FALL 2019: MATH 558 HOMEWORK SOLUTIONS

HW 1. Section 1.3: **14.** To prrove $A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C)$, let $x \in A\backslash(B \cup C)$. Then x is in A, but not in $B \cup C$. In particular, x is not in B. Thus, $a \in A\backslash B$. Similarly x is not in C, so $a \in A\backslash C$. Thus, $x \in (A\backslash B) \cap (A\backslash C)$, so $A\backslash(B \cup C) \subseteq (A\backslash B) \cap (A\backslash C)$.

Now suppose $x \in (A\backslash B) \cap (A\backslash C)$. Then $x \in A$, but $x \notin B$, while at the same time $x \notin C$ Thus, $x \notin (B \cup C)$. Therefore, $x \in A\backslash(B \cup C)$ and hence,$(A\backslash B) \cap (A\backslash C) \subseteq A\backslash(B \cup C)$, which shows the two sets are equal.

20. $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = 2n$, for all $n \geq 1$ is one-to-one, but not onto. On the other hand, $g : \mathbb{N} \to \mathbb{N}$ defined by $g(n) = \frac{n}{2}$, if n is even and $g(n) = n$ if n is odd, then g is onto, but not one-to-one. Note, that if n is even, then $g(2n) = n$ and if n is odd, then $g(n) = n$, so g is onto. Since $g(1) = 1 = g(2)$, g is not one-to-one.

22. Given $f : A \to B$ and $g : B \to C$.

- (a) Suppose f, g are 1-1. If $g \circ f(a_1) = g \circ f(a_2)$ then $f(a_1) = f(a_2)$, since g is 1-1. But then $a_1 = a_2$, since f is 1-1. Thus, $f \circ g$ is 1-1.
- (b) If $g \circ f$ is onto: Suppose $c \in C$. Then $c = (g \circ f)(a)$, for some $a \in A$. Thus, $g(f(a)) = c$, showing g is onto.
- (c) If $g \circ f$ is 1-1: Suppose $f(a_1) = f(a_2)$, for $a_1, a_2 \in A$. Then $g(f(a_1)) = g(f(a_2))$, and thus $a_2 = a_1$, since $g \circ f$ is 1-1. Therefore f is 1-1.
- (d) Suppose $g \circ f$ is 1-1 and f is onto: If $g(b_1) = g(b_2)$, for $b_1, b_2 \in B$, take $a_1, a_2 \in A$, such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Then $g(f(a_1)) = g(f(a_2))$. Since $g \circ f$ is 1-1, $a_1 = a_2$. Applying f we have $b_1 = f(a_1) = f(a_2) = b_2$, showing g is 1-1.
- (e) Suppose $g \circ f$ is onto and g is 1-1: Take $b \in B$. Then $g(b) \in C$, so there exists $a \in A$ such that $g \circ f(a) = g(b)$. Thus, $g(f(a)) = g(b)$, so $f(a) = b$, since g is 1-1. Thus shows f is onto.

HW 2. Section 1.3: **25.** (a) Not an equivalence relation since $2 \sim 1$, but $1 \not\sim 2$.
(b) Not an equivalence relation, since $0 \not\sim 0$.
(c) Not and equivalence relation, since $0 \sim 4$ and $4 \sim 8$, but $0 \not\sim 8$.
(d) This is an equivalence relation. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5]$, where the union is a disjoint union and $[i]$ means all integers whose remainder is i upon dividing by 6.

29. (a) $(x, y) = 1 \cdot (x, y)$, for all $(x, y)\mathbb{R}\backslash(0, 0)$, so the reflexive property holds.
(b) If $(x_1 y_1) = \lambda(x_2, y_2)$, with $\lambda \neq 0$, then $(x_2, y_2) = \lambda^{-1}(x_1, y_1)$, which shows that the symmetric property holds.
(c) Suppose $(x_1, y_2) = \lambda(x_2, y_2)$ and $(x_2, y_2) = \gamma(x_3, y_3)$, then $(x_1, y_1) = \lambda\gamma(x_3, y_3)$, and the product $\lambda\gamma$ is not zero, so the transitive property holds.

Note that two points in $\mathbb{R}\backslash(0, 0)$ are equivalent if and only if they lie on the same line through the origin. Just the distinct lines through the origin are the distinct equivalence classes.

HW 3. To see that the relation $a \sim b$ if and only if $a - b$ is divisible by 4 is an equivalence relations:

- (a) Since $0 = a - a$ is divisible by 4, $a \sim a$.
- (b) Since $b - a = -(a - b)$, it follows that if $a \sim b$, then $b \sim a$.
- (c) If $a \sim b$ and $b \sim c$, then 4 divides $a-b$ and 4 divides $b-c$. Thus 4 divides the sum $(a-b)+(b-c) = a-c$, which shows $a \sim c$.

