SOLUTIONS TO EXERCISES 1.3, 1.12, 1.14, 1.16

JOHN DOYLE

Exercise 1.3: Let $|\cdot|$ be a norm on a field k.

a) If $x \in k$ is a root of unity, then $|x| = 1$.
b) For a field k, TFAE:
   i) Every nonzero element of k is a root of unity.
   ii) char $k = p > 0$, and $k/\mathbb{F}_p$ is algebraic.
c) If $k/\mathbb{F}_p$ is algebraic, then the only absolute value on k is the trivial absolute value.

Solution:

a) Let x be an nth root of unity.

$$\begin{aligned} x^n = 1 &\implies |x^n| = |1| \\ &\implies |x|^n = |1| \\ &\implies |x|^n = 1 \\ &\implies |x| \text{ is a positive real } n\text{th root of 1.} \end{aligned}$$

Therefore $|x| = 1$.

□

b) (*(i)* $\implies$ *(ii)*:) Suppose every nonzero element of k is a root of unity. Then every nonzero element satisfies the polynomial $x^m - 1$ for some positive integer m. Let $n = (1 + 1 + \cdots + 1)$, the n-fold sum of 1. Then either $2 = 0$ (hence k has characteristic 2), or there exists $m \in \mathbb{N}$ such that $2^m = 1$. Then $2^m - 1 = 0$; since k has no zero divisors, it must be the case that one of the prime factors p of $2^m - 1$ is zero. Therefore k has characteristic $p > 0$. Finally, because every element of k satisfies the polynomial $x^m - 1 \in \mathbb{F}_p[x]$ for some $m \in \mathbb{N}$, it follows that k is algebraic over $\mathbb{F}_p$.

(*(ii)* $\implies$ *(i)*:) Suppose k has characteristic p and is algebraic over $\mathbb{F}_p$, and let $0 \neq \alpha \in k$. Since k is algebraic, there exists a polynomial $f \in \mathbb{F}_p[x]$ such that $f(\alpha) = 0$. Let $n := \deg f$. Then α is contained a subfield of k that is a degree n extension of $\mathbb{F}_p$, i.e., $\alpha \in \mathbb{F}_{p^n}$. Therefore α satisfies $x^{p^n} = x$; since α is nonzero, it has an inverse, so we conclude that $\alpha^{p^n - 1} = 1$. Thus α is a root of unity.

□

c) By part (b), we have that every nonzero element of k is a root of unity, and by (a) we have that every root of unity has absolute value 1. Therefore it is determined that any absolute value must take the value zero at zero, and 1 at every other element; i.e., every absolute value is trivial.

□

Exercise 1.12: Let R be a valuation ring.

a) Show that $R^\times$ is the set of elements $x \in k^\times$ such that *both* x and x^{-1} lie in R.
b) Show that $R \setminus R^\times$ is an ideal of R and hence is the unique maximal ideal of R. Conclude that R is a local ring.

Solution:

a) Suppose $x \in R^\times$. Then x is a unit in R, and therefore both x and x^{-1} are in R. Now suppose x and x^{-1} are both in R. Then x is a unit in R, so $x \in R^\times$. □

b) Let $\mathfrak{m} := R \setminus R^\times$. We must show that $\mathfrak{m}$ is an additive group and is closed under multiplication by R. First, since 0 is not a unit, it must be in $\mathfrak{m}$. Also, if x is not a unit, then $-x$ is not a unit either, so $\mathfrak{m}$ is closed under additive inverses.

To show that $x, y \in \mathfrak{m} \implies x + y \in \mathfrak{m}$, we will prove the contrapositive, that if $x + y$ is a unit, then either x or y is a unit. So suppose that $x + y \in R^\times$ and $x \notin R^\times$. First, we notice that $\frac{x+y}{x}$ cannot be in R, since

$$\begin{aligned} \frac{x+y}{x} \in R &\implies \frac{x+y}{x} \cdot \frac{1}{x+y} \in R \\ &\implies \frac{1}{x} \in R, \end{aligned}$$

which contradicts the fact that x is not a unit. Now

$$\begin{aligned} \frac{x+y}{x} \notin R &\implies 1 + \frac{y}{x} \notin R \\ &\implies \frac{y}{x} \notin R. \end{aligned}$$

Since R is a valuation ring, it then follows that $\frac{x}{y}$ is an element of R. Now we get

$$\begin{aligned} \frac{x}{y} \in R &\implies \frac{x}{y} + 1 \in R \\ &\implies \frac{x+y}{y} \in R \\ &\implies \frac{x+y}{y} \cdot \frac{1}{x+y} \in R \qquad \text{since } (x+y) \in R^\times \\ &\implies \frac{1}{y} \in R. \end{aligned}$$

Therefore $y \in R^\times$, and, as we mentioned above, we may conclude that $\mathfrak{m}$ is closed under addition. Finally, we must show that $\mathfrak{m}$ is closed under multiplication by R. We will again prove this by contrapositive; if $rx \notin \mathfrak{m}$, then $x \notin \mathfrak{m}$.

$$\begin{aligned} rx \in R^\times &\implies \exists s \in R \text{ such that } s(rx) = 1 \\ &\implies (sr)x = 1 \\ &\implies x \in R^\times \end{aligned}$$

Hence $x \in \mathfrak{m} \implies rx \in \mathfrak{m}$. Therefore, $\mathfrak{m}$ is an ideal. Since its complement consists only of units, it is necessarily the unique maximal ideal of R. □

Exercise 1.14: Let k be a field, and let v be a valuation on k.

a) Put $\Gamma = v(k^\times)$. Show that Γ is a subgroup of $(\mathbb{R}, +)$. The subgroup Γ is called the *value group*.
b) Show that a valuation is trivial if and only if its value group is $\{0\}$.
c) Show that every nontrivial discrete subgroup of $(\mathbb{R}, +)$ is cyclic.
d) Deduce that every discrete valuation is equivalent to one with value group $\mathbb{Z}$.

