November 7, 2018

Algebra II, Sheet 1

Remarks and Solutions

Jendrik Stelzner

Exercise 3.

(a)

Remark 1. The proven isomorphism $k[G] \cong k[x]/(x^{p^r})$ depends heavily on the fact that $\operatorname{char}(k) = p$: The isomorphism

$$k[G] \cong k[\mathbb{Z}/p^r] \cong k[x](x^{p^r} - 1)$$

holds for every field k, while the further isomorphism

$$k[x]/(x^{p^r} - 1) \cong k[x](x^{p^r})$$

uses that $\operatorname{char}(k) = p$ to transform

$$x^{p^r} - 1 = x^{p^r} - 1^{p^r} = (x-1)^{p^r}.$$

If for example $k = \mathbb{C}$ instead, then

$$x^{p^r} - 1 = (x - \omega_1) \cdots (x - \omega_{p^r})$$

for the p^r-th roots of unity $\omega_1, \dots, \omega_{p^r} \in \mathbb{C}$ given by $\omega_j = e^{2\pi i j / p^r}$. These roots of unity $\omega_1, \dots, \omega_{p^r}$ are pairwise distinct and so it follows from the chinese reminder theorem that

$$\begin{aligned}\mathbb{C}[G] \cong \mathbb{C}[x]/(x^{p^r} - 1) &\cong \mathbb{C}[x]((x - \omega_1) \cdots (x - \omega_{p^r})) \\ &\cong \prod_{j=1}^{p^r} \mathbb{C}[x]/(x - \omega_j) \cong \prod_{j=1}^{p^r} \mathbb{C} = \mathbb{C}^{\times p^r}.\end{aligned}$$

(b)

We have seen in the tutorial how one can use the first part of the exercise to classify the finite-dimensional indecomposable, resp. irreducible representations of G over k. But

one can also classify these representations by instead using linear algebra, effectively ignoring the first part of the exercise:

Let V be a representation of G over k. Then the cyclic generator $g \in G$ acts on V via an endomorphisms

$$\varphi\colon V \to V\,, \quad v \mapsto g.v\,.$$

It follows from $g^{p^r} = 1$ that $\varphi^{p^r} = \mathrm{id}$, and hence

$$0 = \varphi^{p^r} - \mathrm{id} = \varphi^{p^r} - \mathrm{id}^{p^r} = (\varphi - \mathrm{id})^{p^r} = p(\varphi)$$

for the polynomial $p(t) \coloneqq (t-1)^{p^r} \in k[t]$, where we used that $\mathrm{char}(k) = p$. If the vector space V is finite-dimensional[1] then this shows that φ is triangularizable with 1 as its only eigenvalue. We can therefore consider its Jordan normal form, which is with respect to a suitable basis $B = (b_1, \ldots, b_n)$ of V given by a block diagonal matrix

$$J = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{bmatrix}$$

with (unipotent) Jordan blocks

$$J_i = \begin{bmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{bmatrix} \in \mathrm{M}_{n_i}(k)\,.$$

The decomposition of the matrix J as a block diagonal matrix corresponds to a decomposition of the vector space V into φ-invariant subspaces. More precisely, we set

$$\begin{aligned} U_1 &\coloneqq \langle b_1, \ldots, b_{n_1} \rangle_k\,, \\ U_2 &\coloneqq \langle b_{n_1+1}, \ldots, b_{n_1+n_2} \rangle_k\,, \\ &\vdots \\ U_s &\coloneqq \langle b_{n_1+\cdots+n_{s-1}+1}, \ldots, b_n \rangle_k\,. \end{aligned}$$

Then $V = U_1 \oplus \cdots \oplus U_s$ is a decomposition into φ-invariant subspaces, and hence a decomposition into subrepresentations.

For V to be indecomposable we therefore need that $s = 1$. We have thus shown that for every finite-dimensional indecomposable representation of G over k there exists a basis of V with respect to which the action of the cylic generator $g \in G$ is given by the matrix

$$U_n \coloneqq \begin{bmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{bmatrix} \in \mathrm{M}_n(k)\,,$$

[1] We don't actually need this assumption.

where $n = \dim(V)$. This observation results in a classification of all finite-dimensional indecomposable, resp. irreducible representations of G over k:

Proposition 2.