Thus, $\sim$ is an equivalence relation.

We now show that the distinct equivalence classes are:

(i) $[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\} = \{4n \mid n \in \mathbb{Z}\}$.
(ii) $[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\} = \{4n+1 \mid n \in \mathbb{Z}\}$.
(iii) $[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\} = \{4n+2 \mid n \in \mathbb{Z}\}$.
(iv) $[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\} = \{4n+3 \mid n \in \mathbb{Z}\}$.

Notice that in each case, the set in the middle clearly equals the set on the right.

For (i), for any such integer in the set on the right, $0 - 4n = -4n$ is divisible by 4, and hence the given set belongs to [0]. Conversely if an integer k belongs to [0], then $0 - k$ is divisible by 4 and hence we can wrote $-k = 0 - k = 4n$, for some n, thus $k = -4n$, which show k belongs to the set on the right in (i). Thus equality holds and we have determined the equivalence class of [0]. The argument for the other cases is similar. For example, if $4n+3$ belongs to the set on the right in (iv), then $3-(4n+3) = -4n$, which is divisible by 4, so that $4n+3$ belongs to [3]. Conversely, if k belongs to [3], then $3-k$ is divisible by 4, so $3 - k = 4n$, for some n. Thus, $k = 3 + 4(-n)$, which shows that k belongs to the set on the right in (iv) and therefore this set equals [3].

HW 4. Section 1.3: **21.** (a) Clearly, $(x, y) \sim (x, y)$, for all (x, y).
(b) If $(x, y) \sim (x_1, y_2)$, then $x^2 + y^2 = x_1^2 + y_1^2$, and so $x_1^2 + y_1^2 = x^2 + y^2$, so $(x_1, y_1) \sim (x, y)$.
(c) If $(x, y) \sim (x_1, y_1)$ and $(x_1, y_1) \sim (x_2, y_2)$, then, $x^2 + y^2 = x_1^2 + y_1^2$ and $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Therefore, $x^2 + y^2 = x_2^2 + y_2^2$, and hence $(x, y) \sim (x_2, y_2)$. Thus $\sim$ is an equivalence relation.

Now suppose (x_1, y_1) belongs to te equivalence class of (x, y). Then $x_1^2 + y_1^2 = x^2 + y^2$. Suppose $R = x^2 + y^2$. Then both (x_1, y_1) and (x, y) both lie on the circle of radius $\sqrt{R}$ centered at the origin. Thus the distinct equivalence classes are all the circles in $\mathbb{R}^2$ centered at the origin.

HW 5. Section 2.3: **9.** Base case: $1 + 2^1 = 3 = 2^{1+1} - 1$.
Inductive step: Suppose $1 + 2 + \cdots + 2^n = 2^{n+1} - 1$. Adding 2^{n+1} to both sides yields:

$$1 + 2 + \cdots + 2^n + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}.$$

The left hand sides equals $2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$, which is what we want.

10. Base case: $\frac{1}{1(1+1)} = \frac{1}{2} = \frac{1}{1+1}$.
Inductive Step: Suppose $\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$. Adding $\frac{1}{(n+1)(n+2)}$ to both sides of this equation yields:

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)}.$$

Working with the right hand side of this equation we have:

$$\frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)(n+2)}{(n+1)(n+2)},$$

which is what we want.

HW 6. Section 2.3: **12.** There are many ways to prove this. One was is by induction on n. If $n = 1$, say, $X = \{a\}$, then $\mathcal{P}(X) = \{\emptyset, \{a\}\}$, which has 2^1 elements.

Inductibe step: Suppose the result is true for sets with n elements. Let X be a set with $n+1$ elements. We can write $X = X' \cup \{a\}$, where X' has n elements. Now X' has 2^n subsets, by our inductive hypothesis. Notice that the set of subsets of X not containing a are exactly the subsets of X'. Thus, there are 2^n subsets of X not containing a. The remaining subsets of X are obtained by adding a to all of the subsets of X'. Thus, there are 2^n subsets of X containing a. Therefore, there are $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ subsets of X, which is what we want.

Another proof uses the binomial theorem: $(x+y)^n = \sum_{i=0}^n x^{n-i}y^i$. If we substitute $x = 1 = y$ in this equation, we get $2^n = \sum_{i=0}^n \binom{n}{i}$. Now, we note that $\binom{n}{i}$ equals the number of subsets of X containing exactly i elements. Adding these as i runs from 0 to n shows that $\sum_{i=0}^n \binom{n}{i}$ is number of subsets of X, which gives what we want.

