mathbb{Z}_{(p)}[\tau]\right)(u) = \underbrace{\gamma(u)}_{=0} \cdot [\mathbf{e}] = 0$, so that $u \in \operatorname{Ker}\left(\mathbb{Z}_{(p)}[\tau]\right)$.

But the map $\mathbb{Z}_{(p)}[\tau]$ is an isomorphism. Thus, $\mathbb{Z}_{(p)}[\tau]$ is injective, so that $\operatorname{Ker}\left(\mathbb{Z}_{(p)}[\tau]\right) = 0$. Hence, $u \in \operatorname{Ker}\left(\mathbb{Z}_{(p)}[\tau]\right) = 0$, so that $u = 0$.

Now, forget that we fixed u. We thus have shown that $u = 0$ for each $u \in \operatorname{Ker}\gamma$. In other words, $\operatorname{Ker}\gamma = 0$. Hence, the map γ is injective (since γ is $\mathbb{Z}_{(p)}$-linear). Qed.

[38] *Proof.* Let X be the functor $\mathbb{Z}_{(p)}[\text{Base}] \in \mathcal{VA}$. Thus, $X\left(\mathbb{F}_p^n\right) = \left(\mathbb{Z}_{(p)}[\text{Base}]\right)\left(\mathbb{F}_p^n\right) = \mathbb{Z}_{(p)}\left[\text{Base}\left(\mathbb{F}_p^n\right)\right]$. Hence, $[\mathbf{e}] \in \mathbb{Z}_{(p)}\left[\text{Base}\left(\mathbb{F}_p^n\right)\right] = X\left(\mathbb{F}_p^n\right)$.

Let $\alpha \in \operatorname{End}(X)$. Then, α can be applied to the element $[\mathbf{e}]$ of $X\left(\mathbb{F}_p^n\right)$. The result is an element $\alpha[\mathbf{e}] \in X\left(\mathbb{F}_p^n\right) = \mathbb{Z}_{(p)}\left[\text{Base}\left(\mathbb{F}_p^n\right)\right]$.

The map $\mathbb{Z}_{(p)}[\tau] : \mathbb{Z}_{(p)}[G] \to \mathbb{Z}_{(p)}\left[\text{Base}\left(\mathbb{F}_p^n\right)\right]$ is an isomorphism, and thus is surjective. Hence, $\mathbb{Z}_{(p)}\left[\text{Base}\left(\mathbb{F}_p^n\right)\right] = \left(\mathbb{Z}_{(p)}[\tau]\right)\left(\mathbb{Z}_{(p)}[G]\right)$. Thus, $\alpha[\mathbf{e}] \in \mathbb{Z}_{(p)}\left[\text{Base}\left(\mathbb{F}_p^n\right)\right] = \left(\mathbb{Z}_{(p)}[\tau]\right)\left(\mathbb{Z}_{(p)}[G]\right)$. In other words, there exists an $u \in \mathbb{Z}_{(p)}[G]$ such that $\alpha[\mathbf{e}] = \left(\mathbb{Z}_{(p)}[\tau]\right)(u)$. Consider this u.

We have $\alpha \in \operatorname{End} X$ and $\gamma(u) \in \operatorname{End}\left(\underbrace{\mathbb{Z}_{(p)}[\text{Base}]}_{=X}\right) = \operatorname{End} X$. Thus, both α and $\gamma(u)$ are elements of $\operatorname{End} X$. In other words, both α and $\gamma(u)$ are natural transformations $X \Longrightarrow X$. Also, $\alpha[\mathbf{e}] = \left(\mathbb{Z}_{(p)}[\tau]\right)(u) = \gamma(u) \cdot [\mathbf{e}]$ (by (50)). Hence, Lemma 8.7b (applied to $Y = X$ and $\beta = \gamma(u)$) yields $\alpha = \gamma\left(\underbrace{u}_{\in \mathbb{Z}_{(p)}[G]}\right) \in \gamma\left(\mathbb{Z}_{(p)}[G]\right)$.