1) For every $n = 1, \dots, p^r$ there exists a unique linear action of G on k^n for which the cyclic generator $g \in G$ acts by multiplication with the matrix U_n.

We denote the resulting n-dimensional representation of G by V_n.

2) The subrepresentations of V_n are precisely $W_i \coloneqq \langle e_1, \dots, e_i \rangle_k$ for $i = 0, \dots, n$.

3) The representation V_n is for every $n = 1, \dots, p^r$ indecomposable. The representation V_n is irreducible if and only if $n = 1$.

4) The indecomposable representations $V_1, \dots, V_{p^r}$ are a set of representatives for the isomorphism classes of finite-dimensional indecomposable representations of G over k. The representation V_1 is up to isomorphism the only irreducible representation of G over k.

Proof.

1) We need to show that there exists a unique group homomorphism $\rho\colon G \to \mathrm{GL}_n(k)$ with $\varphi(g) = U_n$. The uniqueness follows from G being generated by g. For the existence we only need to check that $U_n^{p^r} = \mathbb{1}$. This holds, because if we write

$$U_n = \mathbb{1} + N_n$$

with

$$N_n = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in \mathrm{M}_n(k)$$

then the matrices $\mathbb{1}$ and N_n commute, and it follows that

$$U_n^{p^r} = (\mathbb{1} + N_n)^{p^r} = \mathbb{1}^{p^r} + N_n^{p^r} = \mathbb{1} + 0 = \mathbb{1}\,.$$

2) We abbreviate $N \coloneqq N_n$. The subrepresentations of V_n are precisely the U_n-invariant subspaces, which are by the decomposition $U_n = \mathbb{1} + N$ precisely the N-invariant subspaces (because every subspace is $\mathbb{1}$-invariant). The subspaces W_i are N-invariant because $Ne_j = e_{j-1}$.

We need to show that every N-invariant subspaces $W \subseteq V$ is of the form $W = W_i$ for some i. It sufficies to show that for every $x \in V$ the generated N-invariant subspace

$$\langle x \rangle = \langle x, Nx, N^2x, \dots \rangle_k$$

is of the form W_i for some i; it then follows that $W = \sum_{x \in W} \langle x \rangle$ is again of the form W_i for some i, because every sum of W_j's is again a W_i.

If

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_i \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

with $x_i \neq 0$ then $N^j x \subseteq W_i$ for every $j \geq 0$ and hence $\langle x \rangle \subseteq W_i$. We have on the other hand that

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_{i-1} \\ x_i \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \qquad Nx = \begin{bmatrix} x_2 \\ \vdots \\ x_i \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \qquad \ldots, \qquad N^{i-1}x = \begin{bmatrix} x_i \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

are linearly independent, and hence

$$\dim\langle x \rangle \geq i = \dim W_i \,.$$

Together this shows that $\langle x \rangle = W_i$.

3) This follows from part 2).

4) We have seen previously that every finite-dimensional indepecomposable representation of G over k is isomorphic to some V_n. The representations $V_1, \ldots, V_{p^r}$ are pairwise non-isomorphic because they have different dimensions. □

Exercise 4.

Before we begin with the exercise itself, we recall some group theory:

Let G be a group and let $H \subseteq G$ be a subgroup. Then G acts on the set of left cosets $X \coloneqq G/H = \{gH \mid g \in G\}$ via left multiplication, i.e. via

$$g \cdot (g'H) = (gg')H$$

for all $g \in G$ and $g'H \in X$. This action of G on X is transitive and the stabilizer of $H = 1H \in X$ is given by

$$\mathrm{Stab}_G(H) = \{g \in G \mid gH = H\} \underset{1 \in H}{=\!=} \{g \in G \mid g \in H\} = H \,.$$

Moreover, the map

$$G \to X \,, \quad g \mapsto gx$$

is G-equivariant for every $x \in X$. The Orbit-Stabilizer theorem asserts that every transitive G-set looks like this:

Theorem 3 (Orbit-Stabilizer theorem)**.** Let G be a group and let X be a G-set. Then for every $x \in X$ the map

$$G/G_x \to G.x\,, \quad gG_x \mapsto g.x$$

is both bijective and G-equivariant, i.e. it is an isomorphism of G-sets.

