Kris Harper
MATH 20700
October 27, 2008

Homework 4

**** Problem 1.** *Let (a_n) be a sequence which converges to both a and b. Then $a = b$.*

Proof. Let

$$\lim_{n\to\infty} a_n = a = b$$

and suppose $a \neq b$. Without loss of generality let $a < b$. Consider $0 < (b-a)/2$. Then there exist $N_1, N_2 \in \mathbb{N}$ such that for all $n > N_1$ we have $|a - a_n| < (b-a)/2$ and for all $n > N_2$ we have $|b - a_n| < (b-a)/2$. Let $N = \max N_1, N_2$ so that for all $n > N$ we have $a_n \in (a - (b-a)/2, a + (b-a)/2)$ and $a_n \in (b - (b-a)/2, b + (b-a)/2)$. But these sets are disjoint so this is a contradiction and $a = b$. □

**** Problem 2.** *Let $S \subseteq \mathbb{R}$ be a set. Then S is closed if and only if it contains all its accumulation points.*

Proof. Let S be closed. Then $\mathbb{R}\backslash S$ is open. Let p be an accumulation point of S such that $p \notin S$. Then $p \in \mathbb{R}\backslash S$ and so there exists $\varepsilon > 0$ such that $(p-\varepsilon, p+\varepsilon) \subseteq \mathbb{R}\backslash S$ since $\mathbb{R}\backslash S$ is open. But then

$$((p-\varepsilon, p+\varepsilon)\backslash\{p\}) \cap S = \emptyset$$

which is a contradiction since p is an accumulation point of S.

Now assume that S contains all its accumulation points. Let $x \in \mathbb{R}\backslash S$. Then x is not an accumulation point of S and so there exists some $\varepsilon > 0$ such that

$$(x-\varepsilon, x+\varepsilon) \cap S = \emptyset$$

since $x \notin S$. But then $(x-\varepsilon, x+\varepsilon) \subseteq \mathbb{R}\backslash S$ which means $\mathbb{R}\backslash S$ is open. Thus S is closed. □

**** Problem 3.** *Show that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field.*

Proof. Let $x, y, z \in \mathbb{Q}(\sqrt{2})$ such that $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ and $z = e + f\sqrt{2}$. Then

$$(x+y)+z = ((a+b\sqrt{2}) + (c+d\sqrt{2})) + (e+f\sqrt{2}) = (a+b\sqrt{2}) + ((c+d\sqrt{2}) + (e+f\sqrt{2})) = x + (y+z),$$

$$x + y = (a+b\sqrt{2}) + (c+d\sqrt{2}) = (c+d\sqrt{2}) + (a+b\sqrt{2}),$$
$$(xy)z = ((a+b\sqrt{2})(c+d\sqrt{2}))(e+f\sqrt{2}) = (a+b\sqrt{2})((c+d\sqrt{2})(e+f\sqrt{2}))$$

and

$$xy = (a+b\sqrt{2})(c+d\sqrt{2}) = (c+d\sqrt{2})(a+b\sqrt{2}) = yx$$

which means associativity and commutativity of addition and multiplication are true as they are in the reals. Let $0 = 0 + 0\sqrt{2}$. Then

$$0 + x = (0 + 0\cdot\sqrt{2}) + (a+b\sqrt{2}) = (0+a) + ((0+b)\sqrt{2}) = a + b\sqrt{2} = x.$$

Let $-x = -(a+b\sqrt{2}) = -a - b\sqrt{2}$. Then

$$-x + x = (-a - b\sqrt{2}) + (a + b\sqrt{2}) = (-a+a) + ((-b+b)\sqrt{2}) = 0 + 0\cdot\sqrt{2} = 0.$$

Let $1 = 1 + 0\cdot\sqrt{2}$. Then

$$1 \cdot x = (1 + 0\cdot\sqrt{2})(a + b\sqrt{2}) = (1\cdot a + 2\cdot 0\cdot b) + (1\cdot b + 0\cdot a)\sqrt{2} = a + b\sqrt{2} = x.$$

Let

$$x^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.$$

Then

$$x^{-1}x = \left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right)(a+b\sqrt{2}) = \left(\frac{a-b\sqrt{2}}{a^2-2b^2}\right)(a+b\sqrt{2}) = \frac{a^2-2b^2}{a^2-2b^2} = 1.$$

Finally,

$$x(y+z) = (a+b\sqrt{2})((c+d\sqrt{2})+(e+f\sqrt{2})) = (a+b\sqrt{2})(c+d\sqrt{2}) + (a+b\sqrt{2})(e+f\sqrt{2}) = xy + xz$$

from addition and multiplication in the reals. Since all the axioms are satisfied, $\mathbb{Q}(\sqrt{2})$ is a field. $\square$

** **Problem 4.** *Find* $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$.

Proof. Clearly the identity is an element of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$. Additionally, if we consider the elements $a+b\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$ with $b=0$, then we have $\mathbb{Q}$, for which the only automorphism is the identity. Thus, any element of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ must keep the rational term the same. To find any other automorphims, we consider the product

