

Math 558 Spring 2009

Homework assignments

Homework #1, due January 22

- (a) Find all solutions to the cubic equation $x^3 - 3x = 0$.
(b) Find the solution given by Tartaglia's formula, and say which solution from (a) it equals.
- Use Tartaglia's formula to find a solution of $x^3 - 3x + 2$. Then use high school arithmetic to show it equals an integer. Which integer?
- p. 7 #8
- p. 7 #10
- p. 8 #17 — the book gives an answer, but I want to see the work that shows why.
- Let $\mathbb{S} = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.
 - Which of the following are elements of \mathbb{S} , and which are not?

$$\frac{1}{2}, \quad 1 + \pi\sqrt{3}, \quad 2 - \frac{\sqrt{3}}{2}, \quad \sqrt{5}$$

- If $s, t \in \mathbb{S}$, is $s + t \in \mathbb{S}$? What about $s - t$?
- Calculate zw if $z = 32(\cos \frac{7\pi}{6} + i \sin \frac{7\pi}{6})$ and $w = \frac{1}{4}(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3})$.
 - Calculate (a) $(-1 + \sqrt{3}i)^{51}$; (b) i^{54321} ; (c) $\frac{(1+i)^{39}}{1-i}$.
 - Prove that if z is on the unit circle, so is z^n for any positive integer n . [Hint: you do not need induction; it's a very short proof.]
 - Prove that if z is on the unit circle, then $\frac{1-z}{1+z}$ is on the y -axis.

Reading assignment due January 20: p. 9 - 13

Reading assignment due January 22: section 2.1. Just read for the statements of the main theorems.

Homework #2, due January 29

- Find all elements of (a) $\sqrt[4]{i-1}$; (b) $\sqrt[5]{\sqrt{3}+i}$; (c) $\sqrt[3]{27(\cos \frac{\pi}{10} + i \sin \frac{\pi}{10})}$.
- Use the fact that $1 + \omega + \omega^2 = 0$ to show that $(1 + \omega^2)^{16} = \omega$.
- If $z^n = 1$, what's \bar{z}^n ?¹
- p. 23 #28
- Prove that if ζ is a root of unity then $o(\frac{1}{\zeta}) = o(\zeta)$.
- Let $\zeta = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$. What's $o(\zeta)$? [Don't just write a number down; I should be able to follow your reasoning.]
- (a) Show that if z, w are roots of unity, so is zw .

(b) *Silly Induction Tricks*: Using (a), prove by induction that if ζ is a root of unity, so is ζ^m for all $m \in \mathbb{N}$. Be sure to outline your proof along the lines of *Base case; IH; IS*. [This is a Silly Induction Trick because there's a very easy one-line proof, so using induction is a little bit like killing a fly with a grenade.]

¹Recall that \bar{z} is the conjugate.

R 8. (a) If n is odd, and ζ is a primitive n^{th} root of unity, is ζ^2 also a primitive n^{th} root of unity? Briefly explain.

(b) Show that there is a primitive fourth root of unity whose square is not a primitive fourth root of unity.

B 9. Suppose n is not prime and n is not a square of a prime number. Find three non-primitive elements in $\sqrt[n]{1}$. [Note: this has changed from the first version.]

R 10. Prove that if a, b are constructible and $0 < a < b < 1$ then ab is constructible. [In class, and in the book, we just proved the case: $b > 1$.]

R 11. By induction, show that $5^{1/2^n}$ is constructible for all n .

Reading assignment for January 29: 4.1 (yes, we are skipping chapter 3). Focus on how to do modular arithmetic calculations.

Homework #3, due February 5

B 1. Which elements of $\sqrt[6]{1}$ are primitive?

B 2. Which elements of \mathbb{Z}_6 have a multiplicative inverse in \mathbb{Z}_6 ?

B 3. Which elements a of \mathbb{Z}_6 satisfy the property that every non-zero element of \mathbb{Z}_6 is an integer multiple of a ?

B 4. Solve the equation $x^5 + x^3 + 1 = 0$ in (a) \mathbb{Z}_2 ; (b) \mathbb{Z}_3 ; (c) \mathbb{Z}_4 .

