Math 4108 midterm 2 study sheet

April 20, 2010

- Know the fact that if $f(x) \in F[x]$, where F is a field, and $f(x)$ has a double root, then $f(x)$ and $f'(x)$ have a common factor. Know that this is if and only if in fields of characteristic 0 (i.e. in ch. 0, f has a double root iff $(f, f') \neq 1$), and the same is true in characteristic p... but when you go to apply this to irreducible polynomials, something can go wrong: There are fields of characteristic p for which there are *irreducbile* polynomials $f(x)$ satisfying $(f, f') > 1$ – 'irreducible' does not always imply that there are no double roots.

- Know the definition of "Galois group", and "Galois extension" (normal and separable), know what separability means. Know the Fundamental Theorem of Galois theory – the one-to-one correspondence between subgroups of the Galois group and subfields, along with the one-to-one correspondence between *normal* subgroups of the Galois group and normal extensions. It is good to have at least some rough idea of how this is proved. Also, know what "solvable by radicals" means.

- Given symbols $x_1, ..., x_n$ (which one can think of as roots of some abstract polynomial), let S denote the field of all *symmetric* rational functions $f(x_1, ..., x_n)/g(x_1, ..., x_n) \in E := F(x_1, ..., x_n)$, where F is some field. Know how to show that E is a splitting field for a certain degree-n polynomial, which therefore implies $[E : S] \leq n!$; in fact, know that $[E : S] = n!$, and that $\text{Gal}(E/S)$ is isomorphic to S_n. Using this, the Fundamental Theorem of Galois Theory, and the simplicity of A_n for $n \geq 5$, know how to show that an arbitrary cubic is not solvable by radicals.

- Know that if $\alpha \in K$, where K is a finite extension of a field F having characteristic 0, then the minimal polynomial for α in $F[x]$ is irreducbile. Know that the same is true in finite fields, but at least know that it is not true for *every* field of characteristic $p \neq 0$.

- Know that $x^{p^n} - x$ is the product of all irreducible polynomials of degree diving n. Also know that the roots of this polynomial form a field of order p^n; so, one has that there exists a field of order p^n for all $n \geq 1$. Furthermore, the elements of *any* field of order p^n must be roots of this polynomial; so, by the uniqueness of splitting fields, all fields of order p^n are isomorphic.

- Know and know how to prove that for $N | p^n - 1$,

$$f(x) \ := \ \prod_{d|N} (x^d - 1)^{\mu(N/d)}$$

is a polynomial in $\mathbb{F}_p[x]$ whose roots are all those elements of order N in $\mathbb{F}_{p^n}$. Know how to use this to prove that there are $\varphi(N)$ elements of order exactly N; and, know how to deduce that $\mathbb{F}_{p^n} \setminus \{0\}$ as a multiplicative group, is cyclic of order $p^n - 1$. Note that this group is not the same as $(\mathbb{Z}/p^n Z)^*$.

- Know about the Frobenius automorphism $\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ via $\sigma(x) = x^p$. Know and know how to prove that this generates the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ under composition, and that said group is cyclic and therefore abelian.

- Know the definition of "Derived Series", "Upper Central Series", and "Lower Central Series". You will of course need to know the definition of the "commutator subgroup" $[A, B]$ and commutator $[x, y] = x^{-1}y^{-1}xy$ in order to even begin talking about these.

- Know how to prove various basic things about these series, such as: Suppose $G := G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ is a derived series, then each G_i/G_{i+1} is abelian; and furthermore, if $N \trianglelefteq G$, then G/N is abelian if and only if $G_1 \leq N$. Know that if the length of the Upper or Lower Central series is finite and includes G and $\{e\}$ as terms, then the same is true of the other – i.e. finite Lower CS terminating at $\{e\}$ implies finite Upper CS terminating at G, and vice versa. It is worth knowing roughly how this is proved (via induction). Groups with finite central series with both trivial subgroups ($\{e\}$ and G) are called nilpotent. Know properties of nilpotent groups mentioned in class – in particular, know that they are solvable.

- Know the meaning of "composition series" of a finite group – basically, one decomposes a group G into a chain of normal subgroups whose successive quotients are simple. That is,

$$G := H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_k = \{e\}$$

  has the property that H_i/H_{i+1} is simple. A composition series is *not* necessarily a derived series, or upper or lower central series – it is something else entirely. Know the Jordan-Holder theorem for groups. Know the second isomorphism theorem for groups, and how to prove it.

- Know the definition of a module, along with some basic examples. Here is an unusual example: Given an abelian group G, let $\hat{G} = Aut(G)$, and then form the $\mathbb{Z}$-module consisting of all integer linear combinations of $\hat{G}$; for example if $\sigma_1, ..., \sigma_k \in G$, then consider the mapping

$$(z_1\sigma_1 + \cdots + z_k\sigma_k) \ : \ G \to G,$$

  which acts by

$$(z_1\sigma_1 + \cdots + z_k\sigma_k)(x) \ = \ z_1\sigma_1(x) + \cdots + z_k\sigma_k(x).$$

  (Here, $z_i y = y + \cdots + y$ if $z_i \geq 0$ and is $(-y) + \cdots + (-y)$ if $z_i < 0$.) One can prove that this new mapping (integer linear combination of automorphisms) is itself in $\hat{G}$ (since G is abelian); so, $\hat{G}$ has a $\mathbb{Z}$-module structure.

  Note that if F is a field, then the set of automorphisms of F (say that fix some more basic field) **do not have** a $\mathbb{Z}$-module structure (I think I incorrectly stated this in class); however, if you work just with the additive part of F, then indeed you get a module structure.

  Know a few different ways to construct modules using ideals and rings (e.g. a ring R is naturally an R-module, as is a left-ideal via the 'black hole property').

- Know the statement of the Fundamental Theorem on Finitely Generated Modules over a PID. Know how to deduce the Fundamental Theorem on Finitely Generated Abelian Groups from it.