GROUP ACTIONS OR PERMUTATION REPRESENTATIONS

Recall our very general method of obtaining groups: take an object X of some catogorey (a set with some extra structure) and consider the group Aut$X$ of all automorphisms of X. Since this group reflects the symmetries of X, its properties can be derived from geometric properties of X (so we reverse our point of view: instead of studying X via Aut$X$, we investigate Aut$X$ via X).

If G is an abstract group, it is often a very fruitful idea to investigate representations of G on objects of a suitable category. By a **representation** we mean here simply a group homomorphism from G to Aut$X$.

For example, we could take a vector space V and consider a representation of G on V. Such representations, i.e. homomorphisms from G to $GL(V)$ are called **linear representations**. They play a fundamental role in group theory and many other parts of mathematics.

Another important example form representations of groups on groups, i.e. homomorphisms from G to Aut$H$ for some group H. We will meet such representations when we discuss semidirect products.

Two representations $f_i : G \longrightarrow \mathrm{Aut}X_i$ are called **equivalent** if there is an isomorphism $\alpha : X_1 \longrightarrow X_2$ such that $\alpha f_1(g) = f_2(g)\alpha$ for evry $g \in G$ (note that α induces a group homomorphism from AutX_1 to AutX_2 by $u \mapsto \alpha u \alpha^{-1}$). More generally, we define a morphism between the representations f_1 and f_2 to be any morphism $\alpha : X_1 \longrightarrow X_2$ such that $\alpha f_1(g) = f_2(g)\alpha$ for all $g \in G$

We say that a representation f is **faithful** if ker f is trivial, i.e. if f is an injection.

Our goal in this section is to study **permutation representations**, i.e. representations on sets. Thus a permutation representation of G on a set X is simply a group homomorphism from G to the group $S(X)$ of all permutations of X.

There is another point of view on permutation representations, which is often very convenient, via the notion of a **group action**.

Definition 1. *A (left)* **action** *of a group G on a set X is an operation $*$ which to any element $g \in G$ and any $s \in X$ assigns an element $g * s$ of X and has the following two properties:*
(a) $f * (g * s) = (fg) * s$ for any $f, g \in G$ and $s \in S$;
(b) $e * s = s$ for any $s \in S$, where e is the unit element of G.

Note that (a) and (b) mean that the action $*$ is compatible with the group structure of G. Note also that in a more precise language, an operation $*$ as above is simply a function $G \times X \longrightarrow X$ which satisfies conditions (a) and (b).

We have to explain how we identify actions and permutation representations.

Suppose first that we have a homomorphism $\phi : G \longrightarrow S(X)$. So for $g \in G$ the element $\phi(g)$ is a bijection of X. We can now say that the action of $g \in G$ on $s \in X$ results in $\phi(g)(s) \in X$, i.e. we define $g * s = \phi(g)(s)$. We need to check that conditions (a) and (b) are satisfied, and this is a very simple consequence of the fact that ϕ is a homomorphism:
(a) We have $(fg) * s = \phi(fg)(s) = (\phi(f)\phi(g))(s) = \phi(f)(\phi(g)(s)) = \phi(f)(g * s) = f * (g * s)$.
(b) $e * s = \phi(e)(s) = id(s) = s$ for any $s \in X$.

Thus indeed we get an action from a homomorphism ϕ.

Conversely, suppose we have an action $*$ of G on X. We need to construct a homomorphism $\phi : G \longrightarrow S(X)$ corresponding to this action. For this note that each $g \in G$ gives rise to a function $L_g : X \longrightarrow X$ defined by $L_g(s) = g * s$. Note that $L_g L_{g^{-1}}(s) = L_g(g^{-1} * s) = g * (g^{-1} * s) = (gg^{-1}) * s = e * s = s$, so $L_g L_{g^{-1}} = id$. Similarly, $L_{g^{-1}} L_g = id$, which shows that L_g is a bijection of X (since it has an inverse $L_{g^{-1}}$). Thus we get a function $\phi : G \longrightarrow S(X)$ defined by $\phi(g) = L_g$. It remains to verify that ϕ is a homomorphism, which is a quite simple task: $\phi(fg)(s) = L_{fg}(s) = (fg) * s = f * (g * s) = L_f(L_g(s)) = \phi(f)(\phi(g)(s))$ for any $s \in X$ so in fact $\phi(fg) = \phi(f)\phi(g)$.