R 5. p. 41 #19

R 6. Let $\zeta = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ where $0 \leq k < n$.

(a) Suppose k divides n , and $j = \frac{n}{k}$. What's ζ^j ?

(b) Show that if $1 < k$ and k divides n then ζ is not a primitive n^{th} root of unity.

R 7. Assume the following two theorems (do *not* prove them): 1. The square is constructible. 2. If a regular n -gon is constructible, so is a regular $2n$ -gon. Now, using induction, prove that every regular 2^k -gon is constructible. Be sure to arrange the proof with Base case, IH, and IS clearly marked.

B 8. Use the Euclidean algorithm to find (a) (4280, 142); (b) (140, 42); (c) (780, 54)

B 9. What is the gcd of $2 \cdot 3^2 \cdot 5^3$ and $3 \cdot 5^2 \cdot 7$? Use the fundamental theorem of arithmetic, not the Euclidean algorithm.

B 10. Which of the following pairs are relatively prime? (a) 6, 25; (b) 25, 38; (c) 6, 38; (d) 25, 60.

R 11. Suppose $0 < m < n$ and $(m, n) \neq 1$. Is there some $k \neq 0, k \in \mathbb{Z}_n$ so $km \equiv 0 \pmod{n}$? If so, what is it? If not, why not?

Reading assignment due February 3: 4.2. Focus: be able to apply the definitions of greatest common divisor, relatively prime. You do *not* need to memorize the algorithm. Yet.

Homework #4, due February 12

B 1. Calculate $(3x^2 - 2z^3)^5$ with coefficients in: (a) \mathbb{R} ; (b) \mathbb{Z}_4 ; (c) \mathbb{Z}_5 .

B 2. Calculate $(2x - \frac{1}{x^3})^6$.

B 3. Consider the polynomial $(x - \frac{3}{x^2})^{17}$.

(a) Which of the following powers of x appear in this polynomial?² (i) x^{17} ; (ii) x^{15} ; (iii) x^{14} ; (iv) $\frac{1}{x}$; (v) $\frac{1}{x^2}$.

(b) Find the coefficient of x^{11} in $(x - \frac{3}{x^2})^{17}$.

B 4. Fill in the rest of the following table:

Table 1: Structures so far

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

Note: in the abbreviations above, “add. id.?” is shorthand for: \exists an additive identity; “mult. id.?” is shorthand for: \exists a multiplicative identity; “add. inv.?” is shorthand for: every element has an additive inverse; “mult. inv.?” is shorthand for: every non-zero element has a multiplicative inverse.

R 5. (a) Suppose $0 < m < n$ and m has a multiplicative inverse j in \mathbb{Z}_n . If $k \in \mathbb{Z}_n$, what’s jm ?

(b) Suppose $0 < k, m < n$ and $mk \equiv 0 \pmod{n}$. If $j \in \mathbb{Z}_n$, what’s jm ?

(c) Briefly explain why parts (a) and (b) together with homework #3 problem #11 prove that if $0 < m < n$ and $(m, n) \neq 1$ then m does not have a multiplicative inverse in \mathbb{Z}_n .

R 6. (a) Show that $\forall n \geq 0 \frac{(2n+2)(2n+1)}{(n+1)^2} \geq 2$.

(b) Write out an expression for $\binom{2n}{n}$ of the form $\frac{a!}{b!c!}$.

(c) Prove by induction that $\forall n \in \mathbb{N} 2^n \leq \binom{2n}{n}$. Be explicit about your base case, IH, and IS.

(d) For $n > 1, 2^n < \binom{2n}{n}$. Examine your proof of (c) carefully to explain why.

B 7. Evaluate 3^{1600} in

(a) \mathbb{Z}_7

(b) \mathbb{Z}_{17}

Note: your answer should be an element of the appropriate \mathbb{Z}_n .

B 8. Which $a \in \mathbb{Z}_5$ satisfy $a^{4^{100}} + a^{10} - 1 \equiv 0 \pmod{5}$?

R 9. Prove that $n^5 - n$ is divisible by 15 for every integer n .

R 10. p. 90 #18.

