Lemma Dump

May 1, 2025

Abstract

A list of useful lemmas.

Lemma 1 (Well ordering principle of the natural numbers)**.** *A nonempty partition of the natural numbers have a least element.*

Proof. Consider the successor function construction of the natural numbers. One can construct any partition of the natural numbers by removing natural numbers from the set of natural numbers. This set has a least element of 1 by the principle of mathematical induction. Suppose we remove the least element in any step of the construction leaving behind a nonempty partition fo the natural number. The successor of the least element becomes the new least element. If it does not exist in the set, then consider the successor of that element by the principle of mathematical induction. This terminates since we assumed the remaining partition is nonempty, and the least element would be designated. Since any nonempty partition of the natural numbers can be constructed this way, therefore a nonempty partition of the natural numbers have a least element. □

Lemma 2 (Well ordering principle of the integers)**.** *A nonempty partition of the integers have a least element if one assumes the axiom of choice.*

Proof. Consider the construction by the axiom of choice for $0 < 1 < -1 < 2 < -2 < ....$ One can construct any partition of the integers by removing an integer from this well order. This set has a least element of 0 by the principle of mathematical induction. Suppose we remove the least element in any step of the construction leaving behind a nonempty partition fo the natural number. The successor of the least element becomes the new least element. If it does not exist in the set, then consider the successor of that element by the principle of mathematical induction. This terminates since we assumed the remaining partition is nonempty, and the least element would be designated. Since any nonempty partition of the natural numbers can be constructed this way, therefore a nonempty partition of the natural numbers have a least element. □

Lemma 3. *Let S be a set, and let $\equiv$ be an equivalence relation on the set S. Let a and b be elements of the set S, then either the equivalence classes containing a called S_a is equal to the equivalence class containing b called S_b, or these equivalence classes are disjoint. Further, the set S is the disjoint union of distinct equivalence classes. The number of elements in each equivalence class adds to become the number of elements in the set S.*

Proof. Suppose without loss of generality that a is distinct from b, and the non-empty equivalence classes with more than two elements are not disjoint since if they are disjoint that is one case and we are done. Likewise if there is only one element in the set S. We want to show that if a and b are in the intersection of S_a and S_b, then this intersection is equal to both S_a and S_b. Indeed, b is equivalent to a since it is contained in S_a, so they must be the same equivalence class. Therefore, the intersection of S_a and S_b is equal to S_a and S_b, and if a set has same elements, they are equal. By case analysis, there can only be two cases the equivalence classes S_a is equal to S_b, or they are disjoint. The set S must contain the disjoint union of equivalence classes, since if two equivalence classes intersect they are the same set. Since a set must have distinct elements, the number of elements in each equivalence class under disjoint union add up to the number of elements in the set S. □

When you have a non-empty set graded by the naturals, you can use the well ordering principle. In fact, if you can use the well ordering principle, then you can use the principle of mathematical induction. These are equivalent.

Lemma 4. *Mathematical induction is a valid way to show that statements P_n are true for all natural numbers n.*

Proof. Define the set of all statements where P_n is false as the set S. If the set is empty, then the lemma is true. Suppose the set is nonempty, for contradiction. Consider the case of $n > 1$ without loss of generality, since there is a contradiction from the initial step of P_0 being true by mathematical induction. Since we assume the well ordering principle, therefore this set has a minimal element. We will want to show that this is not the minimal element. The contrapositive of mathematical induction is that if P_{n+1} is false, then P_n is false. If we consider the minimal element to be P_{n+1}, and statements up to P_n are not in the set, then P_n is also in this set. This is contrary to the minimality of P_{n+1} by hypothesis. Since the set must be empty if mathematical induction is valid, therefore mathematical induction is a valid way to show that statements P_n are true for all natural numbers n. □

Lemma 5. *Suppose a and b are integers. Then there exists unique integers, defined as the quotient q and the remainder r, such that $a = qb + r$ with the condition that the remainder r is more than or equal to zero, but less than b.*

