FALL 2019: MATH 558 DAILY UPDATE

Wednesday, December 11. We had Quiz 12, we discussed the format of the final exam and the class filled out the course survey.

Monday, December 9. We proved several facts about left cosets in a group, culminating in a proof of Lagrange's theorem:

Theorem. Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$. In particular, $|G| = s \cdot |H|$, where s is the number of distinct left cosets of H in G.

We then noted that each of the facts proven about left cosets can be shown in a similar fashion for right cosets. Thus, if G is a finite group, then $|G| = t \cdot |H|$, where t denotes the number of distinct right cosets of H in G. It follows that the number of distinct left cosets of H in G equals the number of distinct right cosets of H in G.

Friday, December 6. We proved two more facts about groups in general: (i) Inverses are unique and (i) For any group G and $g_0 \in G$, $g_0G = G$. We then defined the notion of subgroup and gave several examples of subgroups. We also defined the notion of a *left coset* of a subgroup and then calculated the left cosets of $H = \{I, \tau, \tau^2\}$ and $K = \{I, \sigma\}$ in S_3.

Bonus Problem. Due December 9. Let $0 \neq H$ be a proper subgroup of $(\mathbb{Z}, +)$. Prove that H contains a positive integer and that $H = t\mathbb{Z}$, where t is the smallest positive integer in H.

Wednesday, December 4. We had Quiz 11. Then we gave two more families of examples of groups. First, we proved that $\mathrm{Sl}_n(F)$, the $n \times n$ matrices over the field F with determinant equal to 1 is a group under matrix multiplication. We then gave strong evidence for (but did not formally prove) the fact that the group $\mathrm{Sl}_2(\mathbb{Z}_2)$ has twenty-four elements. We then defined the natural coordinate-wise binary operation on the Cartesian product of two groups and proved that this construction leads to a group. We finished the class by proving two standard fact about groups. Namely: (i) the identity element is unique and (ii) cancellation holds.

Monday, December 2. We reviewed the definition of group and some of the examples from the previous lecture. We then calculated the group table for S_3, the symmetric group on three letters.

Monday, November 25. We defined the concept of group. We then gave several examples of groups, including:

(i) The integers under addition.
(ii) Any ring, with addition as its binary operation. In particular $\mathbb{Z}_n$ under addition.
(iii) $\mathrm{Gl}_2(F)$, invertible 2×2 matrices over the field F under multiplication. Similarly $\mathrm{Gl}_n(F)$, invertible $n \times n$ matrices over F forms a group under multiplication.
(iv) The symmetric group S_n, i.e., the set of one-to-one and onto functions from the set $X = \{1, 2, \ldots, \}$ to itself, with composition of functions as its binary operation.

We did also specific calculations in the groups $\mathrm{Gl}_2(\mathbb{Z}_2)$ and S_3.

Friday, November 22. We proved the following theorem.

Theorem. Let F be a field and $f(x) \in F[x]$. Then there exists a field K containing F and $\alpha \in K$ such that $f(\alpha) = 0$.

As a corollary to the theorem, we noted that given any $f(x) \in F[x]$, with degree $f(x) = d$, then there exists a field K containing F and $\alpha_1, \ldots, \alpha_d \in K$ (not necessarily distinct) such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_d)$.

We then stated the Fundamental Theorem of Algebra: Given any non-zero polynomial $f(x) \in \mathbb{C}[x]$, with degree $f(x) = d > 0$, there exist $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ (not necessarily distinct) such that $f(x) = (x - \alpha_1) \cdots (a - \alpha_d)$. As a corollary to the Fudamnetal Theorem of Algebra, we proved the following interesting fact:

Fact. If $f(x) \in \mathbb{R}[x]$ is an irreducible polynomial, then degree $f(x) \leq 2$.

Wednesday, November 20. We proved the following theorem.

Theorem. Let F be a field and $f(x) \in F[x]$ be an irreducible polynomial. Let K denote the commutative ring '$F[x]$ mod $f(x)$'. Then K is a field containing F and $\overline{x} \in K$ is a root of $f(x)$.

