Study Guide for Algebra

Department of Mathematics and Statistics
Amherst College

September, 2016

This study guide was written to help you prepare for the algebra portion of the Comprehensive and Honors Qualifying Examination in Mathematics. It is based on the *Syllabus for Algebra* (*Math 350*) available on the Department website.

Each topic from the syllabus is accompanied by a brief discussion and examples from old exams. When reading this guide, you should focus on three things:

- *Understand the ideas.* If you study problems and solutions without understanding the underlying ideas, you will not be prepared for the exam.
- *Understand the strategy of each proof.* Most proofs in this guide are short—the hardest part is often knowing how to start. Focus on the setup step rather than falling into the trap of memorizing proofs.
- *Understand the value of scratchwork.* Sometimes scratchwork is needed before you start the proof.

The final section of the guide has some further suggestions for how to prepare for the exam.

1 Sets, Functions, and the Integers

There are some fundamental topics that you are unlikely to get tested on directly, but which could come up indirectly. So you should know them. In particular:

For functions and sets, know the following basics

- One-to-one, onto, and bijective maps.
- The identity function and inverse functions.
- Equivalence relations and equivalence classes (at least in specific cases like the right coset relation, and its equivalence classes, the right cosets)

For the integers $\mathbb{Z}$ and natural numbers $\mathbb{N}$, know the following basics:

- The notation $a \mid b$ and the division algorithm in $\mathbb{Z}$.
- Greatest common divisors and least common multiples in $\mathbb{N}$. (This includes the fact that if $\gcd(a, b) = d$, then there exist $m, n \in \mathbb{Z}$ such that $ma + nb = d$.)
- Prime numbers and unique factorization.

2 Groups

Some basic things to know:

- The definition of group.
- Uniqueness of identities and inverses.

The identity of G is usually denoted e or e_G, although for some specific groups it may have a different symbol. (For example, if the operation on G is called $+$, then the identity element is usually called 0.)

Recall that we say G is *abelian* if the group operation is commutative, i.e., if $xy = yx$ for all $x, y \in G$.

Orders of Groups and Elements. Know:

- For $g \in G$ and $n \in \mathbb{Z}$, know what g^n means.
- If the operation on G is called $+$, then we write ng instead of g^n.
- When G is finite, its order $|G|$ is the number of elements in the group.
- When $g \in G$ has finite order, its order $o(g)$ is the smallest integer $m > 0$ with $g^m = e$.
- If $g^m = e$ for some $m \in \mathbb{Z}$, then $o(g) \mid m$.

Be prepared to prove the last statement above using the division algorithm. See **9** and **15** for problems that use $g^m = e \Rightarrow o(g) \mid m$.

3 Subgroups

Know the definition of subgroup and how to prove that a given subset is a subgroup.

1 (January 2012) Let G be a group, and let $H, K \subseteq G$ be subgroups of G. Prove the following standard theorem about subgroups: that $H \cap K$ is a subgroup of G.

Proof. (Nonempty) Since H and K are subgroups of G, we have $e \in H$ and $e \in K$. So $e \in H \cap K$, and hence $H \cap K \neq \varnothing$.
(Closed under $*$) Given $a, b \in H \cap K$, we have $ab \in H$ and $ab \in K$ since H and K are closed under the operation. So $ab \in H \cap K$, as desired.
(Closed under $^{-1}$) Given $a \in H \cap K$, we have $a^{-1} \in H$ and $a^{-1} \in K$ since H and K are closed under inverses. So $ab \in H \cap K$ as desired.
Thus, $H \cap K$ is a subgroup of G. QED

See **3** for another problem where you have to prove that a subset is a subgroup.

Cyclic Subroups. An element $g \in G$ generates the cyclic subgroup $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$. There are many therorems about cyclic groups, but for the algebra exam, one key fact to know is that g has finite order if and only if $\langle g \rangle$ is finite, in which case $o(g) = o(\langle g \rangle)$. [Do you know why this fact is true?]

See **2** and **6** for problems involving cyclic subgroups.

Lagrange's Theorem. This theorem says that if H is a subgroup of a finite group G, then the order of H divides the order of G. That is, $|H| \big| |G|$. When g is an element of a finite group G, Lagrange's Theorem has several important consequences:

- If $|G|$ is prime, then G is cyclic.
- For all $g \in G$, we have $o(g) \big| |G|$.
- For all $g \in G$, we have $g^{|G|} = e$.

These consequences all follow from Lagrange, using the fact that for any $g \in G$, we have $o(g) = |\langle g \rangle|$. [Be sure you know how to use this fact to prove the statements above!] In fact, on the comps, if you have a finite group G and want to conclude any of the three bulleted statements above, you may justify simply by saying "by Lagrange's Theorem." See **2**, **8**, and **9** for problems that use these corollary versions of Lagrange's Theorem.

2 (March 2007) Let $p, q \geq 2$ be prime numbers, and let G be a group of order $|G| = pq$. Let $H \subsetneq G$ be a *proper* subgroup (i.e., H is a subgroup but is not the full group G).
Prove that H is cyclic.

Proof. Since $|G| < \infty$, Lagrange's Theorem says that $|H|\big||G|$. Thus, $|H|$ is one of the four numbers $1, p, q, pq$. However, since H is proper, we must have $|H| < |G| = pq$. Three cases remain:
If $|H| = 1$, then $H = \{e\}$ is the trivial group, which is generated by e and so is cyclic.
Otherwise, H has prime order p or q, and therefore it is cyclic by (a corollary of) Lagrange's Theorem.
QED

Comment. This is a proof that may require some scratchwork and multiple attempts before you figure out how to do it. It's not immediately obvious how to prove that H is cyclic; where are you going to find a generator? But the fact that G is finite, and that we know something pretty specific about the factorization of $|G|$, suggest that Lagrange's Theorem is at least something we could *try*.

Of course, just because a group is finite doesn't necessarily mean you should use Lagrange's Theorem. But it's worth trying it *in your scratchwork* to see if it might lead to something good. Just be ready to try *other* things, too, in case your first thought doesn't work out.

Note: It would also be a good idea for you to know the *proof* of Lagrange's Theorem, because that proof uses another very important concept: cosets.

4 Cosets

Given a subgroup $H \subseteq G$, know the definitions of left coset gH and right coset Hg. Also know:

- Two right cosets Hx and Hy are either the same set or disjoint sets. (That is, if they share even one element, they are exactly the same set.) The same holds for left cosets.

  (On the other hand, a right coset and a left coset can intersect each other without being the same set.)
- $Hx = Hy \iff xy^{-1} \in H \iff x \in Hy$.
- $xH = yH \iff y^{-1}x \in H \iff x \in yH$.
- In particular, $Hx = H \iff x \in H \iff xH = H$.
- When H is finite, all cosets of H have the same number of elements.

The second item above describes the *right coset relation* [or *criterion for equality of right cosets*], and the third is the *left coset relation* [or *criterion for equality of left cosets*]. They are **really** important, so let's say them again:

$$\boxed{Hx = Hy \iff xy^{-1} \in H} \qquad \text{and} \qquad \boxed{xH = yH \iff y^{-1}x \in H}$$

Know these facts, and be able to prove them quickly from scratch (to help ensure you don't get them backwards).

Note: in discussing the coset relation so far, we have been writing the group operation as multiplication. However, if G is abelian and the group operation is written as addition, then the left and right cosets of $H \subseteq G$ coincide and are written

$$H + a = \{h + a \mid h \in H\}.$$

Here, the coset relation becomes

$$H + a = H + b \iff a - b \in H \iff a \in H + b.$$

Most algebra exams include a problem that uses coset relations. See **8** and **10** for such examples involving groups. See also **21**, **25**, and **27** for examples involving rings.

Sometimes there are problems involving cosets directly in the statement, like this one:

3 (January 2016) Let G be a group, let $H \subseteq G$ be a subgroup, and define the set K to be

$$K = \{x \in G \mid Hx = xH\}.$$

Prove that K is a subgroup of G.