Now, forget that we fixed α. We thus have proven that $\alpha \in \gamma\left(\mathbb{Z}_{(p)}[G]\right)$ for each $\alpha \in \operatorname{End}(X)$. In other words, $\operatorname{End}(X) \subseteq \gamma\left(\mathbb{Z}_{(p)}[G]\right)$. Since $X = \mathbb{Z}_{(p)}[\text{Base}]$, this rewrites as $\operatorname{End}\left(\mathbb{Z}_{(p)}[\text{Base}]\right) \subseteq \gamma\left(\mathbb{Z}_{(p)}[G]\right)$. In other words, the map γ is surjective. Qed.

[39] *Proof.* The definition of γ yields $\gamma(1) = \mathbb{Z}_{(p)}\left[\underbrace{1^*}_{=\operatorname{id}_{\text{Base}}}\right] = \mathbb{Z}_{(p)}\left[\operatorname{id}_{\text{Base}}\right] = \operatorname{id}_{\mathbb{Z}_{(p)}[\text{Base}]}$ (by Remark 8.1f **(a)**, applied to $P = \text{Base}$). Qed.

Now, any $v \in \mathbb{Z}_{(p)}[G]$ and $u \in \mathbb{Z}_{(p)}[G]$ satisfy

$$\gamma(uv) = \gamma(v) \circ \gamma(u) \tag{52}$$

[40]. In other words, γ is multiplicative when viewed as a map $\mathbb{Z}_{(p)}[G]^{\mathrm{op}} \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\mathrm{Base}]\right)$ (because uv is the product of v and u in the $\mathbb{Z}_{(p)}$-algebra $\mathbb{Z}_{(p)}[G]^{\mathrm{op}}$). Combining this with $\gamma(1) = \mathrm{id}_{\mathbb{Z}_{(p)}[\mathrm{Base}]}$, we conclude that γ is a $\mathbb{Z}_{(p)}$-algebra homomorphism $\mathbb{Z}_{(p)}[G]^{\mathrm{op}} \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\mathrm{Base}]\right)$ (because γ is a $\mathbb{Z}_{(p)}$-linear map $\mathbb{Z}_{(p)}[G]^{\mathrm{op}} \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\mathrm{Base}]\right)$). Since γ is bijective, we thus conclude that γ is a $\mathbb{Z}_{(p)}$-algebra isomorphism $\mathbb{Z}_{(p)}[G]^{\mathrm{op}} \to \operatorname{End}\left(\mathbb{Z}_{(p)}[\mathrm{Base}]\right)$. Thus, $\operatorname{End}\left(\mathbb{Z}_{(p)}[\mathrm{Base}]\right) \cong \mathbb{Z}_{(p)}[G]^{\mathrm{op}}$ as $\mathbb{Z}_{(p)}$-algebras. This proves Lemma 9.0c. □]

- **Proposition 9.2:** Replace "The map" by "The $\mathbb{Z}_{(p)}$-linear map".
- **Proof of Proposition 9.2:** After "in the i'th space", add "(whenever $\underline{v} \in \mathrm{Base}(V)$)".

[40] *Proof of (52):* Let $v \in \mathbb{Z}_{(p)}[G]$ and $u \in \mathbb{Z}_{(p)}[G]$. We must prove the equality (52). This equality is $\mathbb{Z}_{(p)}$-linear in each of u and v (since γ is a $\mathbb{Z}_{(p)}$-linear map). Hence, for the proof of this equality, we can WLOG assume that both u and v belong to the basis $([g])_{g\in G}$ of the $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}[G]$. Assume this. Thus, $u = [g]$ and $v = [h]$ for some elements $g \in G$ and $h \in G$. Consider these g and h. We have

$$\begin{aligned}\gamma\left(\underbrace{u}_{=[g]}\underbrace{v}_{=[h]}\right) &= \gamma\left(\underbrace{[g][h]}_{=[gh]}\right) = \gamma([gh]) \\ &= \mathbb{Z}_{(p)}\left[\underbrace{(gh)^*}_{\substack{=h^*g^* \\ \text{(by (51))}}}\right] \qquad \text{(by the definition of } \gamma) \\ &= \mathbb{Z}_{(p)}[h^*g^*].\end{aligned}$$