For the non-book problem: Suppose there exists a positive integer that is neither prime nor a product of primes. We seek a contradiction. Let X be the set of such numbers. Then $X \neq \emptyset$. By the Well Ordering Principle, there is a least element in X, say n. By definition of X, n is not a prime number. Therefore,

$n = ab$, with $1 < a, b, < n$. Thus, since n is the least element in X, neither a nor b belong to X. Therefore, a is either a prime or a product of primes and b is either a prime or a product of primes. But then $n = ab$ is a product of primes, which is a contradiction. Thus, every positive integer is either a prime or a product of primes.

HW 7. Section 2.3: **15a**. To find the GCD of 14 and 39, long division leads to the following equations:

$$\begin{aligned} 39 &= 2 \cdot 14 + 11 \\ 14 &= 1 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

,

which shows that $1 = \gcd(14, 39)$. Working with these equations in reverse order, we have:

$$\begin{aligned} 1 &= -1 \cdot 2 + 1 \cdot 3 \\ 1 &= -1 \cdot (11 - 3 \cdot 3) + 1 \cdot 3 = -1 \cdot 11 + 4 \cdot 3 \\ 1 &= -1 \cdot 11 + 4 \cdot (14 - 1 \cdot 11) = -5 \cdot 11 + 4 \cdot 14 \\ 1 &= -5 \cdot (39 - 2 \cdot 14) + 4 \cdot 14 = -5 \cdot 39 + 14 \cdot 14. \end{aligned}$$

15f. To find $\gcd(-4357, 3754)$, long division leads to the equations:

$$\begin{aligned} -4357 &= (-2) \cdot 3754 + 3151 \\ 3754 &= 1 \cdot 3151 + 603 \\ 3151 &= 5 \cdot 603 + 136 \\ 603 &= 4 \cdot 136 + 59 \\ 136 &= 2 \cdot 59 + 18 \\ 59 &= 3 \cdot 18 + 5 \\ 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

which shows that $1 = \gcd(-4357, 3574)$. I leave it to you to check that $1 = (1463) \cdot (-4357) + (1698) \cdot (3574)$.

17c. One way to prove that the nth Fibonacci number f_n satisfies $f_n = \frac{a^n - b^n}{\sqrt{5}}$, for $a = \frac{1+\sqrt{5}}{2}$ and $b = \frac{1-\sqrt{5}}{2}$ is to observe that a and b are roots of the polynomial $x^2 - x - 1$. Thus, $a^2 = a + 1$. Multiplying by a^{n-1}, we get that $a^{n+1} = a^n + a^{n-1}$, for all $n \geq 1$. Similarly $b^{n+1} = b^n + b^{n-1}$ for all $n \geq 1$.

Now, we can prove the required statement by induction on n. When $n = 1$, $\frac{a^1 - b^1}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = f_1$, and when $n = 2$, $\frac{a^2 - b^2}{\sqrt{5}} = \frac{\frac{1+2\sqrt{5}+5}{4} - \frac{1-2\sqrt{5}+5}{4}}{\sqrt{5}} = 1 = f_2$.

Suppose the formula hold for n, with $n \geq 2$. Then

$$f_{n+1} = f_n + f_{n-1} = \frac{a^n - b^n}{\sqrt{5}} + \frac{a^{n-1} - b^{n-1}}{\sqrt{5}} = \frac{(a^n + a^{n-1}) - (b^n + b^{n-1})}{\sqrt{5}} = \frac{a^{n+1} - b^{n+1}}{\sqrt{5}},$$

as required.

20. There is no need to use induction for this problem. We begin by observing that if n is a perfect square, then $n = m^2$, for some integer m. If m is even, $m = 2s$, for some s, so $n = 4s^2 = 4k$, for $k = s^2$. If m is odd, then $m = 2s + 1$, for some s, in which case, $n = (2s + 1)^2 = 4s^2 + 4s + 1 = 4k + 1$, for $k = s^2 + s$.

HW 8. Section 2.3: **22.** If $a \in \mathbb{Z}$, then we can write $a = nq + s$, with $0 \leq s < n$. Therefore $a - s = nq$, so n divides $a - s$. This means a is equivalent to s, and thus $[a] = [s]$. For $0 \leq s < r \leq n - 1$, the difference

$r - s$ is less than n, but not zero, and hence not divisible by n. Therefore, r and s are not equivalent, and the classes $[r]$ and $[s]$ are distinct. Thus, there is one equivalence class for each $0 \le s \le n-1$.

28. This is a proof by contradiction. Suppose $2^p - 1$ is prime and p is not prime. Then we can write $p = m \cdot n$, with both m and n greater than 1. Using the identity $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$, we obtain:

$$2^p - 1 = 2^{m\cdot n} - 1 = (2^m)^n - 1 = (2^m - 1)((2^m)^{n-1} + (2^m)^{n-2} + \cdots + 2^m + 1).$$

Since each term in the product on the right hand side of this equation is greater than one (since $m, n > 1$), we get the contradiction that $2^p - 1$ is not prime. Therefore, p is prime.

