Brief Solution Descriptions and Technique Summary

June 6, 2005

1 Techniques

Here is a summary of some techniques. It is by no means an exhaustive list.

Whenever you need a subgroup, a normal subgroup, or a homomorphism, consider group actions. You may not need them, but they often make life much simpler for you. It is a fantastic idea to familiarize yourself with the following standard group actions:
1)G acts on itself by left multiplication
2)G acts on a subgroup H or itself by conjugation
3)G acts on the set of its subsets by conjugation
4)G acts on the set of left cosets of a subgroup H by multiplication
5)G acts on the set of p-Sylow subgroups by conjugation
There are many other group actions that come up in the course of doing problems, but these 5 seem to be the most common.

The orbit-stabiliser theorem - Given an orbit O containing the element x, we have $|O| = [G : G_x]$. G_x is called the stabiliser of x. Its definition is $G_x = \{g \in G | gx = x\}$. One could try to directly calculate the size of an orbit, but for many actions this would be quite hard. Thus, if you want to know the size of an orbit, you should always try the orbit-stabiliser theorem first. Also, the fact that $G_x \leq G$ limits the possibilities for the size of the orbit by Lagrange's theorem. Note that sometimes it is not obvious that we wanted to know the size of an orbit of some group action (e.g. Jan90 #1 doesn't explicitly tell you this).

Note that familiarity with product groups (groups of the form HK) is essential in both non-Sylow problems and Sylow problems. The main theorems to know are the formula $|HK| = \frac{|H||K|}{|H \cap K|}$, the fact that $K \trianglelefteq G$ implies HK is a group (actually a weaker hypothesis suffices - see p95), and the fact that $K \trianglelefteq G$ and $H \trianglelefteq G$ implies $HK \trianglelefteq G$. The last one is particularly useful for classification problems because in those problems you want to obtain large normal subgroups of G.

shows that Ker $\phi \leq H$ and the 1st isomorphism theorem yields [G:Ker $\phi] \leq$ n!

Aug89 #3i - $g^n H = H$ for some $n \in Z$. Thus $g^n \in H$, so $(g^n)^m = e$ for some $m \in Z$.

Jan90 #1 - If G acts on P(G) (the set of subsets of G) by conjugation, then the set of conjugates of H is the orbit of H under this action. Apply the orbit-stabiliser theorem to find that $[G : N_G(H)]$ is the number of conjugates of H. $|H| \leq |N_G(H)|$ is then used to obtain a contradiction.

Jan91 #1a - Unwind the definitions and whatnot.

Aug93 #1 - If $K \trianglelefteq G$ and $H \leq G$ then $H \vee K = HK$. Apply this theorem to the subgroups in the problem and manipulate things elementwise.
Jan96 #6 - Use group actions and the orbit-stabiliser theorem. Depending on your choice of group action you may also need to exhibit a bijection between the stabiliser and $x^{-1}Hx \cap K$.

Jan99 #2 - Unsure how to briefly describe this one.

2.2 Sylow Problems

Fal84 #2 - G is simple so there are 8 7-Sylow subgroups by Sylow III. Sylow II says that conjugation on the set of 7-Sylow subgroups is a group action. This induces a homomorphism $\phi : G \rightarrow S_8$. Ker $\phi = \{1\}$ otherwise we contradict simplicity. The result then follows from the 1st isomorphism theorem.

Jan90 #2 - Sylow III gives us that the 11-Sylow subgroup P and the 13-Sylow subgroup Q are normal in G. Thus $PQ \trianglelefteq G$. There is a 2-Sylow subgroup R of order 2 by Sylow I. So, PQR = G and $PQ \cap R = \{1\}$ by Lagrange. Thus $G \cong PQ \rtimes R$. Now determine the possible homomorphisms $\phi : R \rightarrow Aut(PQ)$ to determine the possible structures for the semidirect product of PQ and R. Check whether any of the distinct homomorphisms give rise to isomorphic groups.

Sum91 #5 - Look at G/K. Sylow III tells us there is a 25 element normal subgroup of G/K. The correspondence theorem (Dummit + Foote p100 Theorem 20) tells us there is normal subgroup of G of order 2500.