Proof. We prove that K is a subgroup of G as follows.
(1) Let e be the identity element of G. Then $He = H = eH$, so $e \in K$.
(2) Given $a, b \in K$, we have $H(ab) = (Ha)b = (aH)b = a(Hb) = a(bH) = (ab)H$. So $ab \in K$.
(3) Given $a \in K$, we have $Ha = aH$. Multiplying by a^{-1} on the left and the right gives

$$\begin{aligned} a^{-1}(Ha)a^{-1} &= a^{-1}(aH)a^{-1} \\ \implies a^{-1}H(aa^{-1}) &= (a^{-1}a)Ha^{-1}, \end{aligned}$$

which implies $a^{-1}H = Ha^{-1}$. Thus $a^{-1} \in K$, proving that K is a subgroup. QED

Comment 1. The above equations are equations of *sets*. Be careful when you manipulate them, to make sure that you are not just pushing symbols around, but that you actually understand what you are doing. For example, $H(ab)$ and Ha are really

$$H(ab) = \{h(ab) \mid h \in H\} \quad \text{and} \quad Ha = \{ha \mid h \in H\}.$$

So in the first equation of (2) above, when we said $H(ab) = (Ha)b$, what we were really saying was that

$$H(ab) = \{h(ab) \mid h \in H\} = \{(ha)b \mid h \in H\} = \{xb \mid |x \in Ha\} = (Ha)b.$$

Comment 2. The proofs of (1) and (2) are fairly straightforward, but thinking of (3) requires some scratchwork. Given $Ha = aH$, multiplying each side by a^{-1} makes sense. But how do you know whether to multiply on the left or on the right? Answer: you don't know! So pick one and see what happens. That is: do some scratchwork! Multiplying by a^{-1} on the left gives

$$a^{-1}(Ha) = a^{-1}(aH) \implies a^{-1}Ha = (a^{-1}a)H = eH = H.$$

Since $a^{-1}Ha = H$ still has a on the right, multiplying by a^{-1} on the right is also needed.

The Index of a Subgroup. When a group G is a union of finitely many left cosets of a subgroup H, we say that H has finite index in G, and the index of H in G is defined to be

$$[G : H] = \text{number of distinct left cosets of } H \text{ in } G.$$

The same holds for right cosets. An example is $n\mathbb{Z} \subseteq \mathbb{Z}$ with index $[\mathbb{Z} : n\mathbb{Z}] = n$. Can you explain why? When G is finite, $[G : H] = |G|/|H|$, since all cosets of H have the same number of elements. (Do you know *why* all cosets of H have the same cardinality? And do you know how this fact is used to prove Lagrange's Theorem?)

5 Normal Subgroups

Given a subgroup $H \subseteq G$, know that H being normal in G is equivalent to any of the following conditions:

- $gH = Hg$ for all $g \in G$.
- $gHg^{-1} = H$ for all $g \in G$.
- $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Many problems involve proving that a subgroup is normal. Here are some:

4 (January 2012) Let G be a group, and let $H, K \subseteq G$ be normal subgroups of G. Prove that $H \cap K$ is a normal subgroup of G. You may assume without proof that $H \cap K$ is a subgroup.

Proof. Given $a \in H \cap K$, $g \in G$, we know that $gag^{-1} \in H$ and $gag^{-1} \in K$ since H and K are normal. Thus, $gag^{-1} \in H \cap K$, so $H \cap K$ is normal in G as desired. QED

5 (January 2011) Suppose that $H \subseteq G$ is a subgroup with the property that for every $x, y \in G$, we have $xyx^{-1}y^{-1} \in H$. Prove that H is a **normal** subgroup of G.

Proof. Assume $g \in G$ and $h \in H$. By the given property of H, we have $ghg^{-1}h^{-1} \in H$. Since H is closed under multiplication, $ghg^{-1} = ghg^{-1}(h^{-1}h) = (ghg^{-1}h^{-1})h \in H$ as desired. QED

Comment. You want to prove $ghg^{-1} \in H$ for $h \in H$, but the hypothesis doesn't quite look like that—instead, it involves $ghg^{-1}h^{-1}$. **DON'T** fall into the trap of starting with the hypothesis. Instead, start with the object that you're trying to **prove** things about – namely ghg^{-1} – and rewrite it in a way that the thing from your hypothesis – namely $ghg^{-1}h^{-1}$ – appears. This gives

$$ghg^{-1} = (ghg^{-1})(h^{-1}h) = (ghg^{-1}h^{-1})h$$

and leads to the proof given above. The key point is to think about the **goal** first, and then do **scratchwork** to figure out how you can work in the hypothesis.

6 Let G be a group, and let $s \in G$. The *centralizer* of s in G is defined to be

$$C(s) = \{g \in G : gs = sg\}.$$

(a) Prove that $C(s)$ is a subgroup of G.
(b) Prove that $\langle s \rangle$ is contained in $C(s)$. (Recall that $\langle s \rangle$ is the subgroup of G generated by s.)
(c) Prove that $\langle s \rangle$ is a **normal** subgroup of $C(s)$.

Proof. (a): (Nonempty): We have $es = s = se$, and therefore $e \in C(s)$. So $C(s) \neq \varnothing$.
(Closed under $*$): Given $g, h \in C(s)$, we have

$$(gh)s = g(hs) = g(sh) = (gs)h = (sg)h = s(gh),$$

so $gh \in C(s)$, as desired.
(Closed under inverses): Given $g \in C(s)$, we have $gs = sg$, so

$$g^{-1}s = g^{-1}sgg^{-1} = g^{-1}gsg^{-1} = sg^{-1},$$

so $g^{-1} \in C(s)$, as desired. QED (a)
(b): Given $x \in \langle s \rangle$, we have $x = s^n$ for some $n \in \mathbb{Z}$. So

$$xs = s^n s = s^{n+1} = ss^n = sx,$$

so $x \in C(s)$, as desired. QED (b)
(c): Given $g \in C(s)$ and $h \in \langle s \rangle$, there is some $n \in \mathbb{Z}$ such that $h = s^n$. So

$$(ghg^{-1})s = gs^n g^{-1}s = s^n gg^{-1}s = s^n s = s^{n+1} = ss^n = ss^n gg^{-1} = sgs^n g^{-1} = s(ghg^{-1}).$$

Thus, $ghg^{-1} \in C(s)$, as desired. QED

Other problems involve *using* the fact that a subgroup is normal to prove something else.

7 (February 2013) Let G be a group, let $H \subseteq G$ be a subgroup, and let $N \triangleleft G$ be a **normal** subgroup. Define

$$NH = \{xh : x \in N \text{ and } h \in H\}.$$

Prove that NH is a subgroup of G.

Proof. (Nonempty): Since N and H are both nonempty, we may choose $x \in N$ and $h \in H$. Then $xh \in NH$, so $NH \neq \varnothing$.
(Closed under $*$): Given $x, y \in NH$, write $x = n_1h_1$ and $y = n_2h_2$, for some $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Since N is a normal subgroup of G, we have $h_1N = Nh_1$. Thus, there is some $n_3 \in N$ such that $h_1n_2 = n_3h_1$. So

$$xy = (n_1h_1)(n_2h_2) = n_1(h_1n_2)h_2 = n_1(n_3h_1)h_2 = (n_1n_3)(h_1h_2) \in NH,$$

as desired, since $n_1n_3 \in N$ and $h_1h_2 \in H$.
(Closed under inverses): Given $x \in NH$, write $x = nh$ with $n \in N$ and $h \in H$. Since N is a normal subgroup of G, we have $hN = Nh$. Thus, there is some $n_1 \in N$ such that $nh = hn_1$. So

$$x^{-1} = (nh)^{-1} = (hn_1)^{-1} = n_1^{-1}h^{-1} \in NH,$$

as desired, since $n_1^{-1} \in N$ and $h^{-1} \in H$. QED

Alternate Proof. (Nonempty): Since N and H are both nonempty, we may choose $x \in N$ and $h \in H$. Then $xh \in NH$, so $NH \neq \varnothing$.
(Closed under $*$): Given $x, y \in NH$, write $x = n_1h_1$ and $y = n_2h_2$, for some $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Then

$$xy = (n_1h_1)(n_2h_2) = n_1(h_1n_2)(h_1^{-1}h_1)h_2 = \big(n_1(h_1n_2h_1^{-1})\big)(h_1h_2).$$

Now $n_1, n_2 \in N$, and hence $h_1n_2h_1^{-1} \in N$ since N is normal, and therefore $n_1(h_1n_2h_1^{-1}) \in N$. Since $h_1h_2 \in H$, then the above equation shows $xy \in NH$, as desired.
(Closed under inverses): Given $x \in NH$, write $x = nh$ with $n \in N$ and $h \in H$. Then

$$x^{-1} = (nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}.$$

Now $h^{-1}n^{-1}h \in N$ since N is normal in G, and $h^{-1} \in H$, so the above equation shows $x^{-1} \in NH$, as desired. QED

Comment. Serious scratchwork is required for either version of this proof. The key thing to keep in mind when you are allowed to *use* the hypothesis that N is normal in G (rather than when you need to *prove* it's normal) is that if you ever see an expression like gn with $n \in N$, you can replace it with the expression $n'g$ with $n' \in n$; same g, possibly a different $n' \in N$. (This is the idea used in the first proof above.) Or, as we did in the alternate proof, if you can get a conjugate expression like gng^{-1} to appear, then you know it's in N; so try to rearrange things to get conjugates to appear.