Proof. Assume b is larger than a without loss of generality, if they are equal then the quotient is 1 and the remainder is 0 which is unique. Otherwise, one can swap between a and b. Since the integers are closed under subtraction by assumption (one will have to use the successor function and define subtraction, or use the fact that the integers are a ring), therefore $a - nb$ is an integer, for n an integer. These integers are all unique, one can apply mathematical induction on $n = 1$ to show that all these integers are unique to each other. We now show that there exists a case where r is less than b. This must exist without loss of generality, since if $r = a - nb$ is greater than b, then redefine the remainder r to be $a - (n+1)b$ which must be less than b but still greater than 0, with the quotient being $n+1$ and all these case follow from the closure of the integers as a ring under subtraction. Therefore, the remainder r exists, and the corresponding coefficient of integer b must be the quotient n. □

This is not a good proof of this lemma, but it is mine.

Lemma 6. *Let a and b be nonzero integers, then there exists a linear combination with coefficients u and v in the integers such that $au + bv$ is equal to the greatest common divisor $gcd(a,b)$.*

Proof. A divisor of a is an integer u such that au is an integer. A divisor of b is an integer v such that bv is an integer. The greatest common divisor exist, since $au + bv$ is an integer, so it is equal to $gcd(a,b)w$, where $gcd(a,b)w$ is a product of an integer w that is not equal to 1 and 1 without loss of generality, if it is 1 we are done and it is nonzero without loss of generality since once can choose divisors of u and v to make it nonzero. We have $gcd(a,b)m_a u + gcd(a,b)m_b v = gcd(a,b)w$ so $m_a u + m_b v = w$. We can iterate this process, and since w is nonzero and with each step, the integers w decreases, by the well ordering of the integers, w will terminate at 1 after correcting up to sign by taking -1 when necessary onto integers u and v, and the product of $gcd(a,b)m_{a_1}m_{a_2}...$ and $gcd(a,b)m_{b_1}m_{b_2}...$ terminates the the integers u and v of interest. □

This is a nice proof idea which is to find a representing object fo rthis construction.

Lemma 7. *Suppose S is a set. Suppose the set S is a disjoint union of subsets. Define a relation on elements a and b of set S, where a is related to b are in the same subset of the set S. Show that this is an equivalence relation.*

Proof. An element a is related to itself, since they are in the same subset in the disjoint union. The relation is reflexive. If a is in the same set as b, then b is in the same set as a since the subset $\{a,b\}$ is in the subset of S. The relation is symmetric. If a is in the same set as b, and b is in the same set as c since the subset $\{a,b,c\}$ is in (or is) the subset of S and a is in the same set as c. The relation is transitive. For cases with insufficient elements, they follow reflexivity, symmetry, and transitivity vacuously. Since the relation is reflexive, symmetric and transitive, therefore the relation defined in the lemma is an equivalence relation. □

Lemma 8 (Cauchy's Theorem)**.** *If a finite group G has the property that its order is $|G|$ is divisible by a prime p, then the group G has an element of order p*

Proof. Consider the set of all p-tuples g^i being the identity in G in the product group G^p and the action of a finite p-group P on it, determined by $p-1$ elements since the product of $p-1$ elements has an inverse by construction. Since $p-1$ is not divisible by p, then this action has a fixed point g, corresponding to the element of order p in the group G. □

Lemma 9 (p-group fixed point theorem)**.** *Suppose P is a finite p-group. Suppose X is a set in which the finite p-group P acts, then the subset X^p of fixed points satisfy $|X^P|$ is congruent to $|X|$ modulo P. Particularly, if $|X|$ is not congruent to 0 modulo p, then this action has a fixed point.*

Proof. A set X can be decomposed into a finite disjoint union of subsets.