Remark 4. The Orbit-Stabilizer theorem is a version of the first isomorphism theorem for G-sets.

The Orbit-Stabilizer theorem asserts that if we want to construct a bijection

$$G/H \to X$$

for some group G, subgroup $H \subseteq G$ and set X, then we need to construct a transitive action of G on X such that H is the stabilizer of some point $x \in X$.

Example 5 (Topology)**.** The group $\mathrm{SO}(n+1)$ acts on the sphere $\mathbb{S}^n$ by rotation. This action is transitive, and the stabilizer of $e_1 \in \mathbb{S}^n$ is given by $\mathrm{SO}(n)$, when regarded as a subgroup of $\mathrm{SO}(n+1)$ via the embedding

$$A \mapsto \begin{bmatrix} 1 & 0 \\ 0 & A \end{bmatrix}.$$

It hence follows from the Orbit-Stabilizer theorem that

$$\mathrm{SO}(n+1)/\mathrm{SO}(n) \xrightarrow{\cong} \mathbb{S}^n\,, \quad A\,\mathrm{SO}(n) \mapsto Ae_1$$

is an isomorphism of $\mathrm{SO}(n+1)$-sets. (It follows from $\mathrm{SO}(n+1)$ being compact and $\mathbb{S}^n$ being Hausdorff that this continuous bijection is already a homeomorphism.)

(a)

We consider the action of $G = \mathrm{GL}_n(k)$ on the set X of flags in k^n via

$$g.(F_i)_{i=0}^n = (gF_i)_{i=0}^n\,,$$

where for every subspace $U \subseteq k^n$ and every $g \in G$ the subspace $gU \subseteq k^n$ is given by

$$gU = \{gu \mid u \in U\}\,.$$

This does indeed define an action of G on X because

$$\mathbb{1}.(F_i)_{i=0}^n = (\mathbb{1}F_i)_{i=0}^n = (F_i)_{i=0}^n$$

for every $(F_i)_{i=0}^n \in X$, and

$$g.(h.(F_i)_{i=0}^n) = g.(hF_i)_{i=0}^n = (ghF_i)_{i=0}^n = (gh).(F_i)_{i=0}^n$$

for all $g, h \in G$ and all $(F_i)_{i=0}^n \in X$.

We now consider the standard flag $S = (S_i)_{i=0}^n \in X$ given by

$$S_i \coloneqq \langle e_1, \dots, e_i \rangle_k$$

for all $i = 0, \dots, n$. We have for every matrix $g \in G$ that

$$\begin{aligned}
& g \in \mathrm{Stab}_G(S) \\
\iff\ & g.S = S \\
\iff\ & g.\langle e_1, \dots, e_i \rangle_k = \langle e_1, \dots, e_i \rangle_k \text{ for every } i = 0, \dots, n \\
\iff\ & g.\langle e_1, \dots, e_i \rangle_k \subseteq \langle e_1, \dots, e_i \rangle_k \text{ for every } i = 0, \dots, n \\
\iff\ & g.e_j \in \langle e_1, \dots, e_i \rangle_k \text{ for all } 1 \leq j \leq i \leq n \\
\iff\ & \text{the } j\text{-th column of } g \text{ is contained in } \langle e_1, \dots, e_i \rangle_k \text{ for all } 1 \leq j \leq i \leq n \\
\iff\ & g \text{ is of the form } \begin{bmatrix} * & \cdots & * \\ & \ddots & \vdots \\ & & * \end{bmatrix} \\
\iff\ & g \text{ is upper triangular}\,,
\end{aligned}$$

