University of Toronto
Faculty of Arts and Science
Solutions to Final Examination, April 2019
Duration: 3 hrs

MAT246H1S - Concepts in Abstract Mathematics

Examiners: D. Burbulla, S. Homayouni

Time: 9 AM-12 Noon, April 22, 2019. Aids permitted: None.

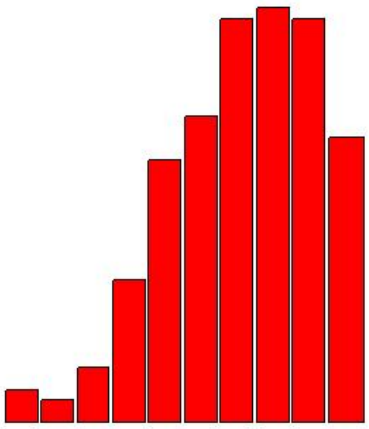
General Comments:

- Since it was only required to do 12 questions, there were many pages left blank. In particular, many students ended up skipping one or two of Questions 3, 5, 6, 7, 8, 9, 10, 11, 12 and 14. The breakdown of the number of zero's by question is:

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
3	0	28	4	99	44	86	49	55	31	35	98	5	130

- On the whole, the proof questions were done very poorly. Note that Question 12 was actually a very simple question, but many students didn't even try it.
- There were only six questions with passing averages: Questions 1, 2, 3, 9, 10 and 13. For the most part these questions were either *definitions* or *computations.* It seems as if *proofs* are still a challenge to most students.

Breakdown of Results: 216 students wrote this exam. The marks ranged from 2/140 to 129/140, and the average was 67.2/140. However, since we ended up taking your score on the exam as a mark *out of 100,* the average on the exam is in effect 67.2%. (It turned out that fifteen students had a mark greater than 100.) A histogram of the results by decade is to the right:



1. [course avg: 7.33/10] Define the following. Your definitions must be concise, accurate, complete and a *definition,* not an equivalent condition.

   (a) [2 marks] A multiplicative inverse of the natural number a, modulo m.

   Solution: a multiplicative inverse of the natural number a, modulo m, is an *integer* (accept *natural number*) x such that
   $$a\,x \equiv 1 \,(\mathrm{mod}\, m).$$

   (b) [3 marks] A tower of fields.

   Solution: a finite sequence $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_n$ of subfields of $\mathbb{R}$ such that $\mathcal{F}_0 = \mathbb{Q}$, and for each i, from 1 to n, there is a positive number $r_i \in \mathcal{F}_{i-1}$ such that $\sqrt{r_i} \notin \mathcal{F}_{i-1}$ but $\mathcal{F}_i = \mathcal{F}_{i-1}(\sqrt{r_i})$, is called a *tower of fields.* We have
   $$\mathcal{F}_0 \subset \mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_{n-1} \subset \mathcal{F}_n.$$

   (c) [1 mark] A surd.

   Solution: a *surd* is a number that is in some field that is in a tower of fields.

   (d) [1 mark] An algebraic number.

   Solution: a real number is *algebraic* if it is a root of a polynomial with integer coefficients.

   (e) [1 mark] The power set of a set $\mathcal{S}$.

   Solution: the *power set of* $\mathcal{S}$, denoted by $\mathcal{P}(\mathcal{S})$, is the set of all subsets of $\mathcal{S}$.

   (f) [1 mark] $\mathbb{Q}(\sqrt{7})$

   Solution: $\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$

   (g) [1 mark] The characteristic function $f_{\mathcal{T}}$ of a subset $\mathcal{T}$ of the set $\mathcal{S}$.

   Solution: the *characteristic* function $f_{\mathcal{T}} : \mathcal{S} \longrightarrow \{0, 1\}$ is the function defined by
   $$f_{\mathcal{T}}(s) = \begin{cases} 1, & \text{if } s \in \mathcal{T} \\ 0, & \text{if } s \notin \mathcal{T} \end{cases}$$

2. [course avg: 8.3/10]

2.(a) [3 marks] Use the Euclidean algorithm to show that 60 and 43 are relatively prime.

Solution: use the Euclidean algorithm.

$$\begin{aligned} 60 &= 1 \cdot 43 + 17 && (1)\\ 43 &= 2 \cdot 17 + 9 && (2)\\ 17 &= 1 \cdot 9 + 8 && (3)\\ 9 &= 1 \cdot 8 + 1 && (4)\\ 8 &= 8 \cdot 1 + 0 && (5) \end{aligned}$$

Thus

$$\gcd(60, 43) = 1.$$

2.(b) [4 marks] Find a solution to the congruence $43\,x \equiv 11 \pmod{60}$

Solution: use part (a) to find a multiplicative inverse of 43 modulo 60:

(4) $\Rightarrow 1 = 9 - 8$;

(3) $\Rightarrow 1 = 9 - (17 - 9) = 2 \cdot 9 - 17$;

(2) $\Rightarrow 1 = 2(43 - 2 \cdot 17) - 17 = 2 \cdot 43 - 5 \cdot 17$;

(1) $\Rightarrow 1 = 2 \cdot 43 - 5(60 - 43) = 7 \cdot 43 - 5 \cdot 60$.