Solution:

a) By the definition of a valuation, $v(k^\times) \subset \mathbb{R}$. Also, when restricted to $k^\times$, the map v is a homomorphism from the multiplicative group $k^\times$ to the additive group $(\mathbb{R}, +)$. Thus the image of v must be a subgroup of $(\mathbb{R}, +)$.

$\square$

b) First, suppose v is a trivial valuation. Then, by definition of trivial, $v(k^\times) = \{0\}$. Now suppose $v(k^\times) = \{0\}$. Then every element of $k^\times$ gets mapped to 0. Since 0 must necessarily get mapped to ∞, this is the trivial valuation.

$\square$

c) Let Γ be a discrete subgroup of $(\mathbb{R}, +)$. Let $\Gamma^+ := \Gamma \cap \mathbb{R}^+$. We will first show that Γ^+ has a least element γ, and then we will show that γ generates the group Γ.

Suppose Γ^+ does not have a least element. Then there exists a strictly decreasing sequence $\{x_1, x_2, \ldots\}$ contained in Γ^+. Since each x_i is positive, the x_i must converge. In particular, $\{x_i\}$ is a Cauchy sequence; let $y_i = x_i - x_{i+1}$. Since Γ is a group, it is closed under addition and additive inverses, so $y_i \in \Gamma \forall i$. Using the fact that the original sequence was Cauchy, we therefore have that the sequence $\{y_i\}$ converges to zero. Since $0 \in \Gamma$, it follows that Γ is not discrete. Therefore every discrete group has a least positive element γ.

Now suppose for contradiction that γ does not generate Γ. Then there exists $\beta \in \Gamma$ such that $\beta \neq n\gamma$ for any $n \in \mathbb{Z}$. We may assume that $\beta \in \Gamma^+$; otherwise, take $-\beta$. Then there exists some $m \in \mathbb{Z}$ such that $m\gamma < \beta < (m+1)\gamma$. Then

$$\begin{aligned} 0 < \beta - m\gamma &< (m+1)\gamma - m\gamma \\ &= \gamma. \end{aligned}$$

So $\beta - m\gamma$ is a positive element of Γ that is less than γ, which contradicts the minimality of γ. Hence γ must generate Γ. Therefore Γ is cyclic.

$\square$

d) Since every nontrivial subgroup of $\mathbb{R}$ must be infinite ($(\mathbb{R}, +)$ has no nonzero elements of finite order), it follows from (c) that every nontrivial discrete subgroup of $\mathbb{R}$ must be infinite cyclic, i.e., isomorphic to $\mathbb{Z}$. Say $\gamma \in \Gamma$ is the least positive element of Γ, which we certainly have by part (c). Then define the valuation v' by

$$v'(x) = \frac{1}{\gamma} \cdot v(x)$$

This is still a valuation, as it satisfies the definition of a valuation, and it is equivalent to v by definition of equivalence. Since the value group of v is

$\gamma \cdot \mathbb{Z}$, it follows that the value group of v' is $\mathbb{Z}$.

□

Exercise 1.16: Let A be an abelian group, written additively. Recall that A is *divisible* if for all $x \in A$ and $n \in \mathbb{Z}^+$ there exists $y \in A$ such that $ny = x$. (Equivalently, the multiplication map $[n] : A \to A$ defined by $x \mapsto nx$ is surjective.)

a) Show that no nontrivial discrete subgroup of $\mathbb{R}$ is divisible.
b) Show that a quotient of a divisible group is divisible.
c) Show that if k is algebraically closed, then $k^\times$ is a divisible abelian group.
d) Deduce that an algebraically closed field admits no discrete valuations.

Solution:

a) Let Γ be a subgroup of $(\mathbb{R}, +)$. As we showed in the proof of Exercise 1.14, $\Gamma \cap \mathbb{R}^+$ has a least element γ. Therefore $\frac{\gamma}{2} \notin \Gamma$, from which we conclude that there is no $y \in \Gamma$ such that $2y = \gamma$. Hence Γ is not divisible.

□

b) Suppose A is a divisible group. Let G be a quotient of A; let $\pi : A \to G$ be the quotient map. Let $x \in G$ and $n \in \mathbb{Z}^+$. We will show that there exists $y \in G$ such that $ny = x$.

Let $x' \in \pi^{-1}(x)$. Then, since A is a divisible group, there exists $y' \in A$ such that $ny' = x'$. Let $y = \pi(y')$. Then

$$\begin{aligned} ny &= n\pi(y') \\ &= \pi(ny') \\ &= \pi(x') \\ &= x. \end{aligned}$$

□

c) Suppose k is algebraically closed, and let $x \in k^\times$ and $n \in \mathbb{Z}^+$. Since k is algebraically closed, the polynomial $z^n - x \in k[z]$ has a root; call it y. Then $y^n = x$. Since multiplication by n in an additive group corresponds to raising to the nth power in a multiplicative group, we are done.

□

d) Suppose k is an algebraically closed field. We will show that any valuation is necessarily non-discrete. Let v be a valuation on k. Since we know $\Gamma = v(k^\times$ is a subgroup of $(\mathbb{R}, +)$, we may consider the map $\pi : k^\times \to \Gamma$ which is the restriction of v to $k^\times$. Since this is a surjective map, it is a quotient map. By (c), $k^\times$ is divisible, and by (b) this implies that the quotient Γ is divisible as well. Finally, by part (a), we conclude that Γ cannot be discrete. Hence v is not a discrete valuation.

□