Welcome to Math 204B!

This is Math 204B (Number Theory), offered at UC San Diego in the winter 2021 quarter. It is the continuation of Math 204A (https://math.ucsd.edu/~kkedlaya/math204a/) and will operate similarly. The course web site is https://math.ucsd.edu/~kkedlaya/math204b/.

As in 204A, lecture recordings will be posted publicly on the course web site. There will also be an "epicourse" with discussion on Zulip; this includes the Zoom links for live lectures and office hours. Signup for the epicourse is via a Google Form linked from the course web site.

Plan for today:

- Course logistics, with an emphasis on changes from 204A (about 15 minutes).
- Kummer theory and the Kronecker-Weber theorem (the rest of the time).

If you did not follow 204A, I recommend watching the last two lectures from 204A for some background on the Kronecker-Weber theorem. (Technical note: the videos have been migrated internally, from Panopto to Mediaspace.)

Throughout the term, all times will be announced in Pacific Standard Time (PST = UTC-8).

The topic: class field theory

Math 204A was a general course about algebraic number fields. In Math 204B, we focus on ***class field theory***, the body of results about abelian extensions of number fields developed in the early 20th century. Class field theory serves as a bridge between ***quadratic reciprocity***, the crowning achievement of elementary number theory, and the development of modern number theory centered around the ***Langlands program(me)***.

The primary source I will be following is my own "Notes on class field theory"; the current version is the interactive HTML version posted at https://kskedlaya.org/cft/, which I will be updating during the term. (It was produced using PreTeXt, which I'll say more about on Zulip.) There is also an older PDF version posted at https://kskedlaya.org/papers/cft-overall.pdf.

Lectures

Lectures will be held MWF 10-10:50am via Zoom; epicourse participants are encouraged to attend. Since these are being recorded, please ask questions by typing in Zoom chat. For each lecture, I'll post in advance a link to the Miro live whiteboard, which will let you view screenfuls other than the one I am currently broadcasting. I will also post the filled boards as a PDF at the end of the lecture.

Each lecture is followed by a 30-minute office hour (see below). There will also be a thread in Zulip under "Math 204B Lecture Q&A" for each lecture, where discussion can continue.

The recording for each lecture will be available from the course web site at approximately 12pm. I will announce when this happens in the aforementioned Zulip thread.

Office hours and Zulip

Office hours will be held MWF 11-11:30am and MW 8-8:30pm PST via Zoom; epicourse participants are encouraged to participate. These will not be recorded.

As in 204A, there will be additional office hours for enrolled students only, which will be held in a hybrid in-person/remote mode as conditions allow. See Zulip for details.

You are also encouraged to ask (and answer!) questions anytime on Zulip. Note that there are separate streams for lectures (one thread per lecture) and homework (one thread per assignment). You can also use the OMNI stream for discussion that is a bit off-topic but may be of interest to this community (e.g., conference announcements).

Homework and grading

Homework will consist of 9 weekly problem sets, due on Thursdays. Homework will be submitted through CoCalc as for Math 204A.

For enrolled students, I will count up to 6 problem sets (including fractions) for full credit. In addition, you will have the option (anytime until the end of exam week) to make up one problem set by submitting a short writeup of a topic not covered in lecture; contact me if you wish to exercise this option.

Since the course parameters are more generous than in 204A, I will be a bit less generous about extensions. You are still welcome to request extensions, but please do so ***in advance*** of the homework due date. This will enable me to promptly "un-embargo" the assignments on Zulip to allow for free discussion.

And now, some mathematics...

The Kronecker-Weber theorem and quadratic reciprocity

<u>Theorem</u> Let $K/\mathbb{Q}$ be a (finite) abelian extension
Galois w/ abelian Galois group

<u>Then</u> $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.
$\mathrm{Gal} = (\mathbb{Z}/n\mathbb{Z})^\times$

For example, any quadratic number field has this property.
Gauss: $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right) \subseteq \mathbb{Q}(\zeta_p)$ (Gauss sums)

if q is another prime, then splitting of q in $\mathbb{Q}(\zeta_p)$
is controlled by $q \pmod p$, as then is true in subfield
OTOH splitting in the subfield depends on $\left(\frac{\pm p}{q}\right)$

The local Kronecker-Weber theorem

Theorem Let $K/\mathbb{Q}_p$ be a finite abelian extension.