Thus $7 \cdot 43 \equiv 1 \pmod{60}$, and so

$$43\,x \equiv 11 \pmod{60} \Rightarrow 7 \cdot 43\,x \equiv 7 \cdot 11 \pmod{60} \Rightarrow x \equiv 77 \equiv 17 \pmod{60},$$

and $x = 17$ is one solution to the congruence.

2.(c) [3 marks] Prove that if p is a prime number that does not divide a, then $a^{p^2} \equiv a^p \pmod{p^2}$.

Proof: since p does not divide a, p^2 and a are relatively prime. So Euler's Theorem applies.

$$\begin{aligned} \phi(p^2) = p^2 - p \quad &\Rightarrow \quad a^{p^2-p} \equiv 1 \pmod{p^2}\\ &\Rightarrow \quad a^p \cdot a^{p^2-p} \equiv a^p \pmod{p^2}\\ &\Rightarrow \quad a^{p^2} \equiv a^p \pmod{p^2} \end{aligned}$$

3. [course avg: 6.88/10]

3.(a) [4 marks] Use Wilson's Theorem to prove:

if p is a prime number greater than 3, then $2(p-3)! \equiv -1 \pmod{p}$.

Solution: Wilson's Theorem states: if p is prime then $(p-1)! + 1 \equiv 0 \pmod{p}$. We have

$$\begin{aligned} (p-1)! + 1 \equiv 0 \pmod{p} &\Rightarrow (p-1)! \equiv -1 \pmod{p} \\ (\text{for } p > 3) &\Rightarrow (p-1)(p-2)(p-3)! \equiv -1 \pmod{p} \\ &\Rightarrow (-1)(-2)(p-3)! \equiv -1 \pmod{p} \\ &\Rightarrow 2(p-3)! \equiv -1 \pmod{p} \end{aligned}$$

3.(b) [6 marks] Find the remainder when $(38! + 65^{41})^{43}$ is divided by 41.

Solution: work inside the brackets first. Observe that 41 is a prime.

- By part (a), $2 \cdot 38! \equiv -1 \pmod{41}$. Then

$$21 \cdot 2 \cdot 38! \equiv -21 \pmod{41} \Rightarrow 38! \equiv -21 \pmod{41}.$$

- Since 41 does not divide 65, Fermat's Theorem implies $65^{40} \equiv 1 \pmod{41}$. Thus

$$65^{41} \equiv 65^{40} \cdot 65 \equiv 65 \equiv 23 \pmod{41}.$$

- Therefore

$$38! + 65^{41} \equiv (-21 + 23) \equiv 2 \pmod{41}.$$

Finally, Fermat's Theorem implies $2^{40} \equiv 1 \pmod{41}$. Putting it all together

$$(38! + 65^{41})^{43} \equiv 2^{43} \equiv 2^3 \equiv 8 \pmod{41}.$$

Thus the remainder when $(38! + 65^{41})^{43}$ is divided by 41 is 8.

4. [course avg: 4.42/10]

4.(a) [4 marks] Let p be an odd prime, let n be a natural number. Prove that if

$$x^2 \equiv 1 \,(\mathrm{mod}\, p^n),$$

then $x \equiv 1 \,(\mathrm{mod}\, p^n)$ or $x \equiv -1 \,(\mathrm{mod}\, p^n)$.

Proof: we have $p^n \mid x^2 - 1 = (x-1)(x+1)$. Since p is prime, $p \mid x-1$ or $p \mid x+1$. But p can't divide *both* $x-1$ and $x+1$, for then p divides the difference,

$$p \mid x + 1 - x + 1 = 2,$$

which is impossible since p is an odd prime. Thus p divides only one of the factors $x-1$ and $x+1$. Consequently

$$p^n \mid x^2 - 1 \Rightarrow p^n \mid x-1 \text{ or } p^n \mid x+1 \Rightarrow x \equiv 1 \,(\mathrm{mod}\, p^n) \text{ or } x \equiv -1 \,(\mathrm{mod}\, p^n).$$

4.(b) [2 marks] Show that the congruence $x^2 \equiv 1 \,(\mathrm{mod}\, 8)$ has four solutions in the set $\{0, 1, 2, \ldots, 7\}$.

Solution: $x = 1, 3, 5, 7$ all satisfy $x^2 \equiv 1 \,(\mathrm{mod}\, 8)$.

4.(c) [4 marks] Show that the congruence $x^2 \equiv 1 \,(\mathrm{mod}\ 2^n)$ has four solutions in the set $\{0, 1, 2, \ldots, 2^n - 1\}$ if $n \geq 3$.

Solution: the congruence $x^2 \equiv 1 \,(\mathrm{mod}\, 2^n)$ has the four solutions

$$x = 1,\ 2^{n-1} - 1,\ 2^{n-1} + 1 \text{ or } 2^n - 1,$$

since $1^2 = 1$,

$$(2^n - 1)^2 \equiv (0-1)^2 \ \equiv 1 \ (\mathrm{mod}\, 2^n),$$

and

$$(2^{n-1} \pm 1)^2 \equiv 2^{2n-2} \pm 2 \cdot 2^{n-1} + 1 \equiv 2^n \cdot 2^{n-2} \pm 2^n + 1 \equiv 0 + 0 + 1 \equiv 1 \,(\mathrm{mod}\, 2^n).$$

5. [course average: 2.67/10]

5.(a) [4 marks] Given a polynomial $p(z)$ with real coefficients and a complex root $z_0 = a + bi$ of $p(z)$, prove that $z^2 - 2az + a^2 + b^2$ is a factor of $p(z)$.

