Homework 4, Solutions

M. Gr. after [Gri07]

2012/11/19

1.6 Krull–Schmidt theorem

Exercise 1.6.1. Compute the Krull–Schmidt decomposition of the $D_n = \langle \sigma, \tau : \sigma^2 = \mathrm{id} = \tau^n, \sigma\tau\sigma = \tau^{-1} \rangle$ for $n \leq 8$.

Solution. First consider the center of the D_n. As shown in the lecture this is $\operatorname{cent} D_n = \{1$ for n odd and $\langle \tau^{n/2} \rangle$ for $n \geq 4$ even; for $n = 2$ the whole groups is abelian and non-cyclic, thus $D_2 \cong C_2 \times C_2$. Another normal subgroup is $\langle \tau \rangle$ (of index 2). For n odd this is the only non-trivial normal subgroup. For n even there is also the subgroup $D_{n/2} \cong \langle \sigma, \tau^2 \rangle$ of index 2 and thus normal. By inspection these are the only normal subgroups. If n is divisible by 4, then $\operatorname{cent} D_n \subset \langle \tau \rangle, D_{n/2} \triangleleft D_n$ and thus D_{4k} is simple. For $n = 2(2k+1)$, i.e. divisible by 2, but not 4, then $\langle \tau \rangle \cap D_{n/2} = \{\mathrm{id}\}$ and $\langle \tau \rangle D_2 = D_{n/2} \langle \tau \rangle$, thus $D_{2(2k+1)} \cong D_2 \times \operatorname{cent} D_{2(2k+1)}$. In total we obtained:

$$D_n \begin{cases} \cong C_2 \times D_{n/2} & \text{for } n = 2(2k+1), \\ \text{indecomposable} & \text{else.} \end{cases} \qquad \square$$

Exercise 1.6.2. Compute the Krull–Schmidt decomposition of $\mathrm{GL}_2(\mathbb{F}_n)$ the automorphism group of the vector space $\mathbb{F}_n^2$ where $\mathbb{F}_n$ is the field with n elements (obviously $n \neq 6$ and some other cases).

a. For $n = 2$.

b. Count the number of elements in $\mathrm{GL}_2(\mathbb{F}_3)$.

c*. For $n = 3$.

d. Count the number of elements in $\mathrm{GL}_2(\mathbb{F}_p)$ for $p \in \mathbb{P}$.

Solution.

a. The group $\mathrm{GL}_2(\mathbb{F}_2)$ consists of the 6 elements

$$\left\{\mathbb{1}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\right\}.$$

It is not abelian and thus isomorphic to $S_3 \cong D_3$. This group is indecomposable, because $1 \subset C_3 \triangleleft D_3$ are its only normal subgroups.

d. The elements in $\mathrm{GL}_2(\mathbb{F}_p)$ are

$$\left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda'\end{pmatrix}, \begin{pmatrix}0 & \lambda\\ \lambda' & 0\end{pmatrix}\begin{pmatrix}\lambda & \mu\\ \mu' & \lambda'\end{pmatrix}, \begin{pmatrix}\lambda & \mu\\ 0 & \lambda'\end{pmatrix}, \begin{pmatrix}0 & \lambda\\ \lambda' & \mu\end{pmatrix}, \begin{pmatrix}\lambda & 0\\ \mu & \lambda'\end{pmatrix}, \begin{pmatrix}\mu & \lambda\\ \lambda' & 0\end{pmatrix}\right.$$
$$\left. : \lambda, \lambda', \mu, \mu' \in \mathbb{F}_p^*, \mu' \neq \frac{\lambda\lambda'}{\mu} \text{ in the third case}\right\}.$$

Which are $2(p-1)^2 + 4(p-1)^3 + (p-1)^3(p-2) = (p-1)^2p(p+1)$ elements.

b. In particular for $p = 3$ you obtain $\operatorname{ord}\mathrm{GL}_2(\mathbb{F}_3) = 48$.

c. It is also clear that $\mathrm{GL}_2(\mathbb{F}_p)$ is not abelian, so if you classify all non-abelian groups of order 48, you will come across $\mathrm{GL}_2(\mathbb{F}_3)$.

e. You can also generalize the previous counting for fields of order $N = p^n$. In this case $\operatorname{ord}\mathrm{GL}_2(\mathbb{F}_n) = (p^n-1)^2p^n(p^n+1)$.

f. There are no other finite examples, because a finite field is a finite vector space over a finite primitive field (the $\mathbb{F}_p$).

□

1.7 Group actions (群作用)

Exercise 1.7.1. Explain how the original statement of Lagrange's theorem "*When $x_1, \ldots, x_n$ are permuted in all possible ways, then the number of different values of $f(x_1, \ldots, x_n)$ is a divisor of $n!$.*" relates to orbits and stabilizers.