Monday, November 18. We began by comparing addition and multiplication in the two fields, $F = \mathbb{R}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of $x^2 + x + 1$ and $\tilde{F}$, the field $\mathbb{R}[x]$ modulo $x^2 + x + 1$. (We pointed out that although F s just $\mathbb{C}$, we were using the representation of $\mathbb{C}$ as $\mathbb{R}(\alpha)$.) We then noted that the operations in these fields are essentially identical, except for the naming of their elements. This parallel construction suggests what one should do to construct a field containing a root to a polynomial, when no such field and root are known, *a priori*.

We then illustrated the upcoming general construction by writing out addition and multiplication tables for $\mathbb{Z}_2[x]$ mod $x^2 + x + 1$. We then observed that the resulting commutative ring is a field with four elements containing $\mathbb{Z}_2$, and the class $\overline{x}$ in this field is a root of $x^2 + x + 1$.

Friday, November 15. Exam 2 (in class).

Wednesday, November 13. We had Quiz 10 and reviewed for Exam 2.

Monday, November 11. For a fixed polynomial $f(x) \in F[x]$, we defined the ring we called $F[x]$ mod $f(x)$. The elements in this ring are the equivalence classes under the equivalence relation given by $a(x) \equiv b(x)$ mod $f(x)$ if $a(x) - b(x)$ is divisible by $f(x)$. We noted that the distinct equivalence classes are the classes of all polynomials having degree less than the degree of $f(x)$. We then defined $\overline{a(x)} + \overline{b(x)} = \overline{a(x) + b(x)}$ and $\overline{a(x)} \cdot \overline{b(x)} = \overline{a(x) \cdot b(x)}$, and noted that this gives a new commutative ring. We emphasized the similarity between this construction and the construction of $\mathbb{Z}$ mod n.

Friday, November 8. We proved the following result known as the Rational Root Test, and worked several examples showing how the RRT can be used to find rational roots of integer polynomials or to show such a polynomial is irreducible (if its degree is three).

Theorem (Rational Root Test). Let $f(x)a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. Suppose $\alpha = \frac{r}{s} \in \mathbb{Q}$ is a root of $f(x)$, where $\text{GCD}(r, s) = 1$. Then $r | a_0$ and $s | a_n$.

Wednesday, November 6. Given fields $F \subseteq K$, $f(x) \in F[x]$ an irreducible polynomial of degree d and $\alpha \in K$ a root of $f(x)$, we proved that $F(\alpha) := \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_i \in F\}$ is the smallest subfield of K containing F and α. We pointed out that finding the multiplicative inverse of a non-zero element of $F(\alpha)$ can be done in exactly the same way as was done in the previous lecture. Namely, if $\gamma = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ is a non-zero element of $F(\alpha)$, if we set $\gamma(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$, and find $r(x), s(x) \in F[x]$ satisfying $1 = r(x)\gamma(x) + s(x)f(x)$, with $\deg r(x) < \deg f(x)$, then $\gamma^{-1} = r(\alpha) \in F(\alpha)$.

Monday, November 4. We proved in detail that the set $\mathbb{Q}(\sqrt[3]{2}) := \{\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4} \mid \alpha, \beta, \gamma \in \mathbb{Q}\}$ is the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and $\sqrt[3]{2}$. One key pont was the following: If $a = \alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4}$ is a non-zero element of $\mathbb{Q}(\sqrt[3]{2})$, then its multiplcative inverse is $r(\sqrt[3]{2})$, where $1 = r(x)(\alpha + \beta x + \gamma x^2) + s(x)(x^3 - 2)$, with the degree of $r(x)$ less than the 3.

Friday, November 1. Contrary to the examples done in the previous lecture, we proved that if $\sqrt[3]{2}$ denotes the real cube root of 2 (i.e., the real number where the graph of $y = x^3 - 2$ crosses the x-axis), then the set $L := \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ does not form a field. The reason for this is that the product $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ does not belong to L. The proof of this was by contradiction. We showed that if $\sqrt[3]{4} \in L$, then $\sqrt[3]{2}$ must satisfy a monic polynomial of degree two with coefficients in $\mathbb{Q}$. This ultimately leads to the contradiction that $\sqrt[3]{2}$ is a rational number. We then calculated the two complex cube roots of two and showed that all of the cube roots of 2 be obtained by multiplying $\sqrt[3]{2}$ by the three cube roots of 1. Finally, we stated, but did not prove, that $L' := \{a + b\sqrt[3]{3} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ *is* a field.

