מבוא לתורת החוגים

ד"ר עוזי וישנה

2.10.2005

האובייקט המרכזי שבו עוסק הקורס "תורת החוגים" הוא מבנה מתמטי הנקרא **חוג**. בחבורות, שאתם כבר מכירים, יש פעולה אסוציאטיבית אחת, עם איבר יחידה. בחוגים יש שתי פעולות, ושני איברים מיוחסים: האפס והיחידה. הדוגמאות הבסיסיות ביותר לחוגים הן קבוצת המספרים השלמים, וקבוצת הפולינומים עם מקדמים בשדה (למשל שדה הרציונליים). בנוסף לזה, כל שדה הוא דוגמא לחוג (שדה המספרים הממשיים, שדה המספרים המרוכבים), כמו גם אוסף המטריצות הריבועיות $n \times n$ (עם מקדמים ממשיים, לדוגמא). בכל המקרים האלה, פעולות החיבור והכפל הן הפעולות המוכרות, והן מקיימות כמה אקסיומות ידועות, כמו אסוציאטיביות ודיסטריבוטיביות.

תורת החוגים התחילה בנסיונות של המתמטיקאי הגרמני Ernst Kummer, בשנת 1843, לפתור את השערת פרמה. הרעיונות של Kummer הובילו אותו ללמוד קבוצות מיוחדות של מספרים, שהוא קרא להן 'מספרים אידיאליים'. הפשטה של מבנים אלה יצרה בהמשך את האקסיומות הכלליות של חוג, ואת האידיאלים (שהתפקיד שלהם בתורת החוגים דומה לזה של תת־חבורות נורמליות בתורת החבורות). עד מהרה התברר שחוגים מופיעים בתחומים רבים במתמטיקה, ותורת החוגים התפתחה גם בזכות האלגנטיות והלכידות הפנימית שלה, וגם לצורך היישום שלה בשטחים אחרים.

במשך המחצית הראשונה של המאה העשרים נחקרו משפחות רבות של חוגים, ופותחה תורת מבנה עשירה ורבת עוצמה. המחקר בכיוונים אלה עדיין נמשך, תוך שתשומת הלב מתמקדת בעיקר בסוגי החוגים שמקורם באנליזה, בגאומטריה ובתורת החבורות.

לקורס יש ארבעה חלקים. ראשית, נלמד חוגים באופן כללי, בגישה אקסיומטית: נציג את האקסיומות שמקיימות פעולות החיבור והכפל בחוג, ונראה כיצד לגזור מהן תכונות שאנו פוגשים בכל החוגים המוכרים. יתכן שנקדיש זמן מה לבחינת התפקיד של איבר היחידה בחוג, במיוחד בקשר לתת־חוגים והיחידות שלהם.

אחת האבחנות היסודיות בתורת החוגים היא בין חוגים קומוטטיביים (שבהם הכפל מקיים $ab = ba$), לבין החוגים שאינם כאלה (ליתר דיוק, אינם בהכרח כאלה). בשלב הראשון נעסוק בחוגים לא קומוטטיביים. אי־הקומוטטיביות של הכפל מצריכה הגדרות 'חד צדדיות', וכך נפגוש 'יחידה מימין' ו'יחידה משמאל', 'הפכי מימין' ו'הפכי משמאל'. חשוב יותר, נדון באידיאלים ימניים ושמאליים (הדוגמא הקלה ביותר למבנים אלו: הקבוצות aR ו־ Ra, כאשר R חוג ו־ $a \in R$), וגם באידיאלים דו־צדדיים, הקרויים סתם 'אידיאלים'. אידיאלים מאפשרים לבנות חוגי מנה (באופן דומה לבניה של חבורות מנה), והם מופיעים באופן טבעי כאשר בוחנים את ההעתקות של תורת החוגים ־ ההומומורפיזמים. זו גם הזדמנות להכיר את הפעולות בין אידיאלים (חיבור, כפל, חיתוך), ואת שלושת משפטי האיזומורפיזם של Noether. בנוסף, נציג כמה דרכים לבנות חוגים חדשים מחוגים קיימים (בפרט נציין את הבניות ה'חיצוניות' של מכפלה

ישרה, של מטריצות ושל חוגי פולינומים, ואת הבניה ה'פנימית' באמצעות סיפוח של איברים).