31. Starting with the equation $p^2 = 2q^2$, let d be the greatest common divisor of p and q, and write $p = p'd$ and $q = q'd$. Then $(p'd)^2 = 2(q'd)^2$. Cancelling d^2 from both sides of the equations yields $(p')^2 = 2(q')^2$. Thus, if there are integers p, q satisfying $p^2 = 2q^2$, then there are relatively prime integers satisfying the same equation. So, we may assume, p and q are relatively prime. Then p^2 is even, which forces p to be even, so we can write $p = 2p_1$. Therefore $4p_1^2 = (2p_1)^2 = 2q^2$, so that $2p_1^2 = q^2$. But this forces q^2, and hence q, to be even, which contradicts that p and q are relatively prime. Thus, no pair of integers satisfies the equation $p = 2q^2$. It follows from this that no rational number $\frac{p}{q}$ satisfies $(\frac{p}{q})^2 = 2$, and thus $\sqrt{2}$ is not a rational number.

HW 9. Section 2.3: **21.** Starting with the equations

$$\begin{aligned} a^2 + b^2 &= r^2 \\ a^2 - b^2 &= s^2, \end{aligned}$$

if we add the equations we get $2a^2 = r^2 + s^2$. Thus, r^2, s^2 are both even or both odd, in which case r, s are both even or both odd. But since r, s are relatively prime, they cannot both be even. Thus, r and s are both odd. Therefore, we may write $r = 2k+1$ and $s = 2l+1$, for some integers k, l. Therefore,

$$2a^2 = r^2 + s^2 = (2k+1)^2 + (2l+1)^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4(k^2 + k + l^2 + l) + 2,$$

Dividing the left and right hand sides of these equations by 2 shows that a^2 is odd, and therefore, a is odd. Finally, $b^2 = r^2 - a^2$ is a difference of odd integers, and therefore b^2, and hence b, is even. The proof is now complete.

HW 10. Section 17.4: **4a.** Invoking the division algorithm, we get:

$$\begin{aligned} x^3 - 8x^2 + 21x - 18 &= 1 \cdot (x^3 - 6x^2 + 14x - 14) + -2x^2 + 7x - 3 \\ x^3 - 6x^2 + 14x - 4 &= (-\frac{1}{2}x + \frac{5}{4}) \cdot (-2x^2 + 7x - 3) + (\frac{15}{4}x - \frac{45}{4}) \\ -2x^2 + 7x - 3 &= (\frac{15}{4}x - \frac{45}{4})(-\frac{8}{15}x + \frac{4}{15}). \end{aligned}$$

Thus, $\frac{15}{4}x - \frac{45}{4}$ is the last non-zero remainder, and hence, $x - 3$ is the GCD.

4d. Invoking the division algorithm, we get:

$$\begin{aligned} 4x^3 + x + 3 &= 4 \cdot (x^3 - 2x + 4) + (9x - 13) \\ x^3 - 2x + 4 &= (9x - 13) \cdot (\frac{1}{9}x^2 + \frac{13}{81}x + \frac{7}{729}) + \frac{3007}{729}. \end{aligned}$$

Since the second remainder is a non-zero constant, the next remainder must be zero. There the GCD is a constant, and thus equals 1.

HW 11. Using the division algorithm to find the GCD of $x^2 - 1$ and $x^4 + 6x^3 + x + 1$, we find:

$$\begin{aligned} x^4 + 6x^3 + x + 1 &= (x^2 - 1) \cdot (x^2 + 6x + 1) + (7x + 2) \\ x^2 - 1 &= (7x + 2) \cdot (\frac{1}{7}x - \frac{2}{49}) + -\frac{45}{49}. \end{aligned}$$

Since the second remainder is a non-zero constant, the next remainder must be zero. There the GCD is a constant, and thus equals 1. We will use the two equations above to write $-\frac{45}{49}$ as a polynomial combination of the given polynomials, and then divide by this fraction to obtain the final equation. Starting with the second equation, we have

$$(x^2-1)-(7x+2)\cdot(\frac{1}{7}x-\frac{2}{49})=-\frac{45}{49}.$$

Now, use the first equation to replace $7x+2$ by $x^4+6x^3+x+1-(x^2-1)\cdot(x^2+6x+1)$, to get:

$$(x^2-1)-\{x^4+6x^3+x+1-(x^2-1)\cdot(x^2+6x+1)\}\cdot(\frac{1}{7}x-\frac{2}{49})=-\frac{45}{49}.$$

