

Math 558 Spring 2009

Answers to selected homework problems

Selected answers to homework #1

2. $x = -\sqrt[3]{-1} - \sqrt[3]{1} = -2$

3. $\frac{1}{r} + \frac{1}{s} = \frac{r+s}{rs} = \frac{-b/a}{c/a} = -\frac{b}{c}$

5. $\alpha(\alpha - 4) \geq 0$; so $\alpha \geq 0$ and $\alpha \geq 4$, hence $\alpha \geq 4$; or $\alpha \leq 0$ and $\alpha \leq 4$, hence $\alpha \leq 0$. Answer: all $\alpha \geq 4$ or ≤ 0 .

6. (a) $\frac{1}{2}, 2 - \frac{\sqrt{3}}{2} \in \mathbb{S}$; $1 + \pi\sqrt{3}, \sqrt{5} \notin \mathbb{S}$.

(b) $s + t \in \mathbb{S}$, as is $s - t$. Proof (which you didn't have to give): Let $a, b, c, d \in \mathbb{Q}$. $(a + b\sqrt{3}) \pm (c + d\sqrt{3}) = (a \pm c) + (b \pm d)\sqrt{3}$; since \mathbb{Q} is closed under addition, $a \pm c, b \pm d \in \mathbb{Q}$.

7. $zw = 8(\cos \frac{15\pi}{6} + i \sin \frac{15\pi}{6})$. And $\frac{15\pi}{6} = \frac{5\pi}{2} = \frac{\pi}{2} + 2\pi$.

So $zw = 8(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}) = 8i$.

8. (c) Note that $|1 + i| = \sqrt{2}$ and $\arg(1 + i) = \frac{\pi}{4}$.

$$\frac{(1+i)^{39}}{1-i} = \frac{(1+i)^{39}}{1-i} \cdot \frac{1+i}{1+i} = \frac{1}{2}(1+i)^{40} = \frac{1}{2} \cdot (\sqrt{2})^{40} (\cos(40 \cdot \frac{\pi}{4}) + i \sin(40 \cdot \frac{\pi}{4})) = 2^{19}(\cos 0 + i \sin 0) = 2^{19}.$$

9. If $|z| = 1$ then $|z^n| = |z|^n = 1$.

10. Clever way: $\frac{1-z}{1+z} = \frac{1}{(1+z)/(1-z)}$. We already know from class that if $|z| = 1$ then $\frac{1+z}{1-z}$ is on the y -axis, i.e., there is $r \in \mathbb{R}$ with $\frac{1+z}{1-z} = ri$. So $\frac{1-z}{1+z} = \frac{1}{ri} = \frac{1}{r} \cdot \frac{1}{i} = -\frac{1}{r}i$, which is on the y -axis.

Grinding way: Let $z = a + bi$ where $a^2 + b^2 = 1$. So

$$\frac{1-z}{1+z} = \frac{(1-a) - bi}{(1+a) + bi} = \frac{(1-a) - bi}{(1+a) + bi} \cdot \frac{(1+a) - bi}{(1+a) - bi} = \frac{1 - a^2 - b^2 - 2b(1+a)i}{1 + 2a + a^2 + b^2} = \dots - \frac{b}{1+a}i$$

which is on the y -axis.

Selected answers to homework #2

1. (a) $2^{1/8}(\cos \frac{3\pi}{8} + i \sin \frac{3\pi}{8})$; $2^{1/8}(\cos(\frac{3\pi}{8} + \frac{\pi}{2}) + i \sin(\frac{3\pi}{8} + \frac{\pi}{2}))$; $2^{1/8}(\cos(\frac{3\pi}{8} + \pi) + i \sin(\frac{3\pi}{8} + \pi))$; $2^{1/8}(\cos(\frac{3\pi}{8} + \frac{3\pi}{2}) + i \sin(\frac{3\pi}{8} + \frac{3\pi}{2}))$ or the equivalent.

2. $1 + \omega^2 = -\omega$; $(-\omega)^{16} = (-1)^{16}(\omega^{16}) = (\omega)^{15}(\omega) = \omega$.

Comments: A number of people complicated things by writing out ω in polar form — why bother? Also, a few people wrote (with minor variations) “ $1 + \omega + \omega^2 = 0$, therefore ω is a cube root of unity, so $\omega = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$.” No! You’ve got it backwards. *Because* ω is a principal root of unity, $1 + \omega + \omega^2 = 0$. We didn’t prove that if $1 + x + x^2 = 0$ then x is a cube root of unity, much less the one with smallest non-zero argument. [I should have taken a point off, but it’s early in the semester so I didn’t.]

3. $\bar{z}^n = 1$. Why? Let $z = \cos \theta + i \sin \theta$ where θ is some $\frac{2k\pi}{n}$, $0 \leq k < n$. Then $\bar{z} = \cos \theta - i \sin \theta = \cos(-\theta) + i \sin(-\theta) = \cos(2n\pi - \frac{2k\pi}{n}) + i \sin(2n\pi - \frac{2k\pi}{n}) = \cos(\frac{2(n-k)\pi}{n}) + i \sin(\frac{2(n-k)\pi}{n})$ which is an n^{th} root of unity, so $\bar{z}^n = 1$.

4. Recall the theorem that $\sum \sqrt[n]{1} = 0$. I.e., $\sum_{k=1}^n (\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}) = 0 + 0 \cdot i$. So $\sum_{k=1}^n \cos \frac{2k\pi}{n} = 0$ and $\sum_{k=1}^n \sin \frac{2k\pi}{n} = 0$.

5. $\zeta^n = 1$ iff $1 = \frac{1}{\zeta^n}$. But $\frac{1}{\zeta^n} = (\frac{1}{\zeta})^n$. So $\zeta^n = 1$ iff $(\frac{1}{\zeta})^n = 1$.

