Solution Set 9: Part A

Benjamin Bakker
Mathematics 25a
Prof. Berger

November 26, 2003

A.1. *Let (E, d) be a metric space, and let $f : E \to \mathbb{C}$ be a function. Write $f(x) = a(x) + ib(x)$ where a, b are two functions from E to $\mathbb{R}$.*

(1) *prove that f is continuous if and only if a and b are continuous.*

Solution. For any $x, y \in \mathbb{C}$, if $|a(x) - a(y)| < \epsilon$ and $|b(x) - b(y)| < \epsilon$, then

$$|f(x) - f(y)| = \sqrt{|a(x) - a(y)|^2 + |b(x) - b(y)|^2} < \epsilon\sqrt{2}$$

and similarly, if $|f(x) - f(y)| < \epsilon$, then by the above equality

$$|a(x) - a(y)| < \epsilon \text{ and } |b(x) - b(y)| < \epsilon$$

It then follows that f is continuous if and only if a, b are. In one direction, for all $\epsilon > 0$, if f is continuous, then for any $x \in E$ there exists δ such that $|f(x) - f(y)| < \epsilon$ whenever $d(x, y) < \delta$, in which case the above shows that $|a(x) - a(y)| < \epsilon$ and $|b(x) - b(y)| < \epsilon$. The other direction is the same.

(2) *prove that if f, g are two continuous functions from (E, d) to $\mathbb{C}$ then $f \pm g$ and $f \cdot g$ are also continuous.*

Solution. Let $f(x) = a(x) + ib(x)$ and $g(x) = c(x) + id(x)$. $f \pm g = (a \pm c) + i(b \pm d)$ is continuous if and only if $a \pm c$ and $b \pm d$ are. Similarly, $fg = (ac - bd) + i(ad + bc)$ is continuous if and only if $ac - bd$ and $ad + bc$ are. Sums and products of continuous functions from a metric space into $\mathbb{R}$ are continuous, so $f \pm g$ and fg are continuous.

A.2. *If $m \in \mathbb{Z}_{\geq 1}$ let $\phi(m) = \mathrm{Card}\{1 \leq x \leq m, \gcd(x, m) = 1\}$. If G is a group and if $g \in G$, the order of g is the smallest $m \geq 1$ such that $g^m = e$. Don't confuse this with the order of G which is $\mathrm{Card}(G)$.*

(1) *prove that the order of g is the order of the subgroup it generates in G (assume that G is finite).*

Solution. The subgroup generated by g is $H = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$. g has finite order because G is finite; let n be the order of g. For any $p \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$, $0 \leq r \leq n - 1$ such that $p = nq + r \Rightarrow g^p = g^{nq+r} = g^r$, and $H = \{e, g, \ldots, g^{n-1}\}$. The n elements $e, g, \ldots, g^{n-1}$ are distinct, for if $g^p = g^q$ with $0 \leq p, q \leq n - 1$ and $p \neq q$, then $g^{q-p} = e$ and $0 < |q - p| < n$, so n is not the order of g. Thus, the order of H is n.

(2) *prove that if G is any finite group and if $g \in G$ then the order of g divides the order of G.*

Solution. By the above, the order of the subgroup H generated by g is equal to the order of g. Since G is finite, we have by Lagrange's thm that the order of g divides $\mathrm{Card}(G)$.

(3) *prove that if $n \geq 1$, then $\sum_{d|n} \phi(d) = n$ (here $\sum_{d|n}$ means the sum over all divisors d of n).*

Solution. Let S_d be the set of all integers from 1 to n whose greatest common divisor with n is d. Of course, for any $1 \leq x \leq n$, $\gcd(x, n)$ divides n (and x), so $\sum_{d|n} \mathrm{Card}(S_d) = n$. But $\gcd(x, n) = d$ if and only if $\gcd(x/d, n/d) = 1$; $x \in S_d$ can be anything from d (since $d|x$) to n, so $1 \leq x/d \leq n/d$, and $S_d = \{1 \leq y \leq n/d | \gcd(y, n/d) = 1\} \Rightarrow \mathrm{Card}(S_d) = \phi(n/d)$. Factors of n always come in pairs, d and n/d, so $n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$.

(4) *show that if G is a cyclic group of order n and d divides n, then there are $\phi(d)$ elements in g of order d.*

Solution. Let $G = (e, g, \cdots, g^{n-1})$. If $h = g^k$ satisfies $x^d = e$, then $kd = mn$ for some m; since $k \leq n$, we have $m \leq d$. If $p = \gcd(m, d) \neq 1$, then $d/p < d$, and $h^{d/p} = g^{(m/p)n} = e$ since m/p is an integer, and d is not the order of g. Conversely, if $\gcd(m, d) = 1$, then $\gcd(k, n) = n/d$; $\operatorname{lcm}(k, n) = kd$, and therefore the order of h is d. It then follows that the number of elements of order d is equal to $\operatorname{Card}\{1 \leq m \leq d | \gcd(m, d) = 1\} = \phi(d)$.

