Math 430 – Problem Set 2 Solutions

Due September 21, 2017

2.15(b). Find $d = \gcd(234, 165)$ and integers r and s with $d = 234r + 165s$.

Solution. Running the Euclidean algorithm,

$$\begin{aligned}
234 &= 1 \cdot 165 + 69 \\
165 &= 2 \cdot 69 + 27 \\
69 &= 2 \cdot 27 + 15 \\
27 &= 1 \cdot 15 + 12 \\
15 &= 1 \cdot 12 + 3 \\
12 &= 4 \cdot 3,
\end{aligned}$$

so the greatest common divisor is 3. Now

$$\begin{aligned}
3 &= 15 - 12 \\
&= 15 - (27 - 15) \\
&= 2 \cdot 15 - 27 \\
&= 2 \cdot (69 - 2 \cdot 27) - 27 \\
&= 2 \cdot 69 - 5 \cdot 27 \\
&= 2 \cdot 69 - 5 \cdot (165 - 2 \cdot 69) \\
&= 12 \cdot 69 - 5 \cdot 165 \\
&= 12 \cdot (234 - 165) - 5 \cdot 165 \\
&= 12 \cdot 234 - 17 \cdot 165,
\end{aligned}$$

so we may take $r = 12$ and $s = -17$.

2.30. Prove that there are an infinite number of primes of the form $4n - 1$.

Solution. Suppose, for contradiction, that there are finitely many: $p_1, \ldots, p_k$. Let $N = 4p_1 \ldots p_k - 1$. Since N differers from a multiple of every p_i by 1, it cannot be divisible by any p_i on the list. But it also cannot be divisible only by primes of the form $4n + 1$ since the product of such primes will be congruent to 1 modulo 4, while $N \equiv -1 \pmod 4$. Moreover, N is odd so it is not divisible by any even prime. Thus N must be divisible by at least one prime of the form $4n - 1$ that does not show up on the initial list. This contradiction proves the result. □

3.1(f). Find all $x \in \mathbb{Z}$ satisfying $3x \equiv 1 \pmod 6$

Solution. The multiples of 3 modulo 6 are 0 and 3, so there are no solutions to this equation.

3.7. Let $S = \mathbb{R} \backslash \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Solution.

- We first show that the operation gives a function $S \times S \to S$. Certainly $a * b \in \mathbb{R}$, so we just need to show that if $a, b \in S$ then $a * b \neq -1$. If $a * b = -1$ then $1 + a + b + ab = 0$, or $(1+a)(1+b) = 0$. This is impossible since $a \neq -1$ and $b \neq -1$.
- We show that 0 is the identity for S: for any $a \in S$, we have $0 * a = 0 + a + 0 \cdot a = a = a + 0 + a \cdot 0 = a * 0$.
- We show that the operation is associative:

$$\begin{aligned}
a * (b * c) &= a * (b + c + bc) \\
&= a + b + c + bc + a(b + c + bc) \\
&= a + b + c + bc + ab + ac + abc \\
&= a + b + ab + c + (a + b + ab)c \\
&= (a + b + ab) * c \\
&= (a * b) * c.
\end{aligned}$$

- We show that if $a \in S$ then $\frac{-a}{1+a} \in S$ is its inverse. Note that $\frac{-a}{1+a} \in \mathbb{R}$ since $a \neq -1$. Moreover, if $\frac{-a}{1+a} = -1$ then $-a = -1 - a$, which is impossible. Thus $\frac{-a}{1+a} \in S$. We then compute

$$\begin{aligned}
a * \frac{-a}{1+a} &= a + \frac{-a}{1+a} + \frac{-a^2}{1+a} = 0 \\
\frac{-a}{1+a} * a &= \frac{-a}{1+a} + a + \frac{-a^2}{1+a} = 0
\end{aligned}$$

- Finally, note that $a * b = a + b + ab = b * a$ since addition and multiplication are commutative in $\mathbb{R}$.

Thus $(S, *)$ is an abelian group. $\square$

3.17. Give an example of three different groups with eight elements. Why are the groups different?

Solution. There are five groups of order eight, up to isomorphism: you can select any three. They are

- $\mathbb{Z}_8$,
- $\mathbb{Z}_4 \times \mathbb{Z}_2$,
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$,
- D_4,
- Q_8.

The first three are abelian, and thus different from the last two. The first three are distinguished from each other by the largest order of an element (8 vs 4 vs 2). To see that D_4 and Q_8 are not isomorphic, note that D_4 has four elements of order 2 (the four reflections) while Q_8 only has one (-1).

