1 Directory

- **Fall 2020**: G1 (Problem 6.8), G2 (Problem 2.4), G3 (Problem 6.2), RF1 (Problem 6.11), RF2 (Problem 6.12), RF3 (Problem 6.13), LA1 (Problem 6.14), LA2 (Problem 6.15), LA3 (Problem 6.16)

2 The Sylow Theorems

Problem 2.1: S20

Let p and q be primes. Prove that a group of order pq is solvable.

Proof. Suppose that p, q are prime and G is a group of order pq. If $p = q$, then G has order p^2. Then G must be abelian and is therefore solvable. Assume now that $p \neq q$. By the Sylow Theorems there exists a subgroup $P \leq G$ of order p. Since $p \neq q$ and q is prime, there is exactly one Sylow p-subgroup. Therefore, P is normal in G. Consider the sequence of normal subgroups

$$0 \triangleleft P \triangleleft G$$

and note that G/P is of order q and $P/0$ is of order p. As both of these quotients are of prime order, they are cyclic and therefore abelian. □

Problem 2.2: F19

(a) Suppose that G is a group with exactly two subgroups. Prove that G is finite and of prime order.

(b) Must the converse of the previous part be true?

Proof. Suppose that G is a group with exactly two subgroups. Seeking a contradiction, suppose that G is infinite and choose some non-identity element $x \in G$. If $\langle x \rangle = G$, then G is an infinite cyclic group. That is, $G \cong \mathbb{Z}$. As $\mathbb{Z}$ has infinitely many subgroups, this is a contradiction. So, there exists $y \in G - \langle x \rangle$. In this case, there are three distinct subgroups, $\{e\}, \langle x \rangle, \langle y \rangle$, again a contradiction. Therefore, G must be finite.

Let p be some prime dividing the order of G. By Cauchy's Theorem (4.1), there exists an element x of order p. As there are only two subgroups and $p > 1$, $\langle x \rangle = G$, implying that G is of prime order p. □

Proof. Suppose that G is finite and of prime order p. By Lagrange's Theorem, any subgroup of G is of order 1 or order p. The only subgroup of order 1 is the trivial subgroup and the only subgroup of order p is G. That is, G has exactly two subgroups. □

Problem 2.3: F19

Suppose that G is a finite group with exactly three conjugacy classes. Show that G is isomorphic to either S_3 or to $\mathbb{Z}/3\mathbb{Z}$.

Proof. Let $r, s, t \geq 1$ denote the sizes of the three distinct conjugacy classes. Without loss of generality, we may assume $r = 1$ as conjugacy classes partition a group and the identity element is in its own conjugacy class. Then, $|G| = 1 + s + t$. Note that the conjugacy classes of G are the same as the orbits formed by the action of G acting on itself via conjugation. Therefore, by the Orbit Stabilizer Theorem, s and t must both divide $|G|$.

If G is abelian, then $s = t = 1$ as every element is in its own conjugacy class. This means that $|G| = 3$ and therefore $G \cong \mathbb{Z}/3\mathbb{Z}$ since this is the only group of order 3.

Now assume that G is non-abelian. Then, some conjugacy class of G must be of size greater than 1. Assume that $s \geq 2$. Note that $1 + t = |G| - s$ and since s divides $|G|$, s must divide $1 + t$. Therefore, $s \leq 1 + t$. As both s and t are positive integers, this means that $s = t$ or $s = 1 + t$. If $s = t$, then $|G| = 1 + 2s$ and since s divides $|G|$, s must divide 1. This is only possible if $s = 1$. By assumption, $s \geq 2$ and therefore we may assume that $s = 1 + t$. In this case, $|G| = 2 + 2s = 2(1 + s)$. As $s \geq 2$ and s divides $|G|$, s divides 2. That is, $s = 2$ and therefore $t = 3$. Then, $|G| = 6$. As G is non-abelian, $G \cong S_3$ since this is the only non-abelian group of order 6. □

Proof. Suppose that G is finite and has exactly three conjugacy classes, of sizes r, s, t. As conjugacy classes partition a group, G is of size $r + s + t$.