Solution: since the coefficients of p are real, we know that $\overline{z_0} = a - bi$ is also a root of $p(z)$. Thus

$$(z - z_0)(z - \overline{z_0}) = (z - (a + bi))(z - (a - bi)) =$$

$$z^2 - (a + bi)z - (a - bi)z + (a + bi)(a - bi) = z^2 - 2a\,z + a^2 + b^2$$

is a factor of $p(z)$.

5.(b) [6 marks] Explain why any non-constant polynomial with real coefficients can be factored into a product of polynomials of degrees one or two (i.e. linear or quadratic factors) with real coefficients.

Solution: let $p(z)$ be a polynomial of degree n and suppose the coefficients of $p(z)$ are all real numbers. We know that $p(z)$ can be factored as

$$p(z) = c(z - z_1)(z - z_2)\cdots(z - z_n),$$

for some real constant c and n complex numbers, $z_1, z_2, \ldots, z_n$. Since the coefficients of $p(z)$ are all real, the complex conjugates $\overline{z_1}, \overline{z_2}, \ldots, \overline{z_n}$ are also roots of $p(z)$. Thus the roots of $p(z)$ are real numbers or come in pairs of complex conjugates. Suppose the roots $z_1, z_2, \ldots, z_j$ are all real, and the remaining non-real roots are

$$z_{j+1}, \overline{z_{j+1}}, z_{j+2}, \overline{z_{j+2}}, \ldots, z_{j+k}, \overline{z_{j+k}},$$

where $n = j + 2k$. For each pair of roots $z_{j+m} = a_m + b_m, \overline{z_{j+m}} = a_m - b_m\,i,\ 1 \le m \le k$, part (a) implies

$$(z - z_{j+m})(z - \overline{z_{j+m}}) = z^2 - 2a_m z + a_m^2 + b_m^2$$

is a quadratic factor of $p(z)$. Thus

$$p(z) = c\underbrace{(z - z_1)(z - z_2)\cdots(z - z_j)}_{j\ \ linear factors}\underbrace{(z^2 - 2a_1 z + a_1^2 + b_1^2)(z^2 - 2a_2 z + a_2^2 + b_2^2)\cdots(z^2 - 2a_k z + a_k^2 + b_k^2)}_{k\ \ quadratic factors},$$

all with real coefficients.

6. [course avg: 4.67/10]

6. For each of the following pairs of sets define a bijection from one set to the other, and verify that it is a bijection.

   (a) [5 marks] $\{0,1\}^S$ and $\mathcal{P}(S)$ for any set S. (Recall: A^B is set of all functions $f : B \longrightarrow A$.)

   Solution: we can make use of the characteristic functions, $f_T : S \longrightarrow \{0,1\}$, defined by

$$f_T(s) = \begin{cases} 1, & \text{if } s \in T \\ 0, & \text{if } s \notin T \end{cases},$$

   where $T \subset S$. For T a non-empty subset of S, define $G : \mathcal{P}(S) \longrightarrow \{0,1\}^S$ by $G(T) = f_T$; if $T = \emptyset$, define $G(T)$ to be the zero-map: $(G(\emptyset))(s) = 0$, for all $s \in S$. Check that G is a bijection.

   - G is one-to-one:

$$G(T) = G(U) \Rightarrow f_T(s) = f_U(s) \text{ for all } s \in S \Rightarrow s \in T \text{ if and only if } s \in U \Rightarrow T = U$$

   - G is onto: if $f \in \{0,1\}^S$, let $T = \{s \in S \mid f(s) = 1\}$. Then $G(T) = f_T = f$.

   (b) [5 marks] $[0,1] \times [0,1] \times [0,1]$ and $[0,1]$.

   Solution: if $(x, y, z) \in [0,1] \times [0,1] \times [0,1]$, write each of x, y, z as an infinite decimal:

$$x = 0.a_1a_2 \ldots a_i \ldots, \; y = 0.b_1b_2 \ldots b_i \ldots \text{ and } z = 0.c_1c_2 \ldots c_i \ldots.$$

   Define $f : [0,1] \times [0,1] \times [0,1] \longrightarrow [0,1]$ by

$$f(\,(x, y, z)\,) = 0.a_1b_1c_1a_2b_2c_2 \ldots a_ib_ic_i \ldots$$

   Check that f is a bijection.

   1. f is onto: if $w = 0.d_1d_2d_3 \ldots d_id_{i+1}d_{i+2} \ldots$, let

$$x = 0.d_1d_4d_7 \ldots d_{3j+1} \ldots, \; y = 0.d_2d_5d_8 \ldots d_{3j+2} \ldots, \; z = 0.d_3d_6d_9 \ldots d_{3j} \ldots$$

      for $j = 0, 1, 2, \ldots$. Then $f((x, y, z)) = w$.
   2. f is one-to-one: suppose $f((x, y, z)) = f((x', y', z'))$. Then

$$0.a_1b_1c_1a_2b_2c_2 \ldots a_ib_ic_i \cdots = 0.a'_1b'_1c'_1a'_2b'_2c'_2 \ldots a'_ib'_ic'_i \cdots \Rightarrow a_i = a'_i, \; b_i = b'_i, \; c_i = c'_i,$$

      which means $x = x', y = y', z = z'$. Hence $(x, y, z) = (x', y', z')$.