Solution. Given any function f with n arguments from the same domain D_1, then we have S_n acting on f, i.e. for $\sigma \in S_n$ and $x_1, \ldots, x_n \in D_1$ we define

$$(\sigma^* f)(x_1, \ldots, x_n) := f(x_{\sigma^{-1}1}, \ldots, x_{\sigma^{-1}n}).$$

Given a generic function f (i.e. without any symmetry in its arguments) and a generic tuple $\mathbf{x} \in D_1^n$ (i.e. $x_i \neq x_j$ for $i \neq j$), then this produces $\operatorname{ord} S_n = n!$ values. If on the other hand $f|\mathbf{x}$ is invariant under certain $G \subset S_n$, then these G form a subgroup (e.g. $\mathrm{id} \in G$ is always a symmetry, with $\sigma \in G$ we also have $(\sigma^{-1*}f)(\mathbf{x}) = f(x_{\sigma 1\ldots n}) = f(\mathbf{x})$ and for $\sigma, \tau \in S_n$ we have $((\sigma\tau)^* f)(\mathbf{x}) = f(x_{\tau^{-1}\sigma^{-1}1\ldots n}) = (\tau^* f)(x_{\sigma^{-1}1\ldots n}) = f(x_{\sigma^{-1}1\ldots n}) = f(\mathbf{x})$). Thus by the Lagrange theorem $|S_n \cdot f|\mathbf{x}| = (S_n : G) = n!/(G : 1)$ a divisor of $n!$. □

Exercise 1.7.2. Let G be a group and for $g \in G$ define the **inner automorphism (内自同构)** $c_g \colon G \to G : h \mapsto ghg^{-1}$.

a. Show that the inner automorphisms c_g form a subgroup $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ isomorphic to $G/\operatorname{cent}(G)$.

b. Show that $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$, i.e. a normal subgroup.

Hint: What is $(\phi \circ c_g)(h)$ for $g, h \in G$?

Solution. Define thus the map $C \colon G \to \mathrm{Aut}(G) : g \mapsto c_g$.

a. It is clear that c_g is an automorphism, because $c_g(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = c_g(h)c_g(h')$ and $(c_{g^{-1}} \circ c_g)(h) = g^{-1}ghg^{-1}g = h = \mathrm{Id}_G(h)$, i.e. $c_{g^{-1}}$ is the inverse of c_g. Moreover $c_{gg'}(h) = gg'h(gg')^{-1} = g(g'hg'^{-1})g^{-1} = (c_g \circ c_{g'})(h)$, i.e. C is a group homomorphism. By definition of the inner automorphisms $G/\ker C \cong \mathrm{Inn}(G)$. But $g \in \ker C$ means for all $h \in G$: $ghg^{-1} = h$, i.e. $gh = hg$ or $g \in \operatorname{cent}(G)$. Therefore $\mathrm{Inn}(G) \cong G/\operatorname{cent}(G)$.

b. Let thus $\phi \in \mathrm{Aut}(G)$ and $c_g \in \mathrm{Inn}(G)$, i.e. $g \in G$. For any $h \in G$ the composition $(\phi \circ c_g \circ \phi^{-1})(h) = \phi(g\phi^{-1}(h)g^{-1}) = \phi(g)h\phi(g)^{-1} = c_{\phi(g)}(h)$ and thus $\phi \circ c_g\phi^{-1} \in \mathrm{Inn}(G)$. Therefore $\phi\,\mathrm{Inn}(G)\phi^{-1} \subset \mathrm{Inn}(G)$ and so $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$, i.e. the inner automorphisms are normal in the automorphism group. □

Exercise 1.7.3. Let $\mu \colon G \times X \to X$ be the action of a group G on a set X.

a. Let $x, y \in X$ be two points on the same orbit. Show that their stabilizers are conjugate, i.e. there is an element $g \in G$ such that $\mathrm{Stab}_G(x) = g\,\mathrm{Stab}_G(y)g^{-1}$.

b. Assume that $\mathrm{Stab}_G(x) \cong C_2$ and $\mathrm{Stab}_G(y) \cong C_3$. Can x and y be on the same orbit? (Justify your answer.)

Solution.

a. Let $\mu(g)x = y$ for two points $x, y \in X$ on the same orbit and $g \in G$. Then every $s \in \operatorname{Stab}_G(x)$ induces a $\mu(gsg^{-1})(y) = \mu(g)\mu(s)x = \mu(g)x = y$, i.e. $gsg^{-1} \in \operatorname{Stab}_G(y)$. Moreover for $gsg^{-1} = gtg^{-1}$ we observe that $s = t$ and thus conjugation (multiplication with g from the left and g^{-1} from the right) is injective. As shown in the previous section, it is also an automorphism, i.e. $g \operatorname{Stab}_G(x) g^{-1} = \operatorname{Stab}_G(y)$ (the inverse conclusion can also be obtained by exchanging x and y and replacing g with g^{-1}).

b. Conjugate subgroups are isomorphic, but not all isomorphic subgroups are conjugate (See for example the two factors $\mathbb{Z}/(2)$ in the abelian group $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$). Therefore points with non-isomorphic stabilizer subgroups cannot be on the same orbit.

□

Exercise 1.7.4. Show that in a finite group G of order n, an element of order k has at most n/k conjugates.