The reader will easily verify that the constructions of the action from a permutation representation and the representation from an action are inverse to each other and allow us to identify actions of G on X and homomorphisms from G to $S(X)$.

There are two very important notions associated to any action.

As a first we introduce the notion of an **orbit** of an element $s \in X$ under the action of G. In plane words, the orbit $O(s)$ of s consists of all elements of X which can be obtained by acting by some element of G on s, i.e. we have

Definition 2. *The* **orbit** $O(s)$ *of* s *under the action of* G *is the set* $O(s) = \{g * s : g \in G\}$.

The main property of orbits is contained in the following

Lemma 1. *If* $s, t \in S$ *then either* $O(s) = O(t)$ *or* $O(s) \cap O(t) = \emptyset$.

Proof: First note that if $v \in O(s)$ then $v = f * s$ for some $f \in G$. Thus, for any $g \in G$ we have $g * v = g * (f * s) = (gf) * s \in O(s)$. This shows that $O(v)$ is a subset of $O(s)$. On the other hand, we have $f^{-1} * v = f^{-1} * (f * s) = (f^{-1}f) * s = e * s = s$, so $s = f^{-1} * v \in O(v)$. As above, this implies that $O(s) \subseteq O(v)$, so we have in fact $O(s) = O(v)$. In other words, the orbits of elements belonging to a given orbit are all equal to each other.

Suppose now that the orbits of s and t are not disjoint, so there is $v \in O(s) \cap O(t)$. Then we have $O(s) = O(v) = O(t)$ by the above discussion. □

The lemma says that the orbits partition the set X into pairwise disjoint subsets.

The second notion we want to introduce is the notion of a **stabilizer** $St(s)$ of any $s \in X$. The definition is very simple:

Definition 3. *The* **stabilizer** *of* $s \in X$ *is the subset* $St(s) = \{g \in G : g * s = s\}$ *of* G.

In plain words, the stabilizer of s consists of all those elements of G which act trivially on s (i.e. which fix s). Another very common notation for the stabilizer of s is G_s. We will use both notations.

The main fact about stabilizer is that it is a subgroup of G.

Lemma 2. *(1) For any* $s \in X$, *the stabilizer* $St(s)$ *is a subgroup of* G.

(2) $St(g * s) = gSt(s)g^{-1}$ *for any* $g \in G$ *and* $s \in X$.

Proof: Clearly $e \in St(s)$. If $f, g \in St(s)$ then $f * s = s = g * s$ so $(fg) * s = f * (g * s) = f * s = s$, i.e. $fg \in St(s)$. Also, $g^{-1} * s = g^{-1} * (g * s) = (g^{-1}g) * s = e * s = s$ so $g^{-1} \in St(s)$. This proves (1).

In order to establish (2) note that $f \in St(g*s)$ iff $f*(g*s) = g*s$ iff $(fg)*s = g*s$ iff $g^{-1} * ((fg) * s) = g^{-1} * (g * s) = s$ i.e. iff $(g^{-1}fg) * s = s$ which is equivalent to $g^{-1}fg \in St(s)$ i.e. $f \in gSt(s)g^{-1}$. This proves (2). $\square$

From now on we write gs instead of $g * s$.

The following definition, extending the notion of a stabilizer, is very useful for investigation of group actions:

Definition 4. *Let a group G act on a set X and let Y be a subset of X. The* **stabilizer** *of Y is the subset*

$$St(Y) = \{g \in G : gy \in Y \text{ and } g^{-1}y \in Y \text{ for all } y \in Y\} = \{g \in G : gY = Y\}.$$

A **pointwise stabilizer** *of Y is the subset $G_Y = \{g \in G : gy = y \text{ for all } y \in Y\}$.*

It is a straightforward exercise to verify that both $St(Y)$ and G_Y are in fact subgroups of G. If $Y = \{y\}$ consists of one element, we have $G_Y = St(Y) = St(y) = G_y$.

It is clear from the definition that $St(Y)$ acts on Y.

We say that Y is $G-$**stable** if $St(Y) = G$. For example, any orbit is $G-$stable. In fact we have the following simple

Exercise. A subset Y of X is $G-$stable iff it is a union of some of the orbits of G on X.

