MA 541: Modern Algebra I / Fall 2019
Homework assignment #10
Due Tuesday, 11/26/2019

Comment on problem 3 added 11/21/2019.

(-1) Reading from F: read section 15 pp. 148–151. Read section 34. Look over section 35. You may skip the proofs of Lemma 35.10 and Theorem 35.11 if you wish.

(0) In discussion section of November 26/27, you will show that A_n is simple for all $n \geq 5$. The outline of one possible argument follows. You do not have write up your solution.

Proceed by induction on n.

(a) First, prove that A_5 is simple by filling in the gaps in the argument from class.

Now take $n \geq 6$, and assume that we know that A_{n-1} is simple. For $i \in \{1, \ldots, n\}$, let $H_i \subseteq A_n$ be the set of permutations that fix the index i.

(b) Show that H_i is a subgroup of A_n isomorphic to A_{n-1}.

Let N be a normal subgroup of A_n.

(c) If there is an i so that $N \cap H_i = H_i$, show that every $H_i \leq N$. Conclude that $N = A_n$.

(d) Otherwise, show that $N \cap H_i = \{e\}$ for every i.

(e) Show that if $\sigma \neq e$ is in A_n, then there exists an $i \in \{1, \ldots, n\}$ and a σ' in A_n that is conjugate to but distinct from σ with $\sigma(i) = \sigma'(i)$. Conclude that $\sigma'\sigma^{-1} \in H_i$.

(f) If $N \cap H_i = \{e\}$ for every i, prove that $N = \{e\}$.

(g) Conclude that A_n is simple for every $n \geq 5$.

(1) Let G be a group, and H and K subgroups of G.

(a) Is HK (the set of products hk for $h \in H$ and $k \in K$) necessarily a subgroup of G? Either prove that HK is always a subgroup or give a counterexample.

(b) In any case, HK is certainly a union of left cosets of K: write HK/K for the set of these left cosets. Recall that $H \cap K$ is a subgroup of H. Show that there is a natural bijection between the set of left cosets HK/K and the set of left cosets $H/(H \cap K)$.

(c) If G is a finite group, use the correspondence in (b) to prove that

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

The formula in (c) is a counting version of the Second Isomorphism Theorem, much as F Theorem 10.14 is a counting version of the Third Isomorphism Theorem.

(2) **Groups of order 8:** The goal of this problem is to show that every group of order 8 is isomorphic to exactly one of

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad D_4, \quad Q_8.$$

Let G be a group of order 8. If G has an element of order 8, then G is cyclic and isomorphic to $\mathbb{Z}_8$. So eliminate this case and assume that every element of G has order 1, 2, or 4.

(a) If every element of G has order dividing 2, show that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
(b) Otherwise, let $a \in G$ have order 4. Let $H = \langle a \rangle$. Choose any $b \in G - H$. Show that $G = H \cup Hb$.
(c) If every $b \in G - H$ has order 2, show that $G \cong D_4$.
(d) Otherwise we can find $b \in G - H$ of order 4. Prove that $a^2 = b^2$. (*Hint:* problem 1c.)
(e) To understand the multiplication structure on G completely, it remains to identify ba as an element of Hb. Finish the proof!

(3) (a) Let H be a subgroup of a group G satisfying the following property:

$$\boxed{\text{If } H' \text{ is a subgroup of } G \text{ conjugate to } H \text{ and distinct from } H\text{, then } HH' = G.}$$

Show that H is actually normal in G. (Note: Once you prove that H is normal, you will have shown that no such H' exists: indeed, a normal subgroup has no conjugates not equal to itself. The boxed property is then satisfied vacuously.)

(b) Let p be the smallest prime dividing the order of a finite group G. Prove that any subgroup of index p in G is normal. (For $p = 2$ we already showed this in class, but the same method won't work in general. One option is to use problem 1c.)

(c) Show that there are no simple groups of order 35 or 77.

(4) Show that a group of order p^2 where p is prime is isomorphic either to $\mathbb{Z}_p \times \mathbb{Z}_p$ or to $\mathbb{Z}_{p^2}$. In particular, there are no simple groups of order p^2. (One possibility is to use problem 3b.)

(5) Let G be a group. Given elements $a, b \in G$, the element $aba^{-1}b^{-1}$, sometimes denoted $[a, b]$, is the *commutator* of a and b. Let $[G, G]$ be the subgroup of G generated by all the commutators of all the elements in G. That is $[G, G] = \langle [a, b] : a, b \in G \rangle$.

(a) Show that $[G, G]$ is a normal subgroup of G, and that $G/[G, G]$ is an abelian group.

(b) Suppose G is abelian. What is $[G, G]$?

(c) Suppose G is a nonabelian simple group. What is $[G, G]$?

(d) Compute $[S_n, S_n]$ and $S_n/[S_n, S_n]$ for every $n \geq 2$. (*Hint:* For $n = 3$ and $n \geq 5$ it may be helpful to show that S_n has only one nontrivial proper normal subgroup.)

(6) $\mathbb{Z}_p^\times$ **is cyclic.** This is the promised problem from the cyclicity of units mod n set.

(a) Find all the roots of the polynomial $X^2 + 3X - 4$ in $\mathbb{Z}_{21}$? How many are there?

(b) Suppose G is a finite abelian group. Let M be the maximum of the orders of any of the elements of G. Prove that $g^M = 1$ for any element $g \in G$.
(*Hint:* Use problem 10 on HW #6.)

(c) Let p be a prime. Assume the following statement as a black box:

$$\boxed{\text{A polynomial of degree } n \text{ has no more than } n \text{ roots in } \mathbb{Z}_p.}$$

Use part (b) to show that the group $\mathbb{Z}_p^\times$ is cyclic.