Comparing this with

$$\begin{aligned}\gamma\left(\underbrace{v}_{=[h]}\right) \circ \gamma\left(\underbrace{u}_{=[g]}\right) &= \underbrace{\gamma([h])}_{\substack{=\mathbb{Z}_{(p)}[h^*] \\ \text{(by the definition of } \gamma)}} \circ \underbrace{\gamma([g])}_{\substack{=\mathbb{Z}_{(p)}[g^*] \\ \text{(by the definition of } \gamma)}} = \mathbb{Z}_{(p)}[h^*] \circ \mathbb{Z}_{(p)}[g^*] \\ &= \mathbb{Z}_{(p)}[h^* \circ g^*] \\ &\qquad \left(\begin{array}{c}\text{by Remark 8.1f } \textbf{(b)}\text{, applied to } P = \mathrm{Base}, Q = \mathrm{Base}, R = \mathrm{Base}, \\ \alpha_1 = g^* \text{ and } \alpha_2 = h^*\end{array}\right) \\ &= \mathbb{Z}_{(p)}[h^*g^*],\end{aligned}$$

we obtain $\gamma(uv) = \gamma(v) \circ \gamma(u)$. This proves (52).

- **Proof of Proposition 9.2:** Replace "a reduced word $s_{i_1} \cdots s_{i_r}$ for Σ" by "a reduced word $s_{i_1} \cdots s_{i_r}$ for σ".

- **Proof of Proposition 9.2:** Replace every appearance of "$\widehat{\xi}$" in this proof by "ξ".

- **Proof of Proposition 9.2:** After "$(-1)^r \mu = \widehat{\xi}(T_\sigma)\mu$", add "(since $(-1)^r = \operatorname{sgn}(\sigma) = \xi(T_\sigma)$)".

- **Proof of Proposition 9.2:** After "It follows that $\xi(ab)\mu = \xi(a)\xi(b)\mu$", add "(since $ab\mu = \xi(ab)\mu$ and thus $\xi(ab)\mu = a \underbrace{b\mu}_{=\xi(b)\mu} = a\xi(b)\mu = \xi(b) \underbrace{a\mu}_{=\xi(a)\mu} = \xi(b)\xi(a)\mu = \xi(a)\xi(b)\mu$)".

- **Proof of Proposition 9.2:** You write: "(This could also have been deduced from Proposition 8.11.)". A few details about this deduction would be useful. Namely, here is how it works:

  [*Proof of the fact that ξ is a ring map:* Clearly, we have

  $$(-1)^2 = p + (p-1)(-1),$$
  $$(-1)(-1)(-1) = (-1)(-1)(-1),$$
  $$(-1)(-1) = (-1)(-1).$$

  Thus, the relations in Proposition 8.11 remain valid if each T_k in them is replaced by -1. Hence, Proposition 8.11 shows that there exists a unique $\mathbb{Z}_{(p)}$-algebra homomorphism $\eta : \mathcal{H} \to \mathbb{Z}_{(p)}$ that sends each T_k to -1. Consider this η. Now, if $\sigma \in \Sigma_n$, then we can fix any reduced word $s_{i_1}s_{i_2}\cdots s_{i_r}$ for σ, and then we find

  $$\begin{aligned}\eta\left(\underbrace{T_\sigma}_{\substack{=T_{i_1}T_{i_2}\cdots T_{i_r}\\ \text{(by Corollary 8.10)}}}\right) &= \eta\left(T_{i_1}T_{i_2}\cdots T_{i_r}\right) = \eta\left(T_{i_1}\right)\eta\left(T_{i_2}\right)\cdots\eta\left(T_{i_r}\right)\\ &\qquad\left(\text{since } \eta \text{ is a } \mathbb{Z}_{(p)}\text{-algebra homomorphism}\right)\\ &= \underbrace{(-1)(-1)\cdots(-1)}_{r \text{ times}}\\ &\qquad\left(\text{since } \eta\left(T_{i_p}\right) = -1 \text{ for each } p \text{ (by the definition of } \eta)\right)\\ &= (-1)^r = \operatorname{sgn}(\sigma)\\ &\qquad\left(\text{since } \sigma = s_{i_1}s_{i_2}\cdots s_{i_r} \text{ and thus } \operatorname{sgn}(\sigma) = (-1)^r\right)\\ &= \xi(T_\sigma).\end{aligned}$$