Reading assignment due Tuesday February 10: 5.2. Be able to state Proposition 5.3 and Fermat’s

²i.e., when you have simplified it and no term has a non-zero power of x in both numerator and denominator

Little Theorem (5.4) on p. 86.

Reading assignment due Thursday February 12: 6.1. Look at the structures in R 4 above and be able to say which are fields.

Homework #5, due February 19

Note: an asterisk means it uses material from Tuesday February 17.

B 1. (a) Find all powers 6^k in \mathbb{Z}_{13} . Your answer should have the form: $6^1 = 6, 6^2 = \dots, 6^3 = \dots$

(b) Since 13 is prime, every non-zero element in \mathbb{Z}_{13} is a root of unity. Using (a) and proposition 5,8, what are their orders?

B 2. Noting that $561 = 3 \cdot 11 \cdot 17$, do p. 90 #12

* B 3. (a) p. 105 #1

(b) p. 105 #2

(c) p. 105 #3.

B 4. Look at the chart in homework #3, problem 4. Which of these structures are fields?

R 5. p. 106 #14 (don't forget the hypothesis on p. 105)

R 6. (a) Prove by induction that if $a \in F$ and F is a field then for any $m, n \in \mathbb{N}$, $a^{m+n} = a^m a^n$.
Hint: Fix m and use induction on n .

(b) Using (a), and the definition that $a^{-n} = \frac{1}{a^n}$, prove that for any $m, n \in \mathbb{Z}$, $a^{m+n} = a^m a^n$.

* B 7. Can you find a polynomial P with real coefficients so $(x + 1)P = 5$? If so, what is it? If not, why not?

B 8. Carefully explain, using the field axioms and anything we did in class, why if $a, b, c \in F$ a field then $(a - b)(a^2 + ab + b^2) = a^3 - b^3$. (If you weren't in class, get notes from someone.)

* R 9. (a) If $k \in \mathbb{N}$ and $\deg P = n$, what's $\deg P^k$?

(b) Prove your result for (a) by induction.

Homework #6, due March 5

B 1. Let $P = x^3 + x + 1$. In which of the following fields is P irreducible? Give reasons.

(a) \mathbb{Z}_2

(b) \mathbb{Z}_3

(c) \mathbb{Z}_{11}

B 2. Let $P = x^3 + x + 1$. If P is *not* irreducible in each of the following fields, factor P into irreducible polynomials.

(a) \mathbb{Z}_2

(b) \mathbb{Z}_3

(c) \mathbb{Z}_{11}

B 3. Let $P = x^4 + 2x^2 + 1$. Is P irreducible in \mathbb{R} ? If yes, give reasons. If not, factor P into irreducible polynomials.

R 4. Suppose $P \in F[x]$ and $a \in F$. Prove that the remainder when you divide P by $x - a$ is $P(a)$.

Reading assignment due Thursday March 5: 6.3. In the statements of theorems, what are the parallels to 4.2 and what are the differences?

Homework #7, due March 12

B 1. (a) Find all monic quadratic polynomials in $\mathbb{Z}_3[x]$. [Hint: there are 9.]³

(b) Which of the polynomials in (a) are irreducible?

B 2. Is $x^3 + 2x^2 + 3x + 4$ irreducible in $\mathbb{Z}_5[x]$? How do you know?

R 3. (a) If you multiply $(x^2 + ax + b)(x^2 + cx + d)$, what is the coefficient of x^4 ? x^3 ? x^2 ? x ? What is the constant?

(b) $x^4 + x^3 + 1$ has no linear factors in $\mathbb{Z}_2[x]$. Why?

(c) Using (a) and (b), show that $x^4 + x^3 + 1$ is irreducible in $\mathbb{Z}_2[x]$.

B 4. Let p be a prime, $a \in \mathbb{Z}_p[x]$, $o(a) = p - 1$. Then $x^{p-1} - 1 = \prod_{k=1}^{p-1} (x - a^k)$. Why?

B 5. Using the Euclidean algorithm, find a gcd of $x^5 + x^3 + x^2 + x$ and $x^6 - 1$ in

(a) $\mathbb{Z}_2[x]$

(b) \mathbb{R}

B 6. In $\mathbb{Z}_5[x]$ are there A, B so $(x^2 + 2x + 1)A + (x^2 - 1)B = x + 1$? Briefly explain why.

