# Abstract Algebra- Aluffi

danny.mcallister

July 17, 2019

### 0.1 Chapter 2, Section 4

## 1 Exercises

**Exercise 1.1.** *Show that* $\mathbf{Z}/pq\mathbf{Z} \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ *if and only if* $(p, q) = 1$.

**Exercise 1.2.** *Prove that a group of order n is isomorphic to* $\mathbf{Z}/n\mathbf{Z}$ *if and only if it contains an element of order n.*

**Exercise 1.3.** *Prove that if* $G \cong H$*, G is Abelian iff H is, G is cyclic iff H is, and if G is cyclic, an element that generates G also generates H.*

**Exercise 1.4.** *Prove that no two of the groups* $(\mathbf{Z}, +)$*,* $(\mathbf{Q}, +)$*,* $(R, +)$ *are isomorphic to another.*

**Exercise 1.5.** *Prove that the groups* $(R \setminus \{0\}, \cdot)$ *and* $(\mathbf{C} \setminus \{0\}, \cdot\ )$ *are not isomorphic.*

**Exercise 1.6.** *Are* $(\mathbf{Q}, +)$*, and* $(\mathbf{Q}^+, \cdot)$ *isomorphic?*

**Exercise 1.7.** *Let G be a group. Prove that* $g \mapsto g^{-1}$ *and* $g \mapsto g^2$ *are group homomorphisms if and only if G is Abelian.*

**Exercise 1.8.** *Let G be a group,* $g \in G$*. Prove that the function* $\gamma_g : G \to G$ *defined for all* $a \in G$ *as* $\gamma_g(a) = gag^{-1}$ *is an automorphism of G. (Such automorphisms are called inner automorphisms). Prove that the function* $G \to Aut(G)$ *defined by* $g \mapsto \gamma_g$ *is a homomorphism. Prove that the homomorphism is trivial if and only if G is Abelian.*

**Exercise 1.9.** *Let* $p \neq q$ *be odd primes; show that* $(\mathbf{Z}/pq\mathbf{Z})^*$ *is not cyclic.*

**Exercise 1.10.** *Assume that, if p is prime, the equation* $x^d = 1$ *has at most d solutions in* $\mathbf{Z}/p\mathbf{Z}$*. Prove that the multiplicative group* $G = (\mathbf{Z}/p\mathbf{Z})^*$ *is cyclic.*

**Exercise 1.11.** *Does the equation* $x^3 - 9 = 0$ *have solutions in* $\mathbf{Z}/31\mathbf{Z}$*?*

**Exercise 1.12.** *Prove that* $Aut_{\mathbf{Grp}}(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \cong S_3$.

**Proof 1.1.** *($\Rightarrow$) Let $(p,q)=1$ and consider $\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/q\mathbf{Z}$. Recall in product groups, that $|(a,b)|=lcm(|a|,|b|)$. Hence $|([1]_p,[1]_q)|=lcm(p,q)=pq$, by our assumption. Then let $\varphi:\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/q\mathbf{Z}\to\mathbf{Z}/pq\mathbf{Z}$, by $\varphi(a([1]_p,[1]_q)=[a]_{pq}$. This definition is valid because $([1]_p,[1]_q)$ generates $\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/q\mathbf{Z}$. Consider $a(1,1),b(1,1)\in\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/q\mathbf{Z}$. Then $\varphi(a(1,1)+b(1,1))=\varphi((a+b)(1,1))=[a+b]_{pq}=[a]_{pq}+[b]_{pq}=\varphi(a(1,1))+\varphi(b(1,1))$, so $\varphi$ is a group homomorphism. Then we show it is injective, which together with the identical cardinality of the sets, shows $\varphi$ is a set bijection, and thus a group isomorphism. Let $a(1,1)\neq a'(1,1)$. Then $\varphi(a(1,1))=[a]_{pq}\neq[a']_{pq}=\varphi(a'(1,1))$, where the lack of equality follows from $a\neq a'$ and $a,a'<pq$.*

*($\Leftarrow$) Let $\mathbf{Z}/pq\mathbf{Z}\cong\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/q\mathbf{Z}$. Then there exists some element $(g,h)\in\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/q\mathbf{Z}$, such that $|(g,h)|=pq$, as $|[1]_{pq}|=pq$ in $\mathbf{Z}/pq\mathbf{Z}$, and isomorphisms preserve the order of elements. Then recall that in $\mathbf{Z}/n\mathbf{Z}$, the order of elements divides $n$, and so $|g|\leq p$, $|h|\leq q$. Hence*

$$pq=|(g,h)|=\frac{|g||h|}{(|g|,|h|)}\leq\frac{pq}{(|g|,|h|)}.$$

*Then clearly, for equality, $|g|=p$, $|h|=q$, and $(p,q)=1$.* □

**Proof 1.2.** *Let $G$ be a group of order $n$. We prove $G\cong\mathbf{Z}/n\mathbf{Z}$ iff $\exists\ g\in G$, $|g|=n$.*

*($\Rightarrow$) Let there exist $g\in G$, $|g|=n$. Then define $\varphi:G\to\mathbf{Z}/n\mathbf{Z}$, $\varphi(g^m)=[m]_n$. This is valid because $g$ generates $G$. Then let $j,k\in[1,n]$. $\varphi(g^kg^j)=\varphi(g^{k+j})=[k+j]_n=[k]_n+[j]_n=\varphi(g^k)\varphi(g^j)$, so $\varphi$ is a group homomorphism. We show $\varphi$ is injective, so given the underlying sets have equal cardinality, $\varphi$ is an isomorphism. Let $a,b\in[1,n]$, $a\neq b$. Then $\varphi(g^a)=[a]_n\neq[b]_n=\varphi(g^b)$, so $\varphi$ is injective, and $G\cong\mathbf{Z}/n\mathbf{Z}$.*