In addition, we assigned a problem for bonus points on a quiz (due Monday): Prove that $\sqrt[3]{2}$ is not a rational number.

Wednesday, October 30. We began our discussion of roots of polynomials with coefficients in a field, noting that given $f(x) \in F[x]$, with F a field, there may not exist any roots of $f(x)$ in F, but $f(x)$ may have roots in a larger field K containing F. Our ultimate goal will be to show that given any non-constant $f(x) \in F[x]$,

there exists a field K containing F and $\alpha \in K$ such that $f(\alpha) = 0$. We then showed that even though $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has roots $\pm\sqrt{2}$ in $\mathbb{R}$, one can construct a much smaller field K containing $\mathbb{Q}$ and $\sqrt{2}$, namely $K := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Similarly, we showed that $E := \{a + bi \mid a, b \in \mathbb{Q}\}$ is a field containng $\mathbb{Q}$ and the roots of $x^2 + 1$. In fact, we showed that K and E are the smallest fields with the required properties.

Monday, October 28. We proved that the ring of Gaussian integers is a Euclidean domain, where the associated function v is just the usual norm on the Gaussian integers. Consequently: In the Gaussian integers,

(i) GCDs exist.
(ii) A GCD of any two Gaussian integers is divisible by any common divisor of the given Gaussian integers.
(iii) A GCD of two Gaussian integers is a Gaussian integer combination of the given Gaussian integers.
(iv) Every non-zero, non-unit Gaussian integer can be written uniquely (up to unit multiples) as a product of irreducible Gaussian integers.

We then showed how with $z = 3 + 2i$ and $w = 1 + i$, we can write $z = wq + r$, with q, r Gaussian integers such $N(r) < N(w)$. In fact, we did this in two distinct ways, thereby showing that in a Euclidean domain, when we write $b = aq + r$ with $r = 0$ or $v(r) < v(q)$, q and r need not be unique.

Friday, October 25. We proved the following two theorems, which together show that the Fundamental Theorem of Arithmentic holds for a Euclidean domain.

Theorem A. Let R be a Euclidean domain. Suppose $p_1 \cdots p_r = q_1 \cdots q_s$, where each p_i, q_j in R is an irreducible element. Then $r = s$ and after re-indexing the q_j, $q_i = u_i p_i$, for units $u_i \in R$, for all $1 \leq i \leq r$.

The proof of this Theorem A proceeds by induction on $r \leq s$ and relies upon the proposition proved at the end of class on October 23.

Theorem B. Let R be a Euclidean domain. There every non-zero, non-unit element in R can be written as a product of irreducible elements.

The proof of Theorem B for an element $a \in R$ is by induction on $v(a)$.

Throughout, we emphasized the similarity between the proofs of Theorems A and B with the proofs previously given in the special cases that the $R = \mathbb{Z}$ or $R = F[x]$, with F a field.

Wednesday, October 23. We began the class with Quiz 7. We then reviewed the results from last class concerning greatest common divisors in a Euclidean domain. We followed this by proving a lemma leading to the following proposition:

Proposition. Let R be a Euclidean domain and $p \in R$ an irreducible element such that $p | a_a \cdots a_n$, for $a_1, \ldots, a_n$ non-zero elements in R. Then $p | a_i$, for some i.

We then discussed (but did not formally prove) how this fact leads to a uniqueness statement for factoring elements in a Euclidean domain as a product of irreducible elements.

Monday, October 21. We began in detail our discussion of how the common properties of the integers and polynomials discussed previously, hold in general for Euclidean Domains. We began by showing that if R is a Euclidean Domain with associated function v, then :

(i) $v(1) \leq v(a)$, for all $0 \neq a \in R$.
(ii) If is u is a unit, then $v(ua) = v(a)$, for all $0 \neq a \in R$.
(ii) If a, b are non-zero, non-units in R, then $v(ab) > v(b)$ and $v(ab) > v(b)$.
(iv) $u \in R$ is a unit if and only if $v(u) = v(1)$.

We then defined what it means for an element d in a Euclidean domain to be a greatest common divisor of two non-zero elements. In particular we proved the proposition below.

Proposition. Let R be a Euclidean Domain and a, b non-zero elements in R. Let $d = r_0 a + s_0 b \in R$ be such that $v(d)$ is the least element in the set $\{v(ra + sb) \mid ra + sb \neq 0, r, s \in R\}$. Then:

(i) d is a greatest common divisor of a and b.
(ii) d is divisible by any common divisor of a and b.