כהצצה לתורת המבנה, נכיר שני סוגים מיוחדים של אידיאלים: אידיאלים מקסימליים, ואידיאלים ראשוניים. כל אידיאל מקסימלי הוא ראשוני, אבל ההיפך אינו נכון. אפשר לאפיין אידיאלים כאלה בעזרת תכונות של חוג המנה. אידיאל מקסימלי הוא כזה שחוג המנה ביחס אליו הוא 'חוג פשוט'; אלו הם האטומים של תורת המבנה. אידיאל ראשוני הוא כזה שחוג המנה ביחס אליו הוא 'חוג ראשוני' - לאלו תפקיד מרכזי בתורת המבנה)שבה לא נעסוק יותר(. אם מניחים שהחוג קומוטטיבי, אז חוג פשוט מוכרח להיות שדה, וחוג ראשוני מתאפיין בכך שהשוויון $ab = 0$ מאלץ $a = 0$ או $b = 0$. חוגים כאלה נקראים 'תחומי שלמות', והם הנושא של החלק הבא. למשפט השאריות הסיני (המוכר מפתרון משוואות מודולריות) יש גרסאות כלליות; יתכן שנדחה משפט זה לחלק הבא, כדי להניח שחוג הבסיס קומוטטיבי.

בחלק השני (והמרכזי) נעסוק בסוג מיוחד של חוגים קומוטטיביים: תחומי שלמות. כל החוגים החשובים בגאומטריה אלגברית ובתורת המספרים הם כאלה. כל תת־חוג של שדה הוא כמובן תחום שלמות; בעזרת בניה של 'שדה שברים' (בדומה לבניית הרציונליים מתוך השלמים), נראה שגם ההיפך נכון.

ליחס החילוק יש תפקיד מוביל בתחומי שלמות (איבר a מחלק את b, אם אפשר לכתוב $b = ac$ לאיזשהו c). האיברים ההפיכים הם אלו שמחלקים את 1. איברים שמחלקים זה את זה הם 'חברים', וככל שמדובר בתכונות חילוק, אין ביניהם הבדל.

כדי ללמוד את האיברים השייכים לתחום שלמות, אנחנו מגדירים "איבר אי־פריק" בתור איבר a של החוג, שאי אפשר לכתוב אותו כמכפלה $a = bc$, אלא אם אחד הגורמים הפיך. לדוגמא, בחוג השלמים, כל המספרים הראשוניים הם איברים אי־פריקים. בכיוון מעט שונה, קוראים לאיבר $p \in R$ **איבר ראשוני**, אם האידיאל Rp הוא אידיאל ראשוני: מתברר שאיבר ראשוני הוא כזה שאינו יכול לחלק מכפלה bc בלי לחלק את אחד הגורמים שלה. גם כאן, האיברים הראשוניים של חוג השלמים הם המספרים הראשוניים המוכרים; אבל בחוגים כלליים יותר אלו מושגים שונים. מתברר שהראשוניים הם סוג מיוחס של אי־פריקים (ולא כל איבר אי־פריק הוא גם ראשוני). קל לזכור זאת, אם מבינים את האי־פריקות בתור תכונה של האיבר לעצמו, בעוד שראשוניות היא תכונה הקשורה לאינטרקציה עם איברים אחרים ("קל יותר להיות אי־פריק לעצמך מאשר ראשוני לכולם"). נקודה נוספת שחשוב לזכור: התכונות של איבר תלויות תמיד בחוג שבו עובדים. למשל, 7 הוא הפיך בשדה הרציונלי, ראשוני בחוג השלמים, ופריק בחוג $\mathbb{Z}[\sqrt{2}]$: $7 = (3 + \sqrt{2})(3 - \sqrt{2})$.

מונחים על־ידי המשפט המרכזי של האריתמטיקה ("במספרים שלמים יש לכל מספר פירוק יחיד לגורמים ראשוניים"), אנחנו רוצים להבין באילו תחומי שלמות מתקיימות תכונות דומות. כמובן שהפירוקים המעניינים הם לגורמים אי־פריקים (שהרי כל פירוק אחר אפשר להמשיך ולעדן). נתבונן באיבר של חוג. אם הוא אי־פריק, סיימנו את הפירוק. אחרת, אפשר לכתוב אותו כמכפלה של שני גורמים, ולהמשיך את התהליך עבור כל אחד מהם. לכאורה, מוכרחים בסופו של דבר להגיע למכפלה של גורמים אי־פריקים. כאן עולות שתי שאלות: אחת, **קיום** הפירוק: אולי התהליך ממשיך בלא

סוף, כך שלאיבר שאנו בוחנים אין בכלל פירוק. השניה, **יחידות** הפירוק: אולי אפשר לפרק את אותו מספר בשתי דרכים (כמו ש־ $30 = 2 \cdot 15 = 6 \cdot 5$), ולהגיע ליותר מפירוק אחד (בלי להחשיב שינוי של סדר הגורמים, או כפל באיברים הפיכים).

