MAT 511 **Notes on maximal ideals and subgroups**
9/10/13

A subgroup H of a group G is *maximal* if $H \neq G$, and, if K is a subgroup of G satisfying $H \subseteq K \subsetneq G$, then $H = K$. An ideal I of a ring R is *maximal* if $I \neq R$, and, if J is an ideal of R satisfying $I \subseteq J \subsetneq R$, then $I = J$.

Zorn's Lemma Suppose $\mathcal{P}$ is a nonempty partially-ordered set with the property that every chain in $\mathcal{P}$ has an upper bound in $\mathcal{P}$. Then $\mathcal{P}$ contains a maximal element.

Here a *chain* $C \subseteq \mathcal{P}$ is a totally-ordered subset: for all $x, y \in C$, $x \leq y$ or $y \leq x$. A *maximal element* of $\mathcal{P}$ is an element $x \in \mathcal{P}$ with the property $x \leq y \implies x = y$ for all $y \in \mathcal{P}$. Partially-ordered sets can have several different maximal elements.

Zorn's Lemma says, intuitively, if one cannot construct an ever-increasing sequence in $\mathcal{P}$ whose terms get arbitrarily large, then there must be a maximal element in $\mathcal{P}$. It is equivalent to the Axiom of Choice: in essence we *assume* that Zorn's Lemma is true, when we adopt the ZFC axioms as the foundation of mathematics.

Theorem 1. *If I_0 is an ideal of a ring R, and $I_0 \neq R$, then there exists a maximal ideal I of R with $I_0 \subseteq I$.*

Proof. Let $\mathcal{P}$ be the set of proper (i.e., $\neq R$) ideals of R containing I_0, ordered by inclusion. Then $\mathcal{P}$ is nonempty, since $I_0 \in \mathcal{P}$. Suppose C is chain in $\mathcal{P}$. Let $B = \bigcup_{J \in C} J$. Then, first of all, B is an ideal of R; to prove this one uses the fact that C is a chain. (For instance, to show B is closed under addition, note that, if $x, y \in B$ then $x, y \in J$ for some $J \in C$, because C is a chain, and then $x + y \in J \subseteq B$.) Moreover, $B \neq R$. To prove this it suffices to show $1 \notin B$, and this holds because $1 \notin J$ for all $J \in C$, since C consists of proper ideals. Thus $B \in \mathcal{P}$. This establishes the hypothesis of Zorn's Lemma. Thus $\mathcal{P}$ has a maximal element I, which has the required properties. $\square$

For finite groups the situation is similar.

Theorem 2. *If H is a subgroup of a finite group G, and $H \neq G$, then there exists a maximal subgroup M of G with $H \subseteq M$.*

Proof. Induct on the index $n = |G : H|$ of H in G. If $|G : H| = 1$ then $H = G$ and the statement is vacuous. Suppose $|G : H| > 1$. If H is maximal, take $H = G$. If H is not maximal, then there exists $H' \leq G$ with $H \subsetneq H' \subsetneq G$. Then $|G : H'| < |G : H|$, so there exists a maximal subgroup M of G containing H', by the inductive hypothesis. Then $M \supseteq H$, and the inductive step is complete. Then the statement holds for all $n \in \mathbb{N}$ by mathematical induction. $\square$

Example 3. Let G be the group of rational numbers, under addition. Then G has no maximal subgroups. Indeed, if H is a maximal subgroup of G, then $H \trianglelefteq G$ since G is abelian. Since H is maximal, G/H has no proper subgroups. (This is an application of the Third Isomorphism Theorem.) Then G/H is cyclic of prime order p. From this it follows that $px \in H$ for all $x \in G$. (Note: We write px instead of x^p because the group operation is written in additive notation.)

Let $y \in G - H$ and let $x = \frac{y}{p}$. Then $px \in H$ by the previous paragraph, but $px = y \notin H$. Contradiction. Thus $\mathbb{Q}$ has no maximal subgroups.

This argument generalizes to *divisible* abelian groups.