Gathering like terms, we have

$$\{1+(\frac{1}{7}x-\frac{2}{49})(x^2+6x+1)\}\cdot(x^2-1)+(-\frac{1}{7}x+\frac{2}{49})\cdot(x^4+6x^3+x+1)=-\frac{45}{49}.$$

Therefore,

$$(-\frac{49}{45})\cdot\{1+(\frac{1}{7}x-\frac{2}{49})(x^2+6x+1)\}\cdot(x^2-1)+(-\frac{49}{45})\cdot(-\frac{1}{7}x+\frac{2}{49})\cdot(x^4+6x^3+x+1)=1.$$

HW 12. Section 17.4: **17.** By the division algorithm, we can write $p(x)=(x-a)\cdot q(x)+c$, where $c\in F$ is a constant. Substituting $x=a$, we get: $p(a)=(a-a)\cdot q(x)+c=0+c$, and thus $p(a)=c$, as required.

18. Suppose $p(\frac{r}{s})=0$. Then:

$$0=a_n(\frac{r}{s})^n+a_{n-1}(\frac{r}{s})^{n-1}+\cdots+a_0.$$

Multiply by s^n to get:

$$0=a_nr^n+a_{n-1}r^{n-1}s+\cdots+a_0s^n.$$

Note that s divides every term of the right hand side of the equation above, except possibly a_nr^n. But since s divides the left hand side, s divides a_nr^n. But r and s are relatively primes, so s divides a_n. Likewise, r divides every term on the right hand side of the equation above, except possibly a_0s^n. But r divides the left hand side of the equation, and thus r divides a_0s^n. Since r and s are relatively prime, r divides a_0.

From **17**, we have $p(x)=(x-a)\cdot q(x)+p(a)$. Now, if $p(a)=0$, then $p(x)=(x-a)\cdot q(x)$, so $x-a$ divides $p(x)$. Conversely, suppose $x-a$ divides $p(x)$. Then the remainder upon dividing $p(x)$ by $x-a$ is zero. But this remainder is $p(a)$, so $p(a)=0$.

Note to the class: Let's see how to apply the problems from this homework set. We will use the Rational Root test to prove that $p(x)=x^3+x+1$ is irreducible over $\mathbb{Q}$. If $p(x)$ were NOT irreducible, it could to be written as a product of a monic polynomial of degree one times a monic polynomial of degree two over $\mathbb{Q}$. Thus, $x-a$ would be a factor of $p(a)$, for some $a=\frac{r}{s}$ in $\mathbb{Q}$, i.e., $p(\frac{r}{s})=0$.

We may assume the fraction is in lowest terms, so r and s are relatively prime. By the Rational Root test, r divides 1 and s divides 1, as integers. Thus, $r=\pm1$ and $s=\pm1$. Therefore $a=\pm1$. But $p(1)=3$ and $p(-1)=-1$, a contradiction. Thus, there is no rational root of $p(x)$, and therefore $p(x)$ is irreducible over $\mathbb{Q}$.

HW 13. Sections 17.4: **21.** To see that $F[x]$ has infinitely many irreducible polynomials, suppose to the contrary that there are only finitely many irreducible polynomials, say, $p_1(x),\dots,p_n(x)$. Consider $f(x)=p_1(x)\cdots p_n(x)+1$. Either $f(x)$ is irreducible or has an irreducible factor. The first statement is a contradiction, since $f(x)$ is not equal to any of the $p_i(x)$. But none of the polynomials $p_i(x)$ divides $f(x)$, since the remainder upon dividing $f(x)$ by $p_i(x)$ is 1. Thus, the second statement is also a contradiction. Therefore, there cannot exist only finitely many irreducible polynomials.

22. Suppose $f(x)=a_nx^n+\cdots+a_0$ and $g(x)=b_mx^m+\cdots+b_0$. Say $n\geq m$. Then

$$\begin{aligned}f(x)+g(x)&=a_nx^n+\cdots+a_{m+1}x^{m+1}+(a_m+b_m)x^m+\cdots+(a_0+b_0)\\&=a_nx^n+\cdots+a_{m+1}x^{m+1}+(b_m+a_m)x^m+\cdots+(b_0+a_0)\\&=g(x)+f(x).\end{aligned}$$

HW 14. Addition and multiplication tables for $\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication of non-zero elements in $\mathbb{Z}_7$:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

HW 15. Suppose $f(x), g(x)$ are non-zero polynomials in $R[x]$. We can write $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$, with $a_n \neq 0$ and $b_m \neq 0$. Then $f(x)g(x) = a_n b_m x^{n+m} + \cdots + a_0 b_0$. Since R is an integral domain $a_n b_m \neq 0$, so $f(x)g(x) \neq 0$, which shows that $R[x]$ is an integral domain.

