Selected exercises from *Abstract Algebra* by *Dummit and Foote* (3rd edition).

Bryan Félix

Abril 12, 2017

Section 3.1

Exercise 14. *Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.*

a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.

Proof. Assume there exist q_1, q_2 with $0 \leq q_1, q_2 < 1$ and $q_1 \neq q_2$ such that $q_1 + \mathbb{Z} = q_2 + \mathbb{Z}$. Then, for every $z_1 \in \mathbb{Z}$ there exist $z_2 \in Z$ such that

$$q_1 + z_1 = q_2 + z_2.$$

Without loss of generality, assume $q_1 < q_2$. Then, we rewrite the previous equation as

$$q_2 - q_1 = z_1 - z_2.$$

Observe that $0 < q_2 - q_1 < 1$, in particular $q_2 - q_1 \notin \mathbb{Z}$. Then, since $z_1 - z_2$ is an integer, we arrive at a contradiction. □

b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

Proof. For any $q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ let the representative element be of the form $\bar{q} = \frac{z}{q}$ with $z, q \in \mathbb{Z}$. Then $q \cdot (\bar{q} + \mathbb{Z}) = q \cdot (z/q) + \mathbb{Z} = z + \mathbb{Z} = \mathbb{Z}$. Therefore $|q + \mathbb{Z}| < \infty$. Observe that the cosets $\frac{1}{n} + \mathbb{Z}$ for $n \in \mathbb{N}$ have order n. Therefore there are elements of arbitrarily large order. □

c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

Proof. We show, by contradiction, that for all irrational q the coset $q + \mathbb{Z}$ has infinite order. Assume that the order of $q+\mathbb{Z}$ is finite. Then, there exist an integer m such that $m \cdot (q+\mathbb{Z}) = \mathbb{Z}$. In other words, there exist an integer z such that $m \cdot q = z$. Equivalently $q = \frac{z}{m}$ and q is rational, arriving at a contradiction. □

d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$.

Proof. It is easy to see a natural isomorphism by considering the following.
Addition over the real line works as a translation. On the other hand, the operation of multiplication of elements in the unit circle is equivalent to a rotation . The idea here is to map the rational numbers in $[0, 1)$ to the angles in $[0, 2\pi)$. The natural choice for the isomorphism is $q \mapsto e^{q \cdot 2\pi \cdot i}$. □

Exercise 25.

a) *Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.*

Proof. The first implication is trivial. If $N \trianglelefteq G$ then $gNg^{-1} = N \subseteq N$.
Now, assume that $gNg^{-1} \subseteq N$ for all $g \in G$. We will prove that $N \subseteq gNg^{-1}$ for all $g \in G$ (which implies $gNg^{-1} = N$ and consequently $N \trianglelefteq G$).
Let n be an element of N. Observe that

$$n = g(g^{-1}ng)g^{-1}.$$

From the assumption ($gNg^{-1} \subseteq N$ for all $g \in G$) the element $g^{-1}ng$ has to be an element of N, let it be $\tilde{n}$. Then $n = g\tilde{n}g^{-1}$ and therefore n is an element of gNg^{-1} for all g in G as desired. □

b) *Let $G = GL_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the diagonal, and let g be the diagonal matrix with entries $2, 1$. Show that $gNg^{-1} \subseteq N$ but g does* not *normalize N.*

Proof. Let $n \in N$ have the following form

$$n = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$$

where z is an integer. Therefore, the elements in gNg^{-1} look like

$$gng^{-1} = \begin{pmatrix} 1 & 2\,z \\ 0 & 1 \end{pmatrix}.$$

Clearly gng^{-1} is an element of N for any choice of z but some elements of N are left behind ☹. Namely, all the upper triangular matrices with an odd integer in the upper right entry. Hence, g does not normalize N. □

Exercise 36. *Prove that if $G/Z(G)$ is cyclic then G is abelian.* [If $G/Z(G)$ is cyclic with generator $xZ(G)$, show that every element of G can be written in the form $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.]

Proof. Assume $G/Z(G)$ is cyclic. Then, there exist $xZ(G)$ that generates $G/Z(G)$. Therefore every element of G has the form $g = x^a z$ for some $a \in \mathbb{Z}$ and $z \in Z(G)$. Now, consider two arbitrary elements of G, let them be g and h, and observe the following.

$$\begin{aligned} g\,h &= x^a\,z_1\,x^b\,z_2 \\ &= z_1\,x^a\,x^b\,z_2 && \text{since z comutes with any element.} \\ &= z_1\,x^b\,x^a\,z_2 && \text{since x commutes with itself} \\ &= x^b\,z_2\,x^a\,z_1 && \text{since z commutes with any element.} \\ &= h\,g. \end{aligned}$$

Therefore G is abelian. □

Exercise 42. *Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$.* [Show $x^{-1}y^{-1}xy \in H \cap K$.]