Hence the smallest number n for which $\zeta^n = 1$ is also the smallest number n for which $(\frac{1}{\zeta})^n = 1$.

Comments: You can also do this correctly by using the two-step definition of order, which is what several people did. Some of those people wrote “if $(\frac{1}{\zeta})^k = 1$ then $\zeta^k = 1$ ” without explaining why. It takes a second, but you need to do it.

Here’s another clever proof: If $|z| = 1$ then $z\bar{z} = 1$ (check it out, using $z = a+bi$ and $a^2+b^2 = 1$)¹ so $\frac{1}{z} = \bar{z}$ and it’s a short step from problem 3 (which you should do) to show that $o(z) = o(\bar{z})$.

Other proofs are possible, for example, you can show that $o(\zeta) \leq o(\frac{1}{\zeta}) \leq o(\zeta)$; or you can show that $o(\zeta)$ divides $o(\frac{1}{\zeta})$ which divides $o(\zeta)$. And so on.

6. $|\zeta| = 1$ and $\arg(\zeta) = \frac{\pi}{4} = \frac{2\pi}{8}$. So $o(\zeta) = 8$.

7. (a) If z, w are roots of unity, then $z^m = 1$ for some m and $w^n = 1$ for some n , hence $(zw)^{mn} = 1$.

(b) Assume ζ is a root of unity. We want to show that for all positive integers n , ζ^n is a root of unity.

Base case: $n = 1$. By hypothesis, ζ is a root of unity.

IH: For fixed n , ζ^n is a root of unity

IS: Given IH we want to show that ζ^{n+1} is a root of unity: $\zeta^{n+1} = \zeta \cdot \zeta^n$. By the induction hypothesis, ζ^n is a root of unity. By hypothesis, ζ is a root of unity. Hence ζ^{n+1} is the product of two roots of unity. So, by (a), it is a root of unity.

Comments: People had a lot of trouble with this.

i. A lot of folks assumed in (a) that $z^n = w^n = 1$. But you aren’t told that z, w are both n^{th} roots of unity, just that they are both roots of unity, maybe for different n .

ii. A lot of people tried to prove by induction that if $\zeta^n = 1$ then $\zeta^{n+1} = 1$. But that’s false.

iii. Even folks who sort of got close in (b) had mistakes with quantifiers (\forall, \exists). For example, someone might have an induction hypothesis that said “ ζ^n is a root of unity for all n .” But that’s what you’re trying to prove! The induction hypothesis is: ζ^n is a root of unity for some n .

iv. A lot of folks said in (b) that $\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, but there are other primitive n^{th} roots of unity.

v. A lot of folks had the interesting equation $\zeta^{n+1} = \zeta^n \cdot \zeta = 1 \cdot \zeta = 1$. But $\zeta \neq 1$, it’s a root of 1, not necessarily equal to 1. This is called wishful thinking. The reason it doesn’t work is because you’re trying to prove something that’s not true (see (ii)).

vi. And several folks who wrote something correct in (b) didn’t use (a) but were simply restating the standard one-line proof in a complicated format. I didn’t take points off for this, however.

8. (a) We need to show that if $o(\zeta) = n$ odd, then $o(\zeta^2) = n$.

Let $k = o(\zeta^2)$. $(\zeta^2)^n = 1$ so $k \leq n$. $\zeta^{2k} = 1$ so n divides $2k$. Since n is odd, n divides k . So $k \geq n$. Hence $k = n$.

(b) $-1 \in \sqrt[4]{1}$, but -1 is not a primitive fourth root, because neither i nor $-i$ are powers of

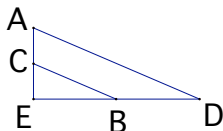
¹and note that this only works when $|z| = 1$

-1.

Comments: Again, in (a), several people assumed $\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$; it need not. Several folks gave some examples; examples aren't proofs. There were several vague arguments — we call this “waving your hands” and it doesn't work.

9. Suppose $n = mk$ where $1 < m < k < n$. Then $\cos \frac{2m\pi}{n} + i \sin \frac{2m\pi}{n}$ is not primitive, because its order is $k < n$. Similarly, $\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ is not primitive, because its order is $m < n$. Finally, 1 is not primitive, because its order is 1.

10.



In the above diagram, EB has length b , ED has length 1, and EA has length a . Furthermore, AD is parallel to CB . Let $c =$ the length of EC . By similar triangles, $\frac{c}{b} = \frac{a}{1}$, so $c = ab$.

Comments: The most common problem was just kind of scribbling stuff down without saying what was going on, for example not being clear what a, b, c were, or not saying that the lines were parallel, or not saying “by similar triangles.” A few people didn't prove the case I asked for, but simply restated the book's proof. That got no credit.

11. We assume the theorem that if a is constructible, so is $\sqrt{|a|}$:

Base case: $n = 1$: $5^{1/2}$ is constructible, since 5 is constructible.

IH: Assume $5^{1/2^n}$ is constructible.

IS: Assuming IH we want to show that $5^{1/2^{n+1}}$ is constructible: $5^{1/2^{n+1}} = \sqrt{5^{1/2^n}}$. By IH, $5^{1/2^n}$ is constructible. So by the theorem $\sqrt{5^{1/2^n}}$ is constructible.

Comments: Most folks did very well. The most common mistake was to misstate IH as “if ... then ...”. An induction hypothesis is always an affirmation that the property we're interested in holds at a single n . It says nothing about what happens at $n + 1$ — that's what the induction step is for. A few people also thought they were asked to prove that $5^{1/2^n}$ is constructible for all n . This fails for $n = 3$. And I was delighted to see how many people drew a 1, 2, $\sqrt{5}$ right triangle to show that $\sqrt{5}$ is constructible. Not necessary, but nice.