which shows that

$$\mathrm{Stab}_G(S) = B\,.$$

We have $G.S = X$: There exists by extension of bases for every flag $(F_i)_{i=0}^n \in X$ a basis $b_1, \dots, b_n$ of k^n such that $b_1, \dots, b_i$ is for every $i = 0, \dots, n$ a basis of F_i. The matrix $g = (b_1, \dots, b_n)$ (i.e. the matrix whose columns are the basis vectors $b_1, \dots, b_n$) is then invertible with

$$g.S_i = g.\langle e_1, \dots, e_i \rangle_k = \langle g.e_1, \dots, g.e_i \rangle_k = \langle b_1, \dots, b_i \rangle_k = F_i$$

for every $i = 0, \dots, n$, and hence $g.S = F$.

It now follows from the Orbit-Stabilizer theorem that we have a bijection

$$\varphi \colon G/B \to X\,, \quad gB \mapsto g.S$$

which is also G-equivariant. The bijection φ assigns to each matrix $g \in G$ with columns $g_1, \dots, g_n$ the flag $g.S = (F_i)_{i=0}^n$ with $F_i = \langle g_1, \dots, g_i \rangle_k$ for every $i = 0, \dots, n$, i.e. the flag spanned by the columns of g (from left to right).

(b)

The bijection φ is a G-equivariant, and therefore also B-equivariant, and thus induces a bijection

$$\{B\text{-orbits in } G/B\} \longrightarrow \{B\text{-orbits in } X\}\,.$$

In the case $n = 2$ every flag $(F_i)_{i=0}^2 \in X$ is uniquely determined by its middle term F_1 (because $F_0 = 0$ and $F_2 = k^2$), which is an arbitrary one-dimensional subspace of k^2. We thus have a bijection

$$\psi \colon X \to \{\text{one-dimensional subspaces of } k^2\} =: X'\,, \quad (F_i)_{i=0}^2 \mapsto F_1\,,$$

and this bijection is G-equivariant, and hence also B-equivariant. We therefore get another induced bijection

$$\{B\text{-orbits in } X\} \longrightarrow \{B\text{-orbits in } X'\}\,.$$

Suppose now that $L \in X'$ is a one-dimensional subspace of k^2. Then L is spanned by a single nonzero vector

$$\begin{bmatrix} x \\ y \end{bmatrix} \in L\,.$$

For $h \in B$ with $h = \left[\begin{smallmatrix} a & b \\ & c \end{smallmatrix}\right]$ the space $h.L$ is spanned by the single vector

$$\begin{bmatrix} a & b \\ & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax+by \\ cy \end{bmatrix}\,. \tag{1}$$

We can now distinguish between two (non-exclusive) cases:

- If $y \neq 0$ then we can choose $c = 1/y$, $a = 1$ and $b = -x/y$ to find that the B-orbit of L contains the line $\langle e_2 \rangle$.
- If $y = 0$ then $x \neq 0$ and we can choose $c = 1$, $a = 1/x$ and $b = 0$ to find that the B-orbit of L contains the line $\langle e_1 \rangle$.

If follows from (1) that the B-orbit of $\langle e_2 \rangle$ does not contain any line L' with $e_1 \in L'$ (because it follows from $c, y \neq 0$ that $cy \neq 0$). Hence the lines $\langle e_1 \rangle$ and $\langle e_2 \rangle$ are not in the same B-orbit.

This shows altogether that $\langle e_1 \rangle$ and $\langle e_2 \rangle$ form a set of representatives for the B-orbits on X'. This shows that there exist precisely two B-orbits on X', and hence two B-orbits on X. The two orbits have as a set of representatives the two flags

$$0 \subseteq \langle e_1 \rangle \subseteq k^2\,, \qquad 0 \subseteq \langle e_2 \rangle \subseteq k^2\,.$$

(c)

It holds for every $h \in B$ that $h.\langle e_2 \rangle = \langle e_2 \rangle$. The B-orbit of the flag $F^2 = (0 \subseteq \langle e_2 \rangle \subseteq k^2)$ consists therefore of only F^2 itself. It follows from

$$|X| = |G/B| = \frac{|G|}{|B|} = \frac{(q^2-1)(q^2-q)}{(q-1)^2 q} = \frac{q(q+1)(q-1)^2}{(q-1)^2 q} = q+1$$

that the other orbit, namely the one of $F^1 = (0 \subseteq \langle e_1 \rangle \subseteq k^2)$, consists of q elements.