Quotient Groups. When $N \subseteq G$ is a normal subgroup, every left coset is a right coset, and vice versa. The set of all cosets of N in G forms a group and is denoted G/N. The group operation is defined by $Na \cdot Nb = Nab$, which is well-defined since N is normal. [Do you know how to prove that?]

When G is finite, G/N is also finite and $|G/N| = [G : N] = |G|/|N|$.

8 (March 2013) Let G be a group, let $N \subseteq G$ be a normal subgroup, and suppose that $[G : N] = 42$, where $[G : N]$ denotes the index of N in G. Prove that $x^{42} \in N$ for every $x \in G$. (*Suggestion: Consider the quotient group G/N.*)

Proof. The quotient group G/N has order 42 since $|G/N| = [G : N] = 42$. Given any $x \in G$, consider the coset $Nx \in G/N$. By Lagrange's Theorem applied to the group G/N and the element Nx, we have $(Nx)^{42} = Ne$, since Ne is the identity element of G/N. Now $(Nx)^{42} = N(x^{42})$ [by definition of the group operation in G/N], and therefore

$$Nx^{42} = Ne, \quad \text{and hence } x^{42} = x^{42}e^{-1} \in N$$

by the coset relation. QED

Comment. This is yet another proof where strategy and scratchwork are helpful. Here is what you know:
- You are told to use G/N.
- You know that $|G/N| = [G : N] = 42$.

Since you need to prove something about x^{42}, this suggests the $g^{|G|} = e$ version of Lagange's Theorem. But you have to be able to apply Lagrange to G/N, where the element is not x but rather Nx, the order is 42, and the identity element is Ne. And you absolutely need to be fluent in using the coset relation to finish the proof.

6 Group Homomorphisms

Know the definition of a group homomorphism $\phi : G \to H$. Know also that if ϕ is a homomorphism, then also:

- $\phi(e_G) = e_H$
- $\phi(g^n) = \phi(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

9 (January 2012) Let G and H be groups. Recall that a homomorphism $\phi : G \to H$ is said to be *trivial* if $\phi(g) = e_H$ for all $g \in G$. If $|G| = 144$ and $|H| = 25$, prove that any homomorphism $\phi : G \to H$ is trivial.

Proof. Given $g \in G$. By Lagrange's Theorem for G, we have $g^{144} = e_G$ Since ϕ is a homomorphism, we have

$$(\phi(g))^{144} = \phi(g^{144}) = \phi(e_G) = e_H.$$

Thus, $\phi(g)$, which is an element of H, has finite order $m = o(\phi(g))$ that divides 144. On the other hand, by Lagrange's Theorem for H, we also have $m|25$, since $|H| = 25$. Thus, m is a common divisor of $144 = 2^4 3^2$ and $25 = 5^2$. Since $\gcd(144, 25) = \gcd(2^4 3^2, 5^2) = 1$, we must have $o\big(\phi(g)\big) = 1$. Thus, $\phi(g) = e_H$, as desired. QED

10 (March 2015) Let G_1, G_2 be groups, let $H_2 \subseteq G_2$ be a subgroup, and let $\phi : G_1 \to G_2$ be a homomorphism. Define

$$H_1 = \{x \in G_1 \mid \phi(x) \in H_2\}.$$

It is a fact, which you may assume, that H_1 is a subgroup of G_1. Prove that for any $x, y \in G_1$, $H_1x = H_1y$ **if and only if** $H_2\phi(x) = H_2\phi(y)$.

Proof. ($\Longrightarrow$) Given $x, y \in G_1$ such that $H_1x = H_1y$, we have $xy^{-1} \in H_1$ [by the right coset relation for H_1]. So $\phi(x)\phi(y)^{-1} = \phi\big(xy^{-1}\big) \in H_2$, by definition of H_1. Thus, [by the right coset relation for H_2], we have $H_2\phi(x) = H_2\phi(y)$.

($\Longleftarrow$) Given $x, y \in G_1$ such that $H_2\phi(x) = H_2\phi(y)$, we have $\phi(x)\phi(y)^{-1} \in H_2$ [by the right coset relation for H_2]. Thus,

$$\phi\big(xy^{-1}\big) = \phi(x)\phi(y)^{-1} \in H_2,$$

and therefore $xy^{-1} \in H_1$, by definition of H_1. Thus, [by the right coset relation for H_1], we have $H_1x = H_1y$. QED

Comment. In retrospect, all the steps of the above ($\Longrightarrow$) proof were reversible, so we could also have done the above proof as a single chain of "$\Longleftrightarrow$" statements.

Alternately, we could have started from both ends and build towards the middle. So here is an alternate version of the above proof, reflecting a "build towards the middle" strategy.

Alternate Proof. Given $x, y \in G_1$, the right coset relations give:

$$H_1x = H_1y \iff xy^{-1} \in H_1 \tag{1}$$

$$H_2\phi(x) = H_2\phi(y) \iff \phi(x)\phi(y)^{-1} \in H_2. \tag{2}$$

Using the definition of H_1, we can write (1) as

$$H_1x = H_1y \iff xy^{-1} \in H_1 \iff \phi(xy^{-1}) \in H_2, \tag{3}$$

and using the fact that ϕ is a homomorphism, we can write (2) as

$$H_2\phi(x) = H_2\phi(y) \iff \phi(x)\phi(y)^{-1} \in H_2 \iff \phi(xy^{-1}) \in H_2. \tag{4}$$

The problem follows now from the equivalences (3) and (4). QED

Comment. In general, if a problem involves equalities of cosets, then you are almost certainly going to need the coset relation. In this example, even if we have no idea what to do, it's worth starting from one side, $H_1x = H_1y$, and applying the coset relation. This immediately gives (1); similarly, $H_2\phi(x) = H_2\phi(y)$ gives (2). Since we are sort of stuck at that point, *only then* do we look at the hypotheses; then the definition of H_1 gives (3), and the fact that ϕ is a homomorphism gives (4).

Suggestion. For more practice, prove that H_1 is a subgroup of G_1.

Kernels and Images. Given a group homomorphism $\phi : G \to H$, know:

- The definition of the kernel $\mathrm{Ker}(\phi) \subseteq G$ and the image $\mathrm{Im}(\phi) \subseteq H$.
- $\mathrm{Ker}(\phi)$ is a normal subgroup of G (be able to prove this).
- $\mathrm{Im}(\phi)$ is a subgroup of H (be able to prove this), but not necessarily normal. Another notation for $\mathrm{Im}(\phi)$ is $\phi(G)$.

Recall that ϕ is one-to-one if and only if $\mathrm{Ker}(\phi) = \{e_G\}$. Be able to prove this.

Isomorphisms. Given a group homomorphism $\phi : G \to H$, know the equivalence between

- ϕ is one-to-one and onto.
- ϕ has an inverse function $\phi^{-1} : H \to G$ that is also a group homomorphism.

In this situation, we say that ϕ is a group isomorphism.

The Fundamental Theorem of Group Homomorphisms. Also called the *First Homomorphism Theorem for Groups*, or the *Basic Homomorphism Theorem*, this theorem says that if $\phi : G \to H$ is a group homomorphism, then there is a group isomorphism $\widetilde{\phi} : G/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$ defined by $\widetilde{\phi}(g\mathrm{Ker}(\phi)) = \phi(g)$.