Proof. We follow the hint.
Let $x \in H$ and $y \in K$. Consider the element $x^{-1}y^{-1}xy$. Since H is normal, the element $y^{-1}xy$ is an element of H and therefore $x^{-1}(y^{-1}xy)$ is an element of H. In the same manner, and since K is normal, the element $x^{-1}y^{-1}x$ is an element of K and therefore $(x^{-1}y^{-1}x)y$ is inside K. Therefore $x^{-1}y^{-1}xy \in H \cap K$. Furthermore $x^{-1}y^{-1}xy = 1$, and equivalently $xy = yx$. □

Section 3.2

Exercise 9. *Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:*

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) : x_i \in G \, and \, x_1 x_2 \cdots x_p = 1\}.$$

a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.

Proof. Since the p-tuples are unordered, we can arbitrarily choose the $p-1$ left coordinates in $|G|^{p-1}$ number of ways. Then, the coordinate x_p is given by the inverse of $x_1\, x_2 \cdots x_{p-1}$ □

Define the relation $\sim$ on $\mathcal{S}$ by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

Proof. Observe that we can translate the rightmost element to the left as follows

$$\begin{aligned} x_1\, x_2 \cdots x_{p-1}\, x_p &= 1 \\ x_1\, x_2 \cdots x_{p-1} &= x_p^{-1} \\ x_p\, x_1\, x_2 \cdots x_{p-1} &= 1 \end{aligned}$$

Since this can done indefinitely, every cyclic permutation of the p-tuple is an element of $\mathcal{S}$. □

c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.

Proof. We proceed by proving the properties of an equivalence relation.

i) $\sim$ is reflexive.
Since any element α is the identity permutation of itself $\alpha \sim \alpha$.

ii) $\sim$ is symmetric.
Assume $\alpha \sim \beta$. Then, β is a cyclic permutation of α. Furthermore, α is the inverse cyclic permutation of β. Then $\beta \sim \alpha$.

iii) $\sim$ is transitive.
Assume $\alpha \sim \beta$ and $\beta \sim \gamma$. Then, since the composition of permutations is a closed operation (in S_n), γ is a permutation of α. Hence $\alpha \sim \gamma$.

□

d) *Prove that an equivalence class contains a single element if and only if it is of the form* $(x, x, \dots, x)$ *with* $x^p = 1$.

Proof. Assume that an equivalence class contains a single element. Let it be $(x_1, x_2, \dots, x_p)$. Then, by part *b*), all of its permutations are in the same equivalence class. Therefore, it must be true that

$$x_1 = x_2 = \dots = x_p.$$

Let the element be x. then $(x_1, x_2, \dots, x_p)$ has the desired form $(x, x, \dots, x)$ an furthermore $x^p = 1$.
Now, assume that $(x, x, \dots, x)$ is an element of $\mathcal{S}$. We proceed by contradiction to show that the equivalence class of $(x, x, \dots, x)$ has order 1.
Assume there exist $(x_1, x_2, \dots, x_p)$ in the equivalence class of $(x, x, \dots, x)$ with at least one entry x_i distinct to x. Then, there must exist a cyclic permutation of $(x_1, x_2, \dots, x_p)$ such that $(x_1, x_2, \dots, x_p) = (x, x, \dots, x)$. Observe that, for all permutations, the element $x_i = x$. Arriving at a contradiction. □

e) *Prove that every equivalence class has order 1 or p (this uses the fact that p is a prime). Deduce that* $|G|^{p-1} = k + pd$, *where k is the number of classes of size 1 and d is the number of classes of size p.*

Proof. We inspect the number of distinct cyclic permutations k of an element in the equivalence class. If $k = 1$ or $k = p$ we obtein the desired result. Therefore we assume that k is of the form $1 < k < p$. In this case it must be true that $x_i = x_{zk+i}$ for all $z \in \mathbb{Z}$. Since k and p are relative prime $zk + i$ generates all the indices modulo p. Therefore $x_i = x$ for all i and we arrive at a contradiction since the permutation contains one element. Therefore, we conclude that $|G|^{p-1} = k + p\,d$ where k is the number of equivalence classes of size 1 and d is the number of equivalence classes of size p. □

f) *Since* $\{(1, 1, \dots, 1)\}$ *is an equivalence class of size 1, conclude from e) that there must be a non identity element x in G with* $x^p = 1$, *i.e., G contains an element of order p.* [Show $p|k$ and so $k > 1$.]