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}.$$

The term $2bd$ implies that the only other possible factorization we can have while keeping the rational terms the same is

$$(ac+2bd) - (ad+bc)\sqrt{2} = (a-b\sqrt{2})(c-d\sqrt{2}).$$

Thus, there exists an automorphism $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ such that $f(a+b\sqrt{2}) = a-b\sqrt{2}$. To show this is true consider

$$f((a+b\sqrt{2})+(c+d\sqrt{2})) = f((a+c)+(b+d)\sqrt{2}) = (a+c)-(b+d)\sqrt{2} = (a-b\sqrt{2})+(c-d\sqrt{2}) = f(a+b\sqrt{2})+f(c+d\sqrt{2})$$

and

$$f((a+b\sqrt{2})(c+d\sqrt{2})) = f((ac+2bd)+(ad+bc)\sqrt{2}) = (ac+2bd)-(ad+bc)\sqrt{2} = (a-b\sqrt{2})(c-d\sqrt{2}) = f(a+b\sqrt{2})f(c+d\sqrt{2}).$$

Thus $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{I, f\}$. $\square$

** **Problem 5.** *Find* $\mathrm{Aut}(F)$ *when* F *is a finite field.*

Proof. There exists a unique field $\mathbb{F}_{p^n}$ with p^n elements for each prime p and each natural number n, up to isomorphism. Letting $q = p^n$ consider the function $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $f(x) = x^p$. Then we see right away that

$$f(xy) = (xy)^p = x^p y^p = f(x)f(y).$$

Additionally, using the binomial theorem we have

$$f(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^p y^{p-k} = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} x^p y^{p-k}.$$

Since p is prime, it will divide $p!$, but not $j!$ for any $1 \leq j \leq p-1$. Hence, the terms for all but $k=0$ and $k=p$ will vanish from the sum and we are left with

$$f(x+y) = x^p + y^p = f(x) + f(y).$$

Hence, f is an automorphism for F_q. But then if we compose this function with itself, it will still be an automorphism, as long as $n \neq 1$. That is, we can compose it with itself n times since the order of F_{p^n} is p^n and p is a prime. Thus $\mathrm{Aut}(F_{p^n})$ is the cyclic group of order n with a generating element f. $\square$

Problem 1. *Show the following for $z = a + bi$ and $w = c + di$:*
1) We have $|z| \geq 0$ and $|z| = 0$ if and only if $z = 0$.
2) We have $|zw| = |z||w|$.
3) We have $|z + w| \leq |z| + |w|$.

Proof. 1) We have $|z| = \sqrt{a^2 + b^2} \geq 0$ since $a^2 \geq 0$ and $b^2 \geq 0$. Let $|z| = 0$. Then

$$0 = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$$

so $a^2 + b^2 = 0$ and since a^2 and b^2 are both greater than or equal to 0, they must both be 0. Then $a = b = 0$ so $z = 0$. Now suppose $z = 0$. Then

$$|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2} = \sqrt{0} = 0.$$

2) We have

$$\begin{aligned}
|zw| &= |(ac - bd) + (ad + bc)i| \\
&= \sqrt{(ac - bd)^2 + (ad + bc)^2} \\
&= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2} \\
&= \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} \\
&= \sqrt{(a^2 + b^2)(c^2 + d^2)} \\
&= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
&= |z||w|.
\end{aligned}$$

3) We have

$$b^2c^2 + a^2d^2 - 2abcd = (ad - bc)^2 \geq 0$$

so

$$b^2c^2 + a^2d^2 \geq 2abcd$$

and

$$(a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \geq a^2c^2 + 2abcd + b^2d^2 = (ac + bd)^2.$$

Then we have

$$2\sqrt{(a^2 + b^2)(c^2 + d^2)} \geq 2(ac + bd)$$

so

$$\begin{aligned}
(|z| + |w|)^2 &= (\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2})^2 \\
&= a^2 + b^2 + 2\sqrt{(a^2 + b^2)(c^2 + d^2)} + c^2 + d^2 \\
&\geq a^2 + b^2 + 2(ac + bd) + c^2 + d^2 \\
&= (a + c)^2 + (b + d)^2 \\
&= |z + w|^2.
\end{aligned}$$

Thus $|z| + |w| \geq |z + w|$. □

Problem 2. *Show that $\mathbb{C}$ is not isomorphic to $\mathbb{R}$.*

Proof. Using the same proof which shows that $\mathrm{Aut}(\mathbb{R})$ contains only the identity, we see that any homomorphism from $\mathbb{R}$ to $\mathbb{C}$ must map every real number to every real number. But then the map is not surjective. $\square$

Problem 3. *Let $S = \{B_r(z) \mid r, \mathrm{Re}(z), \mathrm{Im}(z) \in \mathbb{Q}\}$ be the set of rational balls. Then any open set, $A \subseteq \mathbb{C}$, can be written as a countable union of sets in S.*

Proof. Note that if we consider the points at which the elements in S are centered, we see that S is simply a collection of elements of $\mathbb{Q} \times \mathbb{Q}$. Thus S is countable since $\mathbb{Q}$ is countable.