Proposition 1. *The number of elements in the orbit $O(s)$ is equal to the index $[G : St(s)]$. In particular, if G is finite, then $|O(s)| = |G|/|St(s)|$ divides $|G|$.*

Proof: Our proof will establish a bijection between left cosets of $St(s)$ in G and the elements of $O(s)$. Given a left coset $gSt(s)$ we assign to it the element gs in the orbit of s. This is well defined: if $gSt(s) = hSt(s)$ then $g = ht$ for some $t \in St(s)$ and $gs = (ht)s = h(ts) = hs$, as $ts = s$. Thus we defined a function from left cosets of $St(s)$ to the orbit $O(s)$ of s. This functions is surjective: any element in $O(s)$ is of the form gs for some $g \in G$ hence it is assigned to the coset $gSt(s)$. It is also injective. Indeed, if the cosets $gSt(s)$ and $hSt(s)$ are mapped to the same element in the orbit of s then $gs = hs$. This means that $(h^{-1}g)s = s$, i.e $h^{-1}g \in St(s)$. It follows that $gSt(s) = hSt(s)$. $\square$

Remark. It follows that the number $|St(t)|$ is the same for any element $t \in O(s)$. This however should not be surprising at all, since we proved in Lemma 2 that the groups $St(t)$ and $St(s)$ are conjugate in G, so in particular they have the same number of elements.

We need more definitions.

Definition 5. *We say that the action of G on X is* **transitive***, if there is only one orbit of these action (which then equals X). In other words, the action is transitive if for any two elements s, t in X there is $g \in G$ such that $gs = t$.*

Exercise. Let $\pi : G \longrightarrow S(X)$ be a permutation representation such that the corresponding action of G on X is transitive. Let $x \in X$. Prove that the kernel of π is the largest normal subgroup contained in $St(x)$.

Definition 6. *An element $s \in X$ is called a* **fixed point** *of the action of G on X if the orbit of s equals to $\{s\}$. Equivalently, s is a fixed point iff $St(s) = G$, i.e. if $gs = s$ for every $g \in G$.*

Fixed points should be thought of as elements having many symmetries, so they are of special interest. The set of all fixed points is denoted by $Fix(G)$. More generally, if $T \subseteq G$ is any subset, we define

$$Fix(T) = \{s \in X : ts = s \text{for all } t \in T\}.$$

It is easy to see that $Fix(T) = Fix(< T >)$.

We derive now three fundamental rules of counting associated to a group action of a finite group G on a finite set S.

Rule 1. *If the action of G on S is transitive, then $|S| = |G|/|St(s)|$ for any $s \in S$.*

This rule follows immediately from Proposition 2 and the fact that transitivity of the action means that $O(s) = S$.

Rule 2. *Let p be a prime number which does not divide $|S|$. There is an element $s \in S$ such that $|O(s)|$ is not divisible by p.*

In fact, if the number of elements in every orbit is divisible by p then the number of elements in S, which is the sum of the numbers of elements in orbits, is also divisible by p. But we assumed that this is not the case, so the number of elements in at least one orbit is not divisible by p.

Rule 3. *Suppose that the order of the group G is a power of a prime number p and that G acts on a set S. Let r denote the number of fixed points for this action. Then $p|(|S|-r)$. In particular,*
(i) if $|S|$ is not divisible by p then $r>0$, i.e. there is at least one fixed point.
(ii) suppose $p||S|$. If $r>0$ then $r\geq p$, i.e. if there is a fixed point, the are at least p of them.

In order to justify this rule recall that the number of elements in S is equal to the sum of the numbers of elements in each orbit. Note that by Proposition 2, the number of elements in each orbit divides $|G|$. Since $|G|$ is a power of the prime p, the number of elements in each orbit is a power of p as well. We have r orbits which consist of 1 $(=p^0)$ element each and in all other orbits the number of elements is a multiple of p (being a positive power of p). So the sum of the numbers of elements in the orbits (which is $|S|$) equals $r+$(a multiple of p). Consequently, $p|(|S|-r)$. If $|S|$ is not divisible by p then we immediately get that $r\neq 0$, which justifies (i). If $p||S|$ then also $p|r=|S|-(|S|-r)$. In particular, if $r\neq 0$ then r is at least p, which proves (ii).

Examples and application.

It is time to show that the ideas developed so far can be used in a very fruitful way.