3.22. Show that addition and multiplication mod n are well defined operations. That is, show that the operations do not depend on the choice of the representative from the equivalence classes mod n.

Solution. Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then there are integers r, s with $a = b+rn$ and $c = d + sn$. We find that

$$\begin{aligned} a + c &= b + rn + d + sn \\ &= b + d + (r + s)n, \end{aligned}$$

so $a + c \equiv b + d \pmod{n}$ and thus addition is well defined. Similarly,

$$\begin{aligned} ac &= (b + rn)(c + sn) \\ &= bc + bsn + crn + rsn^2 \\ &= bc + (bs + cr + rsn)n, \end{aligned}$$

so $ac \equiv bd \pmod{n}$ and thus multiplication is well defined. □

3.25. Let a and b be elements in a group G. Prove that $ab^na^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$.

Solution.

- For $n = 0$, this is the statement that $a \cdot 1 \cdot a^{-1} = (aba^{-1})^0$, which is true since both sides are the identity.
- For $n > 0$ we prove the statement by induction. Suppose that $ab^{n-1}a^{-1} = (aba^{-1})^{n-1}$. Then

$$\begin{aligned} (aba^{-1})^n &= (aba^{-1})^{n-1}(aba^{-1}) \\ &= ab^{n-1}a^{-1}aba^{-1} \\ &= ab^na^{-1}. \end{aligned}$$

- Finally, for $n < 0$, let $m = -n$. Using the statement for $m > 0$, we have

$$\begin{aligned} (aba^{-1})^n &= ((aba^{-1})^{-1})^m \\ &= (ab^{-1}a^{-1})^m \\ &= a(b^{-1})^m a^{-1} \\ &= ab^na^{-1} \end{aligned}$$

□

3.31. Show that if $a^2 = e$ for all elements a in a group G then G must be abelian.

Solution. Suppose $a, b \in G$. Then $e = (ab)(ab)$ and $e = (ab)(ba)$ since $b^2 = e$ and $a^2 = e$. Since inverses are unique, $ab = ba$. Thus G is abelian. □

3.33. Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

Solution. For all $a, b \in G$ we have

$$abab = aabb.$$

Multiplying on the left by a^{-1} and on the right by b^{-1} yields $ba = ab$, so G is abelian. □

3.40. Let

$$G = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \right\},$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Solution.

- Since $\det\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} = \cos^2(\theta) + \sin^2(\theta) = 1$, we get that $G \subseteq \mathrm{SL}_2(\mathbb{R})$.
- Setting $\theta = 0$ shows that G contains the identity.
- Since
$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
G is closed under taking inverses.
- We have
$$\begin{aligned} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} &= \begin{pmatrix} \cos(\theta)\cos(\varphi) - \sin(\theta)\sin(\varphi) & -\sin(\theta)\cos(\varphi) - \cos(\theta)\sin(\varphi) \\ \sin(\theta)\cos(\varphi) + \cos(\theta)\sin(\varphi) & \cos(\theta)\cos(\varphi) - \sin(\theta)\sin(\varphi) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta+\varphi) & -\sin(\theta+\varphi) \\ \sin(\theta+\varphi) & \cos(\theta+\varphi) \end{pmatrix}. \end{aligned}$$
Thus G is closed under taking products, and thus G is a subgroup of $\mathrm{SL}_2(\mathbb{R})$. $\square$

3.46. Prove or disprove: if H and K are subgroups of a group G, then $H \cup K$ is a subgroup of G.

Solution. This is only true if $H \subseteq K$ or $K \subseteq H$. It suffices to give a counterexample: if $G = \mathbb{Z}_6$, $H = \{0, 2, 4\}$ and $K = \{0, 3\}$ then $H \cup K = \{0, 2, 3, 4\}$ is not a subgroup since it's not closed under addition.

3.52. Prove or disprove: every proper subgroup of a nonabelian group is nonabelian.

Solution. False. For example, $\{\pm 1, \pm i\} \subset Q_8$ is abelian but Q_8 is not.

3.54. Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{g^{-1}hg : h \in H\}$ is also a subgroup of G.

Solution.

- Note that gHg^{-1} is a subset of G since G is closed under multiplication.
- Since $1 \in H$, we have $1 = g \cdot 1 \cdot g^{-1} \in gHg^{-1}$.
- If $ghg^{-1}, gh'g^{-1} \in gHg^{-1}$ then $ghg^{-1}gh'g^{-1} = ghh'g^{-1} \in gHg^{-1}$ since H is closed under multiplication.
- If $ghg^{-1} \in gHg^{-1}$ then $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$ since H is closed under taking inverses.