Selected answers to homework #3

1. $\cos \frac{\pi}{3} + i \sin \pi$; $\cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3}$

2. 1,5

3. 1,5

4. Let $P(x) = x^5 + x^3 + 1$. $P(0) = 1$; $P(1) = 3$; $P(2) = 41$; $P(3) = 271$. So in \mathbb{Z}_2 there are no solutions; in \mathbb{Z}_3 the only solution is $x = 1$; and there are no solutions in \mathbb{Z}_4 .

5. Suppose $o(\zeta) = n$. Let $\eta = \zeta \cdot \zeta^2 \cdot \dots \cdot \zeta^{n-1}$. Let k be the largest number so $k \leq \frac{n}{2}$. Note that if n is odd then $n - k = k + 1$, while if n is even then $n - k = k$.

Case 1: n is odd. Then $\eta = (\zeta \cdot \zeta^{n-1})(\zeta^2 \cdot \zeta^{n-1}) \cdot \dots \cdot (\zeta^k \cdot \zeta^{n-k})$ I.e., $\eta = 1 \cdot 1 \cdot \dots \cdot 1 = 1 = (-1)^{n-1}$.

Case 2: n is even. Then $\eta = (\zeta \cdot \zeta^{n-1})(\zeta^2 \cdot \zeta^{n-2}) \cdot \dots \cdot (\zeta^k \cdot \zeta^{n-k})(\zeta^{n/2})$. I.e., $\eta = 1 \cdot 1 \cdot \dots \cdot \zeta^{n/2}$. Since $(\zeta^{n/2})^2 = 1$ and $\zeta^{n/2} \neq 1$, $\zeta^{n/2} = -1$. So $\eta = -1 = (-1)^{n-1}$.

Here's an alternate proof:

Note that $\eta = \zeta \cdot \zeta^2 \cdot \dots \cdot \zeta^{n-1} = \zeta^{\sum_{i=1}^{n-1} i} = \zeta^{n(n-1)/2}$.

This again breaks into two cases: If n is odd, then $n-1$ is even and $\eta = (\zeta^n)^{(n-1)/2} = 1^{(n-1)/2} = 1 = (-1)^{n-1}$. If n is even, then $\eta = (\zeta^{n/2})^{n-1}$. So we're done if we can prove that $\zeta^{n/2} = -1$. Which is done as in case 2 of the first proof.

Comments. i. Some people seemed to be assuming what they wanted to prove, that is, every line had the form "... = $(-1)^{n-1}$." The logic of this doesn't work. You have to start with the expression $\zeta \cdot \zeta^2 \cdot \dots \cdot \zeta^{n-1}$ and end up with the expression $(-1)^{n-1}$.

ii. Most people who tried the second method didn't explain why $\zeta^{n/2} = -1$ when n is even.

iii. No matter which method you tried, you needed to break it into two cases, n even and n odd.

6. (a) $\zeta^j = \cos 2\pi + i \sin 2\pi = 1$.

(b) Let $j = \frac{n}{k}$. Note that $j < n$. By (a), $\zeta^j = 1$, so $o(\zeta) < n$.

Comments. Nobody cited (a). Instead everybody essentially reproved it. And some of the people who reproved it made mistakes. Remember: once you've proved something it is proved forever. No need to prove it again.

7. Note that this makes no sense for $k = 1$. Base case: The square is constructible ($k = 2$). IH: For some n , the regular 2^n -gon is constructible. IS. $2^{n+1} = 2 \cdot 2^n$. By IH, the regular 2^n -gon is constructible, so by theorem 2 in the problem, the regular $2 \cdot 2^n$ -gon is constructible. Hence, by induction, all regular 2^n -gons are constructible.

Comments. i. If you didn't put "for some n " (or the equivalent) in your IH you got a point off. Too many folks are still thinking (and sometimes even writing) that the IH is "for all n ". Well then there'd be nothing to prove, yes? ii. A substantial number of folks are still confused by how inductive proofs work. If you got fewer than 2 points on this problem, please come see me ASAP.

8. (a) $4280 = 30 \cdot 142 + 20$; $142 = 7 \cdot 20 + 2$; 2 divides 20. So $(4280, 142) = (142, 20) = (20, 2) = 2$; (b) $(140, 42) = 14$; (c) $(780, 54) = 6$.

9. $2 \cdot 3^2 \cdot 5^2 = 450$.

10. 6, 25 and 25, 38 are relatively prime pairs. The others aren't.

11. Let $g = (m, n) > 1$. Let $b = \frac{m}{g}$ and $k = \frac{n}{g}$. Then $0 < k < n$, hence $k \in \mathbb{Z}_n$. $km = \frac{n}{g}gb = nb$ which is an integer multiple of n . So $km \equiv 0 \pmod{n}$.

Comments. Luckily I didn't ask for a proof, because there were some slipshod proofs there. As long as you got the right k you got full credit. A few people had k a function of the least common multiple of m, n . But then every element of \mathbb{Z}_n would be what's called a zero divisor, and as you'll find out in the next homework that can't happen.

Selected answers to homework #4

1. (a) $243x^{10} - 810x^8z^3 + 1080x^6z^6 - 720x^4z^9 + 240x^2z^{12} - 32z^{15}$

(b) $3x^{10} - 2x^8z^3$

(c) $3x^{10} - 2z^{15}$

2. $64x^6 + 192x^2 + \frac{240}{x^2} + \frac{160}{x^6} + \frac{60}{x^{10}} + \frac{12}{x^{14}} + \frac{1}{x^{18}}$

3. yes for (1), (c), (d); no for (b), (e).

Here's an explanation of why: $x^k \cdot (\frac{1}{x^2})^{17-k} = x^m$ iff $\frac{x^k}{x^{34-2k}} = x^m$ iff $x^{3k-34} = x^m$ iff $3k - 34 = m$. As long as we can solve for k we're fine.