HW 16. Section 16.6: **3a.** Units in $\mathbb{Z}_{10}$: $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}\}$. **3b.** Units in $\mathbb{Z}_{12}$: $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. **3c.** Units in $\mathbb{Z}_7 : \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

$$\begin{aligned} 97 &= 83 \cdot 1 + 14 \\ 83 &= 14 \cdot 5 + 13 \\ 14 &= 13 \cdot 1 + 1. \end{aligned}$$

Using these equations and backwards substitution, we see $1 = 6 \cdot 97 + (-7) \cdot 83$. Thus, 97 divides $1 - (-7)7 \cdot 83$, so that $1 \equiv (-7) \cdot 83 \mod 97$. Thus, $\overline{1} = \overline{-7} \cdot \overline{83}$ in $\mathbb{Z}_{97}$. Since $\overline{-7} = \overline{90}$ in $\mathbb{Z}_{97}$, it follows that $\overline{90}$ is the multiplicative inverse of $\overline{87}$ in $\mathbb{Z}_{97}$.

HW 17. (i) $(a + b\sqrt{3}i) + (c + d\sqrt{3}i) = (a + c) + (b + d)\sqrt{3}i$ and

$$(a + b\sqrt{3}i) \cdot (c + d\sqrt{3}i) = ac + ad\sqrt{3}i + bc\sqrt{3}i - 3bd = (ac - 3bd) + (ad + bc)\sqrt{3}i,$$

therefore R is closed under addition and multiplication. That all of the axioms requiring R to be a ring and integral domain hold follows from the fact that $R \subseteq \mathbb{C}$, and $\mathbb{C}$ is an integral domain (in fact, a field).

(ii) For $x = a + b\sqrt{3}i$ and $y = c + d\sqrt{3}i$.

$$\begin{aligned} N(x \cdot y) &= (ac - 3bd)^2 + ((ad + bc)\sqrt{3})^2 \\ &= (ac)^2 - 6acbd + (3bd)^2 + 3(ad)^2 + 6adbc + 3(bc)^2 \\ &= (ac)^2 + 9(bd)^2 + 3(ad)^2 + 3(bc)^2. \end{aligned}$$

On the other hand,

$$\begin{aligned} N(x) \cdot N(y) &= (a^2 + 3b^2) \cdot (c^2 + 3d^2) \\ &= a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2, \end{aligned}$$

which shows $N(x)N(y) = N(xy)$.

(iii) If $x \in R$ is a unit, then for some $y \in R$, $1 = xy$ and therefore

$$1 = N(xy) = N(x)N(y) = (a^2 + 3b^2)(c^2 + 3d^2).$$

Since $a, b, c, d \in \mathbb{Z}$, this forces $c = d = 0$ and $a, b = \pm 1$.

HW 18. 1. If $a \in R$, then $a = 1 \cdot a$, so $a \sim a$. If $a \sim b$, then $a = ub$, for u a unit. Therefore, $b = u^{-1}a$, for the unit u^{-1}, and thus $b \sim a$. If $a \sim b$ and $b \sin c$, then $a = ub$ and $b = vc$, for units $u, v \in R$. Therefore $a = u(vc) = (uv)c$. Since uv is a unit, $a \sim c$ and thus $\sim$ is a equivalence relation. The class of a in R is just all unit multiples of a.

2. Since $d_1|d_2$, $d_2 = ad_1$, for some $a \in R$. Therefore $v(d_1) \leq v(d_2)$. By symmetry, $v(d_2) \leq v(d_1)$, so $v(d_1) = v(d_2)$.

HW 19. 1. Suppose $1+i = uv$, with $u, v \in \mathbb{Z}[i]$. Then $2 = N(1+i) = N(uv) = N(u)N(v) = (a^2+b^2) \cdot (c^2+d^2)$, for $u = a + bi$ and $v = c + di$. But then one of $a^2 + b^2$ or $c^2 + d^2$, say $a^2 + b^2$, must equal 1. This implies either $a = 0$ and $b = \pm 1$ or $a = \pm 1$ and$b = 0$. Thus, $u = \pm 1$ or $u = \pm i$, which shows that $1 + i$ is irreducible.

2. Since $2 = N(1 - i)$, the proof in 1 shows $1 - i$ is irreducible. Thus $2 = (1 + i) \cdot (1 - i)$ is a product of two irreducible elements in $\mathbb{Z}[i]$.

HW 20. (i) $R = \mathbb{Z}[\sqrt{5}i]$ is an integral domain because it is contained in the field (integral domain) $\mathbb{C}$.