11 (February 2013) Let G_1 and G_2 be groups, let $\phi : G_1 \to G_2$ be a homomorphism, and let $H_1 \subseteq G_1$ be a subgroup. Recall that the set

$$H_2 = \{\phi(x) \mid x \in H_1\}$$

is a subgroup of G_2, called the *image of* H_1 *under* ϕ, sometimes notated $\phi(H_1)$. If G_1 is finite, prove that $|H_2|\big||G_1|$. That is, prove that the order of H_2 divides the order of G_1.

Proof. Let $K = \mathrm{Ker}(\phi)$ denote the kernel of ϕ. Then:

- $\phi(G_1) \cong G_1/K$ by the fundamental theorem of group homomorphisms, so $|\phi(G_1)| = |G_1/K|$.
- We also know that $|G_1/K| = |G_1|/|K|$.

Together, these two facts yield

$$|\phi(G_1)| \cdot |K| = |G_1|, \quad \text{and hence } |\phi(G_1)|\Big||G_1| \tag{1}$$

We also observe the following about H_1 and H_2:

- Since $H_1 \subseteq G_1$, we have $H_2 = \phi(H_1) \subseteq \phi(G_1)$.
- By Lagrange's Theorem, it follows that $|H_2|$ divides $|\phi(G_1)|$.

Since $|H_2|$ divides $|\phi(G_1)|$ by the last bullet, and $|\phi(G_1)|$ divides $|G_1|$ by (1), it follows that $|H_2|$ divides $|G_1|$. QED

Comment. The strategy for this proof has two parts. The first part is to recognize that the fundamental theorem is relevant. Do you see how this follows from the request to prove $|H_2|\big||G_1|$? (Hint: H_2 lives in G_2, while G_1 is the domain of $\phi : G_1 \to G_2$.) The second part of the strategy is to work out what this means for ϕ *before* bringing H_1 and H_2 into the picture.

7 Permutations

S_n and Disjoint Cycle Decomposition. Know:

- The definition of the symmetric group S_n and its order $|S_n| = n!$.
- The two-row notation $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ for permutations.
- Given distinct $i_1, \ldots, i_n$, the n-cycle $(i_1\, i_2 \cdots i_n)$ maps i_1 to i_2, i_2 to i_3, $\ldots$, i_n to i_1, and is the identity elsewhere.
- The order of an n-cycle is its length n.

Be sure you know to write $\sigma \in S_n$ as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_k$ and that

$$o(\sigma) = \text{lcm}(\text{length}\,\sigma_1, \ldots, \text{length}\,\sigma_k).$$

In particular, given a product of two or more permutations, know how to write the result as a product of **disjoint** cycles.

Transpositions and A_n. Some basic things to know:

- "Transposition" is just another word for 2-cycle.
- Every element of S_n can be written a product of transpositions.
- A given $\sigma \in S_n$ can be written as product of transpositions in many ways, so this product is *not* a unique factorization.
- The number of transpositions involved is either always even (σ is even) or always odd (σ is odd).
- The alternating group A_n consists of all even permutations in S_n.
- For $n \geq 2$, the order of A_n is $(n!)/2$.
- An n-cycle can be written as a product of $n-1$ transpositions.
- In particular, every cycle of odd length has **odd order** but is an **even permutation**.
- Similarly, every cycle of even length has **even order** but is an **odd permutation**.

Warning: Most permutations $\sigma \in S_n$ are not cycles. To compute the order $o(\sigma)$, or to decide whether σ is even or odd, write σ in cycle notation and work from there.

12 (January 1997) Suppose that σ is a permutation in the alternating group A_{10} given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 2 & 6 & 10 & 1 & 5 & & & 3 \end{pmatrix}$$

where the images of 8 and 9 have been lost. Determine the images of 8 and 9 under σ. What is the order of σ?

Solution. The two missing outputs are also 8 and 9. If $\sigma(8) = 9$, then we must have $\sigma(9) = 8$, which would give

$$\sigma = (1\ 4\ 6)(2\ 7\ 5\ 10\ 3)(8\ 9).$$

However, since 3-cycles and 5-cycles are even, and 2-cycles are odd, that would make σ an odd permutation. But we were told $\sigma \in A_{10}$, meaning that σ is even.

Contradiction! Therefore σ is *not* the permutation above, and therefore $\sigma(8) \neq 9$.

So we must have $\sigma(8) = 8$, and hence $\sigma(9) = 9$. Thus,

$$\sigma = (1\ 4\ 6)(2\ 7\ 5\ 10\ 3).$$

The order of σ is the lcm of the orders of the individual (disjoint) cycles in the above decomposition. So the order of σ is $o(\sigma) = \text{lcm}(3, 5) = 15$.

13 (January 2010) Let σ be the permutation (4 2 1)(6 1 3 2) in S_6.

(a) Write σ as a product of disjoint cycles in S_6.

(b) Compute the **order** of σ.

(c) Is σ an even or an odd permutation?

Solution. (a) $\sigma = (1\ 3)(2\ 6\ 4)$.

(b) The order of σ is the lcm of the orders of each individual cycle in its decomposition into disjoint cycles. Since the order of an n-cycle is n, we obtain $o(\sigma) = \text{lcm}(3, 2) = 6$.

(c) σ is a product of a 2-cycle and a 3-cycle. The 2-cycle is an odd permutation (since 2 is even), and the 3-cycle is even (since 3 is odd), so σ is even + odd = odd.

---

14 (February 2008) Recall that S_n denotes the group of permutations on n symbols.

(a) Find an element of S_{10} of order 21.

(b) Prove that no element of S_{10} has order 11.

Solution. (a) The order of σ is the lcm of the orders of each individual disjoint cycle comprising σ (and the order of an n-cycle is n). Since $21 = \text{lcm}(3, 7)$, the element $\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7\ 8\ 9\ 10)$ has order 21.

(b) Suppose S_{10} has a permutation σ of order 11. Then σ must have a disjoint cycle structure such that the lcm of the cycle lengths is 11. If the disjoint cycles making up σ have lengths $\ell_1, \ldots, \ell_k$, then

$$11 = o(\sigma) = \text{lcm}(\ell_1, \ldots, \ell_k).$$

Thus each ℓ_i divides 11. Since 11 is prime, each $\ell_i = 1$ or 11. But an 11-cycle requires 11 distinct symbols, which can't happen since we are in S_{10}. So $\ell_i = 1$ for all i, which means that σ is the identity. Yet it has order 11. This contradiction shows that no element of S_{10} has order 11.

Here is a more abstract problem.

15 (February 2007) Fix an integer $n \geq 2$, and write S_n for the permutation group on n letters. Let

$$\phi : S_n \to G$$

be a homomorphism, where G is a group of odd order. (I.e., G is a finite group with an odd number of elements.)

(a) Prove that every **transposition** (i.e., 2-cycle) $\tau \in S_n$ is in $\ker \phi$. That is, prove that $\phi(\tau) = e$.

(b) Prove that ϕ is the trivial homomorphism; i.e., prove that for all $\sigma \in S_n$, we have $\phi(\sigma) = e$.

Proof. (a) Let τ be a transposition, so $o(\tau) = 2$. Since ϕ is a homomorphism,

$$e_G = \phi(e_{S_n}) = \phi(\tau^2) = \phi(\tau)^2,$$

so $o(\phi(\tau))$ divides 2. But $o(\phi(\tau))$ also divides $|G|$ by Lagrange's Theorem. Since $|G|$ is odd, this implies that $o(\phi(\tau)) = 1$. Thus, $\phi(\tau) = e_G$.

(b) We know that S_n is generated by transpositions. Given $\sigma \in S_n$, write σ as a product of transpositions $\sigma = \tau_1\tau_2\cdots\tau_m$. By part (a), $\phi(\sigma) = \phi(\tau_1)\phi(\tau_2)\cdots\phi(\tau_m) = (e_G)^m = e_G$ as desired. QED

8 Rings

Know the basic definitions:

- Ring.
- Commutative ring.
- Ring with unity, or ring with 1. (I.e., R has a *multiplicative* identity, denoted 1 or 1_R.)
- Field.