Then $K \subseteq \mathbb{Q}_p(\zeta_n)$ for some positive integer n.

(reminder: for any finite Galois extension of $\mathbb{Q}_p$, $\mathrm{Gal}(K/\mathbb{Q}_p)$ is solvable)

Local K-W ⟹ Global K-W

Given $K/\mathbb{Q}$ finite abelian, for each ramified prime p, apply LKW to find a common value of n such that $K\mathbb{Q}_p/\mathbb{Q}_p \subseteq \mathbb{Q}(\zeta_n)$. Use Minkowski's theorem that only unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself.

Kummer extensions

"G-extension"

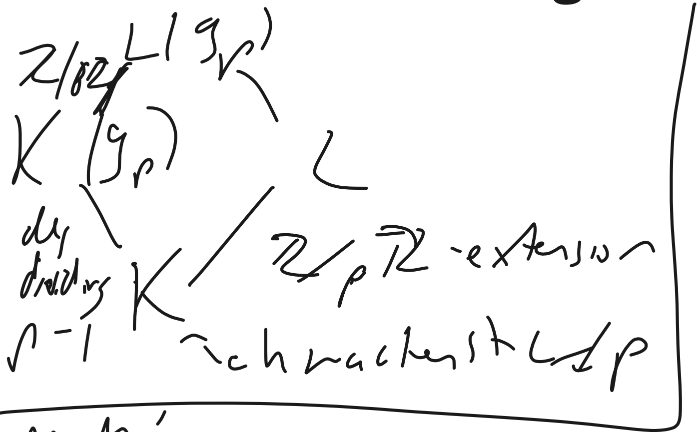
Fix n a positive integer let K be a field of characteristic not dividing n.

Thm (Kummer) Suppose $\zeta_n \in K$ (a primitive n-th root of unity). Then every $\mathbb{Z}/n\mathbb{Z}$-extension of K is of the form $K(a^{1/n})$ for some $a \in K^*$ whose class in $K^*/(K^*)^n$ has exact order n (and conversely).

Moreover, $a, b \in K^*$ define the same extension iff their classes in $K^*/(K^*)^n$ generate the same cyclic subgroup.

e.g. $\mathbb{Q}(\zeta_3)(2^{1/3}) = \mathbb{Q}(\zeta_3)(4^{1/3})$

What about missing roots of unity? (A lemma)



Lemma (1.2.10 in CFT notes)
a Kummer theory

Let K be a field of characteristic $\neq p$ (p prime).

Put $L = K(\zeta_p)$, $M = L(a^{1/p})$ for some $a \in L^*$

- M/K Galois iff $\forall g \in \mathrm{Gal}(L/K)$, images of a, $g(a)$ in $L^*/(L^*)^p$ generate same cyclic subgroup.

M M'

$|\mathrm{Gal}(L/K)|$

L

K

- M/K Galois, abelian iff

$\forall g \in \mathrm{Gal}(L/K)$ $\frac{g(a)}{a^{w(g)}} \in L^*/(L^*)^p$

$w : \mathrm{Gal}(L/K) \to (\mathbb{Z}/p\mathbb{Z})^*$

$g(\zeta_p) = \zeta_p^{w(g)}$

An application of the lemma (p > 2)

Can use this lemma to show:

For $p > 2$, no (Galois) extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$

Idea: calculate

$$\mathbb{Q}_p(\zeta_p)^* / \left((\mathbb{Q}_p(\zeta_p)^*)^p\right)$$

and apply lemma.

(compare $p=2$ hw A/2024A)