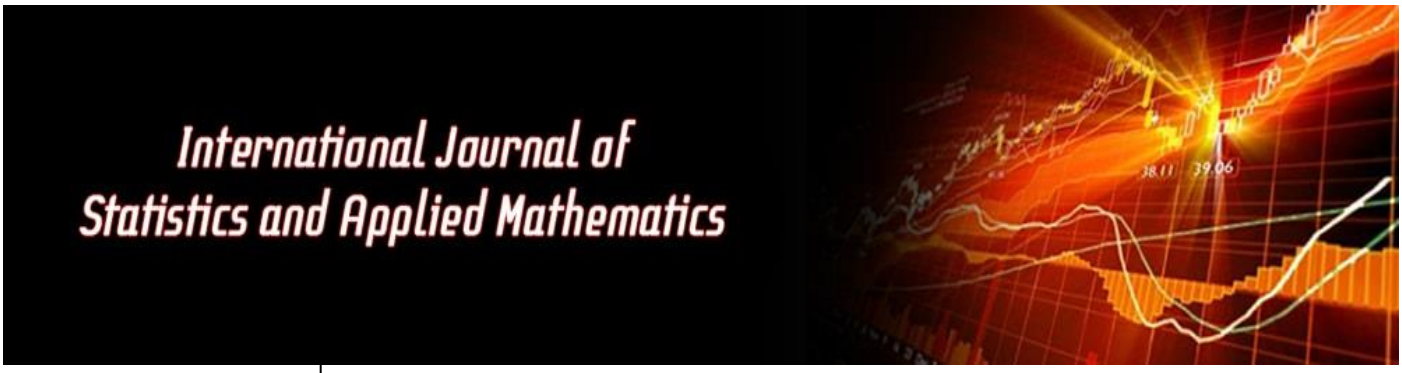
International Journal of Statistics and Applied Mathematics 2017; 2(2): 50-54



ISSN: 2456-1452
Maths 2017; 2(2): 50-54

www.mathsjournal.com
Received: 18-01-2017
Accepted: 21-02-2017

Satish
Assistant Professor, Department of Maths, Govt College Hansi, Haryana, India

Correspondence
Satish
Assistant Professor, Department of Maths, Govt College Hansi, Haryana, India

Analyzing normal subgroups and quotient groups in theory: a mathematical modelling

Satish

Abstract
Around 1770, Lagrange started the investigation of permutations regarding the investigation of the arrangement of equations. He was occupied with understanding arrangements of polynomials in a few factors, and got this plan to examine the conduct of polynomials when their roots are permuted. This prompted what we now call Lagrange's Theorem, however it was expressed. In the event that a function f (x1... xn) of n factors is followed up on by every single conceivable change of the factors and these permuted functions go up against just r values, at that point r is a divisor of n!. It is Galois (1811-1832) who is considered by numerous as the organizer of group theory. He was the first to utilize the expression "group" in a specialized sense; however to him it implied an accumulation of permutations shut under multiplication. Galois Theory will be talked about substantially later in these notes. Galois was likewise propelled by the reasonability of polynomial equations of degree n.

Keywords: normal subgroups, quotient groups, mathematical modelling

Introduction
From 1815 to 1844, Cauchy began to take a gander at permutations as a self-ruling subject, and presented the idea of permutations created by specific elements, and in addition a few documentations still utilized today, for example, the cyclic documentation for permutations, the result of permutations, or the character stage. He demonstrated what we call today Cauchy's Theorem, to be specific that if p is prime divisor of the cardinality of the group, at that point there exists a subgroup of cardinality p. In 1870, Jordan assembled every one of the utilizations of permutations he could discover, from mathematical geometry, number theory, function theory, and gave a brought together introduction (counting crafted by Cauchy and Galois). Jordan made express the ideas of homomorphism, isomorphism (still for change groups), he presented reasonable groups, and demonstrated that the lists in two structure arrangement are the same (now called Jordan-Holder Theorem). In 1870, while dealing with number theory (all the more unequivocally, in summing up Kummer's work on cyclotomic fields to arbitrary fields), Kronecker portrayed in one of his papers a limited arrangement of arbitrary elements on which he characterized a conceptual operation on them which fulfill certain laws, laws which now compare to maxims for limited abelian groups. He utilized this definition to work with perfect classes. He additionally demonstrated a few outcomes now known as hypotheses on abelian groups. Kronecker did not interface his definition with stage groups, which was done in 1879 by Frobenius and Stickelberger. Separated change groups and number theory, a third event of group theory which merits specifying emerged from geometry, and crafted by Klein, and Lie, who contemplated change groups, that is changes of geometric objects. The work by Lie is presently a theme of concentrate in itself, yet Lie theory is past the extent of these notes. The theoretical perspective in group theory rose gradually.