Thus, we have found that $\eta\left(T_\sigma\right) = \xi\left(T_\sigma\right)$ for each $\sigma \in \Sigma_n$. In other words, the maps η and ξ are equal to each other on the basis $\left(T_\sigma\right)_{\sigma\in\Sigma_n}$ of the $\mathbb{Z}_{(p)}$-module $\mathcal{H}$. Hence, these two maps η and ξ must be identical (since they are both $\mathbb{Z}_{(p)}$-linear). In other words, $\xi = \eta$. Thus, ξ is a ring homomorphism (since η is a ring homomorphism). $\square$]

- **Proof of Proposition 9.3:** This proof has several flaws. In particular, the expression "$\left\langle \sigma^* \pi^t \left[\underline{U}\right], \left[\underline{W}\right]\right\rangle$" makes no sense, and the formula $\pi\sigma^*\pi^t = \left|B/U\right| p^{l\left(\sigma^{-1}\rho\right)} T_\sigma$ is false. Let me show a correct (and more detailed) proof:

  [*Proof of Proposition 9.3.* Fix $\sigma \in \Sigma_n$. Let $V \in \mathcal{V}$, and let $\underline{W} \in \operatorname{Flag}\left(V\right)$. For each $\underline{U} \in \operatorname{Flag}(V)$, we have

$$\left\langle \pi\sigma^* \pi^t \left[\underline{W}\right], \left[\underline{U}\right] \right\rangle$$

$$= \left\langle \pi\sigma^* \sum_{\substack{\mathbf{w}\in\operatorname{Base}(V);\\ \pi(\mathbf{w})=\underline{W}}} \left[\mathbf{w}\right], \left[\underline{U}\right] \right\rangle \qquad \left(\text{since } \pi^t\left[\underline{W}\right] = \sum_{\substack{\mathbf{w}\in\operatorname{Base}(V);\\ \pi(\mathbf{w})=\underline{W}}} \left[\mathbf{w}\right]\right)$$

$$= \sum_{\substack{\mathbf{w}\in\operatorname{Base}(V);\\ \pi(\mathbf{w})=\underline{W}}} \left\langle \underbrace{\pi\sigma^*\left[\mathbf{w}\right]}_{=\left[\pi(\sigma^*\mathbf{w})\right]}, \left[\underline{U}\right] \right\rangle = \sum_{\substack{\mathbf{w}\in\operatorname{Base}(V);\\ \pi(\mathbf{w})=\underline{W}}} \underbrace{\left\langle \left[\pi\left(\sigma^*\mathbf{w}\right)\right], \left[\underline{U}\right] \right\rangle}_{=\delta_{\pi(\sigma^*\mathbf{w}),\underline{U}}} = \sum_{\substack{\mathbf{w}\in\operatorname{Base}(V);\\ \pi(\mathbf{w})=\underline{W}}} \delta_{\pi(\sigma^*\mathbf{w}),\underline{U}}$$

$$= \left(\text{the number of all } \mathbf{w} \in \operatorname{Base}(V) \text{ such that } \pi(\mathbf{w}) = \underline{W} \text{ and } \pi\left(\sigma^*\mathbf{w}\right) = \underline{U}\right)$$

$$= \left(\text{the number of all } \left(v_1, v_2, \ldots, v_n\right) \in \operatorname{Base}(V) \text{ such}\right.$$

$$\left.\text{that } \pi\left(v_1, v_2, \ldots, v_n\right) = \underline{W} \text{ and } \pi\left(\underbrace{\sigma^*\left(v_1, v_2, \ldots, v_n\right)}_{=\left(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}\right)}\right) = \underline{U}\right)$$

$$\left(\begin{array}{c}\text{here, we have substituted } \left(v_1, v_2, \ldots, v_n\right) \text{ for the index } \mathbf{w},\\ \text{since each element of } \operatorname{Base}(V) \text{ is an } n\text{-tuple}\end{array}\right)$$

$$= \left(\text{the number of all } \left(v_1, v_2, \ldots, v_n\right) \in \operatorname{Base}(V) \text{ such}\right.$$