(ii) If $xa + b\sqrt{5}i \in R$ is a unit, then for some $y = c + d\sqrt{5}i \in R$, $1 = xy$ and therefore

$$1 = N(xy) = N(x)N(y) = (a^2 + 5b^2)(c^2 + 5d^2).$$

Since $a, b, c, d \in \mathbb{Z}$, this forces $c = d = 0$ and $a, b = \pm 1$.

(iii) The proofs that $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ are very similar, so we will just prove two of them. Suppose $2 = x \cdot y = (a + b\sqrt{5}i) \cdot (c + d\sqrt{5}i)$. Taking the norm of both sides, we get:

$$4 = N(2) = N(xy) = N(x) \cdot N(y) = (a^2 + 5b^2) \cdot (c^2 + 5d^2).$$

Since every term in the equation above is a positive integer and we can only factor 4 as $2 \cdot 2$ or $1 \cdot 4$ using positive integers, either $(a^2 + 5b^2) = 2$, in which case $b = 0$ and $a^2 = 2$, which cannot happen, or one of $a^2 + 5b^2$ or $c^2 + 5d^2$ equals 1. Suppose $a^2 + 5b^2 = 1$. Then $b = 0$ and $a = \pm 1$. This shows that x is a unit. Likewise, if $c^2 + 5d^2 = 1$, y is a unit. Thus, 2 is an irreducible element of R.

The proof that $1 + \sqrt{5}i$ is irreducible is essentially the same. Its norm is 6. If $1 + \sqrt{5}i = xy$, then the norm of x is either 2, 3, 1, or 6. The first two cases cannot happen. If $N(x) = 1$, x is unit. If $N(x) = 6$, $N(y) = 1$ and y is unit. Thus, $1 + \sqrt{5}i$ is irreducible.

(iv) Clearly $2 \cdot 3 = 6 = (1 + \sqrt{5}i) \cdot (1 - \sqrt{5}i)$, and all factors are irreducible, by (iii). Since the only units in R are ± 1, clearly none of the irreducible factors is a unit multiple of any other of the irreducible factors, and hence the two factorizations are distinct. Thus, uniqueness of factorization fails in R.

HW 21. OK, so a randomly chosen example turned out to be trivial: $z = 4w$!

HW 22. Since $L \subseteq \mathbb{C}$, to check that L is a field, it suffices to check that L is closed under addition and mulitplication, and that the multiplicative inverse of L (as a complex number) belongs to L. The first two of these are very easy to check, and the third is standard high school algebra:

$$\frac{1}{a + b\sqrt{5}i} = \frac{1}{a + b\sqrt{5}i} \cdot \frac{a - b\sqrt{5}i}{a - b\sqrt{5}i} = \frac{a - b\sqrt{5}i}{a^2 + 5b^2} = \frac{a}{a^2 + 5b^2} + \frac{-b}{a^2 + 5b^2}\sqrt{5}i.$$

Since $\frac{a}{a^2+5b^2}$ and $\frac{-b}{a^2+5b^2}$ are rational numbers $(a + b\sqrt{5}i)^{-1} = \frac{a}{a^2+5b^2} + \frac{-b}{a^2+5b^2\sqrt{5}i}$ belongs to L. The roots $\pm\sqrt{5}i$ of $x^2 + 5$ are clearly in L. Finally, if $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ is a field that contains the roots of $x^2 + 5$, then since K is closed under addition and multiplication, it contains all expressions of the form $a + b\sqrt{5}i$ and thus contains L.

HW 23. (i) Since $\sqrt[3]{11}$ is a root of $x^3 - 11$, $x - \sqrt[3]{11}$ is a factor of $x^3 - 11$. from the division algorithm, we see that $x^3 - 11 = (x - \sqrt[3]{11}) \cdot (x^2 + \sqrt[3]{11}x + (\sqrt[3]{11})^2)$. Thus, we may use the quadratic formula to find the other two roots.

$$x = \frac{-\sqrt[3]{11} \pm \sqrt{(\sqrt[3]{11})^2 - 4(\sqrt[3]{11})^2}}{2} = \frac{-\sqrt[3]{11} \pm \sqrt{-3(\sqrt[3]{11})^2}}{2} = \frac{-\sqrt[3]{11} \pm \sqrt[3]{11}\sqrt{3}i}{2} = \sqrt[3]{11} \cdot \frac{-1 \pm \sqrt{3}i}{2}.$$

(ii) Since $x^3 - 1 = (x-1)(x^2 + x + 1)$, the cube roots of 1 are $1, \frac{-1\pm\sqrt{3}i}{2}$, so part (ii) now follows from what we have done in part (i)