Jan95 #6 - The simplicity of A_5 and the fact that 5-cycles are even permutations combine to eliminate the possibility that $n_5 = 1$. After that, numerical arguments eliminate various possibilities for n_2 and n_3. For part b, note that we can embed D_8 into S_5. Since all the 2-Sylow subgroups are isomorphic (by Sylow II), they must all be D_8. They act on 5 symbols by fixing one and then treating the other 4 like a square. The 3-Sylow subgroups are 3-cycles, so they fix 2 symbols and rotate the other 3.

More Techniques and Solutions

June 6, 2005

1 More Group Techniques

The group techniques covered in the first handout seem to come up a lot more often than the ones I'm going to mention here.

1.1 Using Invariance

It is useful to know what properties are preserved under isomorphism and homomorphism. The one that has come up most in old prelim problems is the order of an element. An element of order n gets mapped to an element of order n in an isomorphism. This can be used to show two groups are non-isomorphic (if G has more order 5 elements than H then $G \not\cong H$). Also, if two elements are in the same conjugacy class, they must have the same order (since conjugation is an isomorphism). Lastly, for mere homomorphisms, we have the order of f(x) divides the order of x, which is used to determine the possible homomorphisms from one group to another (say, in Sylow/semidirect problems).

Another fact we saw was that conjugation preserves not just order, but cycle type in S_n (in fact, the result is stronger than this - see D+F pg 129).

1.2 Burnside's Formula

$r = \frac{1}{|G|} \sum_{g \in G} |X_g|$. This formula is not used as often as the class equation or the orbit-stabiliser theorem. What it does is count how many orbits there are. r = the number of orbits. $X_g = \{x \in X | gx = x\}$. Note that X_g is not the same as G_x. It should be noted that one can often count the number of orbits without resorting to this theorem.

1.3 Pigeonhole Principle

The Pigeonhole Principle states that if A and B are finite sets and $|A| = |B|$, then for any function $f : A \to B$, f is 1-1 if and only f is onto. Spring 88 #2 (which I didn't assign) is the only prelim problem I could find which uses this formulation of the principle directly. However, there is a corollary of it that gets used more frequently - if $|A| = |B|$ and $A \subseteq B$, then $A = B$ (apply Pigeonhole

Principle to the inclusion map). Note that the Pigeonhole Principle and this corollary don't hold for infinite sets.

2 Ring Techniques

Many ring problems involve the Field/ED/PID/UFD/etc hierarchy. Before getting to that, I'll list some techniques not directly involving that hierarchy.

2.1 The Field and Integral Domain Theorems

Two very useful theorems:
1) I is a prime ideal in R if and only if R/I is an integral domain.
2) I is a maximal ideal in R if and only if R/I is a field

One technique that arises from this theorem is that if you are trying to show an ideal is prime or maximal, look for natural homomorphisms $f : R \to S$ (where S is just another ring) where I is the kernel of that homomorphism. Then, hopefully the image will be something you already know to be a field or an integral domain. Proofs dealing directly with R/I are generally clumsier than those using homomorphisms and the 1st isomorphism theorem. Plus, you get style points for using homomorphisms and the isomorphism theorems.

It should be noted that the 2nd theorem (the field one) is very fundamental to the theory of field extensions, since field extensions are of the form $F[x]/(p(x))$. The maximality of $(p(x))$ guarantees that this is a field.

2.2 Polynomial Ring Tricks

2.2.1 Comparing Coefficients

This is the main trick - If $a_n x^n + ... + a_0 = b_n x^n + ... + b_0$ then $a_0 = b_0, a_1 = b_1, ..., a_n = b_n$. This gets used when you have to deal with polynomial rings at the element level. For example, to prove (2,x) is not principal in Z[x], you compare coefficients a bunch of times to reach a contradiction.