$$\left.\text{that } \underbrace{\pi\left(v_1, v_2, \ldots, v_n\right) = \underline{W}}_{\iff \left(W_i = \operatorname{span}\{v_1, v_2, \ldots, v_i\} \text{ for all } i\right)} \text{ and } \underbrace{\pi\left(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}\right) = \underline{U}}_{\iff \left(U_i = \operatorname{span}\left\{v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(i)}\right\} \text{ for all } i\right)}\right)$$

$$= \left(\text{the number of all } \left(v_1, v_2, \ldots, v_n\right) \in \operatorname{Base}(V) \text{ such}\right.$$

$$\text{that } \left(W_i = \operatorname{span}\left\{v_1, v_2, \ldots, v_i\right\} \text{ for all } i\right)$$

$$\left.\text{and } \left(U_i = \operatorname{span}\left\{v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(i)}\right\} \text{ for all } i\right)\right)$$

$$= \left(\text{the number of all bases } \left(v_1, v_2, \ldots, v_n\right) \text{ of } V \text{ such that for all } i\right.$$

$$\left.\text{we have } U_i = \operatorname{span}\left\{v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(i)}\right\} \text{ and } W_i = \operatorname{span}\left\{v_1, v_2, \ldots, v_i\right\}\right)$$

$$= \begin{cases} (p-1)^n \, p^{l\left(\sigma^{-1}\rho\right)}, & \text{if } \delta\left(\left[\underline{U}\right], \left[\underline{W}\right]\right) = \sigma; \\ 0, & \text{otherwise} \end{cases}$$

(by Corollary 5.5). Hence,

$$\begin{aligned}
\pi\sigma^*\pi^t\left[\underline{W}\right] &= \sum_{\underline{U}\in\operatorname{Flag}(V)} \begin{cases} (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)}, & \text{if } \delta\left(\left[\underline{U}\right],\left[\underline{W}\right]\right)=\sigma; \\ 0, & \text{otherwise} \end{cases} \left[\underline{U}\right] \\
&= \sum_{\substack{\underline{U}\in\operatorname{Flag}(V);\\ \delta([\underline{U}],[\underline{W}])=\sigma}} (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} \left[\underline{U}\right] \\
&= (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} \underbrace{\sum_{\substack{\underline{U}\in\operatorname{Flag}(V);\\ \delta([\underline{U}],[\underline{W}])=\sigma}}}_{\substack{=\sum_{\substack{\underline{U}\in\operatorname{Flag}(V);\\ \delta([\underline{W}],[\underline{U}])=\sigma^{-1}}} \\ \text{(because for each } \underline{U}\in\operatorname{Flag}(V)\text{,} \\ \text{the condition } (\delta([\underline{U}],[\underline{W}])=\sigma) \text{ is} \\ \text{equivalent to } \left(\delta([\underline{W}],[\underline{U}])=\sigma^{-1}\right) \\ \text{(since } \delta([\underline{W}],[\underline{U}])=\delta([\underline{U}],[\underline{W}])^{-1}\text{))}}} \left[\underline{U}\right] \\
&= (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} \sum_{\substack{\underline{U}\in\operatorname{Flag}(V);\\ \delta([\underline{W}],[\underline{U}])=\sigma^{-1}}} \left[\underline{U}\right].
\end{aligned}$$

Comparing this with

$$(p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} \underbrace{T_{\sigma^{-1}}\left[\underline{W}\right]}_{=\sum_{\substack{\underline{U}\in\operatorname{Flag}(V);\\ \delta([\underline{W}],[\underline{U}])=\sigma^{-1}}}\left[\underline{U}\right]} = (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} \sum_{\substack{\underline{U}\in\operatorname{Flag}(V);\\ \delta([\underline{W}],[\underline{U}])=\sigma^{-1}}} \left[\underline{U}\right],$$

we obtain $\pi\sigma^*\pi^t\left[\underline{W}\right] = (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} T_{\sigma^{-1}}\left[\underline{W}\right]$.

Now, forget that we fixed $\underline{W}$. We thus have shown that $\pi\sigma^*\pi^t\left[\underline{W}\right] = (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} T_{\sigma^{-1}}\left[\underline{W}\right]$ for each $\underline{W}\in\operatorname{Flag}(V)$. In other words, the two maps $\pi\sigma^*\pi^t$ and $(p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} T_{\sigma^{-1}}$ are equal to each other on the basis $\left(\left[\underline{W}\right]\right)_{W\in\operatorname{Flag}(V)}$ of the $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}\left[\operatorname{Flag}(V)\right]$. Since these two maps are $\mathbb{Z}_{(p)}$-linear, we can thus conclude that they are identical. In other words, $\pi\sigma^*\pi^t = (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} T_{\sigma^{-1}}$.