7. [course avg: 2.0/10] Prove the following:

(a) [6 marks] If $\mathcal{S}$ and $\mathcal{T}$ are disjoint sets with $|\mathcal{S}| = c$ and $|\mathcal{S}| \leq |\mathcal{T}|$, then $|\mathcal{S} \cup \mathcal{T}| = |\mathcal{T}|$.

Proof: we shall construct a bijection between $\mathcal{S} \cup \mathcal{T}$ and $\mathcal{T}$. Since $|\mathcal{S}| \leq |\mathcal{T}|$, there is a subset $\mathcal{U} \subset \mathcal{T}$ such that $|\mathcal{U}| = c$. Since all of $[0,1], [2,3]$ and $[0,1] \cup [2,3]$ have cardinality c, there are bijections f, g, h such that

$$f : \mathcal{S} \longrightarrow [0,1],\ g : \mathcal{U} \longrightarrow [2,3],\ h : [0,1] \cup [2,3] \longrightarrow \mathcal{U}.$$

Define $F : \mathcal{S} \cup \mathcal{T} \longrightarrow \mathcal{T}$ by

$$F(x) = \begin{cases} h(f(x)) & , \quad \text{if } x \in \mathcal{S} \\ h(g(x)) & , \quad \text{if } x \in \mathcal{U} \\ x & , \quad \text{if } x \in \mathcal{T} \setminus \mathcal{U} \end{cases}$$

Then F is a bijection.

- F is one-to-one: suppose $F(x) = F(y)$. Then (1) $F(x)$ and $F(y)$ are both in $\mathcal{T} \setminus \mathcal{U}$, or (2) $F(x)$ and $F(y)$ are both in $\mathcal{U}$, since $\mathcal{U}$ and $\mathcal{T} \setminus \mathcal{U}$ are disjoint. We take each case separately.
  1. In this case, $F(x) = x$ and $F(y) = y$, so $x = y$.
  2. In this case, there are two distinct possibilities:
     (a) $h(f(x)) = h(f(y))$ or $h(g(x)) = h(g(y))$, and either way $x = y$, since f, g, h are all one-to-one.
     (b) $h(f(x)) = h(g(y))$ [or similarly $h(g(x)) = h(f(y))$.] Then $f(x) = g(y)$, since h is one-to-one. But $f(x)$ can't equal $g(y)$, since $f(x) \in [0,1]$ and $g(y) \in [2,3]$. Thus this case is impossible.
- F is onto: if $t \in \mathcal{T} \setminus \mathcal{U}$, then $F(t) = t$. If $u \in \mathcal{U}$, then $h^{-1}(u) \in [0,1] \cup [2,3]$.
  1. If $h^{-1}(u) \in [0,1]$, then $f^{-1}(h^{-1}(u)) \in \mathcal{S}$ and $F(f^{-1}(h^{-1}(u))) = h(f(f^{-1}(h^{-1}(u)))) = u$.
  2. If $h^{-1}(u) \in [2,3]$, then $g^{-1}(h^{-1}(u)) \in \mathcal{U}$ and $F(g^{-1}(h^{-1}(u))) = h(g(g^{-1}(h^{-1}(u)))) = u$.

(b)[4 marks] There is no set with a countably infinite power set.

Proof: we consider two cases.

1. If S is a finite set, then $|S| = n$, for some $n \in \mathbb{N}$, and
$$|\mathcal{P}(S)| = 2^n < \aleph_0,$$
so the power set is finite.
2. If S is infinite, then $|S| < |\mathcal{P}(S)|$, which is a Theorem in the book. But if S is infinite another Theorem in the book states that $|S| \geq \aleph_0$, which is the smallest infinite cardinal number. Together, these two inequalities imply
$$|\mathcal{P}(S)| > \aleph_0.$$
Hence the power set is uncountably infinite in this case.

.

8. [course avg: 2.37/10]

8.(a) [5 marks] Suppose $h : \mathcal{T} \longrightarrow \mathcal{S}$ is onto and $g : \mathcal{U} \longrightarrow \mathcal{W}$ is one to one. Use these functions to show that

$$|\mathcal{U}^{\mathcal{S}}| \leq |\mathcal{W}^{\mathcal{T}}|.$$

Solution: define $F : \mathcal{U}^{\mathcal{S}} \longrightarrow \mathcal{W}^{\mathcal{T}}$ by $F(f) = g \circ f \circ h$. That is,

$$(F(f))(t) = g(f(h(t))).$$

Then $F(f) : \mathcal{T} \longrightarrow \mathcal{W}$ since $h(t) \in \mathcal{S}, f(h(t)) \in \mathcal{U}$ and $g(f(h(t))) \in \mathcal{W}$. We claim F is one-to-one. Suppose $F(f_1) = F(f_2)$ for functions $f_1, f_2 \in \mathcal{U}^{\mathcal{S}}$. We need to show $f_1 = f_2$. To this end, let $s \in \mathcal{S}$. We need to show $f_1(s) = f_2(s)$. Since h is onto, there is a $t \in \mathcal{T}$ such that $h(t) = s$. Then