R 7. Let $P, Q, R \in F[x]$, F a field. Suppose P is irreducible and P divides QR . Show that either P divides Q or P divides R .

R 8. Let a be a primitive n^{th} root of unity in \mathbb{Z}_p where p a prime, and for $i \leq p - 1$ let $r_i = a^i$. Working in \mathbb{Z}_p :

(a) show that $\sum_{r_1} \dots \cdot r_k = 0$ for $1 \leq k < p - k$. [Hint: look at #4.]

(b) using the methods of chapter 6, show that $\prod_{i=1}^{p-1} a^i = p - 1$.

B 9. Which of the following polynomials are symmetric and which are not? $x^2 + xy + y^2$; $xyz + xy + z$; $x^4y^4 - x^3y^3$.

B 10. Suppose r, s, t, u are the roots of the cubic equation $x^4 + ax^3 + bx^2 + cx + d$. Express $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} + \frac{1}{u}$ in terms of the coefficients a, b, c, d .

R 11. Suppose $r, -r, s, -s, t, -t$ are the zeros of $x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$.

(a) What value is a ? What value is e ?

(b) Are there any values of r, s, t for which $b = 0$? If so, what are they? If not, why not?

[Use the methods of 6.4. Do *not* multiply $(x - r)(x + r)(x - s)(x + s)(x - t)(x + t)$.]

Reading assignment due Thursday March 12: 7.1. Focus on the construction of specific Galois fields: using $x^2 + x + 1$ over \mathbb{Z}_2 (p. 130); using $x^3 + x^2 + 1$ over \mathbb{Z}_2 (p. 132); using $x^4 + x^3 + x^2 + x + 1$ over \mathbb{Z}_2 (p. 132).

Homework #8, due March 26

B 1. (a) Show that $x^2 + 2x + 2$ is irreducible in $\mathbb{Z}_3[x]$.

(b) Write out all elements of $GF(3, x^2 + 2x + 2)$, where γ is the Galois imaginary.

(c) Let γ be as in (b). Write out the cyclic table for γ .

(d) Is γ primitive?

(e) What's $(\gamma + 1)^{-1}$?

(f) Solve the equation $(1 + \gamma)x + \gamma = 1 + \gamma^2$ in $GF(3, x^2 + 2x + 2)$.

B 2. $x^4 + x + 1$ is irreducible in \mathbb{Z}_2 .

³“Monic” means that the leading coefficient is 1. In this case, we are looking for polynomials of the form $x^2 + \dots$

- (a) Write out all elements of $GF(2, x^4 + x + 1)$, where γ is the Galois imaginary.
 (b) Let γ be as in (a). Write out the cyclic table for γ .
 (c) Is γ primitive?
 (e) What's $(\gamma + 1)^{-1}$?
 (f) Solve the equation $(1 + \gamma)x + \gamma = 1 + \gamma^2$ in $GF(2, x^4 + x + 1)$.

B 3.(a) If Q is not irreducible, can PQ be irreducible?

(b) If Q is linear and $\deg P \geq 1$ can PQ be irreducible?

R 4. Find all irreducible quartics in $\mathbb{Z}_2[x]$. [Hint: a quartic is either a product of two quadratics or has a linear factor. Use #3.]

R 5. Show that if $a \in GF(p, P)$ then $a^p = a$ iff $a \in \mathbb{Z}_p$. [Hint: Elements of \mathbb{Z}_P are all zeroes of what polynomial?]

B 6. Let γ be the Galois imaginary for $x^2 + x + 1$ over \mathbb{Z}_5 . We discovered in class that $o(\gamma) = 3$ and that $\gamma^2 = 4\gamma + 4$. Let $A_0 = \{1, \gamma, 4\gamma + 4\}$.

(a) What's $2\gamma A_0 = \{2\gamma, 2\gamma \cdot \gamma, 2\gamma \cdot \gamma^2\}$? Write these elements in the form $a + b\gamma$ where $a, b, \in \mathbb{Z}_5$.