- (a) $m = 17$. $3k - 34 = 17$ iff $3k = 51$ iff $k = 1$.
 - (b) $m = 15$. $3k - 34 = 15$ iff $3k = 49$ which is not divisible by 3.
 - (c) $m = 14$. $3k - 34 = 14$ iff $3k = 48$ iff $k = 16$.
 - (d) $m = -1$. $3k - 34 = -1$ iff $3k = 33$ iff $k = 11$.
 - (d) $m = -2$. $3k - 34 = -2$ iff $3k = 32$ which is not divisible by 3.
- 4.

Table 1: Structures so far

set	closed +?	closed \times ?	add. id.?	mult. id.?	add. inv?	mult. inv?
\mathbb{N}	yes	yes	yes	yes	no	no
\mathbb{Z}	yes	yes	yes	yes	yes	no
\mathbb{Q}	yes	yes	yes	yes	yes	yes
\mathbb{R}	yes	yes	yes	yes	yes	yes
\mathbb{C}	yes	yes	yes	yes	yes	yes
$\sqrt[n]{1}$	no	yes	no	yes	n/a	yes
$\{z : \exists n z^n = 1\}$	no	yes	no	yes	n/a	yes
\mathbb{Z}_n, n not prime, $n > 1$	yes	yes	yes	yes	yes	no
\mathbb{Z}_p, p prime	yes	yes	yes	yes	yes	yes

5. (a) $jm = 1$ so $jmk = k$.

(b) $mk = 0$ so $jmk = 0$.

(c) Suppose $(m, n) = g > 1$. Then by #3 problem 11, there is $k \neq 0$ so $mk = 0$. If m had a multiplicative inverse j then $k = jmk = 0 \neq k$.

Comment. The most common error was not being well organized in part (c).

6. (a) $\frac{(2n+2)(2n+1)}{(n+1)^2} = \frac{2(2n+1)}{n+1} \geq 2$ iff $4n + 2 \geq 2n + 2$ iff $4n \geq 2n$ iff $n \geq 0$.

(b) $\frac{(2n)!}{n! n!}$

(c) Base case: $n = 0$. $1 = 2^n = \binom{0}{0}$.

IH: For some n , $2^n \leq \binom{2n}{n}$

IS: $\binom{2(n+1)}{n+1} = \frac{(2n+2)(2n+1)(2n)!}{(n+1)!(n+1)!} = \frac{(2n+2)(2n+1)}{(n+1)^2} \binom{2n}{n} \geq 2 \binom{2n}{n} \geq 2 \cdot 2^n = 2^{n+1}$.

(d) The key calculation is that $\binom{2(n+1)}{n+1} = \frac{(2n+2)(2n+1)}{(n+1)^2} > 2 \binom{2n}{n}$ iff $4n > 2n$ which is true for $n \geq 1$.

Comments. There were other methods, some of them quite clever. I didn't grade (d). A few people are still having trouble with "For all" instead of "for some" in the IH. Some people got full credit even though their calculations in the IS weren't quite correct. And there was a tendency in (a) to write down calculations without the all-important logical context of "iff."

7. (a) $1600 = 6 \cdot 266 + 4$. So in \mathbb{Z}_7 , $3^{1600} = (3^6)^{266} \cdot 3^4 = 3^4 = 81 = 4$.

(b) $1600 = 16 \cdot 100$. So in \mathbb{Z}_{17} , $3^{1600} = (3^{16})^{100} = 1$.

8. We are restricted to $a \in \mathbb{Z}_5$, so we can use FLT. Hence $a^4 = 1$, so $(a^{4^{100}}) = (a^4)^{4^{99}} = 1$ and $a^{10} = (a^4)^2 \cdot a^2 = a^2$. Hence we are solving $1 + a^2 - 1 = 0$ or $a^2 = 0$. So $a = 0$.

9. It suffices to show that, for all n , $n^5 - n$ is divisible by both 5 and 3. First, in \mathbb{Z}_5 , $n^5 - n = n - n = 0$. Hence $n^5 - n$ is divisible by 5 for all n . Second, in \mathbb{Z}_3 , $n^5 - n = (n^2)^2 \cdot n - n = n - n = 0$. So $n^5 - n$ is divisible by 3 for all n .

10. Let $n = o(a)$. Just as with complex roots of unity, $\sum_{i=0}^{n-1} a^i = \frac{1-a^n}{1-a}$. Since $a \neq 1$, the denominator is not 0. Since $n = o(a)$, the numerator = 0. So $\sum_{i=0}^{n-1} a^i = 0$.

Answers to homework #5

1. (a) $6^1 = 6, 6^2 = 10, 6^3 = 8, 6^4 = 9, 6^5 = 2, 6^6 = 12, 6^7 = 7, 6^8 = 3, 6^9 = 5, 6^{10} = 4, 6^{11} = 11, 6^{12} = 1$.

(b) $o(1) = 1; o(2) = o(6^5) = 12; o(3) = o(6^8) = 6; o(4) = o(6^{10}) = 6; o(5) = o(6^9) = 4; o(6) = 12; o(7) = o(6^7) = 12; o(8) = o(6^3) = 4; o(9) = o(6^4) = 3; o(10) = o(6^2) = 6; o(11) = o(6^{11}) = 12, o(12) = o(6^6) = 2$.

2. $561 = 2(280)+1 = 10(56)+1 = 16(35)+1$.

In \mathbb{Z}_3 , $n^{561} - n = (n^2)^{280} \cdot n - n = n - n = 0$. Hence $n^{561} - n$ is divisible by 3.

In \mathbb{Z}_{11} , $n^{561} - n = (n^{10})^{56} \cdot n - n = n - n = 0$. Hence $n^{561} - n$ is divisible by 11.

In \mathbb{Z}_{17} , $n^{561} - n = (n^{16})^{35} \cdot n - n = n - n = 0$. Hence $n^{561} - n$ is divisible by 17.

So $n^{561} - n$ is divisible by $3 \cdot 11 \cdot 17 = 561$.