$$\begin{aligned} F(f_1) = F(f_2) &\Rightarrow (F(f_1))(t) = (F(f_2))(t) \\ &\Rightarrow g(f_1(h(t))) = g(f_2(h(t))) \\ &\Rightarrow g(f_1(s)) = g(f_2(s)) \\ &\Rightarrow f_1(s) = f_2(s), \text{ since } g \text{ is one-to-one} \\ &\Rightarrow f_1 = f_2, \text{ since } s \text{ is any element of } \mathcal{S} \end{aligned}$$

Thus F is one-to-one, which means $|\mathcal{U}^{\mathcal{S}}| \leq |\mathcal{W}^{\mathcal{T}}|$.

8.(b) [5 marks] Given an infinite set A that is a subset of $\mathbb{N}$ define a bijection $g : \mathbb{N} \longrightarrow A$.

Solution 1: A is an infinite subset of $\mathbb{N}$, so

$$\aleph_0 \leq |A| \leq |\mathbb{N}| = \aleph_0.$$

By the Cantor-Bernstein Theorem, $|A| = \aleph_0$. That is, A is countably infinite so we can list the elements of A :

$$A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\}.$$

Define $g : \mathbb{N} \longrightarrow A$ by

$$g(n) = a_n.$$

Then (clearly) g is a bijection:

- one-to-one: $g(n) = g(m) \Rightarrow a_n = a_m \Rightarrow n = m$
- onto: if $a_n \in A$, then $g(n) = a_n$.

Solution 2: define $g : \mathbb{N} \longrightarrow A$ recursively by

- $g(1)$ is the least element of A,
- $g(n+1)$ is the least element of $A \setminus \{g(1), g(2), \ldots, g(n)\}$.

Then g is well-defined by the Well-Ordering Principle and the fact that A is infinite. Then you need to check that g is one-to-one and onto.

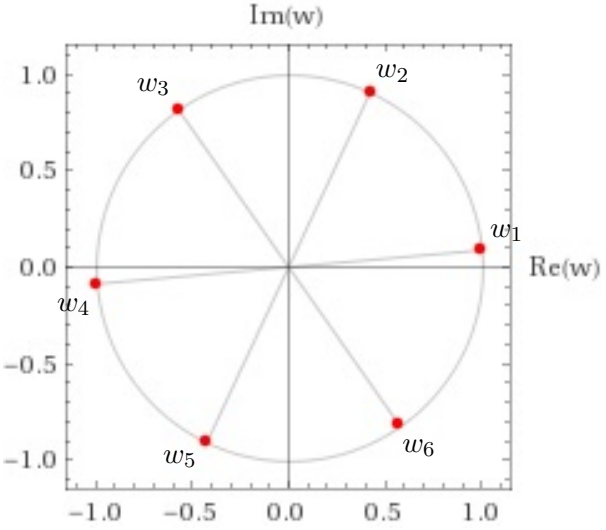
9. [course avg: 5.38/10] Find all the solutions $z \in \mathbb{C}$ to the equation $2(z+i)^6 - i = \sqrt{3}$, and plot them in the complex plane.

Solution: let $w = z + i$. Then

$$w^6 = \frac{\sqrt{3}}{2} + \frac{1}{2}i = \cos 30^\circ + i \sin 30^\circ.$$

Let $w = r(\cos\theta + i \sin\theta)$. Then by De Moivre's Theorem, $w^6 = r^6(\cos(6\theta) + i\sin(6\theta))$. Then

$$\begin{aligned} w^6 = \cos 30^\circ + i \sin 30^\circ &\Rightarrow r^6(\cos(6\theta) + i\sin(6\theta)) = \cos 30^\circ + i \sin 30^\circ \\ &\Rightarrow r^6 = 1 \text{ and } 6\theta = 30^\circ + 360^\circ k \\ &\Rightarrow r = 1 \text{ and } \theta = 5^\circ + 60^\circ k \\ &\Rightarrow \theta = 5^\circ,\ 65^\circ,\ 125^\circ,\ 185^\circ,\ 245^\circ \text{ or } 305^\circ \end{aligned}$$



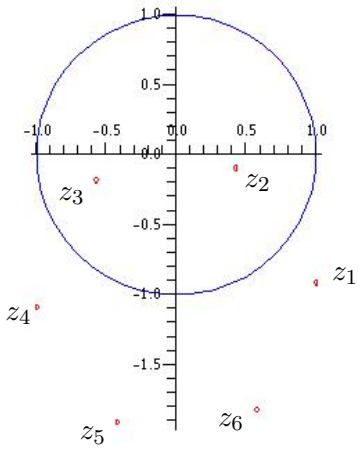
Thus the six distinct values for w are

$$w_1 = \cos 5^\circ + i \sin 5^\circ, w_2 = \cos 65^\circ + i \sin 65^\circ,$$

$$w_3 = \cos 125^\circ + i \sin 125^\circ, w_4 = \cos 185^\circ + i \sin 185^\circ,$$

$$w_5 = \cos 245^\circ + i \sin 245^\circ, w_6 = \cos 305^\circ + i \sin 305^\circ.$$

The figure to the left shows how the six distinct values of w are symmetrically distributed around the origin of the complex plane. However $z = w - i$; so the distribution of the six distinct values of z are obtained from the values of w by shifting them all down by 1 unit. See the figure below, where the blue circle is the unit circle, $|z| = 1$, and the red points are the six solutions:



10. [course avg: 7.13/10]

10.(a) [5 marks] Show that the equation $x^3 - x + \sqrt{3} = 0$ has no constructible root by first making a suitable substitution.