(d)

The group B acts on G from the left by left multiplication, and from the right by right multiplication. The space H_q consists of all functions $f\colon G \to \mathbb{C}$ which are both left invariant and right invariant under these actions of B on G. These are precisely those functions $f\colon G \to \mathbb{C}$ which are constants on the double cosets

$$BgB = \{b_1 g b_2 \mid b_1, b_2 \in B\}\,,$$

where $g \in G$. If we denote the set of such double cosets by

$$B\backslash G/B = \{BgB \mid g \in G\}\,,$$

then a basis of H_q is therefore given by the characteristic functions I_D of the double cosets $D \in B\backslash G/B$; the characteristic function I_D is given by

$$I_D \colon G \to \mathbb{C}\,, \quad g \mapsto \begin{cases} 1 & \text{if } g \in D\,, \\ 0 & \text{if } g \notin D\,. \end{cases}$$

We can determine $B\backslash G/B$ with the following lemma:

Lemma 6. Let G be a group and let $K, H \subseteq G$ be two subgroups. Then the map

$$H\backslash(G/K) \to H\backslash G/K\,, \quad H(gK) \mapsto HgK$$

is a well-defined bijection.

Proof. We start with the well-defined map

$$\varphi'' \colon G \to H\backslash G/K \quad g \mapsto HgK\,.$$

It holds for all $g \in G$ and $k \in K$ that

$$\varphi''(g \cdot k) = HgkK = HgK = \varphi''(g)\,,$$

which shows that φ'' descends to a well-defined map

$$\varphi' \colon G/K \to H\backslash G/K\,, \quad gK \mapsto HgK\,.$$

It holds for all $h \in H$ and $gK \in G/K$ that

$$\varphi'(h \cdot gK) = HhgK = HgK = \varphi'(gK)\,,$$

which shows that φ' further descends to a well-defined map

$$\varphi \colon H\backslash(G/K) \to H\backslash G/K\,, \quad H(gK) \mapsto HgK\,.$$

We find in the same way that the well-defined map

$$\psi' \colon G \to H\backslash(G/K)\,, \quad g \mapsto H(gK)$$

satisfies

$$\psi'(h \cdot g \cdot k) = H((hgk)K) = (Hh)g(kK) = HgK = \psi'(g)\,,$$

for all $h \in H$, $k \in K$ and $g \in G$, and therefore descends to a well-defined map

$$\psi' \colon H\backslash G/K \to H\backslash(G/K)\,, \quad KgK \mapsto H(gK)\,.$$

The maps φ and ψ are mutually inverse, which shows that φ is a bijection with inverse $\varphi^{-1} = \psi$. □

We have already seen that $B\backslash(G/B)$ has (for $n = 2$) precisely two elements. It follows from Lemma 6 that $B\backslash G/B$ has precisely two elements. One of these double cosets is $B1B = B$, and the other one is necessarily the complement $B' \coloneqq G \setminus B$ (because G is the disjoint union of the double cosets in $B\backslash G/B$).

The space H_q has therefore two basis elements, namely the characteristic functions I_B and $I_{B'}$.

Before we further determine the algebra structure on H_q we first check that the given multiplication is both well-defined and associative.