כדי לטפל בשאלה הראשונה, אנחנו מגדירים **חוג נותרי** (על־שם המתמטיקאית Emmy Noether): זהו חוג שכל אידיאל שלו נוצר סופית (כלומר, נוצר על־ידי מספר סופי של איברים). זהו מושג מרכזי בתורת החוגים, שאנחנו נטעם ממנו רק על קצה המזלג. נוכיח שבחוג נותרי, תהליך הפירוק חייב להיות סופי, כלומר, לכל איבר קיים פירוק לגורמים אי־פריקים.

באשר לשאלת היחידות, חשוב להדגיש שפירוק לגורמים ראשוניים (שהם כזכור אי־פריקים מיוחסים), אם הוא קיים, הוא תמיד יחיד (בין כל הפירוקים לגורמים אי־פריקים). אנחנו מגדירים **תחום פריקות יחידה** בתור תחום שלמות, שבו לכל איבר קיים פירוק יחיד לגורמים אי־פריקים (באנגלית חוג כזה נקרא Unique Factorization Domain, ובקיצור UFD). מתברר שבתחום כזה כל איבר אי־פריק הוא ראשוני, ולכן הגדרה שקולה יכולה להיות ־ תחום שלמות שבו לכל איבר יש פירוק לראשוניים. תחום פריקות יחידה אינו בהכרח נותרי, אבל חוג נותרי שבו כל אי־פריק הוא ראשוני, הוא תחום פריקות יחידה.

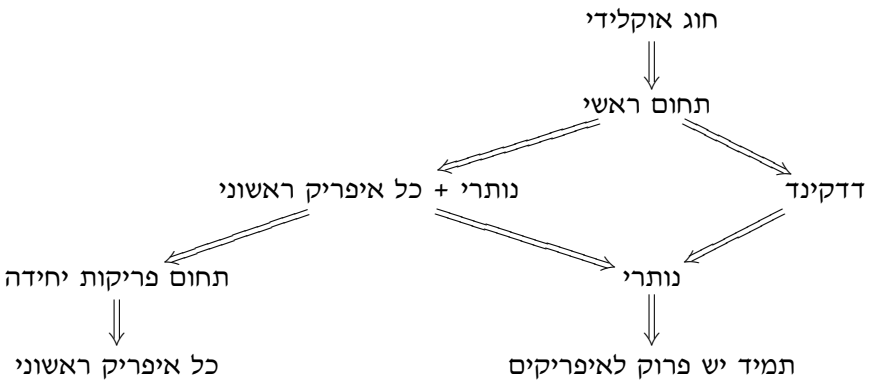
חסר לנו עדיין תנאי שימושי שיבטיח שתחום שלמות הוא אכן תחום פריקות יחידה. הפירוק לראשוניים מאפשר להגדיר (בתחומי פריקות יחידה) את המושג "**מחלק משותף מקסימלי**". הבעיה היא שהקשר בין המחלק המשותף המקסימלי לאיברים שהוא מחלק אינו מספיק מדויק: במספרים השלמים אפשר להציג את המחלק המשותף המקסימלי של a ו־ b כצירוף שלם שלהם, וזה לא כך בכל תחום פריקות יחידה. כדי להתגבר על הבעיות האלה, אנחנו מגדירים **תחום ראשי** (או ־ תחום אידיאלים ראשיים, Principal Ideal Domain), בתור תחום שלמות, שבו כל אידיאל נוצר על־ידי איבר אחד. תכונה זו סוגרת את המעגל ומחזירה אותנו אל הרעיונות המקוריים של Kummer. בחוג כזה, כל 'מספר אידיאלי' הוא מספר, ותו לא.