Example 1. Suppose that G acts on a set S. Let H be s subgroup of G. We can restrict our attention to elements of H and we get in this way an action of H on S called the restriction of the action of G to H. Such restriction can be quite useful. For example, G need not be a $p-$group so we can not apply our Rule 3, but after restricting to a subgroup which is a $p-$group we can try to apply this rule.

Example 2. Suppose that G acts on S and that T is a $G-$ *stable* subset of S. Then G acts on the set T. For example, if $s\in S$ then the orbit $O(s)$ is $G-$stable.

Indeed, if $t \in O(s)$ then $t = fs$ for some $f \in G$ and then $gt = g(fs) = (gf)s \in O(s)$ for any $g \in G$.

Example 3. Let H be a subgroup of G and let X be the set of all left cosets of H in G. We define an action of $g \in G$ on a coset aH by $g * aH = (ga)H$. We leave it as an exercise to check that this is indeed an action and that it is transitive. Note that Rule 1 for this action is nothing but Lagrange's theorem (observe that $H = St(eH)$). We call this action **the representation of G on the left cosets of H by left multiplication**.

It turns out that every transitive action is of this sort. More precisely, we have the following:

Exercise. Suppose that G acts transitively on X. Let $x \in X$ and set $H = St(x)$. Prove the representation of G on X and the representation on the left cosets of H are equivalent.

Remark. The moral of this exercise is that every action is built up from transitive actions (orbits) and transitive actions are determined by the subgroup structure of G.

In the special case when $H = \{e\}$, we can identify left cosets of H in G with elements of G (the coset $\{g\} = gH$ is identified with g). Thus we get an action of G on G which is usually called **the action of G on itself by left translations**. This action has associated permutation representation $G \longrightarrow S(G)$, which is easily seen injective. Thus we established the following fundamental result

Cayley's Theorem. *Every group is isomorphic to a subgroup of $S(X)$ for some set X. If G is finite then X can be chosen finite too.*

The representations of G on the left cosets of subgroups can be helpful in an investigation of G. For example, if H has index n then the permutation representation on left cosets of H is a homomorphism to a group of order $n!$. Thus the kernel of this representation has index at most $n!$, and it is a normal subgroup of G. This answers one of the questions in Homework 1.

Note the following important corollary:

Proposition 2. *If G is finite, p is a prime divisor of $|G|$ and H is a subgroup of G of index $n < p$, then G is not simple.*

Example 4 Suppose that G acts on S. Then G acts on the set $P(S)$ of all subsets of S as follows: if $U \in P(S)$ then $gU = \{gs : s \in U\}$. A straightforward verification that this is indeed an action is left as an exercise.

Fix an integer $k \leq |S|$ and denote by $P_k(S)$ the set of all $k-$element subsets of S. It is clear that it is a $G-$invariant subset of $P(S)$. Explicitly, if $U \in p_k(S)$ then $U = \{s_1, ..., s_k\}$ and $gU = \{gs_1, ..., gs_k\}$.

Example 4 allows to construct many interesting actions. As an illustration, let $S = \{1, 2, ..., n\}$ and $G = S_n$, so G naturally acts on S. Let $k \leq n$. Then we have an action of G on $P_k(S)$. We claim that this action is transitive. In fact, given k elements $s_1, ..., s_k$ of S there is a permutation f which maps i to s_i for all $i \leq k$, i.e. $f * i = s_i$. Thus $f * \{1, 2, ..., k\} = \{s_1, ..., s_k\}$. This shows that the orbit of $V = \{1, 2, ..., k\}$ is the whole $P_k(S)$, i.e. the action is transitive.

What is the stabilizer of V? Note that a permutation f is in $St(V)$ iff it maps the set V onto itself and then it also maps the set $S - V$ onto itself. So elements of $St(V)$ can be thought of as pairs consisting of a bijection of V and a bijection of $S - V$. But there are $k!$ bijections of V and $(n-k)!$ bijections of $S - V$, so we have $k!(n-k)!$ possibilities for $f \in St(V)$, i.e. $|St(V)| = k!(n-k)!$ (an exercise: show that $St(V)$ is isomorphic to $S_k \times S_{n-k}$). By Rule 1, we conclude that $|S(k)| = |G|/|St(V)| = n!/k!(n-k)!$. In other words, the number of $k-$element subsets of a set with n elements is $n!/k!(n-k)!$. The number $n!/k!(n-k)!$ is often denoted by $\binom{n}{k}$ and called the Newton symbol or Newton binomial coefficient.