If R is a ring with unity, then any $x \in R$ that has a *multiplicative* inverse x^{-1} is called a *unit*. The set of all units of R is denoted $R^\times$ and forms a group under the multiplication operation, with identity element 1_R.

Some quick notes about a ring R and an element $x \in R$:

- We have $0_R x = x 0_R = 0_R$.
- Since $(R, +)$ forms a group, for an integer n, we write nx to denote x added to itself n times (or subtracted, if n is negative; or 0_R if $n = 0$).
- For a *positive* integer n, we write x^n for x multiplied by itself n times. If R has unity, then $x^0 = 1_R$; if in addition x is a unit (i.e., if x has multiplicative inverse), then $x^{-n} = (x^{-1})^n$.

Warnings

- Don't talk about just the "identity" of a ring R. Be clear about whether you mean the *additive* identity (which you should just call 0 or 0_R) or the *multiplicative* identity (which you should just call 1 or 1_R, assuming R is a ring with unity).
- **Never** denote either identity of a ring by e. If you mean zero, say 0. If you mean one, say 1. Use e for the identity of a group, and use 0 and 1 for rings.
- Don't talk about just the "inverse" of $x \in R$ when working with rings. Make sure you are clear whether you mean the *additive* inverse $-x$ (also known as the *negative*) or the *multiplicative* inverse x^{-1} (if x is a unit, which it might not be).
- Don't confuse "unity" with "unit". The word "unity" refers to the multiplicative identity 1 (if R even *has* a multiplicative identity), but "unit" refers to a element of R that has a multiplicative inverse.

Polynomial Rings. If R is a commutative ring, the polynomial ring $R[x]$ consists of all polynomials in x with coefficients in R. See **20** for a problem that involves the polynomial ring $\mathbb{Z}[x]$. The important case of $k[x]$, when k is a field, is treated in more detail in Section 13 of this Study Guide.

9 Ideals

Ideals. A subset $I \subseteq R$ is an *ideal* if it satisfies the following properties:

1. $I \neq \varnothing$.
2. For all $x, y \in I$, we have $x - y \in I$
3. For all $x \in I$ and $r \in R$, we have $rx \in I$ and $xr \in I$.

Properties 1 and 2 say that I is a subgroup of R under addition, and property 3 is sometimes informally called the "sticky" property.

Note the following:

- Sometimes an ideal is called a "two-sided ideal". (There are other objects, not on the comps syllabus, called left ideals and right ideals.) In practice, though, one almost always says just "ideal."
- When the ring is commutative, we have $rx = xr$, so the sticky property simplifies to: For all $x \in I$ and $r \in R$, we have $rx \in I$.
- An ideal I always contains the zero element of the ring. (Can you prove this?)
- Let R be a ring with unity 1, and let $I \subseteq R$ be an ideal. Then I contains 1 if and only if $I = R$. (Can you prove this?) See **17** and **24** for problems that uses this fact.
- Some books define an ideal I to be a subring of R with the sticky property. This is a valid but redundant definition; **don't use it on the exam**. It requires checking $xy \in I$ for all $x, y \in I$ and then checking the same thing for all $x \in I$ and $y \in R$.

16 (January 2016) Define what it means for a subset $I \subseteq R$ to be an ideal of R.

Note: If you use other technical terms like "closed," "subring," "subgroup," etc., you must fully define those terms as well.

Answer: $I \subseteq R$ is an ideal if:

1. $I \neq \varnothing$.
2. For all $x, y \in I$, we have $x - y \in I$
3. For all $x \in I$ and $r \in R$, we have $rx \in I$ and $xr \in I$. DONE!

Comment. We often see answers to this question that look like the following:

Answer: $I \subseteq R$ is an ideal if:

1. I is a subgroup of R under $+$.
2. For all $x \in I$ and $r \in R$, we have $rx \in I$ and $xr \in I$.

But you cannot say "DONE!" at this point. Although it is technically a correct definition, it does not follow the instructions, since it uses the technical term "subgroup". But if you add

~~3. *I is a subgroup of R under + if it forms a group under + itself.*~~

then you are not done, since "group" is also a technical term that you have to define. This is why you should strike this out. But if you replace it with

3. I is a subgroup of R under $+$ if it is nonempty and closed under subtraction.

then you are *still* not done since "closed" is also a technical term! So you would have to add

4. I is closed under $-$ if for all $x, y \in I$, we have $x - y \in I$. FINALLY DONE!

Conclusion. Hopefully the moral is clear here. You should definitely think of the concepts like "subgroup under $+$" and "closed under subtraction" in your head, but you're going to have to write out their meanings anyhow. So by all means *think* "closed," but *write* "$\forall x, y \in I$, we have $x - y \in I$."

---

17 (February 1982) Prove that if an ideal I of the ring $\mathbb{Z}$ contains two relatively prime integers, then $I = \mathbb{Z}$.

Proof. By hypothesis, there exist $a, b \in I$ with $\gcd(a, b) = 1$. Thus, there are integers $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. But $ma, nb \in I$ by the sticky property, so $1 = ma + nb \in I$ since I is closed under $+$. For any $x \in \mathbb{Z}$, then, we have $x = x \cdot 1 \in I$ by the sticky property. So $I = \mathbb{Z}$ QED

18 (January 2012) Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \,\middle|\, a, b, c \in \mathbb{R} \right\}$. You may assume that R is a ring under the operations of matrix addition and matrix multiplication. Prove that the set

$$I = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

is an ideal of R.

Proof. (I non-empty) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I$, so $I \neq \varnothing$.

(I closed under $-$) Given $r = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ and $s = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$, $r - s = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in I$.

(Sticky) Given $r = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in R$ and $s = \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$, $rs = \begin{bmatrix} ax & ay \\ 0 & 0 \end{bmatrix} \in I$ and $sr = \begin{bmatrix} ax & bx+cy \\ 0 & 0 \end{bmatrix} \in I$.
QED

Here is problem that uses a definition you are not expected to have seen before.

19 (January 2010) Let R be a commutative ring and $S \subseteq R$ a subset of R. Define the *annihilator* of S in R to be

$$\mathrm{Ann}(S) = \{r \in R \,|\, rs = 0 \text{ for every } s \in S\}.$$

Prove that $\mathrm{Ann}(S)$ is an ideal of R.

Proof. (Nonempty) We have $0 \in \mathrm{Ann}(S)$, since $0s = 0 \ \forall s \in S$. So $\mathrm{Ann}(S) \neq \varnothing$.
(Closed under $-$) Given $a, b \in \mathrm{Ann}(S)$ and $s \in S$, we have $(a-b)s = as - bs = 0 - 0 = 0$, so that $a - b \in \mathrm{Ann}(S)$.
(Sticky) Given $r \in R$ and $x \in \mathrm{Ann}(S)$, and given any $s \in S$, we have $(rx)s = r(xs) = r(0) = 0$. Thus, $rx \in \mathrm{Ann}(S)$. Since R is commutative, $xr = rx \in \mathrm{Ann}(S)$. QED

Comment. This problem assumes no prior knowledge of annihilators. In part, this problem tests whether you can read a mathematical definition that you have never seen before and use it in a proof.

Suggestion. For practice, prove that if S, T are subsets of R, then $\mathrm{Ann}(S) \cap \mathrm{Ann}(T) = \mathrm{Ann}(S \cup T)$.

Here is a problem about ideals in a polynomial ring.

20 (March 2015) Let $R = \mathbb{Z}[x]$ be the ring of polynomials (in one variable) with integer coefficients. Note that the constant polynomial 6 and the degree one polynomial $x + 1$ are both elements of R. Define

$$I = \{6f + (x+1)g \mid f, g \in R\}.$$

Prove that I is an ideal of R.