Solution: if x is constructible, so is $\dfrac{x}{\sqrt{3}}$, since the constructible numbers form a field. Let

$$y = \frac{x}{\sqrt{3}} \Leftrightarrow x = y\sqrt{3}.$$

So if the given equation has a constructible root so do the equations

$$(y\sqrt{3})^3 - (y\sqrt{3}) + \sqrt{3} = 0 \Leftrightarrow \sqrt{3}(3y^3) - \sqrt{3}y + \sqrt{3} = 0 \Leftrightarrow 3y^3 - y + 1 = 0.$$

This last equation has integer coefficients, so by a Theorem in the book it should have a rational root, but it doesn't. By the Rational Roots Theorem the only possible rational roots of the polynomial $q(y) = 3y^3 - y + 1$ are

$$y = \pm 1,\ \pm\frac{1}{3},$$

none of which work:

- $q(1) = 3 - 1 + 1 = 3 \neq 0$
- $q(-1) = -3 + 1 + 1 = -1 \neq 0$
- $q(1/3) = 1/9 - 1/3 + 1 = 7/9 \neq 0$
- $q(-1/3) = -1/9 + 1/3 + 1 = 11/9 \neq 0$

10.(b) [5 marks] Does the polynomial $x^9 - x^6 + 3x^3 - 2$ have a constructible root?

Solution: if x is constructible, so is $y = x^3$, since the constructible numbers form a field.

$$x^9 - x^6 + 3x^3 - 2 = 0 \Leftrightarrow y^3 - y^2 + 3y - 2 = 0.$$

That is, if the 9-th degree polynomial in x has a constructible root, so does the cubic polynomial in y. Let $p(y) = y^3 - y^2 + 3y - 2$. By a Theorem in the book: if $p(y)$ has a constructible root it must have a rational root. By the Rational Roots Theorem, the only possibilities are

$$y = \pm 1,\ \pm 2,$$

none of which work:

- $p(1) = 1 - 1 + 3 - 2 = 1 \neq 0$
- $p(-1) = -1 - 1 - 3 - 2 < 0$
- $p(2) = 8 - 4 + 6 - 2 = 6 \neq 0$
- $p(-2) = -8 - 4 - 6 - 2 < 0$

11. [course avg: 4.84/10] Let $\{a_n : n \in \mathbb{N}\}$ be a sequence of real numbers satisfying

$$a_1 = 1 \text{ and } a_n = \sqrt{\frac{\sin\left(\frac{\pi}{2^n}\right)}{1 + a_{n-1}^3}}, \text{ for } n \geq 2.$$

Prove that a_n is constructible for all natural numbers n.

Proof: by induction on n. If $n = 1$, then $a_1 = 1$, which is constructible. Now assume a_{n-1} is constructible for $n > 1$. We need to show a_n is also constructible. If a_{n-1} is constructible, then so are

$$a_{n-1}^3, 1 + a_{n-1}^3 \text{ and } \frac{1}{1 + a_{n-1}^3},$$

since the set of constructible numbers is a field. (And by definition, $a_n \geq 0$ for all n, so $1 + a_{n-1}^3 \neq 0$.) Since the square root of a constructible number is also constructible, a_n will be constructible if

$$\sin\left(\frac{\pi}{2^n}\right)$$

is constructible. To prove this we can use a separate induction proof:

- $\sin\left(\frac{\pi}{2^1}\right) = 1$ is constructible.
- If $\sin\left(\frac{\pi}{2^{n-1}}\right)$ is constructible, then so is $\cos\left(\frac{\pi}{2^{n-1}}\right) = \sqrt{1 - \sin^2\left(\frac{\pi}{2^{n-1}}\right)}$. This means the angle measured by $\pi/2^{n-1}$ radians is constructible. Then, by a theorem in the book, this angle can be bisected by straight edge and compass, so

  $$\frac{1}{2}\left(\frac{\pi}{2^{n-1}}\right) = \frac{\pi}{2^n}$$

  is also a constructible angle. But this means that $\cos\left(\frac{\pi}{2^n}\right)$, and consequently $\sin\left(\frac{\pi}{2^n}\right)$, are both constructible numbers.
- Thus $\sin\left(\frac{\pi}{2^n}\right)$ is constructible for all $n \in \mathbb{N}$.

Putting it altogether, a_n is constructible, which competes the proof.

12. [course avg: 2.99/10] According to the Gauss-Wantzel Theorem a regular n-gon is constructible if and only if $\phi(n)$ is a power of 2, where ϕ is the Euler phi function. Make use of this result to prove the following:

(a) [4 marks] If $n = p^k$ for odd prime p and the regular n-gon is constructible, then $k = 1$ and $p - 1$ is a power of 2. (Such primes are called Fermat primes. Only five are known: 3, 5, 17, 257 and 65537.)