Suppose now that $n = p^s m$ for some prime p. Let $f = (1, 2, 3, ..., p^s)(p^s + 1, ..., 2p^s)...((m-1)p^s + 1, ..., mp^s)$ be a permutation of S written as a product of disjoint cycles. All these cycles have length p^s, so f has order p^s. Let H be the cyclic subgroup of G generated by f. Thus H is a $p-$group of order p^s. Consider the restriction of the action of G on $P_{p^s}(S)$ to H. Suppose that U is a fixed point for this action. Let $a \in U$. Note that we may write $a = lp^s + b$ for some $0 \leq l < m$ and $0 < b \leq p^s$ and then the orbit of a under H is $\{lp^s + 1, ..., (l+1)p^s\}$. Since V is $H-$stable, this orbit is contained in V so it equals V (they have the same number of elements). We see that the fixed points of the action of H are the sets $\{1,2,3,...,p^s\}, \{p^s+1,...,2p^s\},...,\{(m-1)p^s+1,...,mp^s\}$. In particular, the number of fixed points of the action of H on $P_{p^s}(S)$ is m. By Rule 3, we have $p|\binom{n}{p^s} - m$.

We can summarize the above considerations in the following

Theorem 1. *The number of $k-$element subsets of an $n-$element set equals $\binom{n}{k} = n!/k!(n-k)!$. If $n = p^s m$, where p is a prime then $p|\binom{n}{p^s} - m$.*

We will use this theorem in the next example to derive one of the most important theorems about finite groups.

Example 5 Let G be a finite group and p a prime divisor of $|G|$. Thus we may write $|G| = p^s m$ for some integers m not divisible by p and $s > 0$. Let S be the set of all subsets of G of order p^s, i.e. $S = P_{p^s}(G)$. The group G acts on itself by left multiplication (see Example 3) so it acts on S according to Example 4. Explicitly, if $A = \{a_1,...,a_{p^s}\}$ is an element of S (i.e. a subset of G of order p^s) and $g \in G$ then we have $g * A = \{ga_1,...,ga_{p^s}\}$. By Theorem 1, S has $\binom{p^s m}{p^s}$ elements $p||S|-m$. Since $(m,p) = 1$, we see that $|S|$ is not divisible by p. By Rule 2, there exists an element $T \in S$ whose orbit $O(T)$ has cardinality not divisible by p. Recall that $|O(T)| = |G|/|St(T)|$. It follows that the stabilizer $St(T)$ has order divisible by p^s. On the other hand, for any A the stabilizer of A has at most p^s elements. In fact, let $a \in A$. If $g \in St(A)$ then $ga \in A$ so we have at most p^s possibilities for ga and each choice uniquely determines g (if $ga = b$ then $g = ba^{-1}$). Thus the number of elements in $St(T)$ is both divisible by p^s and not larger than p^s, i.e. $|St(T)| = p^s$. Thus we found a subgroup $St(T)$ of G which has p^s elements. The existence of such subgroup is a very important theorem:

Theorem 2. *(Sylow) If G is a finite group such that $|G| = p^s m$, where p is a prime and $(p,m) = 1$ then G has a subgroup of order p^s.*

Subgroups whose existence we just established are very important in group theory and we introduce the following definition

Definition 7. *Let G be a finite group such that $|G| = p^s m$ where p is a prime and $(p,m) = 1$. Any subgroup of G of order p^s is called a* **Sylow $p-$subgroup** *of G*

As a corollary of Theorem 2 we get the following result due to Cauchy:

Theorem 3. *(Cauchy) Let G be a finite group and p a prime divisor of $|G|$. Then G has an element of order p.*

Proof: Let P be a Sylow $p-$subgroup of G, so $|P| = p^s$ for some $s > 0$. Let $a \in P$, $a \neq e$. The order of a divides p^s, so it equals p^k for some $0 < k \leq s$. Now $a^{p^{k-1}}$ has order p. $\square$

Exercise. Let G be a finite group and p a prime number such that $p||G|$. Consider the set S of all $p-$tuples $(a_1, ..., a_p)$ of elements from G such that $a_1 a_2 ... a_p = e$, i.e.

$$S = \{(a_1, ..., a_p) : a_i \in G \text{ for all } i, \text{ and } a_1 ... a_p = e\}$$

Let C be a cyclic group of order p and f a generator for C. We define an action of C on S as follows: if $s \in C$ then $s = f^i$ for a unique $0 \leq i < p$ and we set $s * (a_1, ..., a_p) = (a_{i+1}, a_{i+1}, ...a_p, a_1, a_2, ..., a_i)$.

a) Check that this is indeed an action of C on S.

b) Show that the number of elements in S equals $|G|^{p-1}$.

c) Show that each fixed point for this action is of the form $(g, ..., g)$ for some $g \in G$ such that $g^p = e$.

d) Conclude that G has a nontrivial element of order p (so we get a different proof of Cuchy's theorem).

