August 2009 Algebra Prelim

Sarah Arpin

1

Give examples of the following or explain why no such example exists.

(a) A non-abelian group of order 48.

(b) A finite nilpotent group G and a normal subgroup N such that G/N is not nilpotent.

(c) A group G and a prime p such that G has exactly 5 Sylow p-subgroups.

Solution:

(a) The dihedral group $D_{48} = \langle r, s | r^2 4 = s^2 = 1, rs = sr^{-1} \rangle$ is not abelian.

(b) If G is nilpotent, then any subgroup and any quotient group of G must be nilpotent as well.
A group is nilpotent if and only if it is the direct product of its Sylow p-subgroups, and its Sylow p-subgroups are unique for each p dividing the order of G, so:

$$G \cong P_1 \times ... \times P_s$$

where P_i is the unique Sylow p_i-subgroup for each prime p_i dividing the order of G. If N is a subgroup of G, then N is a subgroup of this direct product, so N is itself a direct product in the same form and is thus also nilpotent.
Quotients of nilpotent groups are nilpotent.

(c) Yes, there does exist such a group. Let n_p denote the number of Sylow p-subgroups of a group G. If $n_p = 5$, then by the Sylow theorems $5 \equiv 1(mod p)$, so $p = 2$.
Consider a group of order 10, and suppose $n_2 = 5$. Then, there are 5 elements of order 2.
$n_5 \equiv 1(mod 5)$ and $n_5 | 2$, so $n_5 = 1$, and we have 4 elements of order 5. This leaves the final element as the identity, so this is valid so far.
Since $n_5 \equiv 1(mod 5)$, the Sylow 5-subgroup of G must be normal, and since $P_5 \cap P_2 = 1$, G is equivalent to a semi-direct product:

$$G \cong P_5 \rtimes P_2$$

To check that this is a semidirect product, we have to make sure that there is some nontrivial $\varphi \in \text{Hom}(P_2, \text{Aut}(P_5))$. Since $\text{Aut}(P_5) \cong \mathbb{Z}_4^\times$, there are two generators to map to, and thus there does exist a nontrivial φ for this semidirect product.

2

If G is an abelian group acting on a finite set X, then the action of G on $X \times X$ defined by

$$g \cdot (x, y) = (g \cdot x, g \cdot y) \text{ for all } (x, y) \in X \times X \text{ and } g \in G$$

has at least $|X|$ orbits.

(a) Prove this statement in the case that the action of G on X is transitive.

(b) Prove this statement in the case that the action of G on X is an arbitrary action.

Solution:

(a) If G acts transitively on X, then $|\mathcal{O}_G(x)| = |X|$ for all $x \in X$.
By the orbit stabilizer theorem, we know

$$|G| = |\mathcal{O}_G(x)||\text{Stab}_G(x)|$$

Since we know G acts transitively,

$$|G| = |X||\text{Stab}_G(x)|$$

If $g \in \text{Stab}_G(x, y)$, then:

$$\begin{aligned} g \cdot (x, y) &= (x, y) \\ (g \cdot x, g \cdot y) &= (x, y) \end{aligned}$$

So $g \in \text{Stab}_G(x)$ and $g \in \text{Stab}_G(y)$, and we have $\text{Stab}_G(x, y) = \text{Stab}_G(x) \cap \text{Stab}_G(y)$.
Since we know that G is transitive, we can also show that $\text{Stab}_G(x) = \text{Stab}_G(y)$:
Take $g \in \text{Stab}_G(x)$. Since G acts transitively on X, there exists some $h \in G$ such that $h \cdot x = y$.
Consider the action of g on x:

$$\begin{aligned} g \cdot x &= x \\ g \cdot (h \cdot y) &= h \cdot y \\ gh \cdot y &= h \cdot y \text{ and since } G \text{ is abelian:} \\ hg \cdot y &= h \cdot y \\ h \cdot (g \cdot y) &= h \cdot y \\ g \cdot y &= y \end{aligned}$$

So $\text{Stab}_G(x) \subseteq \text{Stab}_G(y)$.
The reverse containment holds in a symmetric way, so we have $\text{Stab}_G(x) = \text{Stab}_G(y)$.
Combining this with what we have above:

$$\text{Stab}_G(x, y) = \text{Stab}_G(x) \cap \text{Stab}_G(y) = \text{Stab}_G(x)$$