Proof. (Nonempty) Let $f = g = 0 \in R$. Then $6f + (x+1)g \in I$, so $I \neq \varnothing$.
(Closed under $-$) Given $a, b \in I$, write $a = 6f_1 + (x+1)g_1$ and $b = 6f_2 + (x+1)g_2$ with $f_1, f_2, g_1, g_2 \in R$. Then

$$a - b = 6f_1 + (x+1)g_1 - \big(6f_2 + (x+1)g_2\big) = 6(f_1 - f_2) + (x+1)(g_1 - g_2) \in I.$$

(Sticky) Given $a \in I$ and $h \in R$, write $a = 6f + (x+1)g$ with $f, g \in R$. Then

$$ah = ha = h\big(6f + (x+1)g\big) = 6(hf) + (x+1)(hg) \in I$$ QED

10 Quotient Rings

Recall that an ideal $I \subseteq R$ is a subgroup under addition, so the cosets of I are usually written

$$I + r = \{s + r \mid s \in I\},$$

although sometimes you see $r + I$ since addition is commutative. The definition of ideal guarantees that the set of cosets

$$R/I = \{I + r \mid r \in R\}$$

becomes a ring, called the quotient ring, under the following operations:

$$(I + a) + (I + b) = I + (a + b) \qquad \text{and} \qquad (I + a)(I + b) = I + ab.$$

21 (January 2009) Let $I \subseteq R$ be an ideal of R, and suppose that $xy - yx \in I$ for every $x, y \in R$. Prove that the quotient ring R/I is commutative.

Proof. Given $I + a, I + b \in R/I$, our assumption on I implies that $ab - ba \in I$. By the coset relation, we obtain $I + ab = I + ba$. Then

$$(I + a)(I + b) = I + ab = I + ba = (I + b)(I + a),$$

so R/I is commutative, as desired QED

Comment. Remember that when dealing with quotient rings, cosets are **always** written additively, and so the coset relation is the additive version $I + a = I + b \iff a - b \in I$.

DO NOT WRITE cosets as Ia when I is an ideal of a ring.

Suggestion. Prove the converse: If R/I is commutative, then $xy - yx \in I$ for every $x, y \in R$.

22 (January 2014) A nonzero element a of a ring is said to be *nilpotent* if there is a positive integer $n \geq 1$ such that $a^n = 0$. (The element 0 itself is *not* said to be nilpotent.)
Let R be a commutative ring, and let $I \subseteq R$ be an ideal. Prove that the following two statements are equivalent.
(a) The quotient ring R/I contains no nilpotents.
(b) For every element $b \in R$ such that $b^m \in I$ for some positive integer $m \geq 1$, we have $b \in I$.

Proof. ($\Longrightarrow$) Given $b \in R$ and $m \geq 1$ with $b^m \in I$, we have

$$(I + b)^m = I + b^m = I + 0.$$

Since $I + 0$ is the zero element of R/I, it follows that $I + b$ is either nilpotent or zero in R/I. But by assumption (a), $I + b$ is not nilpotent. Therefore, $I + b = I + 0$, which means $b = b - 0 \in I$.

($\Longleftarrow$) Suppose $I + b \in R/I$ is a nilpotent. Then there is some integer $m \geq 1$ such that $(I + b)^m = I + 0$. That is,

$$I + b^m = (I + b)^m = I + 0,$$

and hence $b^m = b^m - 0 \in I$. By property (b), we have $b \in I$. Thus, $I + b = I + 0$, contradicting the assumption that $I + b$ is nilpotent, and proving that R/I has no nilpotents. QED

Comment. As in **19**, this problem asks you to deal with a definition (nilpotent) you are not expected to have seen before. Also, as in **21**, we need to use the additive version $I + a = I + b \iff a - b \in I$ of the coset relation.

Problems **25** and **27** also use the coset relation in a quotient ring.

11 Ring Homomorphisms

Know:

- The definition of ring homomorphism $\phi : R \to S$.
- If $\phi : R \to S$ is a ring homomorphism, then $\phi(0_R) = 0_S$. [But even if both rings have 1, we might *not* have $\phi(1_R) = 1_S$!]
- If $\phi : R \to S$ is a ring homomorphism, then for all $x \in R$ and all $n \in \mathbb{Z}$, we have $\phi(nx) = n\phi(x)$.
- If $\phi : R \to S$ is a ring homomorphism, then for all $x \in R$ and all $n \in \mathbb{N}$, we have $\phi(x^n) = \phi(x)^n$.
- The definition of kernel $\mathrm{Ker}(\phi) \subseteq R$ and image $\mathrm{Im}(\phi) = \phi(R) \subseteq S$.
- The conditions for ϕ to be a ring *isomorphism*.

Be able to show that the kernel of a ring homomorphism $\phi : R \to S$ is an ideal of R. Here is a related problem.

23 (February 2008) Let $\phi : R \to S$ be a ring homomorphism. Let $I \subseteq R$ be an ideal of R, and set

$$J = \{x \in I \mid \phi(x) = 0_S\},$$

where 0_S denotes the zero element of S. Prove that J is an ideal of R.

Proof. (Nonempty) We have $0_R \in I$ and $\phi(0_R) = 0_S$, so $0_R \in J$. Thus, $J \neq \varnothing$.
(Closure under $-$) Given $x, y \in J$, we have $x, y \in I$ and hence $x - y \in I$. Moreover, $\phi(x - y) = \phi(x) - \phi(y) = 0_S - 0_S = 0_S$, so $x - y \in J$.
(Sticky) Given $x \in J$ and $r \in R$, we have $x \in I$, and hence $rx, xr \in I$. Moreover,

$$\phi(rx) = \phi(r)\phi(x) = \phi(r)0_S = 0_S, \quad \text{and}$$
$$\phi(xr) = \phi(x)\phi(r) = 0_S\phi(r) = 0_S,$$

so $rx, xr \in J$.

The Fundamental Theorem of Ring Homomorphisms, Also called the *First Homomorphism Theorem for Rings* or the *Basic Homomorphism Theorem for Rings*, this theorem says that if $\phi : R \to S$ is a ring homomorphism, then there is a ring isomorphism $\widetilde{\phi} : R/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$ defined by $\widetilde{\phi}(\mathrm{Ker}(\phi) + r) = \phi(r)$.

12 Quotient Rings and Fields

Criteria for R to be a Field. Know that a commutive ring with unit is a field if and only if its only ideals are $\{0\}$ and the whole ring. Be prepared to prove this. For example, here is a problem asking to prove one direction of this statement:

24 (March 2005) Let F be a field and let $J \subseteq F$ be an ideal of F. Prove that either $J = \{0\}$ or $J = F$.

Proof. If $J = \{0\}$, then we are done. If $J \neq \{0\}$, then there is $a \in J$ with $a \neq 0$. Since F is a field, a has a multipllicative inverse a^{-1}. Then $1 = a^{-1}a \in J$ since J is an ideal. But an ideal that contains 1 is the whole ring, so $J = F$. QED

Maximal Ideals. Know the definition of a maximal ideal $M \subseteq R$.

Criteria for R/M to be a Field. Let R be a commutative ring with unit. Know that ideal $M \subseteq R$ is maximal if and only if R/M is a field. Here is a problem that asks you to prove part of this result.

25 (February 2013) Suppose that R is commutative and has a multiplicative identity 1. Let $I \subseteq J \subseteq R$ be ideals, and suppose that the quotient ring R/I is a field.

If $I \subsetneq J$, prove that $1 \in J$.

[In fact, it is a Theorem from Math 350 that $J = R$ in this case, but you are only being asked to prove that $1 \in J$. In particular, however, you may **not** quote the $J = R$ theorem.]

Proof. Because $I \subsetneq J$, there exists $r \in J \setminus I$. By the coset relation, $r \notin I$ implies $I + r \neq I + 0 = 0_{R/I}$. Thus, $I + r$ is nonzero. By the definition of field, every nonzero element of R/I has a multiplicative inverse. Hence, there exists $I + s \in R/I$ such that

$$(I + r)(I + s) = I + 1.$$

So $I + rs = I + 1$, and therefore $1 - rs \in I \subseteq J$ by the coset relation.
Note that $rs \in J$, because J is an ideal of R and $r \in J$. Thus, since J is closed under addition, we have $1 = (1 - rs) + rs \in J$. QED

Comment. This is a problem where getting started can be a challenge. Your goal is to show that $1 \in J$, which probably means that you want to find a way to express 1 as some combination of elements of J. Since it's not immediately obvious how to do that, we look to the hypotheses for clues. We see:

- $I \subsetneq J$, which suggests picking $r \in J$ with $r \notin I$.
- R/I is a field, which suggests that multiplicative inverses of nonzero elements may be relevant.