3. $x^7 + x^4 + x + 1 = (x^3 + x^2 + 1)(x^4 - x^3 + x^2 - x + 2) + (-3x^2 + 2x - 1)$.

(a) In \mathbb{Z}_2 , quotient is $x^4 + x^3 + x^2 + x$ and remainder is $x^2 + 1$.

(b) In \mathbb{Z}_3 , quotient is $x^4 + 2x^3 + x^2 + 2x + 2$ and remainder is $2x + 2$.

(c) In \mathbb{Z}_5 , quotient is $x^4 + 4x^3 + x^2 + 4x + 2$ and remainder is $2x^2 + 2x + 4$.

4. Rings but not fields: \mathbb{Z}, \mathbb{Z}_n for n not prime, $n > 1$.

Fields (and therefore rings): $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ for p prime.

Not rings (and therefore not fields): $\mathbb{N}, \sqrt[n]{1}$, the set of all roots of unity in \mathbb{C} .

5. We are given that $\frac{a}{b} = \frac{c}{d}$, hence $ad = bc$. We want to show that $\frac{a+b}{a-b} = \frac{c+d}{c-d}$. Note that this includes an implicit hypothesis that $a \neq b$ and $c \neq d$. (Because otherwise the problem makes no sense.)

$\frac{a+b}{a-b} = \frac{c+d}{c-d}$ iff $(a+b)(c-d) = (c+d)(a-b)$ iff $ac - ad + bc - bd = ac + ad - bc - bd$ iff $bc - ad = ad - bc$ iff $ad - bc = 0$ iff $ad = bc$ which is true by hypothesis.

6. (a) Fix $a \in F$. Fix $m \in \mathbb{N}$. We need to show that $\forall n \ a^{m+n} = a^m a^n$.

Base case: $n = 0$. $a^{m+0} = a^m = a^m \cdot 1 = a^m a^0$.

IH: Suppose, for some m , $a^{m+n} = a^m a^n$.

IS: $a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} \cdot a$ by the recursive definition of exponentiation. $a^{m+n} \cdot a = a^m a^n \cdot a$ by IH. $a^n \cdot a = a^{n+1}$ by recursive definition of exponentiation. So $a^{m+(n+1)} = a^m a^{n+1}$.

(b) Fix $a \in F$. By (a), if $m, n \geq 0$ then $a^{m+n} = a^m a^n$.

Suppose $n < 0 \leq m$. Then $a^m a^n = a^m \cdot \frac{1}{a^{|n|}} = \frac{a^m}{a^{|n|}} = a^{m-|n|} = a^{m+n}$. [Note: We're might be

cheating a little bit by saying that $\frac{a^m}{a^{|n|}} = a^{m-|n|}$, or you can take that as part of the definition of exponentiation. If you don't, you have to do this case inductively, holding n fixed and varying m .]

Suppose $n, m < 0$. Then $a^{m+n} = a^{-|m|-|n|} = \frac{1}{a^{|m|+|n|}} = \frac{1}{a^{|m|}a^{|n|}} = \frac{1}{a^{|m|}} \cdot \frac{1}{a^{|n|}} = a^m a^n$.

7. No. $\deg(x+1)P \geq 1$ and $\deg 5 = 0$.

8. $(a-b)(a^2+ab+b^2) = a(a^2+ab+b^2) - b(a^2+ab+b^2)$ by the distributive law.

$a(a^2+ab+b^2) - b(a^2+ab+b^2) = (a^3+a^2b+ab^2) - (ba^2+ab^2+b^3)$ by the distributive law.

$(a^3+a^2b+ab^2) - (ba^2+ab^2+b^3) = a^3+a^2b+ab^2 - ba^2 - ab^2 - b^3$ by the associative law and the distributive law.

$a^3+a^2b+ab^2 - ba^2 - ab^2 - b^3 = a^3+a^2b+ab^2 - a^2b - ab^2 - b^3$ by the commutative law.

$a^3+a^2b+ab^2 - a^2b - ab^2 - b^3 = a^3+a^2 - a^2+ab^2 - ab^2 - b^3$ by the commutative law.

$a^3+a^2 - a^2+ab^2 - ab^2 - b^3 = a^3 - b^3$ by additive identity.

Note: you can be a lot pickier, for example, you might agonize over whether $-ba^2$ should be considered $-(ba^2)$ or $(-b)a^2$. If the second, things will take a little longer.

9. (a) kn

(b) Let $\deg P = n$ for some fixed n .

Base case: $k = 1$. $P = P^1$ so $\deg P = \deg P^1$.

IH: For some k , $\deg P^k = kn$.

IS: $P^{k+1} = P \cdot P^k$. By IH, $\deg P^k = kn$.

So $\deg P^{k+1} = \deg P + \deg P^k = n + kn = (k+1)n$.

Answers to homework #7

7. Suppose P is irreducible and P divides QR . We want to show that either P divides Q or P divides R .

Method I. (Not the proof in The Book — if you weren't in class March 12 ask someone what I mean — but quick and elegant.) If P does not divide Q then, since P is irreducible, 1 is a gcd of P, Q . So there are A, B with $AP + BQ = 1$. Hence $APR + BQR = R$. Since P divides P and P divides QR , P divides $APR + BQR = R$.

Comment: Some people who tried this method did not explain why A, B existed, i.e., that P, Q are relatively prime. You can't skip this.

Method II. (which doesn't quite work) Suppose P does not divide Q . Since P divides QR there is some M so $PM = QR$, i.e., $R = \frac{M}{Q}P$, so P divides R .

Comment: There's a good idea here, but it doesn't work. The notation $\frac{M}{Q}$ isn't legal: $F[x]$ is a ring, not a field, so it doesn't have division. To make the idea work we need:

Theorem: For any $P \in F[x]$ there is a unique sequence of irreducible monic polynomials $Q_1 \dots Q_k$, for $1 \leq i \leq k$ unique $n_i \in \mathbb{N}$ with each $n_i > 0$ and unique $a \in F$ so $P = a(Q_1)^{n_1} \dots (Q_k)^{n_k}$.