Definition 1.1
A group is a non-empty set G on which there is a binary operation $(a, b) \rightarrow ab$ such that

- if a and b belong to G then ab is also in G (closure),
- $a(bc) = (ab)c$ for all a, b, c in G (associativity),
- there is an element $1 \in G$ such that $a1 = 1a = a$ *for all* $a \in G$ (identity),

- if a ∈ G, then there is an element a −1 ∈ G such that $aa^{-1} = a^{-1} a = 1$ (inverse).
- A group G is called abelian if the binary operation is commutative, i.e., $ab = ba$ for all $a, b \in G$.

Remark There are two standard notations for the binary group operation: either the added substance documentation, that is (a, b) 7→a + b in which case the personality is indicated by 0, or the multiplicative documentation, that is (a, b) 7→ab for which the character is meant by 1.

Examples 1.1
1. Z with the expansion and 0 as character is an abelian group.
2. Z with the multiplication isn't groups since there are elements which are not invertible in Z.
3. The arrangement of n × n invertible lattices with genuine coefficients is a group for the grid item and personality the framework In. It is signified by GLn(R) and called the general direct group. It isn't abelian for $n \geq 2$.

The above cases are the most effortless groups to consider. The theory of algebra however contains numerous cases of well known groups that one may find, once outfitted with more devices (for instance, the Lie groups, the Brauer group, the Witt group, the Weyl group, the Picard group,...to name a couple).

Definition 1.2 The request of a group G, signified by |G|, is the cardinality of G, which is the number of elements in G. We have just observed unbounded groups up until now. Give us a chance to take a gander at a few cases of limited groups.

Examples 1.2
1. The unimportant group G = {0} may not be the most energizing group to take a gander at, yet at the same time it is the main group of request 1.
2. The group G = {0, 1, 2... n − 1} of integers modulo n is a group of request n. It is once in a while indicated by Zn (this ought not to be mistaken for padic integers however!).

Definition 1.3
A subgroup H of a group G is a non-purge subset of G that structures a group under the binary operation of G.

Examples 1.3
1. In the event that we consider the group $G = Z4 = \{0, 1, 2, 3\}$ of integers modulo 4, $H = \{0, 2\}$ is a subgroup of G.
2. The arrangement of n × n matrices with genuine coefficients and determinant of 1 is a subgroup of GLn(R), signified by SLn(R) and called the uncommon straight group.

Now, with a specific end goal to guarantee that the above illustrations are really sub-groups, one need to really check the definition. The recommendation underneath gives a simpler paradigm to choose whether a subset of a group G is really a subgroup

Proposition 1.1
Let G be a group. Let H be a non-empty subset of G. The following are equivalent:
1. H is a subgroup of G.
   a. x, y ∈ H implies xy ∈ H for all x, y.
   b. x ∈ H implies x^{-1} ∈ H.
   c. x, y ∈ H implies xy^{-1} ∈ H for all x, y. Proof.

We prove that $1 \Rightarrow 3. \Rightarrow 2 \Rightarrow 1$
- $\Rightarrow 3.$ This part is clear from the definition of subgroup.
- $\Rightarrow 2.$ Since H is non-empty, let x ∈ H. By assumption of 3 we have that $xx^{-1} = 1 \in H$ and that $1x^{-1} \in H$ thus x is invertible in H. We now know that for $x, y \in H$, x and y^{-1} are in H, thus $x (y^{-1})^{-1} = xy$ is in H.
- $\Rightarrow 1.$ To demonstrate this bearing, we have to check the meaning of group. Since conclusion and presence of an opposite are valid by presumption of 2, and that associativity takes after from the associativity in G, we are left with the presence of a personality. Presently, if $x \in H$, at that point $x-1 \in H$ by presumption of 2, and along these lines $xx-1 = 1 \in H$ again by suspicion of 2, which finishes the confirmation.

We will frequently utilize the last identicalness to watch that a subset of a group G is a subgroup. Since we have these structures of groups and subgroups, let us introduce a guide that enables traveling between different groups and that regards the individual group operations.