Proof. Since $p\,|\,|G|^{p-1}$, then $p\,|\,k + pd$. Hence, $p\,|\,k$ and therefore $k > 1$. We conclude that there must be an element x of order p. □

Exercise 10. *Suppose H and K are subgroups of finite index in the (possibly infinite) group G with* $|G : H| = m$ *and* $|G : K| = n$. *Prove that* $\operatorname{lcm}(m, n) \le |G : H \cap K| \le mn$. *Deduce that if m and n are relatively prime then* $|G : H \cap K| = |G : H| \cdot |G : K|$.

Exercise 18. *Let G be a finite group, let H be a subgroup of G and let* $N \trianglelefteq G$. *Prove that if* $|H|$ *and* $|G : N|$ *are relatively prime then* $H \le N$.

Proof. Since H is already a group, we only need to show that for all h in H, h is an element of N.
Take your favourite h in H. We inspect the set hN in the quotient G/N. Note that $(hN)^{|G:H|} = N$ (since $|G : N|$ is the order of the quotient group). Furthermore, $(hN)^{|H|} = (h^{|H|})N = 1 \cdot N = N$. Therefore (from a previous result) $(hN)^{\gcd\{|G:N|,|H|\}} = N$, but $\gcd\{|G : N|, |H|\} = 1$. Hence $hN = N$ and, therefore, your favourite h is an element of N. □

Exercise 21. *Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index.*

Proof. Assume that there exist a proper subgroup of $\mathbb{Q}$ with finite index $[\mathbb{Q} : N] = n$. Since $\mathbb{Q}$ is abelian, then $N \trianglelefteq \mathbb{Q}$, and therefore $\mathbb{Q}/N$ is a group of order n. Therefore, for all $q \in \mathbb{Q}$, nq is an element of N. Then, consider the element $\frac{q}{n} \in \mathbb{Q}$. Observe that, by the previous assertion, $n\frac{q}{n} = q$ is an element of N. Hence $N = \mathbb{Q}$.
For the second part, assume there exist $N \leq \mathbb{Q}/\mathbb{Z}$ such that its index is finite. Then, consider the two homomorphisms

$$\varphi : \mathbb{Q}/\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})/N$$

with $\ker(\varphi) = N$ and

$$\sigma : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$$

with $\ker(\sigma) = \mathbb{Z}$.
Then, the homomorphism $\varphi \circ \sigma : \mathbb{Q} \to (\mathbb{Q}/\mathbb{Z})/N$ with $\ker(\varphi \circ \sigma) = \sigma^{-1}(\varphi^{-}1(N))$ defines a subgroup of $\mathbb{Q}$ with finite index. A contradiction to the earlier problem. $\square$

Exercise 23. *Determine the last two digits of* $3^{3^{100}}$. [Determine $3^{3^{100}} \mod \varphi(100)$ and use exercise 22.]

Proof. The goal today is to figure the value of $3^{(3^{100})} \mod 100$. We notice that 3 and 100 are relative prime, therefore, from Euler's formula we know that $3^{40} \equiv 1 \mod 100$, ($\varphi(100) = 40$). Now we compute $3^{100} \mod 40$ to further simplify our herculean task. Again, observe that 3 and 40 are relative prime, therefore $3^{16} \equiv 1 \mod 40$, ($\varphi(40) = 16$). The latter implies that $3^{100} = 3^{6(16)+4} \equiv 3^4 \mod 40$, or equivalently $3^{100} \equiv 81 \equiv 1 \mod 40$. Therefore 3^{100} can be written as $n \cdot 40 + 1$ for some $n \in \mathbb{Z}$.
Now

$$\begin{aligned} 3^{3^{100}} &\equiv 3^{n \cdot 40+1} \mod 100 \\ &\equiv (3^{40})^n \cdot 3 \mod 100 \\ &\equiv 1^n \cdot 3 \mod 100 \\ &\equiv 3 \mod 100. \end{aligned}$$

Then, the last two digits are zero and three in that order. $\square$

Section 3.3

Exercise 3. *Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either*

i. $K \leq H$ *or*

ii. $G = HK$ *and* $|K : K \cap H| = p$.

