

# תוכן העניינים

xi

הקדמה

## 1 חלק א: תורת החבורות

### 1 מושגים בסיסיים

7	1.1	דוגמאות לחבורות
9	1.1.1	חבורת התמורות
9	1.1.2	החבורה הדיהדרלית $D_n$
10	1.1.3	חבורות מטריצות והחבורות הקלאסיות
12	1.1.4	מכפלה ישרה
12	1.2	איזומורפיזם של חבורות
14	1.3	חבורות סופיות ולוח הכפל שלהן
16	1.4	קבוצות יוצרים
18	1.4.1	חבורות צקליות
25	1.4.2	גרף קיילי
26	1.5	חבורת האוטומורפיזמים
28	1.6	מחלקות של תת-חבורות
32	1.6.1	משפט לגרנז'
34	1.7	תת-חבורה נורמלית

### 2 פעולה של חבורה על קבוצה

45	2.1	משפט מסלול-מייצב
47	2.2	מחלקות צמידות
50	2.3	המשמר (נורמליזטור) של תת-חבורה
51	2.4	משפט קושי

### 3 הומומורפיזמים וחבורות מנה

52	3.1	הומומורפיזם של חבורות
57	3.2	חבורות מנה
62	3.3	משפטי האיזומורפיזם
62	3.3.1	משפט האיזומורפיזם ה-I
64	3.3.2	משפט ההתאמה
67	3.3.3	משפט האיזומורפיזם ה-III
68	3.3.4	משפט האיזומורפיזם ה-II
70	3.4	חבורות פשוטות
70	3.5	עוד על מכפלה ישרה

### 4 חבורות תמורות

75	4.1	תמורות בכתיב מחזוריים
78	4.2	מחלקות הצמידות של $S_n$
80	4.3	סימן של תמורה

85	פשוטות $A_n$ בעבור $n \geq 5$	4.4
89	<b>חבורות <math>p</math> ומשפטי סילו</b>	<b>5</b>
89	חבורות- $p$	5.1
91	משפטי סילו	5.2
95	חבורות $p \cdot q$	5.2.1
97	<b>סדרות נורמליות וסדרות הרכב</b>	<b>6</b>
97	סדרות הרכב	6.1
100	משפט ז'ורדן-הולדר	6.2
105	משפט המיון של החבורות הפשוטות הסופיות	6.2.1
106	חבורות פתירות	6.3
107	החבורה הנגזרת	6.3.1
108	הסדרה הנגזרת	6.3.2
110	קריטריון נוסף לפתירות	6.3.3
113	דוגמה: כל החבורות מסדר $> 60$ הן פתירות	6.3.4
115	חבורות נילפוטנטיות וסדרות מרכזיות	6.4
118	<b>תורת המבנה של חבורות אבליות נוצרות סופית</b>	<b>7</b>
119	חבורות אבליות חופשיות	7.1
124	חבורות אבליות נוצרות סופית	7.2
129	<b>מילה על חבורות חופשיות</b>	<b>8</b>
134	יוצרים ויחסים	8.1
137	<b>חלק ב: תורת החוגים</b>	
139	<b>חוגים: מושגי יסוד</b>	<b>9</b>
139	הגדרה ודוגמאות	9.1
146	הומומורפיזמים של חוגים	9.2
148	אידאלים	9.3
152	חוגי מנה	9.4
155	משפטי האיזומורפיזמים לחוגים	9.5
157	<b>חוגים קומוטטיביים</b>	<b>10</b>
157	תחום שלמות ושדה שברים	10.1
160	חילוק, חבורות ופריקות בתחום שלמות	10.2
163	אידאלים מקסימליים	10.3
165	אידאלים ראשוניים	10.4
165	משפט השאריות הסיני לחוגים	10.5
167	תחום אוקלידי	10.6
171	תחום ראשי	10.7
175	תחום פריקות חד-ערכית	10.8

179	10.9	חוגי מנה של חוג הפולינומים מעל שדה
181	10.10	מבוא לשדות סופיים
184	10.11	קריטריונים לאי-פריקות של פולינומים

## 189 חלק ג: תורת השדות ותורת גלואה

### 191 11 הרחבת שדות: מושגים בסיסיים

191	11.1	השדה
193	11.2	הרחבת שדות
195	11.3	הרחבות אלגבריות
202	11.4	שדות סגורים אלגברית
205	11.5	משפט אודות החבורה הכפלית של שדה