(b) What's $3\gamma A_0$? Write these elements in the form $a + b\gamma$ where $a, b, \in \mathbb{Z}_5$.

(c) What's $4\gamma A_0$? Write these elements in the form $a + b\gamma$ where $a, b, \in \mathbb{Z}_5$.

(d) Does $GF(5, P)^+ = A_0 \cup 2\gamma A_0 \cup 3\gamma A_0 \cup 4\gamma A_0$? If not, how many elements are missing?

R 7. Show that if $\deg P = 3$ and P is irreducible over \mathbb{Z}_2 , $\alpha \in GF(2, P)$ and $\alpha \neq 0$ then α is primitive.

R 8. Let P is irreducible over \mathbb{Z}_p , where p is a prime.

(a) Show that the sum of all elements of $GF(p, P)$ is either 0 or 1.

(b) There is exactly one the Galois fields for which the sum of its elements is 1. What is it?

(c) Show that the product of the non-zero elements of $GF(p, P)$ is -1.

R 9. Let P is irreducible over \mathbb{Z}_p , where p is a prime, $\deg P = n$. If m is relatively prime to $p^n - 1$, how many m^{th} roots of unity are there in $GF(p, P)$?

Reading assignment due Thursday March 26: 8.1 Be able to recognize when one polynomial is a variant of another.

Homework #9, due Thursday, April 2.

B 1. How many distinct variants does each of the following functions have?

(a) $rstu + rs$

(b) $rs + tu$

(c) $(r + s - t)^4$

(d) $\frac{rst}{tu}$

B 2. Find a function of n variables with exactly n distinct variants.

R 3. Let σ be a cycle of length n . What is σ^n ? Explain why.

B 4. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 4 & 3 & 2 & 1 & 7 \end{pmatrix}$. What's σ^2 ? $\sigma \circ \tau$? $\tau \circ \sigma$?

B 5. Let $\sigma = (14675), \tau = (87632)$. What's $\sigma \circ \tau$? $\tau \circ \sigma$?

R 6. For each $k \in \mathbb{N}$ with $1 \leq k \leq n$, find a function of n variables with exactly $\binom{n}{k}$ distinct

variants.

B 7. If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 3 & 1 & 8 & 6 & 4 & 2 \end{pmatrix}$, what's σ^{-1} ?

R 8. Let $\sigma = (123\dots n - 1 n)$. What's σ^{-1} ?

B 9. Find σ^{-1} if $\sigma = (142)(2435)$. Hint: see Lemma 8.3 p. 160.

B 10. (a) Decompose $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 8 & 10 & 9 & 4 & 1 & 7 & 2 & 6 \end{pmatrix}$ into disjoint cycles.

(b) Express $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 8 & 10 & 9 & 4 & 1 & 7 & 2 & 6 \end{pmatrix}$ as a composition of transpositions.

B 11. Just like B10, except for $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 4 & 6 & 5 & 3 & 2 \end{pmatrix}$.

B 12. Which of the following are ruled out by Cauchy's theorem?

(a) A function with 50 variables and exactly 49 distinct variants.

(b) A function with 50 variables and exactly 48 distinct variants.

(c) A function with 50 variables and exactly 47 distinct variants.

(d) A function with 50 variables and exactly 46 distinct variants.

B 13. Write the cycle $(abcdef)$ as the composition of transpositions in two distinct ways.

B 14. If σ is a cycle with an even number of elements (e.g., $(abcdef)$), is σ even or odd? If σ is a cycle with an odd number of elements, is σ even or odd?

B 15. (a) Write out the polynomial Δ_7 in gory detail.

(b) Let σ be a cycle with an even number of elements. Does $\sigma\Delta_7 = \Delta_7$ or $-\Delta_7$?

Reading assignment: p. 158 - 161. Focus: There are two decomposition theorems. What do they say?

Homework #10, due Thursday, April 16.

B 1. (a) Write out the table for the group $(\mathbb{Z}_6, +)$

(b) Write out the table for the group (S_3, \circ) [Recall that S_3 is the group of permutations on the numbers $\{1, 2, 3\}$]

(c) (\mathbb{Z}_7^+, \cdot) is also a group with 6 elements. It can be arranged in a table that looks like exactly one of the tables above. Which one? How do you know?