Definition 4. A group G is *divisible* if, for every $y \in G$ and for every natural number n, there exists $x \in G$ with $x^n = y$.

It is equivalent that the statement hold for all prime numbers n, since $x^{pq} = (x^p)^q$. The group of rational numbers under addition is a divisible group.

Proposition 5. *If G is a divisible group, then G has no nontrivial finite quotients.*

Proof. Suppose G is divisible, and $H \triangleleft G$ with G/H finite. Let $|G/H| = n$. Then $x^n \in H$ for all $x \in G$. (This follows easily from Lagrange's Theorem.) Assume G/H is not trivial, and choose $y \in G - H$. Since G is divisible, there exists $x \in G$ with $x^n = y$. But $x^n \in H$ by the previous observation, while $y \notin H$ by assumption. Contradiction. Thus G has no nontrivial finite quotients. $\square$

Proposition 6. *For any group G, G has no nontrivial finite quotients if and only if G has no finite-index subgroups.*

Proof. One implication is clear. Suppose H is a subgroup of G of finite index n. By a proposition from class (and also Exam 1.1(c)), there is a normal subgroup N of G with $N \subseteq H$ and $|G : N|$ dividing $n!$. Then G/N is a finite quotient of G. $\square$

Proposition 7. *For any group G, if G has a nontrivial finite quotient, then G has a maximal subgroup.*

Proof. Let $N \trianglelefteq G$ with G/N finite, and apply Theorem 2 to the trivial subgroup $1_{G/N}$. The statement then follows from the third isomorphism theorem. $\square$

Corollary 8. *Suppose G has a unique maximal subgroup or is abelian and has a maximal subgroup, then G has a nontrivial finite quotient.*

Proof. If G has a unique maximal subgroup M, then M is characteristic. (It is the Frattini subgroup of G.) Then M is normal, and G/M has no subgroups (by the third isomorphism theorem). Then G/M is cyclic of prime order p. If G is abelian, then any maximal subgroup is normal, and the same argument applies. $\square$

Theorem 9. *Suppose G is abelian and is not divisible. Then G has a maximal subgroup.*

Proof. This result requires Zorn's Lemma. Let p be a prime. Since G is abelian, the function $\phi\colon G \to G$ defined by $\phi(G) = px$ is a homomorphism. (Here we are writing G additively.) Let pG denote the image of ϕ. Since G is not divisible, $pG \neq G$ for some prime p. Then pG is normal in G, and G/pG has the property that $py = 0$ for all $y \in G/G^p$. Then G/pG is a vector space over the field $\mathbb{Z}_p$. A familiar application of Zorn's Lemma is the statement that every vector space V over a field has a basis (called a Hamel basis): one applies Zorn to the partially-ordered set of linearly-independent subsets of V. So we have a basis $\mathcal{B}$ of G/pG as a vector space over $\mathbb{Z}_p$. Pick $b_0 \in \mathcal{B}$ and let $\overline{M}$ be the span of $\mathcal{B} - \{b_0\}$. Then $\overline{M}$ is a maximal linear subspace of G/pG, hence is a maximal subgroup of G/pG. By the third isomorphism theorem, $\overline{M} = M/pG$ for $M \leq G$, and M is a maximal subgroup of G. □

Let us put together all these partial results.

Corollary 10. *Suppose G is an abelian group. Then the following are equivalent:*

(i) G has a maximal subgroup.

(ii) G has a subgroup of finite index.

(iii) G has a finite quotient.

(iv) G is not divisible.

Corollary 11. *Let G be an arbitrary group. Then*

(i) if G has a finite quotient, then G has a maximal subgroup.

(ii) if G has a maximal subgroup, then G is not divisible.

(iii) if G has a unique maximal subgroup, then G has a finite quotient.

(iv) if G has a subgroup of finite index, then G has a finite quotient.

The question that motivated the whole discussion remains unanswered:
Question: is there an infinite group with a unique maximal subgroup?

I suspect the following is true, but I haven't found a proof.

Conjecture 12. A_∞ is the unique maximal subgroup of S_∞.