(iii) If d_1 and d_2 are greatest common divisors of a and b, then $d_2 = ud_1$, for some unit $u \in R$.

Friday, October 18. We discussed division properties for an integral domain and the inconsequential, but unavoidable, role played by units in statements concerning factoring elements in an integral domain. We then calculated the units in the rings $\mathbb{Z}$, $F[x]$ (F, a field) and $\mathbb{Z}[i]$. We ended class by defining what it means for an integral domain to be a Euclidean Domain, and noted that $\mathbb{Z}$ and $F[x]$ are Euclidean Domains.

Wednesday, October 16. We had Quiz 6. Then we reviewed the definition of an integral domain and the definition of a field. We pointed out that all of the results we previously proved for $F[x]$, for $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ hold for $F[x]$ when F is an arbitrary field. In particular, we assigned as extra credit turning in a proof of the Fundamental Theorem of Arithmetic for $F[x]$ that includes all relevant preliminaries. Finally, we proved the following proposition.

Proposition. Let $n \geq 2$. For the ring $\mathbb{Z}_n$, the following are equivalent:

(i) n is a prime number.
(ii) $\mathbb{Z}_n$ is a field.
(iii) $\mathbb{Z}_n$ is an integral domain.

Wednesday, October 9. We verified that for $n > 1$, $\mathbb{Z}_n$ is a ring. We also proved a few elementary properties of rings. We then defined what it means for a commutative ring to be a integral domain or a field. We ended class by proving the following proposition:

Proposition. Let R be a commutative ring.

(i) If R is a field, then R is an integral domain.
(ii) Suppose R is an integral domain and $a, b, c \in R$. If $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$.

Monday, October 7. We reviewed the definition of a ring. Then we computed addition and multiplication tables for the rings $\mathbb{Z}_5$ and $\mathbb{Z}_4$. We noted that the group table for $\mathbb{Z}_5$ shows that every non-zero element in $\mathbb{Z}_5$ has a multiplicative inverse, while the group table for $\mathbb{Z}_4$ shows that the class of 2 in $\mathbb{Z}_4$ does not have a multiplicative inverse.

Friday, October 4. Exam 1.

Wednesday, October 2. We discussed the format of Exam 1. We then defined the concept of a ring and gave several examples of rings.

Monday, September 30. We completed the proof of the following theorem:

Fundamental Theorem of Arithmetic for monic polynomials. Let $f(x) \in F[x]$ be a monic polynomial of degree greater than zero. Then there exist monic, irreducible polynomials $p_1(x), \ldots, p_r(x) \in F[x]$ such that $f(x) = p_1(x) \cdots p_r(x)$. Moreover, if $f(x) = q_1(x) \cdots q_s(x)$, with each $q_j(x) \in F[x]$ monic and irreducible, then $r = s$, and after re-indexing, $p_i(x) = q_i(x)$, for all $1 \leq i \leq r$.

As a corollary, we then proved that any non-constant polynomial in $F[x]$ can be written uniquely as an element of F times a product of irreducible, monic polynomials in $F[x]$. We finished class by recapitulating the similarity between the results (and their poofs) we have obtained over the integers and the corresponding results over $F[x]$.

Friday, September 27. We proved a number of consequences of the existence of GCD for polynomials in $F[x]$, including:

(i) Suppose $f(x), g(x) \in F[x]$ are non-zero polynomials with $\gcd(f(x), g(x)) = 1$. If $f(x)$ divides $g(x)h(x)$, then $f(x)$ divides $h(x)$.
(ii) Suppose $f(x) \in F[x]$ is a monic, irreducible polynomial. Given $g(x) \in F[x]$, then the GCD of $f(x)$ and $g(x)$ is 1 or $f(x)$.
(iii) Suppose $f(x) \in F[x]$ is a monic irreducible polynomial and $f(x)$ divides the product $g_1(x) \cdots g_r(x)$. Then $f(x)$ divides $g_j(x)$, for some $1 \leq j \leq r$.

We then used the properties above to prove the following uniqueness statement.