If G is abelian, every conjugacy class must be of size 1. Therefore, $|G| = 3$ and thus $G \cong \mathbb{Z}/3\mathbb{Z}$.

Suppose now that G is not abelian. Without loss of generality, assume that $r = 1$ since the identity element must be in a conjugacy class of size 1. □

Problem 2.4: F20

(a) Give two examples of non-abelian groups of order 48 that are non-isomorphic.

(b) Show that a group of order 48 cannot be simple.

Proof. Let $G = D_{48}$ and $H = D_{24} \times \mathbb{Z}_2$ where D_{48} and D_{24} are the dihedral groups of orders 48 and 24, respectively. Each of G and H are of order 48 and are clearly non-abelian. However, these groups are non-isomorphic. The generating element for rotation in G has order 48. However, the highest possible order for an element in H is 24 since the order of an element $(x, y) \in H$ is the least common multiple of the order of x in D_{24} and the order of y in $\mathbb{Z}_2$. □

Proof. Let G be of order 48. Notice that $48 = 2^4 \cdot 3$. By the Sylow Theorems, the number of Sylow 2 subgroups n_2 is either 1 or 3 as it must divide 3 and be equivalent to 1 modulo 2. Similarly, the number of Sylow 3 n_3 subgroups is either 1, 4, or 16. If G is not simple than $n_2, n_3 \neq 1$ since either being equal to 1 would guarantee a normal subgroup. This means that $n_2 = 3$ and $n_3 = 4$ or $n_3 = 6$. Each Sylow 2 subgroup is of size 16. Suppose that H and K are two distinct Sylow 2 subgroups. Then, $H \cap K$ is a subgroup of H and must be of order 1,2,4, or 8. If $|H \cap K| \leq 4$, then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K} \geq 64.$$

But, $HK \subseteq G$ and therefore this is impossible. Thus, $|H \cap K| = 8$. As any subgroup of index two is normal, $H \cap K$ is normal in each of H and K. The normalizer N of $H \cap K$ in G includes H, K, and $H \cap K$ and therefore must be of size at least $\text{lcm}(8, 16) = 24$. Since the normalizer is also a subgroup in G, either $|N| = 24$ or $|N| = 48$ since $|H|$ must also divide $|N|$. In either case, N is normal in G as N is either of index 2 or equal to G. This is a contradiction to G being simple. □

Problem 2.5: S19

Prove that every group of order 21 has a normal subgroup of index 3, but that not every group of order 21 is abelian.

Proof. Suppose that $|G| = 21$. By the Sylow Theorems, there exists a Sylow 7-subgroup, say P, of order 7. There's exactly one Sylow-7 subgroup because the only number that divides 1 and is equivalent to 1 modulo 7 is 1. Therefore P is normal in G and $|G/P| = 3$. □

Proof. Consider the subgroup of $M_{2\times 2}(\mathbb{Z}_7)$ given by $G = \langle A, B \rangle$ where

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$A = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}.$$

Upon inspection,

$$A^7 = B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$BAB^{-1} = A^2.$$

This group is non-abelian but is of order 21.

I should probably add more details here about why this construction is guaranteed to be of order 21. It's clear there are at most 21 elements, but how do we show that there are no duplicates? □

3 $G/Z(G)$ is Cyclic

Problem 3.1: S20

Let G be a group and H a subgroup of G contained in the center $Z(G)$ of G such that G/H is cyclic.

(a) Show that G is abelian.

(b) Show that every group of order p^2 with p a prime is abelian. *It may be assumed that a p-group has nontrivial center.*

Proof. Suppose that $G/H = \langle gH \rangle$ for some $g \in G$. Let $a, b \in G$. By assumption, $a = g^k H$ and $b = g^m H$ for some $k, m \in \mathbb{N}$. Therefore, $a = g^k h_1$ and $b = g^m h_2$. Since elements in H commute with every element in G and powers of G commute with one another,

$$ab = g^k h_1 g^m h_2 = g^m h_2 g^k h_1 = ba$$

proving that G is abelian. □

Proof. Suppose that $|G| = p^2$ with p a prime. Because G is a p-group, it has nontrivial center and thus $|Z(g)| > 1$. By Lagrange's Theorem, $|Z(G)| = p$ or $|Z(G)| = p^2$. If $|Z(G)| = p^2$, $Z(G) = G$. If $|Z(G)| = p$, $|G/Z(G)| = p$. That is, $G/Z(G)$ is cyclic and therefore G is abelian. □

Problem 3.2: S19

(a) Suppose that G is a group and $G/Z(G)$ is cyclic. Prove that G is abelian.