### 207 12 בניות בסרגל ובמחוגה

207	12.1	בניות בסיסיות
211	12.2	בניות בסרגל ובמחוגה בשפה אלגברית

### 218 13 מבוא לתורת גלואה

218	13.1	חבורת האוטומורפיזמים של שדה
220	13.2	חבורת האוטומורפיזמים של הרחבת שדות
221	13.2.1	חבורת האוטומורפיזמים של הרחבות אלגבריות פשוטות
223	13.2.2	חבורת האוטומורפיזמים של הרחבות צקלוטומיות
224	13.3	שדה פיצול של פולינום
226	13.4	התאמת גלואה

### 232 14 ספרביליות

232	14.1	פולינומים ספרביליים והרחבות ספרביליות
236	14.2	הרחבת שיכונים של שדות

### 240 15 נורמליות

240	15.1	הרחבות נורמליות
242	15.2	הרחבות גלואה
243	15.3	עוד על שדות פיצול

### 245 16 המשפט היסודי של תורת גלואה

245	16.1	קריטריון נוסף להרחבת גלואה סופית
247	16.2	המשפט היסודי

### 254 17 מסקנות מתורת גלואה

254	17.1	שדות סופיים
257	17.2	פולינומים צקלוטומיים ומצולעים משוכללים
263	17.3	הרחבות פשוטות ומשפט האיבר הפרימיטיבי
264	17.4	המשפט היסודי של האלגברה

267	<b>18 פתרון פולינומים באמצעות רדיקלים</b>
269	18.1 הרחבות רדיקליות-פשוטות
273	18.2 הרחבות רדיקליות וחבורות גלואה פתירות
276	18.3 פולינום בלתי פתיר מעל $\mathbb{Q}$
278	18.4 המשוואה הפולינומיאלית הכללית
281	18.4.1 הנוסחה הכללית למשוואה ריבועית
282	18.4.2 הנוסחה הכללית למשוואה מעוקבת
286	18.4.3 עוד על פולינומים סימטריים
288	18.5 חבורות גלואה של פולינומים ממעלה $\geq 4$ מעל $\mathbb{Q}$
292	18.6 רדיקלים בשדות ממציין ראשוני

294 **19 דרגת הטרנסצנדנטיות של הרחבה**

299 **נספחים**

301	<b>A שימושים: אלגוריתמים להצפנה וקודים מתקני שגיאות</b>
301	A.1 אלגוריתמים פומביים להצפנה
301	A.1.1 האלגוריתם של RSA
303	A.1.2 אלגוריתם ההצפנה של רבין
305	A.2 קודים מתקני שגיאות
306	A.2.1 קוד ריד-סולומון
307	A.2.2 האלגוריתם של שמיר לשיתוף-סוד

308 **B הלמה של צורן**

310 **C הוכחה אנליטית למשפט היסודי של האלגברה**

311 **מפתח**

## הקדמה

האלגברה המודרנית (כפי שהתפתחה בראשית המאה ה-20) שואפת לכנס תחת קורת-גג אחת דוגמאות שונות בעלות סממנים דומים, לזקק את המשותף להן באמצעות אקסיומות המגדירות **מבנה אלגברי**, ולהוכיח משפטים כלליים על אותו מבנה, שיהיו ישימים בכל אחת מהדוגמאות. בקורסים באלגברה לינארית למדנו על שדות ועל מרחבים וקטוריים. ראינו כיצד תובנות מאנליזה וקטורית ב- $\mathbb{R}^2$  או ב- $\mathbb{R}^3$  ניתנות להכללה גם למרחבים וקטוריים מעל שדות סופיים, או למרחבים אינסוף-ממדיים.

בחלק הראשון של הספר נעסוק במושג **החבורה**, שהוא מושג מרכזי ברבים מענפי המתמטיקה והמדע בכלל. אי אפשר להתקדם היום בתורת המספרים, בפיזיקה של אנרגיות גבוהות או בקריסטלוגרפיה בלי תורת החבורות. תורת החבורות התבררה ככל-כך מרכזית לענפי הגאומטריה השונים, עד שפליקס קליין ניסה להעמיד עליה את כל יסודות הגאומטריה ב"תכנית ארלנגן" (Erlangen) שפרסם בשנת 1872.

בחלקו השני של הספר נכיר מושג נוסף – **החוג** – שגם לו תפקיד מרכזי ברוב תחומי המתמטיקה, ובמיוחד בתורת המספרים ובגיאומטריה אלגברית.

בחלק השלישי נדון בתורת השדות וביהלום שבכתר – תורת גלואה. תורה זו פותחה במאה ה-19 על-ידי מספר מתמטיקאים שעיקריים שבהם נילס אבל (Abel) ואווריסט גלואה (Galois). האחרון מצא את מותו הטראגי בגיל 21, אבל הספיק להשאיר מורשת ששינתה את פני האלגברה המודרנית והשפיעה רבות על תחומים רבים במתמטיקה. תורה זו, שגילתה קשר עמוק בין שני נושאים לכאורה שונים: פתרון משוואות פולינומיאליות מעל שדות מחד ותורת החבורות מאידך, מהווה את אחת מפסגות ההישגים של המתמטיקה לאורך הדורות. היא גם זו המאגדת את חלקי הספר ליחידה אחת.