We can also apply the orbit stabilizer theorem to the action of G on $X \times X$:

$$|G| = |\mathcal{O}_G(x, y)||\text{Stab}_G(x, y)|$$

Plugging in what we know about $|G|$ from its action on X and using the fact that $\text{Stab}_G(x, y) = \text{Stab}_G(x)$:

$$|X||\text{Stab}_G(x)| = |\mathcal{O}_G(x, y)||\text{Stab}_G(x)|$$

$$|X| = |\mathcal{O}_G(x, y)|$$

Also, $|X \times X| = (\text{number of orbits}) \cdot (\text{size of each orbit})$, so:

$$|X|^2 = (\text{number of orbits}) \cdot |X|$$

$$|X| = (\text{number of orbits})$$

(b) Let $\mathcal{O}_1, ..., \mathcal{O}_n$ be the distinct orbits of G acting on X.
G acts transitively on the set $\{\mathcal{O}_1, ..., \mathcal{O}_n\}$, so for each $i = 1, ..., n$ if we define the action of G on $\mathcal{O}_i \times \mathcal{O}_i$, this action has exactly $|\mathcal{O}_i|$ orbits.
Denote the following set:

$$\Omega := (X \times X) \setminus \left(\bigcup_{i=1}^{n} (\mathcal{O}_i \times \mathcal{O}_i \right)$$

Now, we can count:

$$\begin{aligned}
(\#\text{ of orbits of } G \text{ on } X \times X) &= \sum_{i=1}^{n} (\#\text{ of orbits on } \mathcal{O}_i \times \mathcal{O}_i) + (\#\text{ of orbits on } \Omega) \\
&\geq \sum_{i=1}^{n} (\#\text{ of orbits on } \mathcal{O}_i \times \mathcal{O}_i) \\
&= \sum_{i=1}^{n} |\mathcal{O}_i| \\
&= |X|
\end{aligned}$$

□

3

Let R be a commutative unital ring with $1 \neq 0$. Show that if every proper principal ideal of R is a prime ideal, then R is a field.

Solution:
Let R be an ideal with the property that every proper principal ideal is a prime ideal.
First, note that since (0) is a principal ideal, it must also be prime, so R is an integral domain.
Now, take a nonzero element $a \in R$ and consider the ideal (a^2).
If $(a^2) = R$, then $1 \in (a^2)$, so there exists some element $r \in R$ such that $ra^2 = 1$, which implies $ra(a) = 1$ and $(a)ra = 1$. This means that a has an inverse: $a^{-1} = ra$.
If $(a^2) \neq R$, then (a^2) is a proper ideal of R. By assumption (a^2) must also be a prime ideal, so since $a^2 \in (a^2)$ we must have $a \in (a^2)$. Then there exists some element $r \in R$ such that $ra^2 = a$. Since we are in an integral domain, we can cancel and we get $ra = 1$. This means that a has an inverse: $a^{-1} = r$.
Since a was chosen as an arbitrary nonzero element of R, we have shown that every nonzero element has a multiplicative inverse, so R is a field.

$\square$

4

Let

5

Let p be a prime number, q a power of p, and let f be an irreducible polynomial in $\mathbb{F}_p[x]$. Prove that any two irreducible factors of f over the field $\mathbb{F}_q$ have the same degree.

6

Let E be a finite Galois extension of F, and suppose that E has a subfield M such that $F \subsetneq M \subsetneq E$ and M is contained in every intermediate field between F and E that is different from F. Prove that:

(a) $[E : F]$ is a prime power

(b) for any two intermediate fields K_1, K_2 between F and E we have $K_1 \leq K_2$ or $K_2 \leq K_1$.

Solution:

(a) Note that, by the fundamental theorem of Galois theory, $[E : F] = |\mathrm{Gal}(E/F)|$.
Set $G = \mathrm{Gal}(E/F)$ and let H be the subgroup of G that has the corresponding fixed field M. Every other subgroup K of G must be a subgroup of H, because H is a maximal subgroup of G, and by assumption K must have a corresponding fixed field that contains M, so if $K \lneq G$, $K \leq H$.
This means that H is the unique subgroup of G of $|H|$, so H is characteristic in G, and in particular H is normal in G.
The index of a maximal normal subgroup is necessarily prime, so $[G : H] = p$, for some prime p.
Consider the set of cosets of H in $G : \{H, \sigma_1 H, ..., \sigma_{p-1} H\}$, so there is some $\sigma \in G$ where $\sigma \notin H$.
Then, $\langle \sigma \rangle = G$, because otherwise $\langle \sigma \rangle$ would have to be contained in H, but $\sigma \notin H$ prevents this. Thus, G is a cyclic group.
Since G is cyclic, it must be the direct product of its Sylow p-subgroups, and each Sylow p-subgroup must be unique. The Sylow p-subgroups for different primes P intersect only in the identity, so if there is more than one H cannot be one of these groups, but it must properly contain all of them, which would make $H = G$ which is again a contradiction. Thus, there can only be one Sylow p-subgroup of G, so $|G|$ only has one prime divisor and we have $|G| = p^k$ for some prime p and some $k \in \mathbb{N}$.

(b) The result follows from the subgroup diagram of a cyclic group of order p^k: It is a straight line.

$\square$