And then we have use this theorem to imitate the proof using unique factorization that if n divides mk and n is prime then n divides k .

This is The Book's proof, but it's not as easy to follow as Method I. And it needs a theorem we haven't proved.

8. OUCH! This had two misprints. 1. n should be $p-1$. The statement as written is false: if $p = 5$ then $2^2 = -1 = 4$, hence $2^4 = 1$, not 4. 2. In part (a), you want $k < p-1$, not $k < p-k$.

Because of the misprints I didn't grade it. Here is a correct answer.

Assume a is a primitive $p - 1^{\text{th}}$ root of unity in \mathbb{Z}_p , hence $\{a^i : 1 \leq i \leq p - 1\}$ is the set of all solutions to $x^{p-1} - 1 = 0$.

(a) If $k < p - 1$ then the coefficient of x^k in the above equation is 0, so $\sum a^1 \cdot \dots \cdot a^k = 0$.

(b) Let $m = a^1 \cdot \dots \cdot a^{p-1}$. $(-1)^{p-1}m = -1$ and $p - 1$ is even, so $m = -1$. But in \mathbb{Z}_p , $-1 = p - 1$. So $m = p - 1$.

11. The roots of $x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$ were $r, -r, s, -s, t, -t$.

(a) $a = r + -r + s + -s + t + -t = 0$.

$e = r(-s^t - t^2) - r(-s^2 - t^2) + s(-r^2 - t^2) - s(-r^2 - t^2) + t(-r^2 - s^2) - t(-r^2 - s^2) = 0$.

(b) By similar calculations, $b = -r^2 - s^2 - t^2$. $b = 0$ iff $r^2 + s^2 + t^2 = 0$. In some fields (e.g., \mathbb{Q} or \mathbb{R}) this can't happen unless $r = s = t = 0$. But if $\sqrt{-1} \in F$ there are solutions: $r = \pm\sqrt{-1}, s = 1, t = 0$ are two such solutions, and there are many more.

Comment: Lots of folks forgot about fields other than \mathbb{R} . But there are lot of others besides \mathbb{C} with $\sqrt{-1}$. For example, in \mathbb{Z}_5 , $2^2 = 4 = -1$.

Answers to homework #8

5. The problem: Let $a \in GF(p, P) = GF$. Show that $a^p = a$ iff $a \in \mathbb{Z}_p$.

The proof: \Leftarrow : By Fermat's little theorem, if $a \in \mathbb{Z}_p$ then $a^p = a$ in \mathbb{Z}_p . Since the arithmetic of GF extends the arithmetic of \mathbb{Z}_p , $a^p = a$ in GF .

\Rightarrow : By the previous paragraph, every element of \mathbb{Z}_p is a root of $x^p - x$ in GF , and since $\#\mathbb{Z}_p = p$ there can be no other roots in GF .

Comments: 1. A number of people assumed for the first part that $\deg P = 1$. $\deg P$ is arbitrary. 2. People had all kinds of complicated arguments with all kinds of wishful thinking, that is, claims were made without any reason behind them. There was a hint given: elements of \mathbb{Z}_p are zeroes of what polynomial? I think people misread this hint as: elements of GF are zeroes of what polynomial?

7. The problem: Show that if $\deg P = 3$ and P is irreducible over \mathbb{Z}_2 then every element of $GF(2, P)$ is primitive.

But this problem is false. The correct statement is: every element of $GF(2, P)$ which is neither 0 nor 1 is primitive. Most folks gave a correct argument for the correct result, so I gave them full credit.

Solution: $\#GF(2, P) = 8$, so $\#GF(2, P)^+ = 7$. Hence the primitive element of $GF(2, P)^+$ has order 7, so every power of it (other than 1) has an order which divides 7. But the only number other than 1 which divides 7 is 7.

Comment: There were other correct arguments, most of them more complicated. There were also some arguments which I couldn't follow, i.e., they seemed like non sequiturs. If you got a 0 on this problem you are encouraged to try to convince me otherwise.

8. Let $GF = GF(p, P)$ where $\deg P = n$.

(a) $\sum_{\alpha \in GF} \alpha = 0$ or $\sum GF = 1$. Why? $x^{p^n} - x = \prod_{\alpha \in GF} (x - \alpha)$, so $\sum_{\alpha \in GF} \alpha$ is the coefficient of x^{p^n-1} . If $p > 2$ or $n > 1$, this coefficient is 0. If $p = 2$ and $n = 1$, this coefficient is 1.

(b) By part (a), $GF(2, 1) = \mathbb{Z}_2$.

(c) $x^{p^n-1} - 1 = \prod_{\alpha \in GF^+} (x - \alpha)$ so $\prod_{\alpha \in GF^+} (-\alpha) = -1$. Since GF^+ is even, $\prod_{\alpha \in GF^+} \alpha = -1$.

Comment: Almost nobody did (a) and (b) by looking at coefficients of the Galois polynomial or its associated polynomial (in (c)). Instead, people took a primitive element and imitated the proofs for \mathbb{Z}_p . There were lots of minor algebraic errors, but more importantly the argument in (a) that said “you can pair every element with its additive inverse” begged the question: how do you know that 0 is the only element which is its own additive inverse (in $GF(2, P)$, it isn't). There were similar problems with (c). I graded generously. Because this problem had so many parts, it was worth 6 points.

9. Suppose m is relatively prime to $p^n - 1$. If $\alpha \in GF^+$ then $o(\alpha)$ divides $p^n - 1$. If $\alpha^m = 1$ then $o(\alpha)$ divides m . So $(m, p^n - 1)$ is divisible by $o(\alpha)$. Hence $o(\alpha) = 1$ and $\alpha = 1$. I.e., 1 is the only m^{th} root of unity in GF.

