Dummit and Foote Exercises.

Marco Biroli

October 16, 2019

Chapter 1

Preliminaries.

1.1

- We know that:

  $$20 = 2^2 \cdot 5 \quad \text{and} \quad 13 \text{ is prime.}$$

  So $(20, 13) = 1$ and $\mathrm{lcm}(20, 13) = 260$ and $2 \cdot 20 - 3 \cdot 13 = 1 = (20, 13)$.

- Similarly we have:

  $$69 = 3 \cdot 23 \quad \text{and} \quad 372 = 2^2 \cdot 3 \cdot 31 \quad \text{so } (69, 372) = 3 \quad \text{and } \mathrm{lcm}(69, 372) = 2^2 \cdot 3 \cdot 23 \cdot 31 = 8556$$

  We also have:

  $$372 = 69 \cdot 5 + 27, \quad 69 = 27 \cdot 2 + 15, \quad 27 = 15 \cdot 1 + 12, \quad 15 = 12 \cdot 1 + 3, \quad 12 = 4 \cdot 3$$

  So back-feeding this we have:

  $$3 = 15 - 12 = 2 \cdot 15 - 27 = 2 \cdot 69 - 5 \cdot 27 = 27 \cdot 69 - 5 \cdot 372$$

- ...

1.2

Suppose that $k|a$ and $k|b$ then $a = c \cdot k$ and $b = e \cdot k$. So $as + bt = cks + ekt = k(cs + et)$ therefore $k|(as + bt)$.

1.3

Suppose n is composite, so n is not prime and can be written $n = \sum_{i=1}^{k} p_i^{\alpha_i}$. Then take $a = \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} p_i^{\alpha_i}$ and $b = \sum_{\lceil \frac{k}{2} \rceil}^{k} p_i^{\alpha_i}$. Then it is clear that $n|ab$ but $n \not| a$ and $n \not| b$.

1.4

Let a, b, N be fixed integers with a, b non-zero, set $d = (a, b)$ and suppose x_0, y_0 are particular solutions to $ax + by = N$. Then notice that taking $x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$ gives:

$$ax + by = ax_0 + by_0 + \frac{abt - abt}{d} = N$$

1.5

$\varphi(1)$	$\varphi(2)$	$\varphi(3)$	$\varphi(4)$	$\varphi(5)$	$\varphi(6)$	$\varphi(7)$	$\varphi(8)$	$\varphi(9)$	$\varphi(10)$
1	1	2	2	4	2	6	4	6	4

1.6

We prove the well-ordering of $\mathbb{Z}^+$ by induction on the cardinality of the set A. The base case is trivial, now take a subset A of $\mathbb{Z}^+$ of cardinality n. Then take any element $x \in A$. If $\forall m \in A,\ x < m$ we are done. Otherwise it means that $\exists y \in A,\ y < x$. Then take $B = A \setminus \{x\}$ by induction there is a minimal element $z \in B$ and from definition $z < y < x$ so $\forall m \in A,\ z < m$. This concludes the proof.

1.7

Take p a prime. Suppose there exist a, b integers such that $a^2 = pb^2$, then $p|a^2$, since p is prime this means that $p|a$. So $k^2p^2 = pb^2$ therefore $k^2p = b^2$. By the same reasoning we get that $p|b$ so we need $k^2p = m^2p^2$ which gives that $p|k$, repeating this argument recursively we arrive at a contradiction.

1.8

Let p a prime. Take $n \in \mathbb{Z}^+$ then n can be written as: $\sum_{i=1}^{k} p_i^{\alpha_i}$. Now suppose that $p^\beta|n!$, by the properties of p this means that p^β must divide n or $(n-1)!$. Repeating this recursively gives that p^β must divide at least one $(n-i)$ with $i \in [\![0, n-1]\!]$.

Chapter 2

Introduction to Groups.

2.1 Intro

2.1.1

- $a \star b = a - b$ is not associative since $a \star (b \star c) = a - (b - c) = a - b + c \neq a - b - c = (a - b) - c = (a \star b) \star c$.
- $a \star b = a + b + ab$ is associative since:

$$a \star (b \star c) = a \star (b + c + bc) = a + b + c + bc + ab + ac + abc$$
$$(a \star b) \star c = (a + b + ab) \star c = a + b + ab + c + ac + bc + abc$$

2.2 Dihedral Groups.

2.2.1

Take $x \in D_{2n}$ that is not a power of r then x can be written as $r^k s$. So $rx = r^{k+1}s = r^k(rs) = r^k(sr^{-1}) = xr^{-1}$.

2.2.2

Take $x \in D_{2n}$ that is not a power of r then $x^2 = r^k s r^k s = r^k s s r^{-k} = r^k r^{-k} = 1$.

2.2.3

Let x, y be any elements of order 2 in any group G not that this is equivalent to $x = x^{-1}$ and $y = y^{-1}$. Suppose that $t = xy$, then $tx = xyx$ and $xt^{-1} = xy^{-1}x^{-1} = xyx$. So $tx = xt^{-1}$.