Proposition. Suppose $p_1(x)\cdots p_r(x) = q_1(x)\cdots q_s(x)$, where each $p_i(x)$ and each $q_j(x)$ is a monic irreducible polynomial in $F[x]$. Then $r = s$, and after re-indexing the $q_j(x)$, $p_1(x) = q_1(x), \ldots, p_r(x) = q_r(x)$.

Wednesday, September 25. We proved the following theorem concerning greatest common divisors in $F[x]$:

Theorem. Let $f(x)$ and $g(x)$ be non-zero polynomials in $F[x]$ and let X denote the set of all non-zero polynomial expressions of the form $r(x)f(x) + s(x)g(x)$. Then:

(i) X contains a unique monic polynomial of least degree, which we call the GCD of $f(x)$ and $g(x)$.
(ii) If $d_1(x) \in F[x]$ is a common divisor of $f(x)$ and $g(x)$, then $d_1(x)$ divides the GCD of $f(x)$ and $g(x)$.

Throughout the proof presented in class, we emphasized the similarity of the proof of this theorem with the proof of the corresponding theorem for the integers presented on September 16. We ended class with an example showing how using the Euclidean algorithm to find GCDs works exactly the same for polynomials as it does for integers.

Monday, September 23. We proved the uniqueness portion of the division algorithm for polynomials in $F[x]$. We put particular emphasis on the similarity between the proof of this fact and its corresponding statement over the integers. We then discussed elementary division properties of polynomials and defined the greatest common divisor (GCD) of two non-zero polynomials. We then gave a heuristic argument for why the GCD of two polynomials exists and stated an existence theorem to be discussed during the next lecture.

Friday, September 20. We started our discussion of polynomials with coefficients in F, where F is any one of the three number systems: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. We observed that all of the usual rules of arithmetic apply, e.g., addition and multiplication of polynomials are commutative, associative and satisfy the distributive property, and we also noted that the degree of a product of polynomials is the sum of the degrees of the polynomials comprising the product. We then proved the existence part of the division algorithm for $F[x]$:

Division Algorithm for Polynomials. Let $f(x), g(x)$ be non-zero polynomials with coefficients in F. Then there exist unique $q(x), r(x) \in F[x]$ such that:

(i) $g(x) = f(x)\cdot q(x) + r(x)$
(ii) degree $r(x) <$ degree $f(x)$.

Wednesday, September 18. We proved that if a prime number divides a finite product of integers, then it must divide one of those integers. This enabled us to prove the following proposition:

Proposition. Suppose $n > 1$ and

$$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s,$$

where :

(a) Each p_i, q_j is a prime number
(b) $p_1 \le p_2 \le \cdots \le p_r$ and $q_1 \le q_2 \le \cdots \le q_s$.

Then $r = s$ and $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$.

Putting this together with a previous result showing that every positive integer greater than one can be written as a product of primes, we thereby established:

The Fundamental Theorem of Arithmetic: Every positive integer greater than one can be written **uniquely** as a product of primes.

Monday, September 16. We proved the following theorem characterizing greatest common divisors:

Theorem. Let a, b be non-zero integers and set $X := \{ra + sb \mid r, s \in \mathbb{Z} \text{ and } ra + sb > 0\}$. Then:

(i) $\gcd(a, b)$ is the least element in X.
(ii) If d' is common divisor of a and b, then $d'|d$.

We then derived the following consequences:

(i) Integers a and b are relatively prime if and only if there exist $r, s \in \mathbb{Z}$ such that $1 = ra + sb$.
(ii) If $a, b \in \mathbb{Z}$ are relatively prime and $a|bc$, then $a|c$.
(iii) If p is a prime number and $p|(m \cdot n)$, then $p|m$ or $p|n$, for $m, n \in \mathbb{Z}$.

Friday, September 13. We defined the *greatest common divisor* of two integers and worked several examples showing how repeated iteration of the division algorithm leads to finding the greatest common divisor of two integers. This process is called the *Euclidean algorithm*. For the examples worked in class, we also showed how to use the equations derived by the Euclidean algorithm to write the GCD of integers a and b as an integer combination of a and b.

Wednesday, September 11. We stated and proved a slightly more general version of the Well Ordering Principle: Let X be a non-empty subset of the integers that is bounded below. Then X has a least element.

We then stated and proved the Division Algorithm for the integers: Given integers a and b with $b > 0$, there exists **unique** integers q, r such that : (i) $a = bq + r$ and (ii) $0 \leq r < b$.

