Abstract Algebra Homework 1

Joe Loser

January 22, 2016

This problem set includes problems from sections 1.3 and 2.3.
1.3: Problems 24c and 29
2.3: Problems 15b, 18, and 26.

24c) Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$. Prove

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$$

where $f^{-1}(B) = \{x \in X : f(x) \in B\}$.

<u>Proof</u>: First, we will show $f^{-1}(B_1 \cup B_2) \subset f^{-1}(B_1) \cup f^{-1}(B_2)$. If $x \in f^{-1}(B_1 \cup B_2)$, then $f(x) \in B_1 \cup B_2$. So, either $f(x) \in B_1$ or $f(x) \in B_2$. Therefore, $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$. Hence, $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$, i.e.

$$f^{-1}(B_1 \cup B_2) \subset f^{-1}(B_1) \cup f^{-1}(B_2).$$

Next, we will show that $f^{-1}(B_1) \cup f^{-1}(B_2) \subset f^{-1}(B_1 \cup B_2)$. Let $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Then $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$. So, either $f(x) \in f(B_1)$ or $f(x) \in f(B_2)$. Hence, $f(x) \in B_1 \cup B_2$. Therefore

$$x \in f^{-1}(B_1 \cup B_2).$$

Putting it all together, we have shown that $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$. $\square$

29) Define a relation on $\mathbb{R}^2 \setminus \{(0,0)\}$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a nonzero real number λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Prove that $\sim$ defines an equivalence relation on $\mathbb{R}^2 \setminus \{(0,0)\}$. What are the corresponding equivalence classes? This equivalence relation defines the projective line, which is very important in geometry.

<u>Proof</u>: In order to show $\sim$ is an equivalence relation, we need to show it is reflexive, symmetric, and transitive.
i) <u>Reflexive</u>: Since $x = 1 \cdot x$ and $y = 1 \cdot y$, $(x, y) \sim (x, y)$ for $(x, y) \in \mathbb{R}^2$.

ii) <u>Symmetric</u>: Suppose $(x_1, y_1) \sim (x_2, y_2)$. Then $x_1 = \lambda x_2$ and $y_1 = \lambda y_2$ for some $\lambda \in \mathbb{R} \setminus \{0\}$. Then, $\lambda^{-1} \in \mathbb{R} \setminus \{0\}$ and $x_2 = \lambda^{-1} x_1$ and $y_2 = \lambda^{-1} y_1$. Therefore, $(x_2, y_2) \sim (x_1, y_1)$.

iii) <u>Transitive</u>: Suppose $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. We want to show that $(x_1, y_1) \sim (x_3, y_3)$. So, we have that $x_1 = \lambda x_2, y_1 = \lambda y_2, x_2 = \alpha x_3$ and $y_2 = \alpha y_3$ for some $\lambda, \alpha \in \mathbb{R} \setminus \{0\}$. Therefore, $\lambda \alpha \in \mathbb{R} \setminus \{0\}$ and $x_1 = \lambda \alpha x_3$ and $y_1 = \lambda \alpha y_3$. Hence, $(x_1, y_1) \sim (x_3, y_3)$.

Since $\sim$ is reflexive, symmetric, and transitive, it is an equivalence relation. The corresponding equivalence class of (x, y) is the line passing through (x, y) and the origin, but omitting the origin. $\square$

15b) For the following pair of numbers a and b, calculate $gcd(a,b)$ and find integers r and s such that $gcd(a,b) = ra + sb$.

Solution: Using the Euclidean Algorithm, we have that:

$$\begin{aligned}
234 &= 165(1) + 69 \\
165 &= 69(2) + 27 \\
69 &= 27(2) + 15 \\
27 &= 15(1) + 12 \\
15 &= 12(1) + 3 \\
12 &= 3(4) + 0
\end{aligned}$$

Reversing our steps, 3 divides 12, 3 divides 15, 3 divides 27, 3 divides 69, 3 divides 165, and 3 divides 234. If d were another common divisor of 234 and 165, then d would also have to divide 3. Therefore, $gcd(234, 165) = 3$.

Working backwards through the above sequence of equations, we can find integers r and s that satisfy

$$\gcd(a,b) = \gcd(234,165) = 3 = 234r + 165s.$$

So, we have the following:

$$\begin{aligned}
3 &= 15 + (-1)(12) \\
&= [69 - 2(27)] + (-1)[27 + (-1)(15)] \\
&= [69 - 2(27)] + (-1)(27) + 15 \\
&= 69 + (-3)(27) + 69 - 27(2) \\
&= 2(69) + (-5)(27) \\
&= 2[234 - 165] + (-5)[165 + (-2)(69)] \\
&= 234(2) + 165(-2) + 165(-5) + 10(69) \\
&= 234(2) + 165(-7) + 10(69) \\
&= 234(2) + 165(-7) + 10[234 + (-1)(165)] \\
&= 234(2) + 165(-7) + 234(10) + 165(-10) \\
&= 234(12) + 165(-17)
\end{aligned}$$

Hence, $r = 12, s = -17$ satisfies $234r + 165s = 3$. □

18) Let $a, b \in \mathbb{Z}$ such that $\gcd(a,b) = 1$. Let r, s be integers such that $ar + bs = 1$. Prove that

$$\gcd(a,s) = \gcd(r,b) = \gcd(r,s) = 1.$$

Proof: Let $d := \gcd(a,s)$. We want to show that $d = 1$. By definition of gcd, we have that $d|a$ and $d|s$. Therefore, $d|(ar + bs)$. However, $(ar + bs) = 1$, so $d| \pm 1$. Since $d > 0$ the only option is for $d = 1$.

A similar argument can be made for the remaining pairs of numbers: (r,b) and (r,s). It will conclude with $d| \pm 1$ and again, since $d > 0$ we must have that $d = 1$. □

26) Prove that $\gcd(a,c) = \gcd(b,c) = 1$ if and only if $\gcd(ab,c) = 1$ for integers a, b and c.

Proof:
$\rightarrow$: First, we will show that $\gcd(a,c) = \gcd(b,c) = 1$ implies $\gcd(ab,c) = 1$. Note that $1|ab$ and $1|c$. Then it suffices to show there exists integers x and y such that

$$abc + cy = 1$$

by Corollary A6.

Since $\gcd(a,c) = \gcd(b,c) = 1$, by definition of gcd, there exists integers k, l, m and n such that

$$ak + cl = 1 \text{ and } bm + cn = 1$$

Multiplying these two equations by one another yields the following:

$$abkm + ackn + cblm + ccln = 1$$

which can be factored as such:

$$ab(km) + c(akn + blm + cln) = 1$$

Hence, $x = km, y = akn + blm + cln.$

$\leftarrow$: Next, to prove that $\gcd(ab, c) = 1$ implies $\gcd(a, c) = \gcd(b, c) = 1$, notice that by assumption, there exists integers x and y such that

$$abx + cy = 1.$$

This can be written as $a(bx) + cy = 1$ and $b(ax) + cy = 1$. Hence, there exists integers k', l', m', n' such that

$$ak' + cl' = 1 \text{ and } bm' + cn' = 1.$$

By Corollary A6, this implies that $\gcd(a, c) = \gcd(b, c) = 1$.

Therefore, we have shown that $\gcd(a, c) = \gcd(b, c) \iff \gcd(ab, c) = 1$. $\square$