Proof: $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. For this to be a power of 2, $k-1$ must be zero—otherwise $\phi(p^k)$ would have an odd factor—and for some natural number m,

$$p - 1 = 2^m.$$

(b) [4 marks] A regular m-gon is constructible if m is a product of distinct Fermat primes and any power of 2.

Proof: let $F_1, F_2, \ldots, F_j$ be distinct Fermat primes, and suppose $m = F_1 \cdot F_2 \cdots F_j \cdot 2^k$. Then

$$\begin{aligned} \phi(m) &= \phi(F_1 \cdot F_2 \cdots F_j \cdot 2^k) \\ &= \phi(F_1)\,\phi(F_2) \cdots \phi(F_j) \cdot \phi(2^k) \\ &= (F_1 - 1)(F_2 - 1) \cdots (F_j - 1) \cdot (2^k - 2^{k-1}) \\ &= 2^{n_1} \cdot 2^{n_2} \cdots 2^{n_j} \cdot 2^{k-1} \cdot 1, \end{aligned}$$

which is a power of 2.

(c) [2 marks] Regular $255, 256$ and 257-gons are all constructible, but a regular 258-gon is not.

Solution: we have

- $255 = 3 \cdot 5 \cdot 17$, which is a product of distinct Fermat primes, so a 255-gon is constructible.
- $256 = 2^7$, which is a power of 2, so a 256-gon is constructible.
- 257 is a Fermat prime, so a 257-gon is constructible.
- $258 = 2 \cdot 3 \cdot 43$, so $\phi(258) = \phi(2)\phi(3)\phi(43) = 1 \cdot 2 \cdot 42 = 84$, which is not a power of 2. Thus a 258-gon is not constructible.

13. [course avg: 6.47/10]

13.(a) [6 marks] Determine whether each of the following is a tower of fields:

(*i*) $\mathbb{Q} \subset \mathbb{Q}(\pi)$

Solution: not a tower of fields because π is not algebraic, so not a surd.

(*ii*) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$

Solution: not a tower of fields because $\sqrt[3]{2}$ is not constructible. If it were, $x^3 - 2 = 0$ would have a rational root, but it doesn't, by the Rational Roots Theorem.

(*iii*) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$ (where p is a prime number)

Solution: is a tower of fields since $\sqrt{p} \notin \mathbb{Q}$, and thus $\mathbb{Q}(\sqrt{p})$ is a field extension of $\mathbb{Q}$.

(*iv*) $\mathbb{Q} \subset \mathbb{Q}(3^{1/4})$

Solution: not a tower of fields: $3^{1/4} = \sqrt{\sqrt{3}}$, but $\sqrt{3} \notin \mathbb{Q}$. Aside: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset (\mathbb{Q}(\sqrt{3}))(\sqrt{\sqrt{3}})$ is a tower of fields.

13.(b) [4 marks] Determine whether $\sqrt[3]{6\sqrt{3} - 5}$ is constructible or not. Justify your answer.

Solution: mimic the solution to the last question on Problem Set 4. Let $x = \sqrt[3]{6\sqrt{3} - 5}$. Then

$$x^3 = 6\sqrt{3} - 5 \Leftrightarrow x^3 + 5 - 6\sqrt{3} = 0.$$

Let $p(x) = x^3 + 5 - 6\sqrt{3}$. Assume $p(x)$ has a constructible root. Then $p(x)$ has a root $r = a + b\sqrt{3}$ in $\mathbb{Q}(\sqrt{3})$. Thus

$$r^3 = -5 + 6\sqrt{3}.$$

Additionally, $\bar{r} = a - b\sqrt{3}$ is a root of the polynomial $x^3 + 5 + 6\sqrt{3}$, so

$$(\bar{r})^3 = -5 - 6\sqrt{3}.$$

Therefore

$$(r\,\bar{r})^3 = (-5 + 6\sqrt{3})(-5 - 6\sqrt{3}) = -83 \Rightarrow r\,\bar{r} = -\sqrt[3]{83}.$$

On the other hand,

$$r\,\bar{r} = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2.$$

Comparing these two results gives

$$\sqrt[3]{83} = 3b^2 - a^2 \in \mathbb{Q},$$

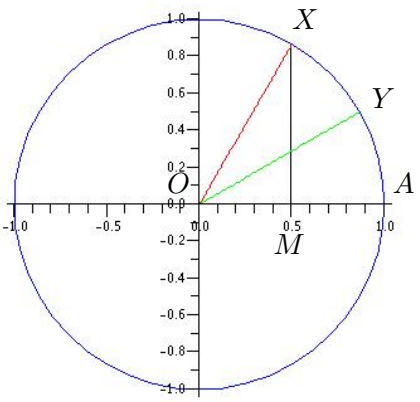
which is a contradiction, since 83 is a prime number.

14. [course avg: 1.72/10]

14.(a) [6 marks] Describe straight-edge and compass constructions you could perform to construct the following angles. (Assume only that the points $(0,0)$ and $(1,0)$ have been labelled in the surd plane. You do not actually have to perform the constructions, but you should use diagrams to illustrate your solution.)