Proof. First, observe that, since H is a normal subgroup then K is a subgroup of the normalizer of H. Therefore (by the good ol' second isomorphism theorem) HK is a subgroup of G. We inspect the following equality

$$p = \frac{|G|}{|H|} = \frac{|G|}{|HK|}\frac{|HK|}{|H|}.$$

There are two cases

1. Case 1: $\frac{|G|}{|HK|} = p$ and $\frac{|HK|}{|H|} = 1$
   Then, it must be the case that $H = HK$ since $H \subset HK$. Then, $1 \cdot K = K$ is a subset of H.

2. Case 2: $\frac{|G|}{|HK|} = 1$ and $\frac{|HK|}{|H|} = p$
   Here, $G = HK$ analogous to the previous case. Furthermore, we have (from a previous section)
   $$|HK| = \frac{|H||K|}{|H \cap K|}$$
   upon rearranging
   $$[K : H \cap K] = \frac{|K|}{|H \cap K|} = \frac{|HK|}{|H|} = \frac{|G|}{|H|} = p$$
   as desired.
   Remark. The latter result is also implied from the second isomorphism theorem as $K/H \cap K \cong HK/H \cong G/H$.

□

Exercise 8. *Let p be a prime and let G be the group of p-power roots of 1 in $\mathbb{C}$. Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.*

Proof. We prove that $\varphi : G \to G$ given by $\varphi(z) = z^p$ is surjective. For arbitrary $z \in G$ let $\varphi^{-1}(z) = z^{1/p}$. Note that this number exist since $z \in \mathbb{C}$. It is left to show that that $z^{1/p} \in G$. Take n such that $z^{(p^n)} = 1$ and observe that

$$(z^{1/p})^{p^{n+1}} = z^{(p^n)} = 1.$$

Therefore $z^{1/p} \in G$ and hence, φ is a surjection. Now observe that

$$\varphi(z_1 z_2) = (z_1 z_2)^p = z_1^p z_2^p = \varphi(z_1)\varphi(z_2).$$

This shows that φ is an homomorphism. Therefore, φ is a surjective homomorphism. We proceed to inspect the kernel of φ. By definition, $\ker(\varphi) = \{z \in G : z^p = 1\}$. This is the set of all *p-complex roots* of 1. Clearly, $\ker(\varphi)$ is non trivial and therefore (by means of the first isomorphism theorm)
$$G/\ker(\varphi) \cong G$$
where $\ker(\varphi)$ is a proper normal subgroup of G. □

Exercise 9. *Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$.*

Proof. Observe that $P \leq N(N)$ since N is normal. Therefore by the good ol' second isomorphism theorem $PN \leq G$. Furthermore $|PN|$ divides $|G| = p^a m$.
We have that P and N are subgroups of PN, therefore

$$|P| \,\big|\, |PN| \quad \text{and} \quad |N| \,\big|\, |PN|$$

or, equivalently

$$p^a \,\big|\, |PN| \quad \text{and} \quad p^b n \,\big|\, |PN|$$

The former implies that $|PN|$ is of the form $p^a\tilde{m}$ where $\tilde{m}$ divides m. The latter further implies that $|PN|$ has the form $p^a nm'$ where nm' divides m.
Note that, by the second isomorphism theorem, $P/P\cap N \cong PN/N$ and therefore

$$\frac{|P|}{|P\cap N|} = \frac{|PN|}{|N|}$$

equivalently

$$\frac{p^a}{|P\cap N|} = \frac{p^a\, n\, m'}{p^b\, n}$$

and, upon rearranging

$$|P\cap N| = \frac{p^b}{m'}.$$

Since p is a prime, the last assertion impies that m' is a power of p, but m' also has to divide m by construction. Therefore $m' = p^0 = 1$.
We go back to the form of $|PN|$ and conclude that $|PN| = p^a\, n$. The computation of $|P\cap N|$ and $|PN/N|$ is now trivial

$$|P\cap N| = \frac{|P||N|}{|PN|} = p^b$$
$$|PN/N| = \frac{|P|}{|P\cap N|} = p^{a-b}$$

as desired. ☐

Exercise 10. *Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a* Hall subgroup *of G if its index in G is relatively prime to its order:* $\gcd(|G:H|,|H|) = 1$. *Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H\cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.*

Proof. We will use the following property. If the order of one element divides the order of $|H|$ and the other one divides the order of the index $[G:H]$ then, it must be true that their greatest common divisor is also one.