The next example will establish very important information about Sylow subgroups.

Example 6. We have seen that a group G acts on itself by left translations. But there is another very important action of G on itself, **the action by conjugation**. It is defined by $g * a = gag^{-1}$ for any $a, g \in G$. The verification that this is indeed an action is straightforward and is left as an exercise. Note that the homomorphism $G \longrightarrow S(G)$ associated to this action has its image in the subgroup Aut$G$ of $S(G)$.

If T is a subset of G then the pointwise stabilizer G_T of T (under the conjugation action) is called the **centralizer** of T and it is denoted by $C_G(T)$. The stabilizer $St(T)$ is called the **normalizer** of T and it is denoted by $N_G(T)$.

Let us now look at the induced action of G on $P(G)$. Since a conjugation is an automorphism of G, this action takes subgroups of G to subgroups. Thus it induces an action of G on the set of all subgroups of G of any given order. In particular, we get an action of G on the set Syl_p of all Sylow $p-$subgroups of G (here p is a fixed prime divisor of $|G|$). We are going to analyze this action more closely. Note first that Syl_p is not empty by Theorem 2.

Let $P \in Syl_p$. Consider the orbit $O(P)$ of P under the action of G. We claim that $P \subseteq St(P)$ and P is a normal subgroup of $St(P)$. In fact, since P is a group, we have $pPp^{-1} = P$ i.e. $p \in St(P)$ for any $p \in P$. Also, for $n \in St(P)$ we have $nPn^{-1} = P$ so P is indeed normal in $St(P)$. It follows that $|P|||St(P)|$ and consequently $|G|/|St(P)| = |O(P)|$ is not divisible by p.

Let Q be some $p-$subgroup of G. We can restrict the action of G on $O(P)$ to the action of Q. Since Q is a $p-$group and $|O(P)|$ is not divisible by p, we see by Rule 3 that the action of Q on $O(P)$ has a fixed point. Call it R. Thus Q is a subgroup of $St(R)$. But this forces $Q \subseteq R$. In fact, we have seen that R is normal in $St(R)$. Consider the natural homomorphism $f : St(R) \longrightarrow St(R)/R$. Let $a \in Q$, so the order of a is a power of p. Since the order of $f(a)$ divides the order of a, it is also a power of p. But p does not divide $|St(R)/R|$, so the only possibility is that $f(a)$ has order 1, i.e. $f(a) = e$. But this means that $a \in ker f = R$. This shows that $Q \subseteq R$. In particular, every $p-$subgroup of G is contained in a Sylow $p-$subgroup.

Suppose now that we take for Q a Sylow $p-$subgroup of G. Then for any fixed point R of Q on $O(P)$ we have $Q \subseteq R$. But Q and R have the same number of elements, so $Q = R$. This shows that $Q \in O(P)$ and that Q is the unique fixed point of the action of Q on $O(P)$. Since Q was arbitrary, we see that all Sylow $p-$subgroups belong to $O(P)$. In other words, $O(P) = Syl_p$, i.e. G acts transitively on Syl_p. In particular, $|Syl_p|||G|$. Since Q is the unique fixed point of the action of Q on Syl_p, Rule 3 shows that $p||Syl_p| - 1$.

We can summarize our investigation in the following fundamental theorem, called **Sylow Theorem**:

Theorem 4. (**Sylow Theorem**) *Let G be a finite group and p a prime divisor of $|G|$. Then:*

— *G has at least one Sylow $p-$subgroup*

— *any two Sylow $p-$subgroups are conjugate in G*

— *the number t_p of Sylow $p-$subgroups divides $|G|$ and $p|(t_p - 1)$*

— *every $p-$subgroup of G is contained in a Sylow $p-$subgroup*