These are acted on by the finite p-group P by hypothesis. Suppose this action does not have a fixed point, then all subsets of this disjoint union are acted on by the finite p-group P, and all have cardinality that is divisible by p. This means the cardinality of the disjoint union is divisible by p, and therefore if this action does not have a fixed point, then $|X|$ is congruent to 0 modulo p. By contrapositive, $|X|$ is not congruent to 0 modulo p, then this action has a fixed point. If we consider the exclusion of subsets acted on by the finite p-group P, then this is equivalent to considering the cardinality of X modulo positive integer p. □

Lemma 10. *Orbits of cyclic group of prime order p have orbit sizes of 1 and p.*

Proof. By the p-group fixed point theorem, using case analysis, there are either fixed points or elements in the orbit of the cyclic group of size p, with no larger orbits since these are of prime order. □

Lemma 11. *Suppose G is a finite p-group. It has nontrivial centre $Z(G)$, and every such group is nilpotent.*

Proof. Consider the self action of the finite p-group G on its conjugate G 1 to rule out the determination of a product of the remaining elements and its inverse.

If G is of prime power order, then this set has the cardinality of $p^n - 1$, which is not divisible by p. By the p-group fixed point theorem, the finite p-group G has a fixed point. This fixed point commutes with every element of the finite p-group G, and hence is a nontrivial central element since it commutes with every other element of g as a fixed point with orbits being disjoint unions. It terminates in the trivial subgroup or a fixed point of finite length since the group G is finite, and hence it is nilpotent. □

Lemma 12 (Fermat's Little Theorem). *Let a be a nonnegative integer, and p be a prime. Then $a^p - a$ is divisible by the prime p.*

Proof. Pick the set X as the partition from 0 to a, and apply the p-group fixed point theorem with the cyclic group P of prime order p. □

Lemma 13. *Prove by mathematical induction tha tthe sum of cubes is $\dfrac{n^2(n+1)^2}{4}$.*

Proof. The base case of 1 can be checked by hand. For the induction step, reverse the completion of the square of (n^2+4n+4) when factorising $(n+1)^2$. □

Lemma 14. *If a divides b and b divides a, then a is equal to b.*

Proof. We have $a = ub$ and $b = va$, solving for $a - nua = 0$ and factorising $a(1-uv) = 0$ gives $uv = 1$. Since the ring of integers has no multiplicative inverses, therefore $u = v = 1$ and hence $a = b$. □

Lemma 15. *Prove that n choose k is equal to n choose $n-k$ for integers n and k.*

Proof. We note that the ring of integers has commutative multiplication. By definition, the coefficient of n choose k is $(n-k)!k!$ which is commutative by the substitution $l = n-k$. □

Lemma 16. *Elements of finite extensions are algebraic. Algebraic elements are always contained in finite extensions.*

Proof. The idea is to suppose an algebraic integer a is in a finite extension of L, then we have $[L:K]$ is n less than infinity, then take $1, a, a^2, ..., a^n$, this is $n+1$ elements of a n-dimensional vector space. Since this is of higher dimension, there must be a nontrivial linear relation $k_0 + k_1 a + ... k_n a^n$, so a is algebraic. For the converse, suppose $p(x)$ is an irreducible polynomial in the field extension $K[x]$, take the quotient of the ideal $K[x]/(p)$ is a field. This is obviously a ring. This a ring, now we check existence of inverses, suppose $q(x)$ is in $K(x)/(p)$, $q(x)$ is nonzero, then q and p are coprime since $p(x)$ is irreducible. Therefore, $a(x)q(x) + b(x)p(x) = 1$ can be found by Euclidean algorithm, so $a(x)$ is inverse of $q(x)$ in $K(x)/((p(x)))$. Since a is a root of $p(x)$ in $K[x]$, where p is irreducible, so $K[x]/p(x)$ is a map to L taking x to a. The image of $K[x]/(p)$ is in L. □

Lemma 17. *Sums, products, quotients and differences of algebraic integers are algebraic. Consequently, roots of polynomials are algebraic.*

Proof. Consider chain of extensions by pairs of algebraic integers, these are finite extensions. Polynomials are finite sums and products of algebraic integers so these are algebraic as well. □