(iii) Write $\alpha = \frac{-1+\sqrt{3}i}{2}$ and $\beta = \frac{-1-\sqrt{3}i}{2}$, so that $r_1 = \sqrt[3]{11}, r_2 = \sqrt[3]{11}\alpha, r_3 = \sqrt[3]{11}\beta$, with $\alpha^3 = \beta^3 = 1$. Then

$$\begin{aligned}(x - r_1)(x - r_2)(x - r_3) &= (x - \sqrt[3]{11})(x - \sqrt[3]{11}\alpha)(x - \sqrt[3]{11}\beta) \\ &= (x^2 - \sqrt[3]{11}(1+\alpha)x + (\sqrt[3]{11})^2)\alpha)(x - \sqrt[3]{11}\beta) \\ &= x^3 - \sqrt[3]{11}(1 + \alpha + \beta)x^2 + (\sqrt[3]{11})^2(\alpha + \beta + \alpha\beta)x - 11\alpha\beta.\end{aligned}$$

But $1+\alpha+\beta = 1 + \frac{-1+\sqrt{3}i}{2} + \frac{-1-\sqrt{3}i}{2} = 0$ and $\alpha\beta = \frac{-1+\sqrt{3}i}{2} \cdot \frac{-1-\sqrt{3}i}{2} = \frac{1+4}{4} = 1$, so $\alpha+\beta+\alpha\beta = \alpha+\beta+1 = 0$. Thus, the last polynomial displayed above is $x^3 - 11$, which is what we want.

HW 24. To calculate $a \cdot b$, multiplying term by term we get

$$\begin{aligned}a \cdot b &= 1 + 2\sqrt[3]{2} + \sqrt[3]{4} + 15\sqrt[3]{4} + 10\sqrt[3]{8} + 5\sqrt[3]{16} \\ &= 1 + 2\sqrt[3]{2} + \sqrt[3]{4} + 15\sqrt[3]{4} + 20 + 10\sqrt[3]{2} \\ &= 21 + 12\sqrt[3]{2} + 16\sqrt[3]{4}.\end{aligned}$$

To find the inverse of a, we use the division algorithm, yielding the equations:

$$\begin{aligned}x^3 - 2 &= (x-2)(x^2 + 2x + 3) + (x+4) \\ x^2 + 2x + 3 &= (x-2)(x+4) + 11.\end{aligned}$$

Using backwards substitution yields $11 = (x^2 - 4x + 5)(x^2 + 2x + 5) - (x-2)(x^3 - 2)$. Substituting $x = \sqrt[3]{2}$, we get $11 = (\sqrt[3]{4} - 4\sqrt[3]{2} + 5)(\sqrt[3]{4} + 2\sqrt[3]{2} + 3)$. Thus, $a^{-1} = \frac{1}{11} \cdot (\sqrt[3]{4} - 4\sqrt[3]{2} + 5)$.

HW 25. To find γ^{-1}, we use the division algorithm to write $x^2 + x + 1 = (2x+3)(\frac{1}{2}x - \frac{1}{4}) + \frac{7}{4}$. Substituting $x = \alpha$ yields $0 = (2\alpha + 3)(\frac{1}{2}\alpha - \frac{1}{4}) + \frac{7}{4}$. Rewriting yields, $\gamma^{-1} = \frac{1}{7} - \frac{2}{7}\alpha$.

HW 26. (i) Since $f(x)$has degree three, it is irreducible over $\mathbb{Q}$ if it has not rational roots. On the other hand, since $f(x) = 2 \cdot (x^2 + 3x + 3)$, it suffices to show that $g(x) = x^2 + 3x + 3$ has no rational roots. By the Rational Root Test, it suffices to see that none of $\pm 1, \pm 3$ are roots of $g(x)$. Since the coefficient of $g(x)$ are positive, we can eliminate 1, 3. On the other hand $g(-1) = 1$ and $g(-3) = 3$, so $g(x)$ and hence, $f(x)$ have no rational roots.

(ii) To find the roots of $f(x) = x^3x - 2x^2 - x - 6$, we first look for rational roots. Trying $\pm 1,]pm, 2, \pm 3, \pm 6$, shows $x = 3$ is a root. We then see $f(x) = (x-3)(x^2 + x + 2)$. Using the quadratic formula on the second term yield the additional roots $\frac{-1\pm\sqrt{7}i}{2}$.

HW 27. (i) $\overline{3+5x} + \overline{1+6x} = \overline{4+11x}$. $\overline{3+5x} \cdot \overline{1+6x} = \overline{3 + 23x + 30x^2}$. To put this last term in its proper form, we use the division algorithm: $3 + 23x + 30x^2 = 30(x^2 + x + 1) + (-7x - 29)$. It follows that $\overline{3+5x} \cdot \overline{1+6x} = \overline{-29 - 7x}$.

(ii) Following the same steps as in HW 25, one sees that $\overline{3+2x}^{-1} = \overline{\frac{1}{7} - \frac{2}{7}x}$.