U$_\text{A}$M Uniwersytet im. Adama Mickiewicza
w Poznaniu

Wydział Matematyki
i Informatyki
ul. Umultowska 87
61–614 Poznań

Adam Mickiewicz University
Faculty of Mathematics
and Computer Science
fax: +48(61)8295315

Seminarium SFARA (Mnożenie Zespolone - CM)

B1-38, piątek, 11.30 - 13.00
Prowadzący: W.Gajda i B.Naskręcki
Uczestnicy: S.Barańczuk, K.Górnisiewicz, M.Zalewski, Ł.Nizio, Ł.Pańkowski, J.Garnek, K.Gierszewski, P.Rzonsowski, A.Łydka, M.Grześkowiak, D.Blinkiewicz.

Kontynujemy jeden z wątków tematycznych rozpoczętych w ubiegłym semestrze podczas lektury książki Coxa *On primes of the form* x^2+ny^2. Wykłady SFARy w okresie od marca do końca maja 2014 będą dotyczyły teorii mnożenia zespolonego na krzywych eliptycznych i na rozmaitościach abelowych. Teoria ciał klas, którą omawialiśmy zimą tego roku klasyfikuje rozszerzenia abelowe ciał liczbowych i ciał lokalnych. Przy tej klasyfikacji powstają ważne ciała klasowe tzw. *ray class fields*, których szczególnym przykładem jest ciało Hilberta ciała liczbowego. Wadą teorii jest brak ogólnej kontrukcji ciał klasowych dla każdego ciała liczbowego. W tym semestrze podczas Seminarium poznamy szczegóły techniczne konstrukcji ray class fields w przypadku ciał kwadratowych urojonych, którą prowadzi się przy pomocy teorii krzywych eliptycznych z mnożeniem zespolonym. W szczególności wykażemy, że ciało Hilberta ciała K, kwadratowego urojonego powstaje przez dołączenie wartości j-niezmiennika pewnej krzywej z mnożeniem zespolonym, a ray class fields powstają z dołączania punktów torsyjnych na tej krzywej. Podobnie ogólne prawo wzajemności Artina dla ciała kwadratowego urojonego sformułujemy w terminach krzywej z CM. Wykłady SFARy w tym semestrze oprzemy na ogólnie dostępnych książkach Silvermana: *Advanced Topics in the Arithmetics of Elliptic Curves*, Langa: Complex Multiplication i notatkach online Milnego na ten temat.

Wykłady 1, 2. (**Wprowadzenie do teorii ciał klas**): Powtórzenie i ugruntowanie podstaw teorii, które znajdą zastosowanie w dalszych wykładach seminarium. Posługując się pierściemiem adeli ciała liczbowego sformułować prawo wzajemności Artina, zdefiniować ciało Hilberta i *ray class fields*. Skorzytsać przy tym z [Silv, Ch. II.3] i ewentualnie z artykułu Tate'a ze zbioru artykułów [CF] lub książek Neukircha lub Langa pod tytułem *Algebraic Number Theory*. Warto przy tym powtórzyć (z dowodem) twierdzenie Kroneckera-Webera nad $\mathbf{Q}$ [Silv, Thm. 5.1]. **14 i 21 marca**, *wykłada* J.Garnek

Wykłady 3, 4. (**Krzywe eliptyczne z mnożeniem zespolonym**): Wykazać, że każdy niezerowy ideał ułamkowy I ciała K określa krzywą eliptyczną $\mathbf{C}/I$ z mnożeniem zespolonym. Przy tym grupa klas ideałów $Cl(\mathcal{O}_K)$ działa tranzytywnie na zbiorze izogenii krzywych z mnożeniem zespolonym. Uzyskuje się w ten sposób homomorfizm grup $Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow Cl(\mathcal{O}_K)$.

- Definicja i konstrukcja krzywej z mnożeniem zespolonym [Silv, Chap. II.1], działanie $Cl(\mathcal{O}_K)$ na zbiorze klas izomorfizmów krzywych z CM przez $\mathcal{O}_K$ [Silv, Prop. II.1.2]. Przy okzazji omówić i wyjaśnić przykład [Silv, Ex. II.1.3.1].
- Omówić strukturę punktów I-torsyjnych na krzywej [Silv, Prop. II.1.4] i [Silv, Cor. II.1.5].
- Sformułować i naszkicować dowody: [Silv, Prop. II.2.1], [Silv, Thm. II.2.2] i oszacowania [Silv, Rem. II.2.2.1].