(5) *in (5)-(7) let K be a field and let G be a finite subgroup of $(K^*, \times)$ of order n. Prove that there are at most d elements $g \in G$ such that $g^d = 1$.*

Solution. An element $g \in G$ satisfies $g^d = 1$ iff it is a root of $x^d - 1$. As shown in class, this polynomial has degree d and therefore has at most d roots in K.

(6) *prove that there exists an element $g \in G$ which is of order n.*

Solution. We first want to show that the number of elements of degree d is no more than $\phi(d)$ for any $d|n$. If there is no element of order d, then this is trivial. If not, there exists an element $g \in G$ of order d, and g generates a subgroup H of order d by (1), all of whose elements satisfy $x^d = 1$. By (5), these are the only elements that satisfy $x^d = 1$, so all elements of order d are contained in H, a cyclic group of order d, and the claim follows by (4). If there were no element of G of order n, then $\operatorname{Card}(G) \leq \sum_{d|n} \phi(d) - \phi(n) = n - \phi(n)$ by (3), and since $\phi(n) \geq 1$, we have a contradiction. Thus, G has an element of order n.

(7) *prove that G is cyclic.*

Solution. This follows immediately from (6).

(8) *let G be the set of invertible elements in $\mathbb{Z}/24\mathbb{Z}$. Prove that G is not a cyclic group.*

Solution. By inspection, the invertible elements are $(\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23})$—actually, you can check by direct computation that the inverse of each invertible element is itself. There are then 7 elements of order 2, but $\phi(2) = 1$, so G is not cyclic.

A.3. *Let S^1 be the set of complex numbers z such that $|z| = 1$ and let C_n be the set of complex numbers such that $z^n = 1$.*

(1) *prove that $(S^1, \times)$ and $(C_n, \times)$ are compact subgroups of $\mathbb{C}^*, \times$.*

Solution. We saw S^1 on last week's problem set, problem A.1.(3) (just identify (x, y) with $x + iy$). Note that the n distinct powers of $e^{2\pi i/n}$, $1, e^{2\pi i/n}, \ldots, e^{2\pi i(n-1)/n}$, all satisfy $z^n = 1$ and are therefore the only elements of C_n.

We know $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is a group under multiplication, so we need only check that both $S^1 \subset \mathbb{C}^*$ and $C_n \subset \mathbb{C}^*$ contain 1 and are closed under $\times$ and inversion; it is sufficient to show that both contain 1 and are closed under $(x, y) \mapsto xy^{-1}$. Clearly $1 \in S^1$ and $1 \in C_n$. If $z, w \in S^1$, then $|zw^{-1}| = |z|/|w| = 1$ so $zw^{-1} \in S^1$; if $z, w \in C_n$, then $(zw^{-1})^n = z^n/w^n = 1 \Rightarrow zw^{-1} \in C_n$. Finally, S^1 is the image of the compact set $[0, 1] \subset \mathbb{R}$ under the continuous homomorphism $f : \mathbb{R} \to \mathbb{C}$ given by $f(t) = e^{2\pi it}$ and is therefore compact, while C_n is a finite union of points and therefore compact.

(2) *are there any other ones?*

Solution. No. Let G be a compact subgroup of $(\mathbb{C} \setminus \{0\}, \times)$. If there is an element $z \in G$ with $|z| > 1$, then $z^n \in G$ for all $n > 0$, and since $d(z^n, 0) = |z|^n \longrightarrow \infty$, G is not compact (i.e., z^n contains no convergent subsequence); likewise, if $|z| < 1$, then $z^{-1} \in G$ and $|z^{-1}| > 1$. Thus, $G \subset S^1$. Of course, we also have $1 \in G$.

We showed in lecture that the only closed subgroups of $\mathbb{R}$ are $0, \alpha\mathbb{Z}, \mathbb{R}$, where $\alpha \in \mathbb{R}$. Since f is a continuous homomorphism and $G \subset S^1$ is compact and therefore closed, $f^{-1}(G)$ is a closed subgroup of $\mathbb{R}$—$f^{-1}(G)$ is a subgroup since $1 \in G \Rightarrow 0 \in f^{-1}(G)$, and if $x, y \in f^{-1}(G)$, $f(xy^{-1}) = f(x)f(y)^{-1} \in G \Rightarrow xy^{-1} \in f^{-1}(G)$). We know that $f^{-1}(1) = \mathbb{Z} \subset f^{-1}(G)$; either $f^{-1}(G) = \alpha\mathbb{Z}$ for some $\alpha \in \mathbb{R}$, in which case $1 = \alpha n$ for some $n \in \mathbb{Z} \Rightarrow f^{-1}(G) = \frac{1}{n}\mathbb{Z}$ and $G = C_n$, or $f^{-1}(G) = \mathbb{R}$, in which case $G = S^1$.