(b) Let p be a prime number and G a non-cyclic finite p-group. Prove that G contains a normal subgroup N such that $G/N \cong C \oplus C$ where C is a cyclic group of order p.

Proof. See 3.1. □

Proof. Suppose that $|G| = p^k$ with $k \geq 2$. Assume that G is not cyclic. □

4 Order Stabilizer Theorem

Note that 4.1 is Cauchy's Theorem and comes up for many Sylow-like problems. There's another version of the proof specifically for the case when $p = 2$ that does not involve group actions.

Problem 4.1: F18

Let G be a finite group with order that is divisible by a prime p. Prove that G contains an element of order p.

Proof. Assume that G is a finite group such that a prime p divides $|G|$. Define a set $X \subseteq G^p$ as

$$X = \{(x_1, \ldots, x_p) \in G^p : x_1 \cdots x_p = e\}.$$

That is, X is the set of all p-tuples of elements in G where the product of the elements is the identity in G. Note that by choosing $x_1, \ldots, x_{p-1}$, x_p is determined as

$$x^p = (x_1 \cdots x_{p-1})^{-1}.$$

This means that $|X| = G^{p-1}$ and therefore p must divide $|X|$.

Next observe that if $x_1 \cdots x_p = e$, multiplying $x_1, \ldots, x_p$ in any order yields the identity. That is, if $(x_1, \ldots, x_p) \in X$, any permutation of this p-tuple is also in X. Therefore, we may let $\mathbb{Z}/p\mathbb{Z}$ act on X via permutation. That is,

$$1 \cdot (x_1, \ldots, x_p) \mapsto (x_p, x_1, \ldots, x_{p-1}).$$

Since the order of $\mathbb{Z}/p\mathbb{Z}$ is prime, every stabilizer subgroup is either of size 1 or of size p. By the Order Stabilizer Theorem, this means that the order of an orbit is either 1 or p. Furthermore, the orbits of this action form a partition of X. Elements of X that are in an orbit of size 1 must be of the form $(x, \ldots, x)$ where $x^p = e$. Since $(e, \ldots, e) \in X$ satisfies this condition, e is in an orbit of size 1. Because orbits are of size 1 or p and partition X, there exists some $x \neq e$ also in an orbit of size 1. If this were not the case, p would not divide X, a contradiction. This chosen x is of order p since $x^p = e$. □

5 Ideals

Problem 5.1: F19

Prove that the set N of nilpotent elements of a commutative ring R is an ideal of R and that R/N has no nilpotent elements.

Proof. Since $0^1 = 0$, $0 \in N$ and thus $N \neq \varnothing$. Suppose that $x, y \in N$ are nonzero with $x^n = y^m = 0$ for some $m, n > 1$. Since R is commutative,

$$(x + y)^{mn} = \sum_{k=0}^{mn} \binom{mn}{k} x^k y^{mn-k}$$

via the Binomial Theorem. Without loss of generality, assume that $n \leq m$. Then whenever $m \leq k \leq mn$, $x^k = 0$. Whenever $0 \leq k \leq m$, $m(n-1) \leq mn - k \leq mn$. This implies that $k \geq m(n-1) \geq n(n-1) \geq n$ and therefore $y^k = 0$. Therefore $(x + y)^{mn} = 0$ and so $x + y \in N$. For any $r \in R$, $(rx)^n = r^n x^n = r^n \cdot 0 = 0$ where the first equality follows from R being commutative. Therefore $rx \in N$. As N is closed under addition and multiplication by elements in R, N is an ideal.