Definition 1.4: Given two groups G and H, a group homomorphism is a map $f: G \to H$ such that
$f(xy) = f(x)f(y)$ for all $x, y \in G$.
Note that this definition quickly infers that the personality 1G of G is mapped to the character 1H of H. The same is valid for the opposite, that is
$f(x^{-1}) = f(x)^{-1}$.

Example 1.4: The map exp: $(R, +) \to (R^*, \cdot)$, $x \mapsto exp(x)$ is a group homomorphism.

Definition 1.5: Two groups G and H are isomorphic if there is a group homomorphism f: G → H which is likewise division. Generally, isomorphic groups are "basically the same".

Example 1.5: In the event that we consider again the group $G = Z4 = \{0, 1, 2, 3\}$ of integers modulo 4 with subgroup $H = \{0, 2\}$, we have that H is isomorphic to $Z2$, the group of integers modulo 2. An urgent definition is the meaning of the request of a group component.

Definition 1.6: The request of a component a∈G is the slightest positive whole number n to such an extent that a = 1. In the event that no such whole number exists, the request of a is limitless. We indicate it by |a|. The basic piece of this definition is that the request is the minimum positive whole number with the given property. The wording request is utilized both for groups and group elements, yet it is typically evident from the setting which one is considered.

Normal Subgroups and Quotient Groups
The conventional introduction of typical subgroups and quotient groups goes something like this. To start with, you characterize a subgroup to be ordinary in the event that it fulfills a specific amusing condition. At that point, given a group G and an ordinary subgroup H, you demonstrate that you can characterize an operation on the cosets of H, and that that operation transforms the set of all cosets into a group, called the quotient group. In a perfect world, you likewise demonstrate that one can't give a characteristic group structure to one side cosets of an arbitrary subgroup: that

legitimizes limiting consideration regarding typical subgroups. The undeniable method for noting this second inquiry is to take a gander at the history. Things being what they are typical subgroups were presented by Galois (who was likewise the organizer of group theory) as a major aspect of his investigation of the solvency of polynomials by radicals. That is somewhat awful, since it implies that to comprehend why typical subgroups were presented, one needs to put in a great deal of work understanding about the theory of explaining polynomials.

Be that as it may, there is another method for supporting the presentation of another idea into science. Rather than taking a gander at the real history of that idea, one can take a gander at an imaginary history. On the off chance that you can recount a conceivable anecdote regarding why an idea may have been imagined, at that point that is adequate to influence it to appear to be sensible. It understands the secret of how anybody could have thought of the idea, and it likewise demonstrates that it was entirely well inescapable that the idea would have been presented at some point or another. In this post, at that point, I'd jump at the chance to give an invented record of why ordinary subgroups and quotient groups were brought into group theory, once a portion of the more fundamental ideas were at that point set up.

The main period of group theory (in this invented account) comprised in detecting that numerous mathematical structures, for example, symmetries of Platonic solids, permutations of a limited set, non-solitary *n x n* matrices, had includes in like manner that could be dreamy out. This prompted the definition of the axioms for group theory: associativity, personality, inverses. It was seen early — in reality, this perception was a piece of what drove the underlying advancement of the subject — that two groups could be characterized distinctively and yet is "essentially the same". For instance, the group of revolutions of a customary pentagon was essentially the same as the group of integers mod 5 under expansion, and the group of symmetries of a rectangle (that wasn't a square) was fundamentally the same as the group of changes of R^3 that comprised of the character and the three half turns about the arrange axes.

The principal endeavors to make exact this instinct that groups could be "unique however essentially the same" were somewhat awkward. Two groups G and H were said to be indistinguishable up to permutation and relabeling please remember that none of what I'm stating is genuine — this definition included] on the off chance that you could discover orderings of the elements of G and the elements of H with the end goal that in the event that you framed the multiplication tables, at that point they would relate, as in if the component recorded in the rth put times the component recorded in the sth put measures up to the component recorded in the t th put in G, at that point the same is valid in H. Afterward, this definition was cleaned up so it turned into the meaning of isomorphism that we are presently acquainted with: an isomorphism from G to H is a bijection $\phi: G \to H$ such that $\phi(xy) = \phi(x)\ \phi\ (y)$ for every $x, y \in G$. Two groups G and H were said to be *isomorphic* if there was an isomorphism between them.