Comment: People tended to make this question somewhat more difficult by looking at powers of a primitive element, and in doing this tended to miss the fact that 1 is an m^{th} root of unity for *all* m . They also spent a lot of energy showing that no element has order m , but didn't discuss the case where $o(\alpha) \neq m$ but $\alpha^m = 1$. Again, I was generous with credit.

Selected answers to homework #9

1. (a) $\binom{4}{2} = 6$; (b) $\binom{4}{2} = 6$; (c) $\binom{3}{2} = 3$; (d) $\binom{4}{2} = 6$
2. Lots of examples. For example $x_1x_2\dots x_{n-1} + x_n$. For another example, $\frac{x_1}{x_1+x_2+\dots+x_n}$. Etc.
3. *Id.* Why? Without loss of generality, suppose $\sigma = (12\dots n)$. Then $\sigma(1) = 2$; $\sigma^2(1) = 3$; ... $\sigma^{n-1}(1) = n$, so $\sigma^n(1) = 1$. In general, $\sigma^k(i) = i + k \pmod{n}$, so $\sigma^n(i) = i$.
6. Again, many examples. E.g., $x_1x_2\dots x_k + x_{k+1}x_{k+2}\dots x_n$. E.g., $\frac{x_1+x_2+\dots+x_n}{x_1x_2\dots x_k}$. Etc.
9. (5342)(241).
10. (a) (1 3 8 7)(2 5 9)(4 10 6); (b) (1 7)(1 8)(1 3)(2 9)(2 5)(46)(4 10) or (1 3)(3 8)(8 7)(2 5)(5 9)(4 10)(10 6)
12. only (d)
14. A cycle with an even number of elements is odd. (E.g., (ab) .) A cycle with an odd number of elements is even (e.g., (abc) .)
15. (b) Δ_7 .

Selected answers to homework #11

3. *Comment.* Most people didn't explain what $(k, n) = 1$ has to do with it. I gave full credit but put a problem in the review asking why you need $(k, n) = 1$.

4. Fix g . We have to show that if $f(h) = ghg^{-1}$ then f is 1-1, f is onto, and each $f(gh) = f(g)f(h)$:

f is 1-1: $f(h) = f(k)$ iff $ghg^{-1} = gkg^{-1}$ iff $g^{-1}ghg^{-1}g = g^{-1}gkg^{-1}g$ iff $h = k$.

f is onto: Let $h \in G$. Let $k = g^{-1}hg$. Then $h = gg^{-1}hgg^{-1} = f(k)$.

$f(kh) = f(k)f(h)$: $f(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = f(g)f(k)$.

Comments. 1. Some people got confused about onto, and started out assuming that every h in G was some $f(k)$. That's what you need to prove. 2. A lot of people also showed things they didn't need to, such as $f(e) = e$ and each $f(h^{-1}) = (f(h))^{-1}$. No points were taken off for this. 3. A few people did something strange and mixed additive and multiplicative notation. A group has only one operation.

6. Answer 1: $(ghg^{-1})^n = g(hg^{-1}g)^nhg^{-1} = gh^n g^{-1} = e$ iff $g^{-1}gh^n g^{-1}g = e$ iff $h^n = e$. So

$o(h) = o(ghg^{-1})$.

Answer 2: By #4, the function $f(h) = ghg^{-1}$ is an automorphism, so necessarily $h, f(h)$ have the same order.

Comment. Most people showed that $(ghg^{-1})^{o(h)} = e$ but neglected to show that no smaller power worked. And nobody gave answer #2. :(

7(c) $(\mathbb{R}, +)$ has no roots of unity except for 0; (\mathbb{R}^+, \cdot) has two roots of unity, 1, -1.

Comment. Eric read \mathbb{R}^+ as $\{x \in \mathbb{R} : x > 0\}$ which affected his comments, so I put the correct answer here.

10. (a) $(1234)^2 = (13)(24) \notin S$.

(b) Add the element $(13)(24)$.

(c) Since $\langle S \rangle$ has order 4, it is either isomorphic to $(\mathbb{Z}_4, +)$ or K . Since it has two elements of order 4, it is isomorphic to $(\mathbb{Z}_4, +)$ and not to K .

Comments: Please do not make tables on a question like this unless there is no other way to explain things. It is time-consuming and hard for the reader to follow.

12. (a) Answer 1: Not commutative, so not cyclic.

Answer 2: Every element has order ≤ 6 .

(b) Answer 1: Let $q = \frac{m}{n}$ where m, n are relatively prime. Then every q^k has a denominator of the form n^j , so $\frac{1}{n+1}$ is not in $\langle q \rangle$.

Answer 2: If $q > 0$ then $-1 \notin \langle q \rangle$. If $q < 0$ then $-q^2 \notin \langle q \rangle$.

Comments: For (a) a lot of people said that elements of S_5 have order ≤ 5 . Not so: $(12)(345)$ has order 6. Nobody gave answer 1. For (b) most people gave answers similar to 1, but not as concrete.

Selected answers to homework #12

5. To show that the function $f(g^k) = h^k$ is an isomorphism you need to show three things: f is 1-1, f is onto, and $f(g^k g^m) = f(g^k) f(g^m)$ for all k, m with $0 \leq k \leq m < o(g)$.

For 1-1: Let $g^k, g^m \in \langle g \rangle$ where $0 \leq k \leq m < o(g)$. $f(g^k) = f(g^m)$ iff $h^k = h^m$ iff $k = m$ (because $k \leq m < o(g)$), and $k = m$ iff $g^k = g^m$ (same reason). Hence $f(g^k) = f(g^m)$ iff $g^k = g^m$.

For onto: If $h^k \in \langle h \rangle$ then $h^k = f(g^k)$.

For preservation of structure: $f(g^k g^m) = f(g^{k+m}) = h^{k+m} = h^k h^m = f(g^k) f(g^m)$.