*($\Leftarrow$) Let $\mathbf{Z}/n\mathbf{Z}\cong G$. Then set the isomorphism to be $\varphi:\mathbf{Z}/n\mathbf{Z}\to G$, and $\varphi([1]_n)=h\in G$. Then, because $\varphi$ preserves orders of elements, $|h|=n$.* □

**Proof 1.3.** *Let $G$, $H$ be groups. We prove (1) $G$ is Abelian iff $H$ is, (2), $G$ is cyclic iff $H$ is, and (3), isomophisms preserve generators. Throughout, let $\varphi$ be isomorphism $\varphi:G\to H$, and $g,h\in G$*

*(1) ($\Rightarrow$) Let $G$ be Abelian. Then $\varphi(gh)=\varphi(g)\varphi(h)=\varphi(hg)=\varphi(h)\varphi(g)$. Because $\varphi$ is surjective, the $\varphi(g)\varphi(h)=\varphi(h)\varphi(g)$ relation holds for all elements of $H$, and $H$ is Abelian.*

*($\Leftarrow$) The proof is identical, but with elements of $H$, $a,b\in H$, and $\varphi^{-1}$.*

*(2) ($\Rightarrow$) Using the fact the isomorphism is an equivalence relation, noting there exists isomorphism $\psi:C_{|G|}\to G$, we can see $C_{|G|}\cong G\cong H$, so $C_{|H|}\cong H$.*

*($\Leftarrow$) The proof is identical.*

*(3) ($\Rightarrow$) Let $g$ generate $G$. Then $|\varphi(g)|=n=|G|=|H|$, so $\varphi(g)$ generates $H$.*

*($\Leftarrow$) The proof is identical.* □

**Proof 1.4.** *Notice that the fact out the cardinality of naturals and rationals gives us most of this: $|\mathbf{Z}|=|\mathbf{Q}|<|\mathbf{R}|$. Then $\mathbf{Z},\mathbf{Q}\ncong\mathbf{R}$.*

*To see $\mathbf{Z}\ncong\mathbf{Q}$, notice that $\mathbf{Z}$ is cyclic, but $\mathbf{Q}$ is not.* □

**Proof 1.5.** *Notice that in* $\mathbf{C}$, $|i| = 4$, *and all elements in* $\mathbf{R}$ *have infinite order, order 1 (1), or order 2 (-1). An isomorphism would preserve order, so there can't be one.* $\square$

**Proof 1.6.** *No. For contradiction, suppose that they are, and let an isomorphism be* $\varphi : (\mathbf{Q}, +) \to (\mathbf{Q}^+, \cdot)$. *Then notice that for all* $y \in Q$, *we can write* $y = 2x$ *for some* $x$. *Consider the image of* $y$ *under the isomorphism:* $\varphi(y) = \varphi(2x) = \varphi(x + x) = \varphi(x)\varphi(x) = \varphi(x)^2$. *That is, the image of every element of* $(\mathbf{Q}, +)$ *is a square in the rationals. This leads to a contradiction, because many rationals, such as the primes* $p = \frac{p}{1}$, *cannot be expressed as such, and hence* $\varphi$ *is not surjective.* $\square$

**Proof 1.7.** *Let* $G$ *be a group, and call* $\psi : G \to G$, $\psi(g) = g^{-1}$, $\phi : G \to G$, $\phi(g) = g^2$. *We prove* $G$ *is Abelian iff each are group homomorphisms.*

*(*$\psi$*)* $(\Rightarrow)$ *Let* $G$ *be Abelian. Then for all* $g, h \in G$, $\psi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \psi(g)\psi(h)$, *so* $\psi$ *is a group homomorphism.*

$(\Leftarrow)$ *Let* $\psi$ *be a group homomorphism. Then* $\psi(gh) = (gh)^{-1} = h^{-1}g^{-1} = \psi(g)\psi(h) = g^{-1}h^{-1}$. *Then we can see that, as* $h^{-1}g^{-1} = g^{-1}h^{-1}$, $(h^{-1}g^{-1})^{-1} = (g^{-1}h^{-1})^{-1}$, *and hence* $gh = hg$, *so* $G$ *is Abelian.*

*(*$\phi$*)* $(\Rightarrow)$ *Let* $G$ *be Abelian. Then for all* $g, h \in G$, $\phi(gh) = ghgh = g^2h^2 = \phi(g)\phi(h)$, *so* $\phi$ *is a group homomorphism.*

$(\Leftarrow)$ *Let* $\phi$ *be a group homomorphism. Then* $\phi(gh) = ghgh = \phi(g)\phi(h) = g^2h^2$. *Given* $ghgh = g^2h^2$, $g^{-1}ghghh^{-1} = g^{-1}g^2h^2h^{-1}$, *so* $hg = gh$ *and* $G$ *is Abelian.* $\square$

**Proof 1.8.** $\square$

**Proof 1.9.** $\square$

**Proof 1.10.** $\square$

**Proof 1.11.** $\square$

**Proof 1.12.** $\square$