Solution. Let $g \in G$ be any element and consider the conjugation action. Note that $\langle g \rangle \subset \operatorname{Stab}_G$, because $g^n g g^{-n} = g$, i.e. $|\operatorname{Stab}_G(g)| \geq \operatorname{ord} g = k$. But by the Stabilizer-Orbit formula we have $|C(g)| = [G : \operatorname{Stab}_G(g)] \leq \frac{n}{k}$. □

Remark (99)**.** Note that for every point $x \in X$ an action $\mu \colon G \times X \to X$ induces a group homomorphism $\mu|_{Gx} \colon G \to S(Gx)$, i.e. from the group G to the permutation group of the orbit. Therefore $\operatorname{Stab}_G(x) = \ker \mu|_{Gx} \triangleleft G$ is a normal subgroup.

Exercise 1.7.5. Determine the class equation of the $D_n := \langle \sigma, \tau : \sigma^2 = \mathrm{id} = \tau^n, \sigma\tau\sigma = \tau^{-1} \rangle$ where $n = 1, 2, \ldots$.

Solution. Analogous to the example in class we have

$$\operatorname{cent}(D_n) = \begin{cases} D_2 & \text{for } n = 2, \\ \{\mathrm{id}, \tau^{n/2}\} & \text{for } n \text{ even}, > 2, \\ \{\mathrm{id}\} & \text{for } n \text{ odd}. \end{cases}$$

The remaining rotations τ^k fall into pairs $\{\tau^k, \tau^{-k}\}$[1] for $1 \leq k < \frac{n}{2}$ or $\{\tau^{n/2}\}$ for n even. Many reflections lie in one big class $\{\sigma\tau^{2k} : -\frac{n}{2} < k < \frac{n}{2}\}$[2] which

[1] because $\sigma\tau^k\sigma = \tau^{-k}$

[2] because $\tau^{-k}\sigma\tau^k = \sigma\tau^{2k}$

is all of them for n odd, and another class $\{\sigma\tau^{2k+1} : 0 \leq k \leq \frac{n}{2}\}$[3] for n even. Therefore

$$|D_n| = 2n = \begin{cases} 4 & \text{for } n = 2, \\ 2 + \frac{n-2}{2} \cdot 2 + 2 \cdot \frac{n}{2}, & \text{for } n \text{ even}, > 2, \\ 1 + \frac{n-1}{2} \cdot 2 + n & \text{for } n \text{ odd}. \end{cases}$$

□

Exercise 1.7.6. Assume that $G/\operatorname{cent}(G)$ is cyclic. Prove that G is abelian.

Solution.

□

Exercise 1.7.7. A **characteristic subgroup (特征子群)** $H \subset G$ is a subgroup that is invariant under all automorphisms, i.e. for all $\phi \in \operatorname{Aut}(G)$: $\phi(H) = H$. In particular characteristic subgroups are invariant under the inner automorphisms and therefore normal.

a. Show that the center $\operatorname{cent}(G)$ is a characteristic subgroup.

b. Prove that every characteristic subgroup $H \subset N$ of a normal subgroup $N \triangleleft G$ is normal $H \triangleleft G$ in G.

c. Assume that $N \triangleleft G$ is characteristic and $N \subset H \subset G$ with $H/N \subset G/N$ characteristic. Show that $H \subset G$ is characteristic.

Solution.

a. Note that every automorphism preserves group multiplication and in-particular is surjective. Therefore for every $\phi \in \operatorname{Aut}(G)$, $z \in \operatorname{cent} G$ and $g \in G$ we have $\phi(z)\phi(g)\phi(z)^{-1} = \phi(zgz^{-1}) = \phi(g)$, i.e. $\phi(z)$ commutes with all images of the surjective map ϕ and must thus be in the center, i.e. $\phi(\operatorname{cent} G) \subset \operatorname{cent} G$. Since again ϕ is bijective, we obtain $\phi(\operatorname{cent} G) = \operatorname{cent} G$, i.e. the center is invariant under all automorphisms.

b. For any element $g \in G$ we know that the conjugation $c_g \colon G \to G$ preserved N, i.e. $\phi = c_g|N \colon N \to N$ is an automorphism. But since $H \subset N$ is characteristic, it is preserved under ϕ, i.e. $H = \phi(H) = gHg^{-1}$ and therefore $H \triangleleft G$.

[3] because $\sigma\tau^{k+1}(\sigma\tau)\tau^{-k-1}\sigma = \sigma\tau^{2k+1}$

c. Let thus $\phi \in \mathrm{Aut}(G)$ be any automorphism. Since $N \triangleleft G$ is characteristic, we know that $\phi(N) = N$ and thus ϕ factors through the projection $\pi\colon G \to G/N$, i.e. induces a map $\bar{\phi} \in \mathrm{End}(G/N)$. Since ϕ was an automorphism, so is $\bar{\phi} \in \mathrm{Aut}(G/N)$. Since $H/N \subset G/N$ is characteristic, we have $\bar{\phi}(H/N) = H/N$. But the latter is a relation for cosets and implies in particular for the sets $H \supset N$ that $\phi(H) = H$. But this means that H is a characteristic subgroup in G.

□