

MATH 113: HW 9: Group actions, Sylow theorems

Due in class on Thursday, November 2.

1. (10 pts) Let G be a group and X be a G -set. If S is a subset of X , let $G_S = \{g \in G \mid gs = s(\forall s \in S)\}$. Is G_S a subgroup of G ? (Proof or counterexample.)

SOLUTION:

Closure: Let $g_1, g_2 \in G_S$. Then $g_1g_2s = g_1s = s$, for all $s \in S$. So G_S is closed.

Identity: Since $es = s$ for all $s \in X$, $es = s$ for all $s \in S$. Therefore $e \in G_S$.

Inverse: Assume that $g \in G_S$. Then $gs = s$ for all $s \in S$. Consider $g^{-1}s$. Since $s = gs$, we have $g^{-1}s = g^{-1}(gs) = (g^{-1}g)s = es = s$, by associativity. Therefore $g^{-1} \in G_S$.

2. (10 pts) Provide an example of a group G and a G -set X such that the action of G on X is transitive but not faithful. (Prove it.)

SOLUTION:

Let $X = \{0, 1, 2, 3, 4, 5, 6\}$ and let \mathbb{Z} act on X by $zx = z +_7 x$. Then given $x_1, x_2 \in X$, let $r \equiv x_2 - x_1 \pmod{7}$. So $r \in \mathbb{Z}$. Therefore $x_1 + r \equiv x_2 \pmod{7}$. Therefore \mathbb{Z} acts transitively on X .

The action is not faithful, since the element $7 \in \mathbb{Z}$ fixes each element of X .

3. (10 pts) Prove that there are no simple groups of order 255.

SOLUTION:

The First Sylow Theorem implies that there is at least one subgroup of order 17. The Third Sylow Theorem implies that the number of Sylow 17-subgroups is congruent to 1 mod 17 and divides 255. The possibilities are 3, 5, and 15, since anything divisible by 17 will not be congruent to 1 mod 17. But 3, 5, and 15 are not congruent to 1 mod 17. Therefore there is only one Sylow 17-subgroup. Since the order of an element must divide the order of the group, this subgroup,

P , is of order 17. But xPx^{-1} is a 17-subgroup, so $xPx^{-1} = P$ for all $x \in G$. Therefore P is a normal subgroup of order 17.

4. (10 pts) Let $|G| = pq$ for p, q positive prime integers such that $p < q$ and p does not divide $q - 1$. Prove that $G \cong \mathbb{Z}_{pq}$.

SOLUTION:

The third Sylow theorem implies that the number, k , of Sylow p -subgroups of G divides pq . Therefore k is either $1, p, q$, or pq . The third Sylow theorem also implies that this number is congruent to 1 mod p . Since p does not divide $q - 1$, q is not congruent to 1 modulo p . So there is only one Sylow p -subgroup, H of G .

There is only one Sylow q -subgroup, K , of G since the number of such must be congruent to 1 mod q and $p \equiv p \pmod{q}$ since $p < q$. Since H is the only group conjugate to H (otherwise there would be other Sylow p -subgroups), we see that H is normal. Similarly, K is normal. Since every non-identity element of H has order p and every non-identity element of K has order q , their intersection must be trivial. Therefore the group generated by H and K must be abelian by the previous homework assignment. But the group generated by H and K has order greater than q but divides pq . Hence this group has order pq and must be the whole group G .

Since G is an abelian group of order pq , it must be isomorphic to either \mathbb{Z}_{pq} or $\mathbb{Z}_p \times \mathbb{Z}_q$. But Theorem 11.5 implies that $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$, since $\gcd(p, q) = 1$.

5. (10 pts) Prove that the set of polynomials $\mathbb{Z}[x]$ in x with coefficients in \mathbb{Z} is a ring under the usual addition and multiplication of functions.

SOLUTION:

R1: Consider $\mathbb{Z}[x]$ under addition. We know that addition of functions is commutative and associative. To show closure, consider

$$p(x) = \sum_{i=0}^n a_i x^i, \quad q(x) = \sum_{i=0}^m b_i x^i.$$

Then

$$p(x) + q(x) = (p + q)(x) = \sum_{i=0}^s (a_i + b_i)x^i \in \mathbb{Z}[x],$$

where s is the maximum of m and n .