2.2.2 The Homomorphism Everyone Should Know About

Let $F : R[x] \to R$ be given by $F(a_n x^n + ... + a_0) = a_0$ (in other words, send a polynomial to its constant term in R). This homomorphism is a map onto R with kernel (x). Thus we obtain $R[x]/(x) \cong R$. Should R be an integral domain or a field then we know (x) is prime or maximal. To create more complex homomorphisms coming out of $R[x]$, one can take homomorphisms $G : R \to S$ and compose them with F.

There is also the evaluation homomorphism (but it doesn't seem to come up in

prelim problems): Given $c \in R$, let $E_c(f) = f(x)$. E_c is a homomorphism from R[x] into R.

2.3 Adding and Multiplying Ideals

$I + J$ has a nice intuitive definition: $I + J = \{x + y | x \in I, y \in J\}$. IJ isn't as nice: $IJ = \{\Sigma^n xy | x \in I, y \in J\}$ - in other words, finite sums of products from I and J. The finite sum part is necessary to keep the ideal closed under addition. Given principal ideals (a) and (b), we do at least get the nice property that $(a)(b) = (ab)$ (via the distributive law and the nice form of principal ideals).

2.4 Element-wise Things in PIDs and UFDs

We get some nice element-wise manipulations in PIDs based on the fact that if you have an ideal of the form (a) then every element of (a) is of the form ra where $r \in R$. So, when working with PIDs (or just with principal ideals), if stuck, start looking at the form of the elements of the ideals. If that is not good enough one can note that PIDs are also UFDs and use unique factorization tricks.

There are some frequently used conversions between things at the element level and things at the set level (with principal ideals): $a|b \Leftrightarrow (b) \subseteq (a)$. If a is a unit, then $(a) = R$ (the full ring). $(a,b) = (d)$ if and only if d is the greatest common divisor of a and b (in general GCD is defined so that $d|a$ and $d|b$, and if $d'|a$ and $d'|b$, then $d'|d$).

In UFDs you get a trick similar to comparing coefficients in polynomial rings - comparing irreducibles. If $p_1 p_2 ... p_n = q_1 q_2 ... q_m$ where the p_i, q_j are all irreducible elements of R, then m=n and for each p_i there is a q_j that is associate to it (they differ by a unit - $p_i = u q_j$ for some unit u).

2.5 Common Norms and Norm Techniques

In polynomial rings, N(f) = the degree of f, gives a norm. This is the norm they use to show F[x] is a Euclidean Domain if F is a field.

In the rings $Z[\sqrt{-D}]$ or $Z[\frac{1+\sqrt{-D}}{2}]$ the norm is always the square of the usual complex number norm (write your typical element in the form $x + iy$ and your norm will be $x^2 + y^2$). There is not a single prelim problem that deviates from this. It is a nice norm because it is multiplicative - $N(ab) = N(a)N(b)$. In these rings, the norm is always a positive integer. Often, even if we aren't in a Euclidean Domain, we can use the norm to reason about units and whatnot: In these rings, a is a unit $\Leftrightarrow N(a) = 1$.

Note that the norm only hits certain integers. For example, in $Z[\sqrt{-3}]$, the norm is $a^2 + 3b^2$. It is easy to check that there is no $a, b \in Z$ such that $N(a + b\sqrt{-3}) = 2$. Thus if $N(ab) = 4$ then $N(a) = 1$ or $N(b) = 1$. This

3

means a norm 4 element must be irreducible. This line of reasoning gets used in some problems.

2.6 The Hierarchy and Its Many Theorems

This is where a lot of the action is. Its good to know these things and it may even be useful to be able to prove many of them. The hierarchy is this: Every Field is a Euclidean Domain, every Euclidean Domain is a Principal Ideal Domain, every Principal Ideal Domain is a Unique Factorization Domain, every Unique Factorization Domain is an Integral Domain, and every Integral Domain is a Commutative Ring with identity. Aside from knowing the definitions, examples and counterexamples, and the main theorems, the one thing that is useful to keep in mind is that you get cancellation in an integral domain ($ax = ay \Rightarrow x = y$). You do not get this in a mere Commutative Ring with Identity!