B 2. Consider $H = \{1, 3, 5, 7\}$ as a subset of \mathbb{Z}_8 . Write out its multiplication table under multiplication mod 8. Does it look like $(\mathbb{Z}_4, +)$? Does it look like the Klein group K ? Or is it not a group, and if so, why not?

R 3.(a) Let G be a group, $h \in G$. Define $f^h : G \rightarrow G$ by $f^h(g) = gh$. f^h is 1-1 onto (i.e., a permutation of G). Why? Do *not* cite fact 4 from class, since this is just a restatement of it.

(b) Use (a) to show that in a group table, in every column every element of the group appears exactly once.

R 4. The following table is not a group table.

Table 2:

	e	g	h	k
e	e	g	h	k
g	g	e	k	h
h	h	k	g	e
k	k	g	e	h

(a) You can tell immediately by visual inspection. How?

(b) Going deeper: what group axiom is not satisfied? Give an example, e.g., if your answer was "the inverse axiom" you'd have to give an element with no inverse.

Reading assignment due Thursday April 16: section 9.3. Be able to recognize an isomorphism.

Homework #11, due Thursday, April 23.

R1. Which of the following are subgroups of the quaternion group Q ? Briefly explain.⁴

- (a) $\{1, -1\}$
- (b) $\{1, -1, k, -k\}$
- (c) $\{1, i, j, k\}$
- (d) $\{1, i\}$

B2. Recall that D_3 is the set of symmetries of an equilateral triangle: three reflections (about the angle bisectors), two rotations (by $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$) and the identity. Is D_3 isomorphic to S_3 ? Why or why not?

R3. Prove that if k and n are relatively prime then the function $f(x) = kx$ is an automorphism of $(\mathbb{Z}_n, +)$.

R4. Let $g \in G$ a group, and define $f : G \rightarrow G$ by $f(h) = ghg^{-1}$ for all $h \in G$. Prove that f is an automorphism.

B5. Let $n \in \mathbb{Z}, n \neq 0$. Define $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

- (a) $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$. Why?
- (b) $f(k) = nk$ is an isomorphism from $(\mathbb{Z}, +)$ to $(n\mathbb{Z}, +)$. Why?

R6. If $g, h \in G$ then $o(h) = o(ghg^{-1})$. Why?

B7. Explain why in each of the following pairs G, H are not isomorphic.

- (a) $G = S_4, H = (\mathbb{Z}_{24}, +)$
- (b) $G = (\{Id, (13)(24), (13), (24)\}, \circ), H = (\mathbb{Z}_4, +)$
- (c) $G = (\mathbb{R}, +), H = (\mathbb{R}^+, \cdot)$
- (d) $G = (\mathbb{Z}_{11}, +), H = (\mathbb{Z}_{11}^+, \cdot)$

⁴If you didn't get the quaternion handout, you will have to ask me to send it to you. I did not use the table in Stahl. In particular I used different names.

B8. Find an isomorphism from $(\mathbb{Z}_4, +)$ to (\mathbb{Z}_5^+, \cdot) . Explain how you know it's an isomorphism.

B9. (a) Does S_4 have a subgroup of order 5? 4? 3? If you say no, give a reason. If you say yes, give an example.

(b) Does $(\mathbb{Z}_{10}, +)$ have a subgroup of order 5? 4? 3? If you say no, give a reason. If you say yes, give an example.

R10. (a) $S = \{Id, (1234), (4321)\}$ is not a subgroup of S_4 . Why?

(b) $\langle S \rangle$ is gotten by adding one more element to S . What is that element?

(c) Is $\langle S \rangle$ isomorphic to the Klein group? To $(\mathbb{Z}_4, +)$?

B11. Let $H = \{Id, (13)(24), (12)(34), (14)(23)\}$ = the Klein group. Let $G = S_4$.

(a) How many cosets of H in G are there?

(b) Find all the cosets of H in G . [Hint: in class we found two of them.]

R12. (a) S_5 is not cyclic. Why?

(b) (\mathbb{Q}^+, \cdot) is not cyclic. Why?