Comment. Lots of people forgot to prove 1-1 onto. Note that you were not asked to prove that $\langle g \rangle \cong \langle h \rangle$ — we already know that. You were asked to prove that a *specific* function is an isomorphism.

8 (b). The elements of $A_4 \setminus K$ all have the form (ijk) . Show that each $(ijk)K = K(ijk)$.

Method I. Show that each $(ijk)K = K(ijk)$.

$(123)K = \{(123), (134), (243), (142)\} = K(123)$.

$(132)K = \{(132), (234), (124), (143)\} = K(132)$.

Since if $\tau \in \sigma K$ and $\sigma K = K\sigma$ then $\tau K = K\tau$, that's all we need to check.

Method II. Show that $\tau\sigma\tau^{-1} \in K$ for all $\tau \in A_4 \setminus K, \sigma \in K$. For example, compute $(123)[(12)(34)](132) = (14)(23)$; $(123)[(13)(24)](132) = (12)(34)$; $(123)[(14)(23)](132) = (13)(24)$. By symmetry (every possible way of arranging things is taken care of), $(ijk)\sigma(ikj) \in H$ for every $\sigma \in K$.

Comment. Most people did Method I, but a lot of people didn't realize that once the union of your cosets equalled the original group A_4 you were done. If you proved that K is normal in S_4 you got extra credit.

9. Let $S = \{\sigma_g : g \in G\} \subset G!$. We need to show that $Id \in S$; that every element in S has an inverse in S , and that S is closed under composition. Because associativity holds in $G!$, associativity automatically holds in S .

$Id \in S$: Let e be the identity in G . We show that $\sigma_e \sigma_g = \sigma_g$ for all $\sigma_g \in S$: For all $h \in G$ $\sigma_e \sigma_g(h) = egh = gh = \sigma_g(h)$. So $\sigma_e \sigma_g = \sigma_g$ for all $\sigma_g \in S$, and σ_e is the identity.

Every element in S has an inverse: We will show that $(\sigma_g)^{-1} = \sigma_{g^{-1}}$ for all $g \in G$: $\sigma_g \sigma_{g^{-1}}(h) = h = \sigma_e(h)$ for all $g, h \in G$. So $\sigma_g \sigma_{g^{-1}} = \sigma_e = Id$.

S is closed under composition: For all $g, h, k \in G$, $\sigma_g \sigma_k(h) = gkh = \sigma_{gk}(h)$, so every $\sigma_g \sigma_k = \sigma_{gk} \in S$.

Comment. People had surprising amount of trouble with this. In particular, there was a lot of confusion between $G!$ and $G - \sigma_g \in G!$ for each $g \in G$, but G is not a subset of $G!$, in fact $\{\sigma_g : g \in G\} \cap G = \emptyset$.

11. The task: If G is finite, use the fact that the order of every element of G divides the order of G to prove both the FLT and that the Galois polynomial has its key property.

First, state the FLT: For all $a \in \mathbb{Z}$, if p is prime then $a^p \equiv a \pmod{p}$.

Proof of FLT: Every $a \in \mathbb{Z}_p^+$ is a root of unity where $o(a)$ divides $\mathbb{Z}_p^+ = p - 1$. Hence each $a^{p-1} \equiv 1$ for $0 < a < p$, i.e., for any nonzero integer a , $a^{p-1} \equiv 1 \pmod{p}$. So for any integer a , $a^p \equiv a \pmod{p}$.

Second, state the key property of the Galois polynomial: Let $GF = GF(p, P)$ where P is irreducible over \mathbb{Z}_p and has degree n . For every $a \in GF$, $a^{p^n} = a$.

Proof: $\#GF^+ = p^n - 1$, so if $a \in GF^+$, its multiplicative order divides $p^n - 1$, hence $a^{p^n - 1} = 1$. But then for every $a \in GF$, $a^{p^n} = a$.

Comment. People tended to go backwards, e.g., starting with FLT proved that the order of an element divides the order of the group. Also, there was some confusion on exactly what the FLT said, what the Galois polynomial is, and what the key property of the Galois polynomial is. 12. (a) f is a homomorphism: $G = \langle 3 \rangle$ and $f(3^k 3^m) = f(3^{k+m}) = k + m = f(3^k) + f(3^m)$. The kernel is $H = \{3, 6\}$. $G/H = H, 1 + H = 4 + H, 2 + H = 5 + H$.

12. (a) f is a homomorphism: $G = \langle 3 \rangle$ and $f(3^k 3^m) = f(3^{k+m}) = k + m = f(3^k) + f(3^m)$. The kernel is $H = \{3, 6\}$. $G/H = H, 1 + H = 4 + H, 2 + H = 5 + H$.

(b) This problem makes no sense. The group I was thinking of is the additive group of third degree polynomials over the field \mathbb{Z}_3 , i.e., $(\{ax^3 + bx^2 + cx + d : a, b, c, d \in \mathbb{Z}_3\}, +)$. With that correction, let's solve the problem.

f is a homomorphism: Let $P = ax^3 + bx^2 + cx + d, Q = a'x^3 + b'x^2 + c'x + d'$. $f(P+Q) = b+b' = f(P)+f(Q)$. The kernel is $\{ax^3 + cx + d : a, c, d \in \mathbb{Z}_3\}$. The elements of G/H are $H, x^2 + H, 2x^2 + H$.

(c) f is a homomorphism: Let $z = a + bi, z' = a' + b'i$. $f(z + z') = b + b' = f(z) + f(z')$. The kernel is \mathbb{R} . The elements of G/H are all $bi + \mathbb{R}$. [I didn't ask, but G/H is isomorphic to $(\mathbb{R}, +)$.]

(d) f is a homomorphism: $f(x + y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$. The kernel is $H = \{0\}$. The elements of G/H are all $r + H$. [I didn't ask, but f is an isomorphism.]