2.6.1 The Relationships Between R and R[x]

1) R is a field $\Leftrightarrow$ R[x] is a Euclidean Domain
2) R is a field $\Leftrightarrow$ R[x] is a PID
3) R is a UFD $\Rightarrow$ R[x] is a UFD

So, you really need the condition of field to get R[x] is a PID. Any lesser condition and the best you can get is R[x] is a UFD. In particular F[x,y] is not a PID, even if F is a field, but a polynomial ring over a field in any number of variables is a UFD.

2.6.2 All Prime Ideals Are Maximal When...

If R is a PID, then every prime ideal is a maximal ideal. By the hierarchy, this result holds for fields and Euclidean Domains.

2.6.3 The Relationships Between Primeness and Irreducibility

1) If R is a mere Integral Domain, then prime elements are always irreducible.
2) If R is a PID, then a nonzero element is prime $\Leftrightarrow$ it is irreducible.

The 1st one can be useful when doing element-wise manipulations in a UFD (using the comparing irreducible factors trick). The 2nd one can be used to make arguments like this: If p(x) is an irreducible element of F[x] (where F is a field), then (p(x)) is prime, and since F is a field, F[x] is a PID, hence (p(x)) is not just prime but maximal, hence F[x]/(p(x)) is a field!

4

3 Abridged Solutions/Hints

Jan97 #1 - For each $x \in G$ there is a group K such that $H \leq K \Rightarrow hx = xh$. For K, one can use either $<x>$ or $C_G(x)$.

Aug95 #1 - Same Sylow techniques as in first handout. Note that $f : Z_3 \to Aut(Z_{11}) \times Aut(Z_{17})$ must be trivial. So, its abelian and cyclic.

Jan91 #1b - See text, its a standard (and very useful) result.

Aug90 #3 - For part a, note that conjugation preserves cycle types and the group H consists of all elements of the type (ab)(cd), so conjugation keeps elements in H. $|A_4/H| = 3$ so it must be cyclic. For part b, $H \subseteq C_G(H)$ since H is abelian. For $C_G(H) \subseteq H$ note that the 3 elements of type ()() are in a conjugacy class. Thus for any $x \in H$, $[G : C_G(x)] = 3$ giving $|C_G(x)| = 8$. Then note for $x, y \in H$, $C_G(x) \cap C_G(y) = H$. The result follows. For part c, we use part b to show ker $\phi = H$ and then apply first isomorphism theorem.

Aug89 #3ii - $n_7 = 1$ or 8. If $n_7 = 8$ then only 8 elements aren't order 7 elements. Thus $n_2 = 1$ as $|P_2| = 8$ for any 2-Sylow subgroup.

Aug89 #4 - For part a, rewrite the group in invariant factor form: $Z_{5 \cdot 3^3 \cdot 2^2} \times Z_{5 \cdot 3^2 \cdot 2} \times Z_{3^2 \cdot 2}$. The first factor gives the largest cyclic subgroup. For part b, rewrite the group in elementary divisor form: $(Z_5 \times Z_5) \times (Z_{3^3} \times Z_{3^2} \times Z_{3^2}) \times (Z_{2^2} \times Z_2 \times Z_2)$. Note all the order 3 elements come from the middle term. Use counting to get 26 of them.

Aug88 #1 - You get $Z_7 \rtimes Z_3$ by the usual techniques. The two homomorphisms leading to nonabelian groups give rise to isomorphic groups.

Fal80 #3 - You can't use simple numerical arguments. Note that if G was simple then $n_3 = 4$. By Sylow II, there is a group action on the 3-Sylow subgroups by conjugation which yield a homomorphism $\phi : G \to S_4$. Ker $\phi = 1$ makes ϕ 1-1 which would mean $36 \leq 24$ which can't be. Ker $\phi = G$ would make the 4 3-Sylow subgroups normal (each would be fixed by conjugation of any element of G). This can't be, so we have a nontrivial kernel, making G non-simple.

p151 #50 - There exists $g \in G$ such that $gxg^{-1} = y$. Now look at $C_G(y)$. Show $C_G(y)$ contains both P and gPg^{-1}. Use Sylow II to obtain a $c \in C_G(y)$ such that $cgPg^{-1}c^{-1} = P$. So, $cg \in N_G(P)$. Also, $cgxg^{-1}c^{-1} = cyc^{-1} = y$.