1. To show: $\gcd(|H\cap N|,[N:H\cap N]) = 1$.
   Observe that from the second isomorphism theorem

   $$H/H\cap N \cong HN/N.$$

   It is clear that $|H\cap N|$ must divide the order of H .
   Now, observe the following

   $$\frac{|N|}{|H\cap N|}\frac{|G|}{|HN|} = \frac{|HN|}{|H|}\frac{|G|}{|HN|}$$
   $$= \frac{|G|}{|H|}$$

   Therefore, the index $[N:H\cap N]$ divides the index $[G:H]$ as desired.

2. To show: $\gcd(|HN/N|, [G/N : HN/N]) = 1$.
   Again, from the second isomorphism theorem we have that

$$\begin{aligned}\frac{|HN|}{|N|}|H \cap N| &= \frac{|H|}{|H \cap N|}|H \cap N| \\ &= |H|\end{aligned}$$

   Therefore the order of HN/N divides the order of H.
   Now observe that

$$\left(\frac{|G|}{|N|} / \frac{|HN|}{|N|}\right) \frac{|HN|}{|H|} = \frac{|G|}{|H|}$$

   Therefore the index $[G/N : HN/N]$ divides the index $[G : H]$ as desired.

□

Section 3.4

Exercise 5. *Prove that subgroups and quotient groups of a solvable group are solvable.*

Proof. We show each statement individually.

1. Subgroups of a solvable group are solvable.
   Let H be any subgroup of G and assume that G has decomposition

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_l = G$$

   where G_{i+1}/G_i is abelian. Consider the sets $H \cap G_i$. We will show that the composition

$$1 = H \cap 1 = H \cap G_0 \leq H \cap G_1 \leq \cdots \leq H \cap G_l = H \cap G = H$$

   satisfies $H \cap G_i \trianglelefteq H \cap G_{i+1}$ and $H \cap G_{i+1}/H \cap G_i$ is abelian for all i.

   (a) $H \cap G_{i+1} \trianglelefteq H \cap G_{i+1}$.
   We proceed by showing that for all $k \in H \cap G_{i+1}$, $k(H \cap G_{i+1}) = (H \cap G_{i+1})k$.
   Take any $x \in k(H \cap G_{i+1})$, then x has the form

$$x = kh$$

   for some $h \in (H \cap G_{i+1})$. Furthermore

$$x = (khk^{-1})k.$$

   Since $k \in H \cap G_{i+1}$, then $khk^{-1} \in H$. Also, since $G_i \trianglelefteq G_{i+1}$, $k \in G_{i+1}$ and $h \in G_i$ the conjugation khk^{-1} is an element of G_i. Hence x has the form

$$x = \tilde{h}k$$

   where $\tilde{h}$ is an element of $H \cap G_i$. In particular $\tilde{h} \in H \cap G_{i+1}$. and therefore

$$x \in (H \cap G_{i+1})k.$$

   Hence $k(H \cap G_{i+1}) \subseteq (H \cap G_{i+1})k$
   The reverse containment is analogous.

(b) The quotient $H \cap G_{i+1}/H \cap G_i$ is abelian for all i.
Observe that the quotient

$$H \cap G_{i+1}/H \cap G_i$$

is a subgroup of G_{i+1}/G_i which, by assumption, is abelian. Therefore $H \cap G_{i+1}/H \cap G_i$ is abelian as well.

2. Quotient groups of a solvable group are solvable.
Let N be any normal subgroup of G and assume that G has decomposition

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_l = G$$

where G_{i+1}/G_i is abelian.
Consider the quotient group G/N and the quotients G_iN/N. We will show that the composition

$$1 = N = G_0N/N \leq G_1N/N \leq \cdots \leq G_lN/N = GN/N = G/N$$

satisfies $G_iN/N \trianglelefteq G_{i+1}N/N$ and $(G_{i+1}N/N)/(G_iN/N)$ is abelian for all i.

(a) $G_iN/N \trianglelefteq G_{i+1}N/N$

(b) $(G_{i+1}N/N)/(G_iN/N)$ is abelian
Using the third isomorphism theorem

$$(G_{i+1}N/N)/(G_iN/N) \cong G_{i+1}N/G_iN$$

which is a subgroup of G_{i+1}/G_i, and therefore abelian.

$\square$