Now, forget that we fixed σ. We thus have shown that

$$\pi\sigma^*\pi^t = (p-1)^n\, p^{l\left(\sigma^{-1}\rho\right)} T_{\sigma^{-1}} \qquad \text{for each } \sigma\in\Sigma_n. \tag{53}$$

On the other hand, every $\sigma\in\Sigma_n$ satisfies

$$l(\sigma\rho) = l\left(\sigma^{-1}\rho\right) \tag{54}$$

[41].

Now,

$$\begin{aligned}
e &= \pi\omega\pi^{t} \\
&= \pi\left|G/U\right|^{-1}\sum_{\sigma\in\Sigma_n}\operatorname{sgn}(\sigma)\,\sigma^{*}\pi^{t} \qquad \left(\text{since } \omega = \left|G/U\right|^{-1}\sum_{\sigma\in\Sigma_n}\operatorname{sgn}(\sigma)\,\sigma^{*}\right) \\
&= \left|G/U\right|^{-1}\sum_{\sigma\in\Sigma_n}\underbrace{\operatorname{sgn}(\sigma)}_{=\operatorname{sgn}\left(\sigma^{-1}\right)}\qquad\underbrace{\pi\sigma^{*}\pi^{t}}_{\substack{=(p-1)^{n}p^{l\left(\sigma^{-1}\rho\right)}T_{\sigma^{-1}}\\ \text{(by (53))}}} \\
&= \left|G/U\right|^{-1}\sum_{\sigma\in\Sigma_n}\operatorname{sgn}\left(\sigma^{-1}\right)(p-1)^{n}p^{l\left(\sigma^{-1}\rho\right)}T_{\sigma^{-1}} \\
&= \left|G/U\right|^{-1}\underbrace{(p-1)^{n}}_{\substack{=\dfrac{|G/U|}{|G/B|}\\ \text{(by (48))}}}\quad\underbrace{\sum_{\sigma\in\Sigma_n}\operatorname{sgn}\left(\sigma^{-1}\right)p^{l\left(\sigma^{-1}\rho\right)}T_{\sigma^{-1}}}_{\substack{=\sum\limits_{\sigma\in\Sigma_n}\operatorname{sgn}(\sigma)p^{l(\sigma\rho)}T_{\sigma}\\ \text{(here, we have substituted } \sigma \text{ for } \sigma^{-1}\\ \text{in the sum, since the map } \Sigma_n\to\Sigma_n,\ \sigma\mapsto\sigma^{-1}\\ \text{is a bijection)}}} \\
&= \underbrace{\left|G/U\right|^{-1}\frac{|G/U|}{|G/B|}}_{=|G/B|^{-1}}\sum_{\sigma\in\Sigma_n}\operatorname{sgn}(\sigma)\qquad\underbrace{p^{l(\sigma\rho)}}_{\substack{=p^{l\left(\sigma^{-1}\rho\right)}\\ \text{(since } l(\sigma\rho)=l\left(\sigma^{-1}\rho\right)\\ \text{(by (54)))}}}\qquad T_{\sigma} \\
&= \left|G/B\right|^{-1}\sum_{\sigma\in\Sigma_n}\operatorname{sgn}(\sigma)\,p^{l\left(\sigma^{-1}\rho\right)}T_{\sigma}.
\end{aligned}$$

This proves Proposition 9.3. □]

- **Proof of Proposition 9.4:** Replace "First, we have" by "Proposition 9.3 yields".
- **Proof of Proposition 9.4:** The first chain of equalities in the proof needs some justification (e.g., why do we have $\sum\limits_{\sigma} p^{l\left(\sigma^{-1}\rho\right)} = \left|\coprod_{\sigma} X\left(\sigma^{-1}\rho\right)\right|$, and why is $|G/B|^{-1}\left|\coprod_{\tau} X(\tau)\right| = 1$?). I would actually suggest the following alternative argument:

  Proposition 8.1b **(b)** shows that there is a natural isomorphism $G/B \to \operatorname{Flag}\left(\mathbb{F}_p^n\right)$ of G-sets. Hence, $|G/B| = \left|\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right|$. But every $V \in \mathcal{V}$ satisfies $|\operatorname{Flag}(V)| = \sum\limits_{\sigma\in\Sigma_n} p^{l(\sigma)}$ (by Lemma 8.0a **(b)**). Applying this to $V = \mathbb{F}_p^n$,

[41] *Proof of (54):* Let $\sigma \in \Sigma_n$. Then, Corollary 2.19 **(a)** yields $l\left(\sigma^{-1}\rho\right) = n(n-1)/2 - l(\sigma)$. But Corollary 2.19 **(b)** yields $l(\sigma\rho) = n(n-1)/2 - l(\sigma)$. Thus, $l\left(\sigma^{-1}\rho\right) = n(n-1)/2 - l(\sigma) = l(\sigma\rho)$. This proves (54).

we obtain $\left|\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right| = \sum_{\sigma\in\Sigma_n} p^{l(\sigma)}$. The map $\Sigma_n \to \Sigma_n$, $\sigma \mapsto \sigma^{-1}\rho$ is a bijection (since Σ_n is a group). Hence, we can substitute $\sigma^{-1}\rho$ for σ in the sum $\sum_{\sigma\in\Sigma_n} p^{l(\sigma)}$. We thus obtain $\sum_{\sigma\in\Sigma_n} p^{l(\sigma)} = \sum_{\sigma\in\Sigma_n} p^{l\left(\sigma^{-1}\rho\right)}$. Hence,

$$|G/B| = \left|\operatorname{Flag}\left(\mathbb{F}_p^n\right)\right| = \sum_{\sigma\in\Sigma_n} p^{l(\sigma)} = \sum_{\sigma\in\Sigma_n} p^{l\left(\sigma^{-1}\rho\right)}. \tag{55}$$

Now, Proposition 9.3 yields

$$e = |G/B|^{-1} \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma)\, p^{l\left(\sigma^{-1}\rho\right)} T_\sigma.$$

Applying the map ξ to both sides of this equality, we find

$$\begin{aligned}
\xi(e) &= \xi\left(|G/B|^{-1} \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma)\, p^{l\left(\sigma^{-1}\rho\right)} T_\sigma\right) \\
&= |G/B|^{-1} \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma)\, p^{l\left(\sigma^{-1}\rho\right)} \qquad \underbrace{\xi(T_\sigma)}_{\substack{=\operatorname{sgn}(\sigma) \\ \text{(by the definition of } \xi)}} \\
&\qquad \left(\text{since the map } \xi \text{ is } \mathbb{Z}_{(p)}\text{-linear}\right) \\
&= |G/B|^{-1} \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma)\, p^{l\left(\sigma^{-1}\rho\right)} \operatorname{sgn}(\sigma) = |G/B|^{-1} \sum_{\sigma\in\Sigma_n} \underbrace{(\operatorname{sgn}(\sigma))^2}_{=1} p^{l\left(\sigma^{-1}\rho\right)} \\
&= |G/B|^{-1} \sum_{\sigma\in\Sigma_n} \underbrace{(\operatorname{sgn}(\sigma))^2}_{=1} p^{l\left(\sigma^{-1}\rho\right)} \\
&= |G/B|^{-1} \underbrace{\sum_{\sigma\in\Sigma_n} p^{l\left(\sigma^{-1}\rho\right)}}_{\substack{=|G/B| \\ \text{(by (55))}}} = |G/B|^{-1}\,|G/B| = 1.
\end{aligned}$$