- Zdefiniować homomorfizm $Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow Cl(\mathcal{O}_K)$ i dowieść [Silv, Prop. II.2.4] i [Silv, Thm. II.2.3]. Omówić przykłady krzywych z CM, np. zdefiniowanych nad **Q**. **28 marca i 4 kwietnia**, *wykładają:* Ł.Nizio i M.Zalewski.

Wykłady 5, 6. (**Ciało Hilberta dla** K=$\mathbf{Q}(\sqrt{D})$, $D < 0$): Przede wszystkim należy wykazać, że j-inwariant krzywej eliptycznej z mnożeniem zaspolonym przez $\mathcal{O}_K$ generuje ciało Hilberta.

- Dowieść [Silv, Thm. II.4.3]. Istotnym punktem w tym dowodzie jest [Silv, Prop. II. 4.2], którego dowód należy także omówić. Dla potrzeb następnych wykładów wykazać [Silv, Lemma II.4.5].
- Ponadto wykazać [Silv, Prop. II.5.3] i [Silv, Cor 5.4], które także znajdzie istotne zastosowanie w dalszej części seminarium. **11 i 25 kwietnia**, *wykładają:* S.Barańczuk i P.Rzonsowski.

Wykłady 7, 8. (**Główne twierdzenia o CM**): Podczas tych wykładów (są to dwa centralne wykłady tego seminarium) powinniśmy poznać konstrukcję ray class fields dla ciała kwadratowego urojonego K za pomocą punktów torsyjnych na krzywej eliptycznej z CM przez $\mathcal{O}_K$. Należy rozpocząć od wyjaśnienia konstukcji homomorfizmu wzajemności dla krzywej z CM.

- Definicja funkcji Webera z przykładem [Silv, Ex. II.5.5.1] i pierwsze główne twierdzenie o CM z dowodem [Silv, II.5.6] oraz [Silv, Cor. II.5.7]. Omówić przykład [Silv, Ex. II.8.1].
- Przeprowadzic dowód drugiego zasadniczego twirdzenia mnożenia zespolonego [Silv, Thm, II.8.2].
- Omówić zastosowania twierdzeń głównych o CM do konstrukcji Grössencharakteru i do L-funkcji krzywej: [Silv, II.9 + II.10]. **9 i 16 maja**, *wykładają:* B.Naskręcki i K.Gierszewski.

Wykłady 9, 10. (**Rozmaitości Abelowe z CM**): Celem dwóch ostatnich wykładów SFARy w tym semestrze będzie wprowadzenie do teorii rozmaitości Abelowych z mnożeniem zespolonym. Krótkie podsumowania tej teorii znajdują się w [M, Chap. 9 i 10], w [La Chap. II i II] oraz w [Sha, Chap. II i IV] (patrz też: Serre, Tate: *Good reduction of Abelian varieties*, 1968).

- Definicja CM-typu i ciała CM [La, I.2]. Konstrukcja rozmaitości z mnożeniem zespolonym [La, I.4].
- I-mnożenie i konstrukcja izogenii uniwersalnej [La, III.1, III.2].
- Definicja *reflex field* i *reflex norm* [La, I.5]. Główne twierdzenia mnożenia zespolonego dla rozmaitości Abelowych [La, Thm. 6.1].
- Ponadto zamierzam omówić CM-charaktery i ich zastosowania arytmetyczne patrz [La, IV.1]. **23 i 30 maja**, *wykłada:* W.Gajda.

Literatura

[La], S.Lang, Complex Multiplication, SV 1980.

[M], J.Milne, *Introduction to Shimura varieties*, online notes.

[Sha], G.Shimura, *Abelian varieties with CM and modular forms*, PUP 1998.

[Silv], J.Silverman, *Advanced Topics in the Arithmetic of the Elliptic Curves*, SV 1994.