At this point, individuals had got somewhat of a preference for the absolutely theoretical investigation of group theory: it energized them that they could consider a group, for example, without saying whether its elements were pivots of a pentagon or integers mod 5 or something unique totally. So individuals began considering groups for their own purpose. And one of the main inquiries they asked was this: we realize that bits of homomorphisms are subgroups, yet shouldn't something be said about the opposite? That is, is each subgroup the portion of some homomorphism?

This issue turned out not to be exceptionally fascinating, since there were simple counter examples. For instance, on the off chance that you take the permutation group S3 and take the subgroup that comprises of the personality and the transposition (12), at that point that isn't the piece of any homomorphism. The first evidence of this reality went something like this. Assume we realize that goes to the character. We can utilize that to derive that, say, (23) additionally goes to the character. We do this by "utilizing (12) to do (23)" as takes after. We initially discover a permutation that switches 1 and 3 — the undeniable one being (13). We at that point switch 1 and3, play out the permutation (12) and at long last switch 1 and 3 back once more. All the more formally, we ascertain the permutation (13)(12)(13), and we take note of that since we started and finished by swapping 1 and 3 round, this new permutation does to what the old one did to and the other way around. So the subsequent permutation is (32) rather than (12) — and (32) is the same as (23).

Before long this perception was transformed into a formal definition. A subgroup H was said to be shut under conjugation if $ghg^{-1} \in H$ whenever $h \in H$ and $g \in G$. And now the first inquiry was adjusted in a conspicuous way. The contention used to produce counterexamples could be epitomized in the accompanying proclamation: the part of a homomorphism should dependably be shut under conjugation. (Confirmation: if $\phi(h) = e$, then $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(e) = e$.) So shouldn't something be said about the opposite? Is each subgroup that is shut under conjugation the bit of some homomorphism?

This inquiry is a case of a marvel that happens much of the time in science. You locate an extremely basic important condition for a remark the case. (In this case, being shut under conjugation is a vital condition for a subgroup to be the piece of a homomorphism.) You at that point endeavor to demonstrate that that condition is adequate. It's dependably a lovely astonishment when you oversee, since it is a long way from evident ahead of time that the conditions you have recognized are the main hindrances to getting what you need.

Here, for example, it isn't evident at all that in light of the fact that a subgroup fulfills a condition that it unmistakably needs to fulfill, it must be the portion of some homomorphism. Where's that homomorphism going to originate from? There isn't another group around, not to mention a guide from to that group. This issue was discovered very hard at the time; however the procedure used to unravel it has since turned out to be standard. The first manner of thinking that prompted an answer went something like this. If you are attempting to discover something entangled however has no clue where to begin, at that point imagine you've discovered what you are searching for and see what you can say in regards to it. How about we have a go at something comparative here, I have a group G and a subgroup H that is shut under conjugation. How about we imagine we have a homomorphism ϕ from G to some group K and that the portion of ϕ is H. What would we be able to say in regards to ϕ?

Well, one thing we know immediately is that $\phi(h) = e$ for every $h \in H$, since that was our initial assumption. What can we do with that information? One thing it tells us is

that $\phi(g) = \phi(gh)$ whenever $g \in G$ and $h \in H$, and also that $\phi(g) = \phi(hg)$. So that tells us that $\phi(g) = \phi(g')$ whenever we can find $h \in H$ such that $g' = hg$ or $g' = gh$. Let's explore that a little more. Let g be an element of G. Can we say precisely for which elements $g' \in G$ it *must* be the case that $\phi(g) = \phi(g')$? We've shown that it must when $g' = hg$ or gh for some $h \in H$. To prove that, we used the fact that every $h \in H$ belongs to the kernel of ϕ. But we also know the converse: that every element of the kernel of ϕ belongs to H. So if $\phi(g) = \phi(g')$, then $g^{-1}g' \in H$, since $\phi(g^{-1}g') = \phi(g)^{-1}\phi(g') = \phi(g)^{-1}\phi(g) = e$.

What we have just established, using only the information that H is the kernel of ϕ, is that $\phi(g) = \phi(g')$ if and only if $g^{-1}g' \in H$, which is the same as saying that $g' \in gH$. In other words, ϕ is constant on the left cosets of H but takes different values on different left cosets. But I could have argued slightly differently. I could have shown that $\phi(g) = \phi(g')$ implies that $\phi(g'g^{-1}) = e$, and therefore concluded that $\phi(g) = \phi(g')$ if and only if $g'g^{-1} \in H$, or $g' \in Hg$. This would have demonstrated that is consistent on the privilege cosets of H, and that it takes distinctive values on various right cosets.

