Problem Set 1 - Thomas Boyko - 30191728

1. Let $m, n \in \mathbb{Z}^+$ so that $\gcd(m, n) = 1$. Prove that if $\sqrt{\frac{m}{n}}$ is rational, then m, n are perfect squares.

   Proof. Suppose $m, n \in \mathbb{Z}^+$ coprime, and that $\sqrt{\frac{m}{n}} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. We may also assume that a, b are also coprime; i.e. $\frac{a}{b}$ is the lowest terms we can put $\sqrt{\frac{m}{n}}$.

   Then $\frac{m}{n} = \frac{a^2}{b^2}$, and $mb^2 = na^2$. So $m | na^2$, and since $m \nmid n$, $m | a^2$. Likewise $n | b^2$.

2. Prove that no order can be defined in $\mathbb{C}$ that turns it into an ordered field.

   Proof. Suppose by way of contradiction that we have an order $<$ on $\mathbb{C}$ so that $\mathbb{C}$ is an ordered field. Then the square of any element in $\mathbb{C}$ must be positive. So $1^2 = 1 > 0$, and $(i)^2 = -1 > 0$. But

   $$0 < 1 \implies 0 + 0 < 1 + (-1) = 0.$$

   Which means $0 < 0$, a contradiction. So $\mathbb{C}$ cannot be an ordered field.

3. Write $z = a + bi$, and $w = c + di$. Define the lexicographic order, $z < w$ if $a < c$ and also if $a = c$ but $b < d$. Prove that this turns $\mathbb{C}$ into an ordered set.

   Proof. Take the order defined above, and write z, w as above.

   Then we show that exactly $z < w, z = w$, or $w < z$. Suppose neither $w < z, z < w$ are true. So we know four things:

   $$\begin{aligned} a &\leq c \\ c &\leq a \\ &. \end{aligned}$$

4. Show that a field automorphism $f : \mathbb{R} \to \mathbb{R}$ is either constant zero or identity.

   (a) Prove $f(0) = 0$ and $f(1)$ is either $0, 1$.

   Proof. We easily see $f(0) = 0$:

   $$f(0) = f(0 + 0) = f(0) + f(0) \implies f(0) = f(0).$$

   And similarly, letting $f(1) = x$:

   $$f(1) = f(1 \cdot 1) = f(1) \cdot f(1).$$

   Then $x^2 = x$, so $x(x - 1) = 0$ and $f(1)$ is either 0 or 1.

   (b) Prove $f(n) = nf(1)$ for any $n \in \mathbb{Z}$. Use this to show that $f\left(\frac{m}{n}\right) = \frac{m}{n} f(1)$ for any $m, n \in \mathbb{Z}$, and conclude that $f(q)$ must be either q or 0.

   Proof. We have covered that $f(0) = 0$, and outlined the cases for $f(1)$. Consider $n \in \mathbb{Z}_{>1}$.

   $$f(nx) = f(1 + \ldots + 1) = f(1) + \ldots + f(1) = nf(1).$$

   Now we show that $f(-n) = -f(n)$:

   $$0 = f(0) = f(n - n) = f(n) + f(-n) \implies -f(n) = f(-n).$$

   So clearly $f(n) = nf(1)$ for any $n \in \mathbb{Z}$.