Jan04 #4 - Suppose $(a, x) = (f(x))$ for some $f(x) \in R[x]$. Then $a = f(x)g(x)$ for some $g(x) \in R[x]$. Compare coefficients to yield f is a constant $c \in R$. Now, we also have $x = cg(x)$ for some $g(x) \in R[x]$. Compare coefficients to yield $ck = 1$ for some $k \in R$. Now c is a unit, so we have $(f(x)) = R[x]$ so $1 \in (a, x)$. Compare coefficients to conclude a is a unit giving a contradiction. Q[x] is a

Euclidean Domain since Q is a field. Q[x,y] is not a PID since Q[x] is not a field. Alternatively, form the ideal $(a(x), y)$ for a non-unit $a(x) \in Q[x]$.

Jan98 #3 - Follow the logic of D+F at the top of pg 273. For part b, note that $2 \cdot 2 = 4$ and $(1 + \sqrt{-3})(1 - \sqrt{-3} = 4$. Since 2 and $1 + \sqrt{-3}$ are irreducible and don't differ by a unit, $Z[\sqrt{-3}]$ can't be a UFD.

Aug96 #2 - We have $a^n = 0$ and $b^m = 0$ for some n,m. For additive closure, look at $(a + b)^{n+m}$ and use the binomial theorem to get 0. Now note $(ra)^n = r^n a^n = 0$ so, N is an ideal. For the noncommutative example, look at simple elements in small matrix rings. For part b, unwind the definitions.

Aug94 #3 - Let $F : Z[x] \to Z$ be the homomorphism everyone should know about. Let $G : Z \to Z/5Z$ be the usual map, and let $H = G \circ F$. Now, note that Ker $F = (x)$. By the 1st isomorphism theorem, we get (x) is prime but not maximal since Z is an integral domain, but not a field. Ker H = (5,x) and H maps onto $Z/5Z$, so we have $(5, x)$ is maximal since $Z/5Z$ is a field. Lastly $x+1 \notin (2x, x^2+1)$, yet $(x+1)(x+1) \in (2x, x^2+1)$ so $(2x, x^2+1)$ isn't even prime.

Aug92 #4 - Part a - units are ± 1. Part b - note that $N(a) = 2$ and $N(a) = 8$ are unpossible. $N(4) = 16$ so if $ab = 4$ then $N(a) = 4, N(b) = 4$. The elements such that $N(a) = 4$ are $2, -2, 1 + \sqrt{-3}, 1 - \sqrt{-3}$. Look at these to get the factorizations. Part c - For 5 to be reducible we'd need two norm 5 elements, but $a^2 + 3b^2$ is never 5. Thus 5 is irreducible. $7 = (2 + \sqrt{-3})(2 - \sqrt{-3})$ so its reducible. For part d, 2 is irreducible, but not prime.

Sum91 #3 - Be careful not to use cancellation on this problem (cancellation would make it easy). $a = a^2 = (-a)^2 = -a$. Now, $(a + b)^2 = a^2 + ab + ba + b^2$. Also, $(a + b)^2 = a + b = a^2 + b^2$. Thus, $ab + ba = 0$. Thus $ab = ba$.

Jan90 #5 - Part a - (2,x) in Z[x]. Part b - $\oplus_\omega Z$ in $\sqcap_\omega Z$ is an ideal but is not finitely generated (use contradiction). Part c - Z[x] is a UFD since Z is. But, (2,x) is not principal.

Jan87 #4 - For parts i and ii the definitions unwind nicely. For part iii use the fact that a PID is a UFD and one of the ideals is generated by a prime (hence irreducible!) element.

Jan86 #3 - In parts a and b the definitions unwind nicely. Part c use the great homomorphism with kernel (x).

Spr82 #3 - Write $1 = x + y$ with $x \in I$, $y \in J$. We obtain equations for a and b and then let $c = ay + bx$ and reduce mod I and J. Use a homomorphism $f : R \to R/I \times R/J$ with kernel $I \cap J$. Use part a to show this homomorphism is onto.