We have for all $f_1, f_2 \in H_q$ that

$$\begin{aligned}
(f_1 \cdot f_2)(bg) &= \frac{1}{|B|} \sum_{y \in G} f_1(y) f_2(y^{-1} bg) \\
&= \frac{1}{|B|} \sum_{y \in G} f_1(by) f_2((by)^{-1} bg) \\
&= \frac{1}{|B|} \sum_{y \in G} f_1(by) f_2(y^{-1} b^{-1} bg) \\
&= \frac{1}{|B|} \sum_{y \in G} f_1(by) f_2(y^{-1} g) \\
&= \frac{1}{|B|} \sum_{y \in G} f_1(y) f_2(y^{-1} g) \\
&= (f_1 \cdot f_2)(g)\,,
\end{aligned}$$

and

$$(f_1 \cdot f_2)(gb) = \frac{1}{|B|} \sum_{y \in G} f_1(y) f_2(y^{-1} gb) = \frac{1}{|B|} \sum_{y \in G} f_1(y) f_2(y^{-1} g) = (f_1 \cdot f_2)(g)$$

for all $g \in G$ and $b \in B$, which shows that again $f_1 \cdot f_2 \in H_q$. To show that the multiplication is associative we first note that for any two functions $f_1, f_2 \in H_q$ their product $f_1 \cdot f_2$ can also be written as

$$(f_1 \cdot f_2)(g) = \frac{1}{|B|} \sum_{y \in G} f_1(y) f_2(y^{-1} g) = \frac{1}{|B|} \sum_{\substack{y, y' \in G \\ yy' = g}} f_1(y) f_2(y')\,.$$

With this we find for all $f_1, f_2, f_3 \in H_q$ that

$$\begin{aligned}(f_1 \cdot (f_2 \cdot f_3))(g) &= \frac{1}{|B|} \sum_{\substack{y,y' \in G \\ yy'=g}} f_1(y)(f_2 \cdot f_3)(y') \\ &= \frac{1}{|B|^2} \sum_{\substack{y,y' \in G \\ yy'=g}} f_1(y) \sum_{\substack{y'',y''' \in G \\ y''y'''=y'}} f_2(y'')f_3(y''') \\ &= \frac{1}{|B|^2} \sum_{\substack{y,y',y'' \in G \\ yy'y''=g}} f_1(y)f_2(y')f_3(y'')\end{aligned}$$

for every $g \in G$. We also find in the same way that

$$((f_1 \cdot f_2) \cdot f_3)(g) = \frac{1}{|B|^2} \sum_{\substack{y,y',y'' \in G \\ yy'y''=g}} f_1(y)f_2(y')f_3(y'')\,,$$

for every $g \in G$, which then shows that $f_1 \cdot (f_2 \cdot f_3) = (f_1 \cdot f_2) \cdot f_3$.

We now show that

$$\begin{aligned}I_B \cdot I_B &= I_B\,, \\ I_B \cdot I_{B'} &= I_{B'}\,, \\ I_{B'} \cdot I_B &= I_{B'}\,, \\ I_{B'} \cdot I_{B'} &= qI_B + (q-1)I_{B'}\,.\end{aligned}$$

With this we have then achieved the following things:

- We have describes the multiplication of H_q in terms of the given basis of H_q.
- We have shown that I_B is the multiplicative neutral element for H_q.
- We see that for "$q = 1$" we get the group algebra $\mathbb{C}[\mathbb{Z}/2]$.

Indeed, it holds for every $f \in H_q$ that

$$\begin{aligned}(I_B \cdot f)(g) &= \frac{1}{|B|} \sum_{y \in G} I_B(y) f(y^{-1}g) \\ &= \frac{1}{|B|} \sum_{b \in B} f(b^{-1}g) = \frac{1}{|B|} \sum_{b \in B} f(g) = \frac{|B|}{|B|} f(g) = f(g)\end{aligned}$$

for every $g \in G$, and similarly that

$$\begin{aligned}(f \cdot I_B)(g) &= \frac{1}{|B|} \sum_{y \in G} f(y) I_B(y^{-1}g) = \frac{1}{|B|} \sum_{y \in G} f(gy) I_B((gy)^{-1}g) \\ &= \frac{1}{|B|} \sum_{y \in G} f(gy) I_B(y^{-1}) = \frac{1}{|B|} \sum_{b \in B} f(gb) \\ &= \frac{1}{|B|} \sum_{b \in B} f(g) = \frac{|B|}{|B|} f(g) = f(g)\end{aligned}$$

for every $g \in G$. This shows that $I_B \cdot f = f = f \cdot I_B$ for every $f \in H_q$. We have for every $b \in B$ that