A.3. *If $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{C}[X]$, let R be the largest of the $|z_i|$ where $z_1, \ldots, z_d$ are the roots of P in $\mathbb{C}$. Prove the following inequalities:*

(1) *if $r > 0$ satisfies $r^d \geq \sum_{i=0}^{d-1} |a_i| r^i$, then $R \leq r$.*

Solution. If X is the root with largest norm $|X| = R$, then by the triangle inequality,

$$R^d = |P(X) - a_{d-1}X^{d-1} - \cdots - a_0| \leq |P(X)| + |a_{d-1}|R^{d-1} + \cdots + |a_0| = |a_{d-1}|R^{d-1} + \cdots + |a_0|$$

Suppose $r > 0$ satisfies $r^d \geq \sum_{i=0}^{d-1} |a_i| r^i$. If $r < R$, then

$$\frac{|a_{d-1}|}{r} + \cdots + \frac{|a_0|}{r^d} \leq 1 \text{ and } 1 \leq \frac{|a_{d-1}|}{R} + \cdots + \frac{|a_0|}{R^d}$$

$$\Rightarrow \frac{|a_{d-1}|}{r} + \cdots + \frac{|a_0|}{r^d} \leq \frac{|a_{d-1}|}{R} + \cdots + \frac{|a_0|}{R^d}$$

which is a contradiction since $1/r > 1/R$. Thus, $r \geq R$.

(2) $R \leq \max(1, \sum_{i=0}^{d-1} |a_i|)$ *(Montel)*

Solution. If $1 \geq \sum_{i=0}^{d-1} |a_i|$, then by (1), $R \leq 1$. If $1 < \sum_{i=0}^{d-1} |a_i|$, then if $R > \sum_{i=0}^{d-1} |a_i|$, by the above

$$1 \leq \frac{|a_{d-1}|}{R} + \cdots + \frac{|a_0|}{R^d} < \frac{|a_{d-1}|}{R} + \cdots + \frac{|a_0|}{R} < 1$$

which is a contradiction. Thus, $R \leq \sum_{i=0}^{d-1} |a_i|$ whenever $1 < \sum_{i=0}^{d-1} |a_i|$, and

$$R \leq \max\left(1, \sum_{i=0}^{d-1} |a_i|\right)$$

(3) $R \leq 1 + \max_{0 \leq k \leq d} |a_k|$ *(Cauchy)*

Solution. If $R > 1$, let $a = \max_{1 \leq i \leq d-1} |a_i|$. From (2) we have

$$R \leq |a_{d-1}| + \frac{|a_{d-2}|}{R} + \cdots + \frac{|a_0|}{R^{d-1}} \leq a \sum_{i=0}^{d-1} \left(\frac{1}{R}\right)^i = a \frac{1 - R^{-d}}{1 - R^{-1}}$$

$$\Rightarrow R - 1 \leq a - aR^{-d} \leq a \Rightarrow R \leq 1 + a$$

If $R \leq 1$, then the above inequality is satisfied trivially, so

$$R \leq 1 + \max_{0 \leq k \leq d-1} |a_k|$$

(4) $R \leq |1 - a_{d-1}| + |a_{d-1} - a_{d-2}| + \cdots + |a_1 - a_0| + |a_0|$ *(Montel)*

Solution. Let $Q(X) = (X - 1)P(X)$. The coefficients b_i of Q are

$$Q(X) = XP(X) - P(X) = X^{d+1} + (a_{d-1} - 1)X^d + \cdots + (a_0 - a_1)X - a_0$$

The roots of Q just consist of the roots of P and 1. Thus, $R \geq 1$, in which case we must have, by (2),

$$R \leq \sum_{i=1}^{d} |b_i| = |1 - a_{d-1}| + |a_{d-1} - a_{d-2}| + \cdots + |a_1 - a_0| + |a_0|$$

(5) *if $a_i \in \mathbb{R}$ for all i and $1 \geq a_{d-1} \geq a_{d-2} \geq \cdots \geq a_0 \geq 0$ then $R \leq 1$ (Kakeya)*

Solution. We have $|a_i - a_{i-1}| = a_i - a_{i-1}$ for all $0 \leq i \leq d$, with $a_d = 1$. Thus, by (4),

$$R \leq (1 - a_{d-1}) + (a_{d-1} - a_{d-2}) + \cdots + (a_1 - a_0) + a_0 = 1$$

and all of the roots of P lie on the unit disc.