If you are comfortable with cosets, you will realize that $r \notin I$ means that $I + r$ is a nonzero element of R/I. The above proof uses this to find s which eventually satisfies $1 - rs \in J$. Once you have that, it's easier to see how we might write 1 as a combination of elements of J.

13 Polynomial Rings $k[x]$, for a Field k

A polynomial $f = f(x) \in k[x]$ is a symbolic object (x is just a symbol) in the ring $k[x]$. However, if we replace x with an element $a \in k$ (sometimes called "plugging in"), then we get an element $f(a) \in k$. This operation is compatible with addition and multiplication. Here is a problem that makes use of this.

26 (January 2014) For the polynomial ring $R = \mathbb{R}[x]$, define

$$I = \{f \in R \mid f(2) = f(5) = 0\}.$$

Prove that I is an ideal of R.

Proof. (Nonempty) Note that $0 \in \mathbb{R}$ gives the constant polynomial $0 \in R$. Since $0(2) = 0(5) = 0$, we have $0 \in I$.
(Closed under $-$) Given $f, g \in I$, we have $f(2) = f(5) = g(2) = g(5) = 0$. So
$(f - g)(2) = f(2) - g(2) = 0 - 0 = 0$, and $(f - g)(5) = f(5) - g(5) = 0 - 0 = 0$, and hence $f - g \in I$.
(Sticky) Given $f \in I$ and $g \in R$, we have $f(2) = f(5) = 0$. So
$(gf)(2) = g(2)f(2) = g(2) \cdot 0 = 0$, and $(gf)(5) = g(5)f(5) = g(5) \cdot 0 = 0$. Thus, $gf \in I$.
Since R is commutative, we also have $fg = gf \in I$. QED

The Division Algorithm. Know the statement of the division algorithm in $k[x]$. Here is a problem that uses the division algorithm.

27 (March 2009) Let $\mathbb{F}$ be a field, let $R = \mathbb{F}[x]$ be the ring of polynomials in one variable with coefficients in $\mathbb{F}$, and let $f(x) \in R$ be a polynomial of degree 2009. Let

$$I = \{g(x)f(x) \mid g \in R\}$$

be the set of all polynomials which are multiples of $f(x)$. It is a fact, which you may assume, that I is an ideal of R.
(a) For any $g, h \in R$, prove that $I + g = I + h$ if and only if $(g - h)$ is divisible by f.
(b) Prove that for any $g \in R$, there is a unique polynomial $h \in R$ with $\deg h < 2009$ such that $I + g = I + h$.

Proof. (a) Given $g, h \in R$, we have $I + g = I + h$ if and only if $g - h \in I$, by the coset relation. But the definition of I implies that $g - h \in I$ if and only if $g - h$ is a multiple of f.

(b) Given $g \in R$:

(Existence) The division algorithm yields $q, h \in \mathbb{F}[x]$ such that

$$g = qf + h \quad \text{with} \quad \deg h < \deg f = 2009.$$

Thus $g - h = qf \in I$, so by part (a), $I + g = I + h$, proving existence.

(Uniqueness) Suppose we are given $h, h' \in R$ with $I+g = I+h' = I+h'$, and with $\deg h, \deg h' < 2009$. Then $I + h = I + h'$, so by part (a), $h - h'$ is a multiple of f. That is,

$$h - h' = kf \quad \text{for some} \quad k \in R.$$

If $k \neq 0$, then

$$\deg(h - h') = \deg(kf) = \deg k + \deg f \geq \deg f = 2009.$$

However, the fact that $\deg h, \deg h' < 2009$ implies that $\deg(h - h') < 2009$ also, a contradiction. Thus, we must have $k = 0$, and hence $h - h' = 0$. That is, $h = h'$, proving uniqueness. QED

Every Ideal in $k[x]$ is Principal. Recall that a principal ideal in a commutative ring consists of all multiples of a fixed element. Problem **27** features principal ideals in $k[x]$. This is no accident, since

$$\text{every ideal in } k[x] \text{ is of the form } \langle f \rangle = \{gf \mid g \in k[x]\}.$$

Furthermore, f is unique up to multiplication by a nonzero constant of k. Since the units of $k[x]$ are precisely the nonzero constants, we can equivalently say that f is unique up to multiplication by a unit.

Irreducible Polynomials and Maximal Ideals in $k[x]$. Know the following:

- The definition of reducible and irreducible polynomial in $k[x]$.
- The irreducibility criterion for polynomials $f \in k[x]$ of degree 2 or 3: such a polynomial is irreducible if and only if it has no roots in the field k. (See problem **28** below for a proof of this fact for cubic polynomials; can you do the proof for quadratic polynomials?)
- An ideal $I \subseteq k[x]$ is maximal if and only if $I = \langle f \rangle$, where $f \in k[x]$ irreducible. That is:

$$f \text{ is irreducible} \iff \langle f \rangle \subseteq k[x] \text{ is maximal} \iff k[x]/\langle f \rangle \text{ is a field.}$$

Here some problems about these concepts.

28 (January 1999) Let k be a field. Show that a cubic polynomial $f(x) \in k[x]$ is irreducible in $k[x]$ if and only if $f(x)$ has no roots in k.

Proof. We'll prove f reducible iff f has a root in k.
($\Longrightarrow$): Since f is reducible, there exist $g, h \in k[x]$ with $f = gh$ and with $\deg g, \deg h < 3$. Since $\deg g$ and $\deg h$ are nonnegative integers summing to $\deg f = 3$, one of g and h must have degree 1 and the other must have degree 2. Without loss, $\deg g = 1$. That is, $g(x) = ax + b$ for some $a, b \in k$ with $a \neq 0$. Then $-b/a \in k$, and

$$f\Big(-\frac{b}{a}\Big) = g\Big(-\frac{b}{a}\Big)h\Big(-\frac{b}{a}\Big) = \Big[a\Big(-\frac{b}{a}\Big) + b\Big]h\Big(-\frac{b}{a}\Big) = (-b+b)h\Big(-\frac{b}{a}\Big) = 0 \cdot \Big(-\frac{b}{a}\Big) = 0,$$

and hence $-b/a$ is a root of of f in k.
($\Longleftarrow$): Let $c \in k$ be a root of f, and let $g(x) = x - c \in k[x]$. By the division algorithm for f and g, there exist polynomials $q, r \in k[x]$ with $f = qg + r$ and with either $r = 0$ or $\deg r < \deg g = 1$.
If $r \neq 0$ but $\deg r < 1$, then $\deg r = 0$, which means that $r = b$ is a nonzero constant. Hence,

$$0 = f(c) = q(c)g(c) + r(c) = q(c) \cdot (c - c) + b = 0 + b = b \neq 0,$$

a contradiction. Thus, we must in fact have $r = 0$, and hence $f = qg$. Since $\deg f = 3$ and $\deg g = 1$, we must have $\deg q = 3 - 1 = 2$, and hence we have factored f as a product of two lower-degree polynomials g and q, proving that f is reducible. QED

Comment. This problem is asking you to prove a fact that you are expected to know from Math 350. Obviously, you cannot simply quote the desired fact from the course.

Suggestion. Try proving the same fact for the case that f is a *quadratic* polynomial. Also, prove that the analogous fact is *not* true for for polynomials of degree 4 or higher.

Here is a problem where you need to know a enough about *why* the quotient ring $k[x]/\langle f\rangle$ is a field when f is irreducible to be able to find the inverse of a particular element in the quotient ring.

29 Let $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$, where $\mathbb{F}_3 = \{0, 1, 2\}$ is the field of three elements. Let $I = \langle f\rangle$ be the principal ideal in $\mathbb{F}_3[x]$ generated by f.
(a) Prove that f is irreducible in $\mathbb{F}_3[x]$.
(b) Prove that the quotient ring $\mathbb{F}_3[x]/I$ is a field.
(c) Find the multiplicative inverse of $I + x$ in the quotient ring $\mathbb{F}_3[x]/I$.