These two perceptions are contradictory with each different unless each left coset is a privilege coset and the other way around. So we would do well to watch that. What right coset of H might be equal to gH? Well, it had better contain g, so Hg is a pretty obvious choice. Does $gH = Hg$? The answer is yes if and only if $gHg^{-1} = H$. In any case, H is shut under conjugation, so we're OK [By the way, on the off chance that you are on edge about my written work equations that include not only elements of G but rather subgroups of G and then doing things like multiplying the two sides on the privilege by, then you have great impulses. The thinking is legitimate; however watch that it is substantial. Where do we have to now? We have demonstrated that if is a homomorphism from G to a group K, and if the portion of is H, at that point must be steady on the cosets of H — and we have additionally demonstrated that I'm permitted to state "cosets" in light of the fact that the left and right cosets match. Additionally, must take diverse values on various cosets.

Is that everything we can state? Particularly not If we have an ounce of mathematical interest, at that point eventually we will begin to ponder whether we can say anything in regards to how the values of on various cosets are identified with each other. In the event that we realize that ϕ takes the value a everywhere on the coset g_1H and the value b everywhere on the coset g_2H, can we deduce anything from that? Well, the main thing we know about ϕ is that it is a homomorphism, so let's try to use that fact. If $h_1, h_2 \in H$, then $\phi(g_1h_1) = a$ and $\phi(g_2h_2) = b$,

so $\phi(g_1h_1g_2h_2) = ab$, by the multiplicativity property. By what we have just established, that tells us that ϕ will take the value ab on the entire coset to which $g_1h_1g_2h_2$ belongs. But what is that coset? To answer that we would like to rewrite $g_1h_1g_2h_2$ as a product that begins with something in G and ends with something in H. It would be nice if we could let h_1 and g_2 swap places.

Can we say that $h_1g_2 = g_2h_1$? Unfortunately not, But let's play around a little. We know that H is closed under conjugation, so we might try to find a conjugation. And we can! Rearranging the equation we were hoping for gives us that $g_2^{-1}h_1g_2 = h_1$. There is no reason to suppose that that is true, but we do at least know that the right hand side belongs to H. So we can at least write $g_2^{-1}h_1g_2 = h_3$. And rearranging that tells us that $g_2h_3 = h_1g_2$. So $g_1h_1g_2h_2 = g_1g_2h_3h_2$. That tells us that the coset that contains $g_1h_1g_2h_2$ is g_1g_2H which is as nice an answer as we could have hoped for

How does that help when we don't actually know what ϕ is, or what its image is? It actually helps a lot. We are free to *define* the image. Can we think of a set that's in one-to-one correspondence with the set of all cosets of H? Yes of course we can: just take the set itself! However, hold tight, you may state, isn't that somewhat perilous? There are heaps of sets that are in balanced correspondence with any given set, so what reason is there to believe that the set itself is a decent decision? All things considered, here are two reasons.

a) We are given absolutely no data in the problem other than the group G and the subgroup H, so it is highly likely that the homomorphism ϕ and the group K that ϕ maps to will be built out of G and H in some way.
b) In a sense it doesn't actually matter what set we define the group operation on, since if we define it on a set X and $\beta : X \to Y$ is a bijection, then we can use the group operation on X to define essentially the same group operation on Y by $y_1 \circ y_2 = \beta(\beta^{-1}(y_1) \circ \beta^{-1}(y_2))$.

So now we've managed to cut things down further. We want to define a binary operation on the set of all cosets of H that will make it into a group, and we want the function ϕ that takes g to the coset gH to be a homomorphism. Now let's go back to what we have managed to establish about ϕ. An important property was that $\phi(g_1g_2H) = \phi(g_1H)\phi(g_2H)$ (where $\phi(gH)$ meant the constant value that ϕ takes on the coset gH). But now we've decided that we're going to define $\phi(gH)$ to be gH it. The only thing that we haven't decided is what the binary operation on the set of all cosets should be. But what we established earlier about ϕ forces our hand completely. Since $\phi(g_1H)\phi(g_2H)$ must equal $\phi(g_1g_2H)$ and since $\phi(gH) = gH$, it follows that $(g_1H) \circ (g_2H)$ must be g_1g_2H. We have landed at the meaning of the quotient group and the quotient delineate, in this manner tackled the issue. Normally when the quotient group is characterized, one characterizes the binary operation on the set of cosets and then watches that it is all around characterized. Over the span of the above considerations, we have fundamentally effectively checked this. In my imaginary world, there was one last stage in the early improvement of group theory, which was that every one of the musings that prompted the meaning of the quotient group was painstakingly stifled. The answer for the bits arrangement issue was displayed this way.