כמובן, כל תחום ראשי הוא נותרי. בתחום ראשי, המחלק המשותף המקסימלי של a ו־ b הוא היוצר של האידיאל $Ra + Rb$. מתכונה זו נובע בקלות שכל איבר אי־פריק הוא ראשוני, ולכן כל תחום ראשי הוא תחום פריקות יחידה. תכונה מעניינת נוספת של תחומים ראשיים: כל אידיאל ראשוני לא טריוויאלי בהם הוא מקסימלי. תחומים ראשיים מהווים דוגמא ל'חוגי דדקינד', שהם בעלי חשיבות מכרעת בתורת המספרים האלגברית.

אנחנו מכירים שתי דוגמאות חשובות לתחומים ראשיים: המספרים השלמים, וחוג הפולינומים מעל שדה. בשני המקרים, כדי להוכיח שכל אידיאל נוצר על־ידי איבר אחד, פועלים באינדוקציה (על הערך המוחלט או על המעלה). כדי להכליל על ההוכחה הזו, מגדירים **חוג אוקלידי**, שהוא תחום שלמות עם פונקציית גודל מתאימה. כל חוג אוקלידי הוא תחום ראשי.

דוגמאות למושגים שהוזכרו בחלק זה נקבל מחוגי מספרים, בעיקר מהצורה $\mathbb{Z}[\sqrt{d}]$. אלו כולם תחומי שלמות נותריים, אבל רק מעטים מהם מקיימים את שאר התכונות שהזכרנו.

בחלק השלישי ניישם את התאוריה לחוגי פולינומים, כדי להכין את הקרקע לתורת



איור 1: תכונות של תחומי שלמות

השדות ובפרט לתורת גלואה. נקודת המוצא היא העובדה שחוגי פולינומים מעל שדה, עם פונקציית המעלה, הם חוגים אוקלידיים. מכאן נובע כמובן שהם חוגים ראשיים, שכל פולינום אי־פריק הוא ראשוני, ושמתקיימת בהם פריקות יחידה. מכאן יוצאת בקלות התכונה הבאה של פולינומים מעל שדה: a הוא שורש של $f(\lambda)$ אם ורק אם $(\lambda-a) \mid f(\lambda)$. בפרט, לפולינום יכולים להיות שורשים לכל היותר לפי מעלתו, והשורשים של מכפלת פולינומים מגיעים מן הגורמים שלה.

אם כך, מטרתנו הראשונה היא, בהנתן שדה ופולינום אי־פריק מעליו, לבנות שדה הרחבה שיכיל שורש לפולינום. כהכנה לכך, נבחן את ההומומורפיזם $F[\lambda]\to K$ המוגדר על־ידי הצבת $a \in K$ קבוע במקום λ. התכונות של האיבר a קשורות לגרעין של הומומורפיזם ההצבה, שהוא תמיד אידיאל ראשוני (ולכן אפס או מקסימלי). כך אפשר להבחין בין איברים טרנסצנדנטיים לבין איברים אלגבריים, להגדיר עבור האחרונים **פולינום מינימלי**, ולקבל בניה חיצונית של שדה, איזומורפי ל־ $K[a]$. אם הזמן יאפשר זאת, נתקדם עוד כמה צעדים לכיוון ההגדרה והבניה של **שדה פיצול**, שהוא השדה הקטן ביותר מעליו הפולינום שלנו מתפצל לגורמים ליניאריים.

נצטרך כלים לברר האם פולינום נתון הוא אי־פריק. לשם כך נלמד את **הלמה של גאוס**, הקובעת למשל שאם פולינום בעל מקדמים שלמים הוא אי־פריק מעל חוג השלמים, אז הוא גם אי־פריק מעל הרציונליים; ואת **הקריטריון של אייזנשטיין**, המאפשר להסיק אי־פריקות מתוך תכונות מודולריות של מקדמי הפולינום. נלמד (בתרגיל) כיצד מוצאים שורשים רציונליים לפולינום במקדמים שלמים; חשוב לזכור שהעדר שורשים בשדה מבטיח אי־פריקות של פולינום ממעלה 2 או 3, אבל לא ממעלה גבוהה יותר.