Proof. (a) Since $\deg f = 2$, f is reducible if and only if it has no roots in $\mathbb{F}_3$. Checking shows:

$$f(0) = 1 \neq 0, \qquad f(1) = 2 \neq 0, \qquad f(2) = 2 \neq 0.$$

Since $f(a) \neq 0$ for all $a \in \mathbb{F}_3$, it follows that f is irreducible.
(b) Since f is irreducible, the ideal $I = \langle f\rangle$ is maximal in $\mathbb{F}_3[x]$, by a Math 350 theorem. So by another Math 350 theorem, the quotient $\mathbb{F}_3[x]/I$ is a field.
(c) We need a polynomial $g \in \mathbb{F}_3[x]$ such that $(I + x)(I + g) = I + 1$. However,

$$(I + x)(I + g) = I + 1 \iff I + xg = I + 1 \iff xg - 1 \in I \iff xg + 2 \in I,$$

where the last equivalence uses $-1 = 2$ in $\mathbb{F}_3$. Choosing $g(x) = 2x$ gives

$$xg + 2 = x(2x) + 2 = 2(x^2 + 1) \in I.$$

Thus, by the above equivalences, and by commutativity, we have

$$(I + 2x)(I + x) = (I + x)(I + 2x) = I + 1 = 1_{\mathbb{F}_3[x]/I},$$

and hence $I + 2x$ is the multiplicative inverse of $I + x$ in $\mathbb{F}_3[x]/I$. QED

30 (January 2009)
(a) Prove that $f(X) = X^4 + X^2 + 1$ is **reducible** in the polynomial ring $\mathbb{F}_2[X]$, where $\mathbb{F}_2 = \{0, 1\}$ is the field of two elements.
(b) Prove that $g(X) = X^3 + 2X^2 + 2X + 3$ is **irreducible** in the polynomial ring $\mathbb{F}_5[X]$, where $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ is the field of five elements.

Proof. (a) To be reducible, f must either have a degree one factor (and hence have a root in $\mathbb{F}_2$), or f must be a product of two irreducible factors of degree two. But $f(0) = f(1) = 1$ so f has no roots in $\mathbb{F}_2$. Hence f is the product of two irreducible quadratic factors. The possible quadratic polynomials are X^2, $X^2 + 1$, $X^2 + X$ and $X^2 + X + 1$. The first and third are clearly reducible, and over $\mathbb{F}_2$, we have $X^2 + 1 = (X + 1)^2$, so $X^2 + X + 1$ is the only quadratic irreducible polynomial. Then an explicit calculation (made easier by using $(a+b)^2 = a^2 + b^2$ since we are working over $\mathbb{F}_2$) shows that $f(X) = (X^2 + X + 1)(X^2 + X + 1)$. QED

(b) Since $\deg g = 3$, we know that g is reducible if and only if it has no roots. Checking shows:

$$g(0) = 0^3 + 2(0^2) + 2(0) + 3 = 0 + 0 + 0 + 3 = 3 \neq 0$$
$$g(1) = 1^3 + 2(1^2) + 2(1) + 3 = 1 + 2 + 2 + 3 = 3 \neq 0$$
$$g(2) = 2^3 + 2(2^2) + 2(2) + 3 = 3 + 3 + 4 + 3 = 3 \neq 0$$
$$g(3) = 3^3 + 2(3^2) + 2(3) + 3 = 2 + 3 + 1 + 3 = 4 \neq 0$$
$$g(4) = 4^3 + 2(4^2) + 2(4) + 3 = 4 + 2 + 3 + 3 = 2 \neq 0$$

Since $g(a) \neq 0$ for all $a \in \mathbb{F}_5$, it follows that g is irreducible. QED

Comment. This is a problem where finiteness helps. In part (a), since we are working over a finite field, there are only finitely many polynomials of given degree. Our proof above listed all quadratic polynomials in $\mathbb{F}_2[X]$, and we could determine which were irreducible by plugging in the (finitely many) elements of $\mathbb{F}_2$. We did the same plugging in strategy for part (b).

Here is a problem about how irreducible polynomials correspond to maximal ideals in $k[x]$. More precisely, it's about how *non*-irreducible polynomials correspond to *non*-maximal ideals.

31 (March 2008) Let $g(x) = x^2 + 3 \in \mathbb{F}_7[x]$, where $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ is the field of seven elements.
(a) Prove that g is reducible in $\mathbb{F}_7[x]$.
(b) Let $\langle g \rangle \subseteq \mathbb{F}_7[x]$ denote the principal ideal $\{gh \mid h \in \mathbb{F}_7[x]\}$. Find an ideal $I \subseteq \mathbb{F}_7[x]$ such that $\langle g \rangle \subsetneq I \subsetneq \mathbb{F}_7[x]$.

Proof. (a) Plugging each element of $\mathbb{F}_7$ into g soon shows $g(2) = 0$, so that $(x - 2)$ is a factor of g. Long division reveals that $g(x) = (x - 2)(x + 2)$, confirming that g is reducible.

(b) Let $I = \langle x - 2 \rangle \subseteq \mathbb{F}_7[x]$. Any element of $\langle g \rangle$ is of the form hg for some $h \in \mathbb{F}_7[x]$, and hence

$$hg = \big((x + 2)h\big) \cdot (x - 2) \in I.$$

Thus, we have $\langle g \rangle \subseteq I \subseteq \mathbb{F}_7[x]$. However, $x - 2 \notin \langle g \rangle$, because any multiple hg of g must either be 0 or have degree $\deg(hg) \geq \deg g = 2$, whereas $\deg(x - 2) = 1$. Finally, $1 \notin I$, because any multiple $h \cdot (x - 2)$ of $(x - 2)$ must either be 0 or have degree $\geq \deg(x - 2) = 1$, whereas $\deg(1) = 0$.
Hence, $\langle g \rangle \subsetneq I \subsetneq \mathbb{F}_7[x]$. QED

Comment. Since the ring is $\mathbb{F}_7[x]$, you know in advance that I has to be principal. You should check that $I = \langle x + 2 \rangle$ also works.

14 Preparing for the Algebra Exam

Now that you have finished reading the content part of the Study Guide, what should you do next to prepare for the algebra exam? The key thing to keep in mind is that

You need an active knowledge of algebra.

Here are a some suggestions to help you achieve this.

Read the Study Guide Actively. There are many places where the Study Guide asks you to provide a proof or complete a proof. Do so. This is really important.

Read Your Notes and Your Algebra Book. In many places in the Study Guide, we say "Know the basic facts about ...," without stating the facts precisely. This is deliberate, since we want you to refer to your notes and your algebra book when studying for the exam.

Not everything covered in your algebra course is part of the algebra exam. For example, the class equation from group theory is a lovely topic that will not be on the exam. This Study Guide and the *Syllabus for Algebra* (*Math 350*) list the topics that you need to know.

Know Basic Results and Definitions. Keep in mind that knowing the precise statements of definitions and basic theorems is essential. The adjective "precise" is important here. For example, if a problem asks you to state the Lagrange's theorem for subgroups, then just writing

$$|H||G|$$

will not get full credit. You need to state the whole theorem: If H is a subgroup of a finite group G, then

$$|H||G|.$$

Also, when asked for a definition, you are sometimes instructed to define terms used in your definition. In such a situation, just writing "closed under inverses" would not be sufficient; you would need to explain what "closed" means. (And if you were working in a *ring*, you'd need to specify whether you mean *additive* inverses or *multiplicative* inverses.)

Study Old Exams and Solutions. The Department website has a collection of old exams in algebra, many with solutions. It is very important to do practice problems. This is one of the key ways to acquire an active knowledge of algebra. There are two dangers to be aware of when using old exams and solutions:

- Thinking that the exams tell you what to study. Every topic on the *Syllabus* and in this Study Guide is fair game for an exam question.
- Reading the solutions. This is passive. To get an active knowledge of the material, do problems from the old exams yourself, and *then* check the solutions. The more you can do this, the better.

Work Together, Ask Questions, and Get Help. Studying with your fellow math majors can help. You can learn a lot from each other. Faculty are delighted to help. Don't hesitate to ask us questions and show us your solutions so we can give you feedback. The QCenter has excellent people who have helped many students in the past prepare for the Comprehensive Exam.

Start Now. Properly preparing for the algebra exam will take longer than you think. Start now.