$$\begin{aligned}(I_{B'} \cdot I_{B'})(b) &= \frac{1}{|B|} \sum_{y \in G} I_{B'}(y) I_{B'}(y^{-1}b) \\ &= \frac{1}{|B|} \sum_{b' \in B'} I_{B'}(b'^{-1}b) \\ &= \frac{1}{|B|} \sum_{b' \in B'} \underbrace{I_{B'}(b'^{-1})}_{=1} \\ &= \frac{|B'|}{|B|} \qquad (2) \\ &= q\,, \qquad (3)\end{aligned}$$

where we use for (2) that $b' \in B$ if and only if $b'^{-1} \in B$, and therefore

$$b'^{-1} \in B' \iff b'^{-1} \notin B \iff b' \notin B \iff b' \in B'\,,$$

and we use for (3) that

$$\frac{|B'|}{|B|} = \frac{|G| - |B|}{|B|} = \frac{|G|}{|B|} - 1 = (q+1) - 1 = q\,.$$

Lastly, we have for $b' \in B'$ that

$$\begin{aligned}(I_{B'} \cdot I_{B'})(b') &= \frac{1}{|B|} \sum_{y \in G} I_{B'}(y) I_{B'}(y^{-1}b') \\ &= \frac{1}{|B|} \sum_{b'' \in B'} I_{B'}(b''^{-1}b') \\ &= \frac{1}{|B|} \sum_{\substack{b'' \in B' \\ b'' \notin b'B}} \underbrace{I_{B'}(b''^{-1}b')}_{=1} \qquad (4) \\ &= \frac{|B' \smallsetminus b'B|}{|B|}\end{aligned}$$

$$
\begin{aligned}
&= \frac{|B'| - |b'B|}{|B|} \qquad (5)\\
&= \frac{|B'| - |B|}{|B|}\\
&= \frac{|B'|}{|B|} - 1\\
&= q - 1\,,
\end{aligned}
$$

where use for (4) that

$$b''^{-1}b' \notin B \iff b''B \neq b'B \iff b'' \notin b'B\,,$$

and use for (5) that $b'B \subseteq B'$ because $b' \notin B$.

Remark 7. One can show more generally that

$$B\backslash G/B = \coprod_{\sigma\in S_n} BP_\sigma B\,,$$

where P_σ is the permutation matrix associated to the permutation $\sigma \in S_n$. This decomposition is known as the *Bruhat decomposition* of $\mathrm{GL}_n(k)$, and can be seen (an proven) as a version of the Gauß algorithm.

This then shows that H_q has for every n a basis indexed by the symmetric group S_n. The algebra H_q is known as the *Iwahori–Hecke algebra* of S_n, and can be seen as the deformation of the groups algebra $\mathbb{C}[S_n]$ along a parameter q.

One can more generally define the Iwahori–Hecke algebra of S_n fo every parameter $q \in \mathbb{C}^\times$: Recall that the symmetric groups S_n is can be described by generators $t_1, \dots, t_{n-1}$ (which represent the simple transpositions $t_i = (i, i+1)$) and the relations

(R1) $t_i^2 = 1$ for all $i = 1, \dots, n-1$,

(R2) $t_i t_j = t_j t_i$ for all $i, j = 1, \dots, n$ with $|i - j| \geq 2$,

(R3) $t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}$ for all $i = 1, \dots, n-2$.

(The last two relations are known as the *braid relations*.) We can now define the Iwahori–Hecke algebra H_q for $q \in \mathbb{C}^\times$ as the algebra given by generators $T_1, \dots, T_{n-1}$ and relations

(IH1) $T_i^2 = (q-1)T_i + q$ for all $i = 1, \dots, n-1$,

(IH2) $T_i T_j = T_j T_i$ for all $i, j = 1, \dots, n$ with $|i - j| \geq 2$,

(IH3) $T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1}$ for all $i = 1, \dots, n-2$.

For $q = 1$ this then gives back the group algebra $\mathbb{C}[S_n]$.