בחלק האחרון של הקורס נעסוק במבנה חדש: מודול מעל חוג. זוהי הכללה של מרחבים וקטוריים, שהם המודולים מעל שדה. בגלל המבנה המורכב יותר של חוגים,

התאוריה של מודולים היא עשירה יותר מזו של מרחבים וקטוריים, ויש הרבה יותר דוגמאות. פרט ל'מודולים החופשיים' שהם מודולים מהצורה R^n, המקבילים למרחב וקטורי מממד n, גם אידיאלים וחוגי מנה R/I הם מודולים מעל R. למשל, המודולים מעל $\mathbb{Z}$ הם בדיוק החבורות האבליות. באופן כללי יותר, המודולים מעל חוג מסויים מייצגים את כל האפשרויות שלו 'לפעול' על מבנים אחרים, ובאלגברה לא קומוטטיבית ממשיכים מנקודה זו לפתח את תורת המבנה של חוגים בעזרת המודולים.

נעזר בקיום של אידיאלים מקסימליים, כדי להוכיח שמעל חוגים קומוטטיביים, אם $R^n \cong R^m$ אז $n = m$ (תכונה זו, שנראית מובנת מאליה, אינה נכונה מעל חוגים לא קומוטטיביים). אם כך, מעל חוג קומוטטיבי אפשר להגדיר **דרגה** של מודול חופשי, מושג המכליל את המימד של מרחבים וקטוריים.

אם חוג הבסיס R הוא חוג ראשי, מתקיימת עוד תכונה רצויה: תת־מודול של מודול חופשי M הוא חופשי (עם דרגה קטנה או שווה לדרגה של M). תוצאה מיידית: כל מודול נוצר סופית מעל R הוא מנה של שני מודולים חופשיים. כדי ללמוד מודולים נוצרים סופית, אנחנו מכניסים לזירה מטריצות מעל R. זה מאפשר להציג כל מודול נוצר סופית כמנה R^n/BR^n, כאשר B מטריצה בגודל מתאים, הנקראת **מטריצת היחסים** של המודול.

הדוגמא המרכזית שנחקור היא של המרחב הוקטורי F^n, שהופך למודול מעל חוג הפולינומים $F[\lambda]$ 'בעזרת' מטריצה A: הכפל ב־ λ מוגדר לפי פעולת A. נראה שמטריצת היחסים של המודול הזה היא $\lambda I - A$. בנוסף לזה, המודולים המתקבלים מ־ A ומ־ B איזומורפיים, אם ורק אם A ו־ B צמודות ("דומות").

לגבי הכיוון ההפוך של הקשר בין מודול למטריצת יחסים, קל לראות שאם מכפילים את מטריצת היחסים במטריצה הפיכה מימין או משמאל, המודול אינו משתנה. זוהי הסיבה להגדיר **שקילות** בין מטריצות, ולחפש דרכים למיין מטריצות עד כדי שקילות (מעל שדה, מחלקת השקילות מאופיינת בדרגת המטריצה ותו לא. מעל חוגים אחרים החיים מעניינים יותר). מעניין לבחון את הקשר בין שקילות לבין פעולות אלמנטריות. מעל שדה, מטריצה הפיכה היא מכפלה של מטריצות אלמנטריות, ולכן אפשר לעבור בין מטריצות שקולות על־ידי פעולות אלמנטריות. זה נכון גם מעל חוג אוקלידי, אבל לא בתחום שלמות כללי. מעל חוג ראשי, ואפילו חוג דדקינד, מספיק להוסיף ליוצרים את המטריצות ההפיכות בגודל 2×2. עובדה זו משתקפת באלגוריתמים שנפגוש בהמשך.

משפט המיון (למודולים מעל חוג ראשי): מעל חוג ראשי, כל מטריצה שקולה למטריצה אלכסונית. אם מניחים שאברי האלכסון מקיימים $d_1 \mid \ldots \mid d_n$, אז המטריצה הזו יחידה. (מקוצר זמן אולי נוכיח את המשפט רק עבור חוגים אוקלידיים).

כאשר מתבוננים במודולים מעל $\mathbb{Z}$ ו־ $\mathbb{F}[\lambda]$, שניהם כמובן חוגים ראשיים, מקבלים מן המשפטים האלה מיון שלם של חבורות אבליות נוצרות סופית, ושל מטריצות מעל שדה עד־כדי־צמידות (ואפילו כאשר השדה אינו סגור אלגברית). התורה של מטריצות ז'ורדן מתקבלת כבדרך אגב, אם מניחים שהשדה סגור אלגברית. נוכל להסיק בקלות גם את המשפט הבא, שאינני מכיר לו הוכחה קלה בכלים של אלגברה ליניארית: אם שתי מטריצות ממשיות צמודות זו לזו מעל המרוכבים, אז הן צמודות מעל הממשיים.