Let $A \subseteq \mathbb{C}$ be open such that $z \in A$ and $z = a + bi$. There exists a ball $B_r(z) \subseteq A$ where r may be rational or not. If $r \notin \mathbb{Q}$ then consider some $r' \in \mathbb{Q}$ such that $0 < r' < r$ and then $B_{r'}(z) \subseteq B_r(z) \subseteq A$. We have $B_{r'/2}(z) \subseteq B_{r'}(z) \subseteq A$. Let $z' = a' + b'i$ where $a', b' \in \mathbb{Q}$ and

$$0 < a' < r'/(2\sqrt{2}) + a$$

and

$$0 < b' < r'/(2\sqrt{2}) + b.$$

Then

$$a' - a < r'/(2\sqrt{2})$$

and

$$b - b' < r'/(2\sqrt{2})$$

which means

$$(a - a')^2 < r'^2/8,$$
$$(b - b')^2 < r'^2/8,$$
$$(a - a')^2 + (b - b')^2 < r'^2/4$$

and $|z - z'| < r'/2$. Finally consider $z'' \in B_{r'/2}(z')$. Then $|z' - z''| < r'/2$. But also $|z - z'| < r'/2$ so we have $|z - z''| \leq |z - z'| + |z' - z''| < r'/2 + r'/2 = r'$. Thus $B_{r'/2}(z') \subseteq B_{r'}(z) \subseteq A$. Also $|z - z'| < r'/2 < r'$ so $z \in B_{r'/2}(z')$. Note that $r'/2, \mathrm{Re}(z'), \mathrm{Im}(z') \in \mathbb{Q}$. Thus for any point in A there exists a set from S which contains it and is a subset of A. But there are countably many elements of S and so a countable union of them will be equal to A. $\square$

Lemma 1. *Every sequence has an increasing or decreasing subsequence.*

Proof. Let (a_n) be a sequence. Define n to be a peak point if for all $m > n$ we have $a_m < a_n$. Suppose there are infinitely many peak points for (a_n) and let n_1 be the least peak point. We can do this because peak points are natural numbers. Define the next largest peak point to be n_2 and so on. Note that $a_{n_i} > a_{n_{i+1}}$ for all $i \in \mathbb{N}$. Thus, we have created a decreasing subsequence (a_{n_k}).

If there are no peak points then for all $n \in \mathbb{N}$, there exists $m > n$ such that $a_n \leq a_m$. Then we can make an increasing subsequence by letting $m_1 = 1$. Then there exists $m_2 > 1$ such that $a_1 \leq a_{m_2}$. Now there exists $m_3 > m_2$ such that $a_{m_2} \leq a_{m_3}$. Thus (a_{m_k}) is an increasing subsequence.

Now suppose that there are finitely many peak points for (a_n) and that there exists at least one peak point. Let $n \in \mathbb{N}$ be the largest peak point for (a_n). Then for all $m > n$ we have $a_m < a_n$, but also m is not a peak point and so there exists $m' > m$ with $a_m \leq a_{m'}$. Then create an increasing sequence as before by choosing an arbitrary $m_1 > n$. Then there exists $m_2 > m_1$ such that $a_{m_1} \leq a_{m_2}$. Thus (a_{m_k}) is an increasing subsequence. $\square$

Problem 4. *Show that every bounded sequence in $\mathbb{C}$ has a convergent subsequence.*

Proof. By Lemma 1 there exists a monotonically increasing or decreasing subsequence. But then if this subsequence is bounded it will converge. $\square$

Problem 5. *Let $S \subseteq \mathbb{C}$ be a subset. Show that every neighborhood of an accumulation point of S contains infinitely many points of S.*

Proof. Let x be an accumulation point of S and let $\varepsilon > 0$. Then there exists $x_1 \in B_\varepsilon(x) \cap S$ such that $x_1 \neq x$. Let $\varepsilon_1 = |x - x_1|/2$. Then there exists $x_2 \in B_{\varepsilon_2}(x) \cap S$ such that $x_2 \neq x$. Note that $x_2 \neq x_1$ as well. We can continue in this process so that there must be an infinite number of points in $S \cap B_\varepsilon(x)$. $\square$

Problem 6. *Show that any bounded infinite set in $\mathbb{C}$ has an accumulation point in $\mathbb{C}$.*

Proof. Let S be a bounded infinite set in $\mathbb{C}$. Create an infinite sequence $(a_n)_{n=1}^\infty$ of distinct elements of S. We can do this since S is infinite. Since S is bounded, by Problem 4 there exists a convergent subsequence $(a_{n_k})_{k=1}^\infty$. Let $\lim_{k\to\infty} a_{n_k} = a$. Then let $\varepsilon > 0$. Then there exists N such that for all $k > N$ we have $|a - a_k| < \varepsilon$. Thus there exists k such that $a_{n_k} \in B_\varepsilon(a) \cap S$. Thus a is an accumulation point for S. $\square$