בהצגת הנושאים השונים השתדלנו לפרט ולהביא את מרבית ההוכחות המרכזיות במלואן. אולם במכוון השארנו לעתים חלקים מההוכחה לעבודה עצמית כתרגילים. מעבר לחיסכון במקום, הקורא ישכיל, לטעמנו, אם יהיה שותף פעיל בקריאה ויפתור לאורך הדרך את התרגילים שהצגנו, אם מעט ואם הרבה. חלק מהנושאים מוצג על-ידי תרגילים בלבד.

לכל אורך הדרך, דוגמאות ומקרים פרטיים יהוו חלק חשוב מפיתוח התורה. מעבר לעניין שיש ביישומים של המשפטים הכלליים במקרים פרטיים, יש בדוגמאות אלו כדי לעורר שאלות חדשות ולכוון את התפתחות המקצוע.

החומר המכוסה בספר מתאים לתכנית הלימודים בקורסי "מבנים אלגבריים" באוניברסיטה העברית, אולם נסיוננו מראה שלא ניתן לכסות את כולו בהרצאות בכיתה. אנו ממליצים להשאיר חלק מן הנושאים לשיעורי התרגול (למשל, סעיפים 3.5, 6.3.4, 6.4, 10.8, 15.3, 17.3, 18.4.2, 18.4.3 ו-18.5). ייתכן אף שמורים ייאלצו לוותר כליל על חלק מהנושאים, איש איש על פי טעמו והעדפותיו, ועל-פי רמת הכיתה. עם זאת, אנו מאמינים שהספר מאפשר לתלמיד הרוצה בכך ללמוד בעצמו את כלל החומר.

ספר זה נכתב מתוך תחושה שהספרות העברית הקיימת בנושא המבנים האלגבריים הנלמדים כאן היא מצומצמת מדי, והחומר בסיסי מכדי לשלוח תלמידים לספרות הלועזית. עם זאת, ספרי הלימוד באנגלית העוסקים במבנים אלגבריים הם רבים וחלקם מצוינים. לאלו הרוצים להעמיק בחומר ולקרוא על נושאים שאינם מטופלים בספר הנוכחי, אנחנו ממליצים על הספרים הבאים: An Introduction to the Theory of Groups מאת J. J. Rotman (עבור נושא החבורות), הספרים Abstract Algebra ו-Topics in Algebra מאת I. N. Herstein, הספר Basic Algebra I של Jacobson, ספרו המקיף של S. Lang, ששמו Algebra, הספר המודרני יותר Abstract Algebra מאת D. S. Dummit ו-R. M. Foote, וכן ספרו המצוין של I. Stewart שעוסק בתורת השדות ובתורת גלואה, שכותרתו Galois Theory. ספרים אלו כתובים ברמות שונות של הרחבה, העמקה וקצב, אך אנו בטוחים שכל תלמיד שיחפוץ בכך יוכל למצוא בהם ספר לטעמו.

חובתנו הנעימה להודות לרבים וטובים שסייעו בידינו בכתיבת ספר זה. שלמי תודה לעובדי הוצאת מאגנס ובראשם יהונתן נדב המנכ"ל ורם גולדברג, שניצח על מלאכת ההפקה, על שיתוף פעולה פורה ומקצועי. הוקרתנו המיוחדת ליאיר גלזנר ולשופט הנוסף של הספר שנותר בעילום שם, אשר עשו עבודת שיפוט מקיפה ומעמיקה, העירו הערות רבות ומועילות וסייעו בידינו ללטש את הגרסא הסופית של הספר. אורטל פלדמן סייע בידינו רבות בחלק הטכני של הכתיבה. שינויים רבים בספר היו פועל יוצא של הערותיו החשובות של אורי ברזנר. רבים אחרים סייעו בידינו, אם על-ידי סיכומי הרצאות, הצעת תרגילים או עצה טובה, אם באמצעות הפניה לחומרים נוספים או מציאת טעויות בגרסאות הקודמות (הטעויות הנותרות – באחריותנו בלבד) ועוד. מבין הרבים נזכיר את ליאור ברי-סורוקר, יתיר הלוי, יונתן הרפז, יונתן יהלום, ספי לדקני, אבינעם מן, אורי פרזנציבסקי, יובל קפלן וענר שלו. נודה, לבסוף, לתלמידינו הרבים במשך השנים שמהם השכלנו יותר מכולם.