Suppose that R/N has some nonzero nilpotent element. That is there exists $r \in R - N$ and $m \geq 1$ such that $(r + N)^m = N$. This implies that $r^m \in N$. Choose $n \geq 1$ such that $(r^m)^n = 0$. But this means that $r^{mn} = 0$, contradicting that $r \notin N$. Thus there are no nonzero nilpotent elements in R/N. □

6 Unfinished

Problem 6.1: F19

Let p be a prime number and suppose that $1 \leq n < p^2$ is an integer. Show that every Sylow p-subgroup of the symmetric group S_n is abelian.

Problem 6.2: F20

Let G be a finite group, $x \in G$, and H a subgroup of G.

(a) Prove that the number of conjugates of x in G divides order(G)/order(x).

(b) Prove that the number of conjugates of H in G divides the index of H in G.

Problem 6.3: S20

Let K be a field. Show that every finite subgroup of $K^\times$ is cyclic.

Problem 6.4: S19

State and prove Lagrange's Theorem. Prove that a subgroup of a cyclic group is cyclic.

Problem 6.5: S19

Prove the following:

(a) If R is a commutative ring with no nilpotent elements, then $R[x]$ has no nilpotent elements.

(b) If r is a nilpotent element of a ring with unity, then $1 - r$ is a unit.

Problem 6.6: S19

Prove that $\sigma, \tau \in S_n$ are conjugate if and only if for each $m \geq 2$ the number of m-cycles in a cycle decomposition of σ equals the number of m-cycles in a cycle decomposition of τ.

Problem 6.7: S20

(a) Prove that the centralizer of an element is a subgroup.

(b) If G is a finite group, prove that the number of elements in the conjugacy class divides the order of G.

Problem 6.8: F20

Show that any finitely generated group of $(\mathbb{Q}, +)$ is cyclic. Use this to prove that the direct product $(\mathbb{Q}, +) \times (\mathbb{Q}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

Problem 6.9: S20

Let R be a commutative ring with identity. Show that if p is a prime ideal in R then

$$p(x) = \left\{ \text{all polynomials } \sum_i a_i x^i \text{ with each } a_i \in p \right\}$$

is a prime ideal in $R[x]$.

Problem 6.10: S20

Let $\mathbb{F}_3$ be the field with 3 elements.

(a) Prove that $K = \mathbb{F}_3[x]/(x^2+1)$ is a field.

(b) How many elements does K have?

(c) Prove that $x+1$ generates the multiplicative group of non-zero elements in K.

Problem 6.11: F20

The polynomial $x^3 - x$ has six roots in the ring $\mathbb{Z}/6\mathbb{Z}$. Find a sufficient condition on a commutative ring R which ensures that the number of roots of a polynomial with coefficients in R cannot exceed its degree and justify your assertion.

Problem 6.12: F20

Prove or provide a counter example: Suppose that K is a finite extension of F. $F \subseteq L \subseteq K$, $F \subseteq M \subseteq KL$, $LM = K$ and $L \cap M = F$. Then $[L : F][M : F] = [K : F]$. Here, LM denotes the composition of the fields L and M.

Problem 6.13: F20

(i) Let R be a UFD and d a nonzero element in R. Prove that there are only finitely many principal ideals in R that contain the ideal (d).

(ii) Give an example of a UFD R and a nonzero element $d \in R$ such that there are infinitely many ideals in R that contain (d).

Problem 6.14: F20

It is known that real symmetric matrices are always diagonalizable. You may assume this fact.

(a) What special property do the eigenspaces of a real symmetric matrix have?

(b) Prove that any real symmetric matrix S can be diagonalized by an orthonormal matrix U.

Problem 6.15: F20

Prove or give a counter example.

(a) If a 4×4 real matrix has characteristic polynomial $x^4 - 1$ then its minimal polynomial cannot be $x^2 - 1$.

(b) Every $n \times n$ real matrix is similar over the reals to an upper triangular matrix.

Problem 6.16: F20

Let V be a finite dimensional complex vector space and $T : V \to V$ a linear transformation.

(a) Show that V has a "flag" of subspaces $V_0 = 0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ such that $\dim(V_i) = i$ and $T(V_i) \subseteq V_i$ for each i.

(b) Show that there is a basis for V such that the matrix of T with respect to this basis is upper triangular.