The additive identity is the polynomial $f(x) = 0$. The additive inverse of $p(x) = \sum_{i=0}^n a_i x^i$ is the polynomial $-p(x) = \sum_{i=0}^n (-a_i)x^i \in \mathbb{Z}[x]$. So $\mathbb{Z}[x]$ is an additive group.

The set $\mathbb{Z}[x]$ is closed under multiplication:

$$\begin{aligned} p(x)q(x) &= \left(\sum_{i=0}^n a_i x^i\right)\left(\sum_{i=0}^m b_i x^i\right) \\ &= \sum_{k=0}^{m+n} \left(\sum_{i=0}^k a_i b_{k-i}\right)x^k \in \mathbb{Z}[x] \end{aligned}$$

R2: We know that multiplication of functions is associative, so polynomial multiplication is associative.

R3: Consider

$$p(x) = \sum_{i=0}^n a_i x^i, \quad q(x) = \sum_{i=0}^m b_i x^i, \quad f(x) = \sum_{i=0}^s c_i x^i,$$

$$\begin{aligned}
\sum_{i=0}^n a_i x^i \left(\sum_{i=0}^m b_i x^i + \sum_{i=0}^s c_i x^i \right) &= \sum_{i=0}^n a_i x^i \left(\sum_{i=0}^{\max\{m,s\}=r} (b_i + c_i) x^i \right) \\
&= \sum_{i=0}^n a_i x^i \left(\sum_{i=0}^r (b_i + c_i) x^i \right) \\
&= \sum_{i=0}^{n+r} \sum_{k=0}^i a_k (b_{i-k} + c_{i-k}) x^i \\
&= \sum_{i=0}^{n+r} \sum_{k=0}^i (a_k b_{i-k} + a_k c_{i-k}) x^i \\
&= \sum_{i=0}^{n+r} \left(\sum_{k=0}^i a_k b_{i-k} x^i + \sum_{k=0}^i a_k c_{i-k} x^i \right) \\
&= \sum_{i=0}^{n+r} \left(\sum_{k=0}^i a_k b_{i-k} x^i \right) + \sum_{i=0}^{n+r} \left(\sum_{k=0}^i a_k c_{i-k} x^i \right) \\
&= p(x)q(x) + p(x)f(x)
\end{aligned}$$

The right distributive law is similar.

6. (10 pts) Prove the following properties of an arbitrary ring homomorphism $\phi : R_1 \rightarrow R_2$:
- (a) $\phi(R_1)$ is a subring of R_2 .
 - (b) $\phi(1_{R_1}) = 1_{R_2}$.
 - (c) $\phi(nr) = n\phi(r)$ for $n \in \mathbb{Z}^+$, $r \in R_1$.
 - (d) $\phi(r^n) = \phi(r)^n$.

SOLUTION:

(a) We already know that $\phi(R_1)$ is a subgroup of R_2 under multiplication. Since ϕ is a group homomorphism, $\phi(r_1) + \phi(r_2) = \phi(r_1 + r_2) = \phi(r_2 + r_1) = \phi(r_2) + \phi(r_1)$, so $\phi(R_1)$ is an abelian group under addition. We also know that multiplication in $\phi(R_1)$ inherits the associativity and distributive laws from R_2 . Therefore $\phi(R_1)$ is a subring of R_2 .

(b) Let $r_1 \in R_1$ be some non-identity element. Then $\phi(r_1 1_{R_1}) = \phi(1_{R_1} r_1) = \phi(r_1)$ by the definition of 1_{R_1} . But ϕ is a homomorphism, so $\phi(r_1)\phi(1_{R_1}) = \phi(1_{R_1})\phi(r_1) = \phi(r_1)$. Since there is a unique element 1_{R_2} that satisfies $r_2 1_{R_2} = 1_{R_2} r_2 = r_2$, this element is the element $\phi(1_{R_1})$, which satisfies the property for $\phi(r_1) \in R_1$.

(c) Induct on n . When $n = 1$, it is trivial. When $n = 2$, it is by the definition of a ring homomorphism. Assume that $\phi(kr) = k\phi(r)$. Then $\phi((k+1)r) = \phi(kr + r) = \phi(kr) + \phi(r)$ by definition. So $\phi((k+1)r) = k\phi(r) + \phi(r) = (k+1)\phi(r)$.

(d) Exactly the same proof as in (c) works, replacing addition with multiplication.