MATH 112: HOMEWORK 1 SOLUTIONS

JOHANN GAEBLER

Problem 1

(a): Suppose $xr, (x+r) \in \mathbb{Q}$. Then, by the field axioms, $x = (x+r) - r = x \cdot r \cdot r^{-1} \in \mathbb{Q}$, contrary to assumption. Therefore $x \notin \mathbb{Q}$. □

(b): Suppose $\sqrt{12} \in \mathbb{Q}$; then $\exists a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ such that $\frac{a}{b} = \sqrt{12}$. Therefore $a^2 = 12b^2$. If a prime $p|cd$ for any $c, d \in \mathbb{Z}$, then $p|c$ or $p|d$; therefore $p|a^2 = aa \implies p|a$. Since $3|a^2$, $3|a \implies a = 3c$ for some $c \in \mathbb{Z}$. Therefore $3a^2 = (2b)^2 \implies 3|b$; therefore $gcd(a,b) \neq 1$, contrary to hypothesis. Therefore $\sqrt{12} \notin \mathbb{Q}$. □

(c):

i. Since $x \neq 0$, $\exists x^{-1}$; therefore $y = 1y = (x^{-1} \cdot x)y = x^{-1}(x \cdot y) = x^{-1}(x \cdot z) = z$.

ii. Set $z = 1$; then by part i., $y = 1$.

iii. Set $z = x^{-1}$; then by part i., $y = x^{-1}$.

iv. Replace x with z^{-1} in part iii. Then, set y to z. This gives that $z = (z^{-1})^{-1}$. □

(d): Since $E \neq \emptyset$, choose $e \in E$; then $\alpha \leq e$ and $\beta \geq e$. Thus $\alpha \leq e \leq \beta \implies \alpha \leq \beta$. □

(e): Note that since $\alpha \leq x$ for all $x \in A$, $-\alpha \geq -x$, i.e., $-\alpha \geq x'$ for all $x' \in A$. Therefore $-\alpha$ is an upper bound of $-A$; suppose it is not the least. Then, there exists $\gamma < \alpha$ such that $\gamma \geq x'$ for all $x' \in -A$. Then $\alpha < -\gamma \leq x$ for all $x \in A$; but $\alpha = \inf(A)$, so this is impossible. Therefore $-\alpha$ is the least upper bound of $-A$, as desired. □

Problem 2

Instead of proving that $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ is a field, we will prove the general case, i.e., that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = (\{0, 1, ..., p-1\}, +, \times)$ is a field whenever p is prime.

To do this, we will use the fact that $a \equiv b \mod p \iff p|(a-b)$. Then, we see that since $(a+b) - (b+a) = ab - ba = 0$ and $p|0$ for any $p \in \mathbb{P}$ and $a, b \in \mathbb{N}$, $\mathbb{Z}/p\mathbb{Z}$ is commutative w.r.t. addition and multiplication. The fact that $\mathbb{Z}/p\mathbb{Z}$ is closed w.r.t. addition and multiplication follows from the Euclidean algorithm: dividing $a+b$ and ab by p always gives a remainder between 0 and $p-1$. Associativity follows since for $a, b, c \in \mathbb{Z}$, $a + (b+c) - (a+b) + c = a(bc) - (ab)c = 0$ and $p|0$. The distributive property follows in the same way: $ab + ac - a(b+c) = 0$ and $p|0$, so $a(b+c) \equiv ab + ac$. The existence of the additive inverse is obvious: $a + (p-a) = p \equiv 0$. The existence of multiplicative inverse is trickier in general (we will prove this on the next problem set; however, in the case of $\mathbb{F}_2 = \{0, 1\}$, it suffices to note that $\mathbb{F}_2 \setminus \{0\} = \{1\}$ and $1 \times 1 \equiv 1$.

Of course, it is also possible to prove that the field axioms hold for $\mathbb{F}_2$ by checking each by hand; for instance, checking that the associative property holds for all eight possible sums of three elements.