- **Proof of Proposition 9.4:** Replace "$\widehat{\xi}(e)\,\mu$" by "$\xi(e)\,\mu$".
- **Proof of Proposition 9.4:** I would replace "As $e_{\mathrm{St}} = \pi^t\mu$ we see that $\pi^t(M_{\mathrm{St}}) = \operatorname{image}\left(\pi^t\mu\right) = M'_{\mathrm{St}}$" by the more detailed argument "As $M_{\mathrm{St}} = \operatorname{image}(\mu)$, we see that $\pi^t(M_{\mathrm{St}}) = \operatorname{image}\left(\underbrace{\pi^t\mu}_{=e_{\mathrm{St}}}\right) = \operatorname{image}(e_{\mathrm{St}}) = M'_{\mathrm{St}}$".
- **Proof of Proposition 9.4:** I would replace "Thus, if we let β be the restriction of π^t to M_{St}, we see that β gives an epimorphism $M_{\mathrm{St}} \to M'_{\mathrm{St}}$" by "Thus, π^t restricts to an epimorphism $\beta : M_{\mathrm{St}} \to M'_{\mathrm{St}}$". (This is both shorter and also explains unambiguously what the codomain of β is.)

- **Proof of Proposition 9.4:** After "As the map $\mu\pi^t = e$ restricts to 1 on M_{St}", I would add "(because e is idempotent, and M_{St} is its image)".

- **Proof of Proposition 9.5:** I don't understand the first sentence of this proof: Why does the Yoneda isomorphism exist? (I only know Yoneda isomorphisms for functors to Set, not for functors to $\mathcal{A}$; but even if I were to write down the obvious generalization, there remains the question why $\mathbb{Z}_{(p)}$ [Base] is a Hom-functor.) And supposing that the Yoneda isomorphism exists, why does it yield that $\mathbb{Z}_{(p)}$ [Base] is projective?

  What I do see is that the functor $\mathbb{Z}_{(p)}$ [Base] is "pointwise projective", in the sense that the image of each object of $\mathcal{V}$ under this functor is a projective $\mathbb{Z}_{(p)}$-module. (This is obvious, because the image of an object $V \in \mathcal{V}$ under the functor $\mathbb{Z}_{(p)}$ [Base] is the $\mathbb{Z}_{(p)}$-module $\left(\mathbb{Z}_{(p)}\left[\mathrm{Base}\right]\right)(V) = \mathbb{Z}_{(p)}\left[\mathrm{Base}\left(V\right)\right]$, which is free and therefore projective.) Therefore, the functor M_{St} is "pointwise projective" as well (since, as youpoint out, $M_{\mathrm{St}}(V)$ is a direct summand in $\left(\mathbb{Z}_{(p)}\left[\mathrm{Base}\right]\right)(V)$).

- **Proof of Proposition 9.5:** After "the image of e_{St}, which is a summand in $\mathbb{Z}_{(p)}$ [Base]", I suggest adding "(since e_{St} is idempotent)".

- **Proof of Proposition 9.5:** After "M_{St} is also the image of a self-adjoint idempotent on $\mathbb{Z}_{(p)}$ [Flag]", I suggest adding "(namely, of e)".

- **Proof of Proposition 9.5:** After "the rank of M_{St} is the trace of e", I suggest adding "(since M_{St} is the image of the idempotent endomorphism e)".

- **Proof of Proposition 9.5:** After "the map T_σ is the identity", I would add "(by Corollary 4.6)".

- **Proof of Proposition 9.5:** I would suggest replacing "with trace $|\mathrm{Flag}| = |G/B|$" by "with trace

$$\begin{aligned} \left|\mathrm{Flag}\left(V\right)\right| &= \left|\mathrm{Flag}\left(\mathbb{F}_p^n\right)\right| && \left(\text{since } V \cong \mathbb{F}_p^n \text{ as } \mathbb{F}_p\text{-vector spaces}\right) \\ &= \left|G/B\right| && \left(\begin{array}{c}\text{since Proposition 8.1b } \textbf{(b)} \text{ shows that there is a} \\ \text{natural isomorphism } G/B \to \mathrm{Flag}\left(\mathbb{F}_p^n\right) \text{ of } G\text{-sets}\end{array}\right) \end{aligned}$$

  ".

- **Proof of Proposition 9.5:** I suggest replacing "Next, note that $\mathbb{Z}_{(p)}$ [Flag] $= M_{\mathrm{St}} \oplus N$" by "But e is idempotent; thus, $\mathbb{Z}_{(p)}\left[\mathrm{Flag}\right] = \underbrace{\mathrm{image}\left(e\right)}_{=M_{\mathrm{St}}} \oplus \underbrace{\mathrm{image}\left(1-e\right)}_{=N} = M_{\mathrm{St}} \oplus N$".