Monday, September 9. We had our second quiz followed by a discussion of the Second Principle of Induction. The following statements were proven to illustrate how this principle works:

(i) Every natural number greater than or equal to 2 is either a prime number or a product of prime numbers.
(ii) Every postage value greater than or equal to 12 cents can be obtained using a combination of 4 cent stamps and 5 cent stamps.
(iii) The Well Ordering Principle: Every non-empty set S of natural numbers contains a least element.

Regarding (ii): We noted that though the base cases is $n = 12$, we needed to prove the cases $n = 12, 13, 14, 15$, separately, as the proof of the inductive step for the case of n cents requires subtracting 4 from n. Thus, we need to insure $n - 4 \geq 12$ in this step.

Regarding (iii): If S is a non-empty set of natural numbers, the proof proceeds by induction on the statement: For all $n \geq 1$, if $n \in S$, then S has a least element. Once this statement has been proven, S has a least element, since $n \in S$, for some n, as S is non-empty.

Friday, September 6. We proved that a partition of a set X determines an equivalence relation on X given by $x_1 \sim x_2$ if and only if x_1, x_2 be long to the same subset of the partition. It then follows that the distinct equivalence classes under this relation are just the subsets given in the partition.

We then began a discussion of the Frst Principle of Mathematical Induction, illustrating it with the examples:

(i) $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, for al $n \geq 1$.
(ii) $2^n > n + 4$, for all $n \geq 3$.
(iii) $1 + 4 + 7 + \cdots + (3n - 2) = \frac{n(3n-1)}{2}$, for all $n \geq 1$.

We ended class by showing that the First Principle of Induction does not always work by showing it does not immediately apply when we try to prove the statement: Every natural number greater than or equal to 2 is either a prime number or a product of prime numbers.

Wednesday, September 4. Given a set X with an equivalence relation $\sim$, we proved that:

(i) If $x_1, x_2 \in X$, then either $[x_1] \cap [x_2] =$ or $[x_1] = [x_2]$.
(ii) X is the disjoint union of its distinct equivalence classes.

We noted that this means that the distinct equivalence classes of X partition X. We then noted (but did not prove) that if we have a partition of X, this partition gives rise to an equivalence relation whose equivalence classes are the elements of the partition.

Friday, August 30. Given an equivalence relation, we defined the notion of equivalence class. We then calculated the equivalence classes for the examples from the previous lecture. We also showed that for $X = \mathbb{Z}$ and the relation $n \sim m$ if and only if $n - m$ is divisible by 5, $\sim$ is an equivalence relation. We then showed that

$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$[4] = \{\ldots, -6, -2, 4, 9, 14, \ldots\}$$

are the distinct equivalence classes under the given equivalence relation. It was noted that, in this example, X is the disjoint union of the five equivalence classes above and that this is, in fact, a special case of a general phenomenon.

Wednesday, August 28. We defined what it means for a relation $\sim$ on a set X to be an *equivalence relation*. The relation must satisfy:

(a) $x \sim x$, for all $x \in X$. (The *reflexive* property)
(b) For all $x, y \in X$, if $x \sim y$, then $y \sim x$. (The *symmetric* property)
(c) For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$. (The *transitive* property)

We then showed the following relations are equivalence relations.

(i) X any set and taking $x \sim y$ if and only if $x = y$.
(ii) $X = \{a, b) \mid a, b \in \mathbb{Z}, \text{with } b \neq 0\}$ with $(a, b) \sim (c, d)$ if and only if $ad = bc$.
(iii) X the set of 2×2 matrices over $\mathbb{R}$ with $A \sim B$ if and only if there exists an invertible $P \in X$ with $B = P^{-1}AP$.

Monday, August 26. We discussed the format of the class and presented an overview of topics to be covered during the semester. This was followed by a discussion of basic set theoretic operations (intersections, unions, complements), including DeMorgan's laws which state:

(i) $(A \cup B)' = A' \cap B'$
(ii) $(A \cap B)' = A' \cup B'$

for sets A, B contained in a universal set U. We then defined the notion of a relation between a set X and a set Y (a relation R is just a subset of $X \times Y$), and noted which relations are functions (those for which for all $x \in X$, there is a unique $y \in Y$ such that $(x, y) \in R$).