(i) $30°$

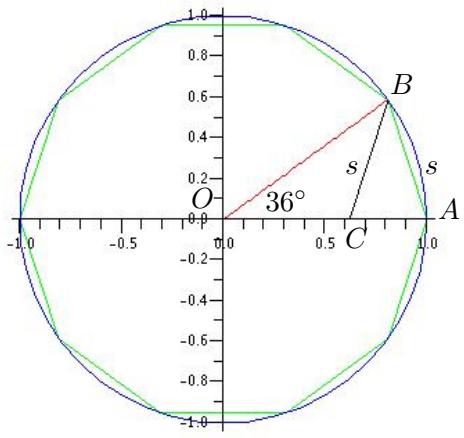
Solution: use the fact that $\cos 60° = 0.5$



1. Construct the circle with radius 1, centre at O.
2. Construct the perpendicular bisector of the line segment OA. (black line MX)
3. Label the point of intersection of the bisector and the circle X.
4. The angle $< OXM$ is $30°$, so you are done.
5. OR: The angle $< XOA$ is $60°$. (red line)
6. Bisect the angle $< XOA$.
7. The angle $< YOA$ is $30°$. (green line)

(ii) $36°$

Solution: in the textbook this construction is part of constructing a regular 10-gon; see Figure. In particular, if the line segment AB, with length s, is one side of the 10-gon, and central angle $< BOA$ is to be $36°$, then the isosceles triangle ΔBOA has angles of $72°$ at B and at A. Bisecting the angle $< OBA$ gives angle $< CBA$, which is also $36°$. Since ΔOBC is an isosceles triangle, the length of OC is s. And: $\Delta OBA \sim \Delta BAC$, by AAA. Thus $s : 1$ as $1 - s : s$. This means



Figure

$$s^2 = 1 - s \Leftrightarrow s^2 + s - 1 = 0.$$

However, to **construct** an angle of $36°$ all you have to take from all of this is the fact that

$$s = \frac{-1 + \sqrt{5}}{2}$$

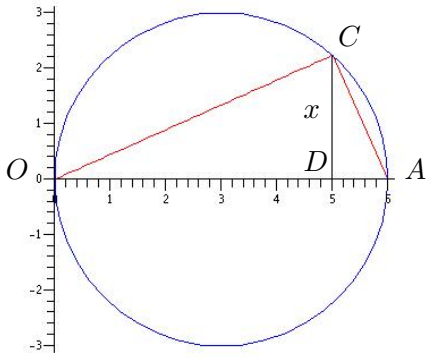
or, by the cosine law, that

$$\cos 36° = \frac{1 + \sqrt{5}}{4}.$$

Thus it all boils down to constructing $\sqrt{5}$. The construction of $\sqrt{5}$ is described on the next page:

The **easiest** way to construct $\sqrt{5}$ is to construct a line segment of length 2 perpendicular to the line segment from $(0,0)$ to $(1,0)$, with the right angle at $(1,0)$. The length of the line segment from $(0,0)$ to $(1,2)$ is $\sqrt{5}$, by the Pythagorean Theorem.

The **general** way to construct $\sqrt{a}$, as outlined in the text, applied to $a = 5$ is:



1. With compass radius at 1, construct the points $(2,0)$ to $(6,0)$, by repeatedly moving 1 unit to the right.
2. Draw the circle of radius 3, centred at $(3,0)$.
3. Construct the perpendicular bisector of the segment from $(4,0)$ to $(6,0)$ at D, the point $(5,0)$. Label the intersection of the bisector and the circle C.
4. Draw the lines OC and CA; $< OCA$ is a right angle.
5. $\Delta COD \sim \Delta DCA$, by AAA.
6. Let x be the length of CD.
7. By similar triangles, $\dfrac{5}{x} = \dfrac{x}{1} \Leftrightarrow x^2 = 5$.
8. Thus the length of CD is $\sqrt{5}$.

Finally, having constructed $\sqrt{5}$ you can construct the point

$$\left(\frac{1+\sqrt{5}}{4}, 0\right) = (\cos 36^\circ, 0)$$

on the horizontal axis. From this point, draw a perpendicular up to the unit circle centred at the origin. Then the line segment from the origin to the intersection point makes an angle of 36° with the x-axis.

14.(b) [4 marks] Outline the proof of Theorem 12.4.13, which states: if n is a natural number, then an angle of n degrees is constructible if and only if n is a multiple of 3.

Solution: by part (a), we know angles of 36° and 30° are constructible. If you construct both of these angles on a common line segment, then the angle between them is 6° and has thus been constructed. Now bisect the angle of 6° to construct an angle of 3°. By duplicating an angle of 3 degrees k times you can construct any angle of $n = 3k$ degrees.

You cannot go smaller than 3° though. If you could construct an angle of 1° then twenty duplications of it would give you an angle of 20°, which we proved in class is not constructible. And if you could construct an angle of 2°, then constructing angles of 3° and 2° on a common line segment would permit you to construct an angle of 1°, which as we've just seen is impossible. (Or, if you could construct an angle of 2° then ten duplications of it would give you angle of 20°, also impossible.)