Reading assignment due Tuesday April 21: p. 203 to top of 207. Foci: What does Lagrange's theorem say? What is a coset? Be able to apply these concepts.

Reading assignment due Thursday April 23: Section 9.6. Focus: What does Cayley's theorem say?

Homework #11, due Thursday, April 30.

B1. For each of the following groups G , find n so $G \cong (\mathbb{Z}_n, +)$:

(a) $(\{(123456)^k : k \in \mathbb{Z}\}, \circ)$

(b) $(\mathbb{Z}_{11}^+, \cdot)$

(c) $(GF(3, P)^+, \cdot)$ where P is irreducible over \mathbb{Z}_3 and $\deg P = 4$

R2. If $n > 2$ then the group $H = \{Id, (12)\}$ is not a normal subgroup of S_n . Why not? Be brief.

B3. Let $H = \{Id, (1234), (13)(24), (4321)\}$, $G = S_n$ for $n \geq 4$.

(a) What's $(12)H$?

(b) What's $H(12)$?

(c) Is H a normal subgroup of G ?

B3. Write out the group tables for the following coset groups:

(a) $G = (\mathbb{Z}_{11}^+, \cdot)$, $H = \{1, 10\}$

(b) $G = S_n$, $H = A_n = \{\text{even permutations in } S_n\}$

(c) $G = (\mathbb{Z}, +)$, $H = \{5k : k \in \mathbb{Z}\}$

B4. Is every subgroup of a cyclic group normal? Why or why not? [Hint: no more than one or two sentences.]

R5. Suppose $g \in G$, $h \in H$, $o(g) = o(h)$. Show that the function $f(g^k) = h^k$ is an isomorphism from the group $\langle g \rangle$ to the group $\langle h \rangle$.

B6. Show that if $g \in G$ a group, then $\langle g \rangle$ is a group.

B7. None of the following groups are cyclic, and all for the same reason. State this reason in 5 words or less:

(a) $S_n, n > 2$

- (b) the quaternions
- (c) ($\{\text{permutations of } \mathbb{N}\}, \circ$)
- (d) ($\{\text{permutations of } \mathbb{R}\}, \circ$)

R8. (a) Which of the following are even and which are odd? (i) a cycle of length 3; (ii) a cycle of length 4.

(b) Show that $K = \{Id, (13)(24), (14)(23), (12)(34)\}$ is a normal subgroup of $A_4 =$ the set of even permutations in S_4 .

(c) Show that K is *not* a normal subgroup of S_4 .

[Remark: We have the same theorem for right cosets of a subgroup H as for left, i.e., they form a partition of G ; they all have the same size; $k \in Hg$ iff $Hk = Hg$. Using this will drastically cut down on your work in (b).]

R9. Let G be a group, $g \in G$. Recall the definition of $\sigma_g : G \rightarrow G$: $\sigma_g(h) = gh$. We've already proved (under a different name) that $S_G = \{\sigma_g : g \in G\} \subset G!$. Prove that S_G is a group of permutations.

R10. Let $\varphi : G \rightarrow H$ be 1-1 onto. Show that if, for all $g, g' \in G$ $\varphi(gg') = \varphi(g)\varphi(g')$ and $[\varphi(g)]^{-1} = \varphi(g^{-1})$, then $\varphi(e_G) = e_H$.

R11. The theorem that the order of an element in a finite group divides the order of the group implies both Fermat's little theorem and the theorem about the characteristic polynomial of a Galois field. How?

B12. For each of the following homomorphisms, (i) check that it's a homomorphism, (ii) find the kernel H , and (iii) describe the elements of G/H :

- (a) $G = (\mathbb{Z}_7^+, \cdot), J = (\mathbb{Z}_3, +), f(3^k) = k \pmod{3}$
- (b) $G = (GF(3, x^3 + 2x + 1), +), J = (\mathbb{Z}_3, +), f(ax^3 + bx^2 + cx + d) = b$
- (c) $G = (\mathbb{C}, +), J = (\mathbb{R}, +), f(a + bi) = b$.
- (d) $G = (\mathbb{R}, +), J = (\{x \in \mathbb{R} : x > 0\}, \cdot), f(x) = 2^x$.