Theorem: *A subgroup H of a group G is the kernel of some homomorphism if and only if it is closed under conjugation.*

Proof: First we show that the condition is necessary. Let $\phi : G \to K$ be a homomorphism with kernel H. Then for every $h \in H$ and every $g \in G$ we have $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e$, which proves that ghg^{-1} also belongs to the kernel of ϕ, and thus also to H. That proves that H is closed under conjugation.

Presently assume that is shut under conjugation. Characterize a group K as takes after. Its elements are the left cosets of H (which, it can be appeared, are additionally the privilege cosets of H). We characterize a binary operation on these cosets by taking $(g_1H) \circ (g_2H)$ to equal g_1g_2H. There are a couple of things we should check. To begin with, we should ensure that the definition we have quite recently given does not change on the off chance that we pick distinctive elements g_1' and g_2' of the cosets g_1H and g_2H. A quick way of doing that is to note that a different way of defining $(g_1H) \circ (g_2H)$ is as the set of all xy such that $x \in g_1H$ and $y \in g_2H$. That definition clearly depends on the cosets themselves and not on how they are described, but does it give us g_1g_2H? Well, it certainly contains g_1g_2H. In the other direction, $g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2 = g_1g_2h_3h_2 \in g_1g_2H$, so it is also contained in g_1g_2H Now let us define a function $\phi : G \to K$ by $\phi(g) = gH$. Then $\phi(g_1g_2) = g_1g_2H$, which, by definition of the group operation on K, is equal to $g_1H \circ g_2H$. Therefore, ϕ is a homomorphism? For $\phi(g) = gH$ to equal H we need $g \in H$, so the kernel of ϕ is H, as required.

Conclusion & Future Scope

Every year a couple of the brighter science understudies discovered this contention sensibly simple to process. So the choice was taken to smother all say of why the group K was built. Rather, it wound up noticeably regular practice to characterize the quotient group G/H for no obvious reason and to bring up just later that the function $g \mapsto gH$, known as the quotient outline a homomorphism with piece H. Presently, finally, the objective of making the idea troublesome for everyone had been triumphantly accomplished. A further advancement was the acknowledgment that the strategy that had been touched base at was extremely broad for sure. After this verification, diverse ideas of "quotient" continued seeming all finished arithmetic, and with an end goal to locate a brought together depiction of them, the thought of an identicalness connection was figured. Yet, that is another story (maybe to be exhibited in another post).

References

1. Cantor G. Contributions to the Founding of the Theory of Transfinite Numbers (translated by P. E. B. Jourdain), Open Court, 1915.
2. Kamke E. Theory of Sets (translated from the 2nd German edition by F. Bagemihl), Dover, 1950.
3. Halmos PR. Naive Set Theory, Van Nostrand, 1960.
4. Kleene SC. Introduction to Metamathematics, Van Nostrand, 1952.
5. Cohen PJ, Hersh R. Non-Cantorian Set Theory", Scientific American, 1967.
6. Suppes PC. Axiomatic Set Theory, Van Nostrand, 1960.
7. Freyd P. Abelian Categories, An Introduction to the Theory of Functors, Harper and Row, 1964.
8. Bruck RH. A Survey of Binary Systems, Springer, 1958.
9. Clifford AH, Preston GB. "The Algebraic Theory of Semigroups", Mathematical Surveys 7, American Mathematical Society, 1961,
10. Weyl H. Symmetry, Princeton University Press, 1952.
11. Hilbert D, Cohn-Vossen S. Geometry and the Imagination, translated by P. Nemenyi, Chelsea, 1956.
12. Hammermesh M. Group Theory and its Application to Physical Problems, Addison-Wesley, 1962.
13. Cotton FA. Chemical Applications of Group Theory, Interscience, 1963.
14. Yale PB. Geometry and Symmetry, Holden Day, 1968.
15. Rotman JJ. The Theory of Groups: An Introduction, Allyn and Bacon, 1965.