Math 536 Homework 1
Spring 2016
Due: Friday, January 22

1. Suppose that H and N are subgroups of a group G and that N is normal in G. Prove that HN is a subgroup of G. (Here HN is the subset of G of all elements of the form $\{h \cdot n : h \in H, \ n \in N\}$). If H is also normal, then show that HN is a normal subgroup of G. (You may *not* use any results on page 94 of Dummit and Foote for this.)

2. Let G be a group, and let $H_1, \dots, H_k$ be subgroups of G. We say that G is an internal direct product of the subgroups H_i if the map

$$(h_1, \dots, h_k) \mapsto h_1 h_2 \cdots h_k : H_1 \times H_2 \times \cdots \times H_k \to G$$

is an isomorphism of groups. This means that each element g of G can be written uniquely in the form $g = h_1 \cdot h_2 \cdot \cdots \cdot h_k$, $h_i \in H_i$, and if $g = h_1 h_2 \cdot \cdots \cdot h_k$ and $g' = h_1' h_2' \cdot \cdots \cdot h_k'$, then

$$gg' = (h_1 h_1')(h_2 h_2') \dots (h_k h_k').$$

Prove that a group G is a direct product of subgroups H_1, H_2 if and only if

(a) $G = H_1 H_2$

(b) $H_1 \cap H_2 = \{e\}$, and

(c) every element of H_1 commutes with every element of H_2.

3. Let N be a normal subgroup of G of index n. Show that if $g \in G$, then $g^n \in N$. Give an example to show that this may be false when N is not normal.

4. Suppose a group G contains a subgroup H in its center (hence H is normal) such that G/H is cyclic. Show that G is commutative.

5. Let G be a group of order $2p$, p an odd prime. Show that G is cyclic or dihedral.

(Recall that the dihedral group D_n of order $2n$ is given by generators and relations

$$D_n = \langle a, b : e = a^n = b^2 = baba \rangle.)$$

Math 536 Homework 2
Spring 2016
Due: Friday, January 29

1. Show that a finite group can't be equal to the union of the conjugates of a proper subgroup.

2. Let G be the group of invertible 4×4 matrices over the complex numbers, and let M be the set of all 4×4 complex matrices.

   (a) Consider the action of $G \times G$ on M given by (g, h) acts on m by the matrix multiplication gmh^{-1}. Describe the orbits of this action.

   (b) Consider the action of G on M by conjugation: g acts on m by the matrix multiplication gmg^{-1}. For what λ and μ are the two matrices below in the same orbit?

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & \mu & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda & \mu \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

(∗) 3. Show that a group of order $2m$, m odd, contains a subgroup of index 2. (Hint: You may use Cayley's theorem, Corollary 4, page 120 in Dummit and Foote, or Jacobson, Corollary on page ~~38~~ 28.)

4. Let K be a conjugacy class of a finite group G contained in a normal subgroup H of G. Prove that K is a union of k conjugacy classes of equal size in H, where $k = (G : H \cdot C_G(x))$ for any $x \in K$.

5. Let N be a normal subgroup of a group G. Suppose that there exists a subgroup K of G with $N \cap K = \{1\}$ and $G = N \cdot K$.

   Any such K is called a *complement to N in G*.

   (a) Given G and N, is the complement K to N in G unique?

   (b) Is K unique up to conjugation in G? No

   (c) Is K unique up to isomorphism?

Math 536 Homework 3
Spring 2016
Due: Friday, February 5

1. Construct all semidirect products of C_p by C_p for p prime. Here C_p denotes the cyclic group with p elements.

2. Let H_8 be the quaternion group of order 8, i.e. the group with presentation

$$< a, b : \, a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1} > .$$

Show that H_8 is **not** a semidirect product of a group of order 4 by a group of order 2.

3. For each odd prime p construct a nonabelian group G of order p^3 and exponent p as a semidirect product.

4. Let T be a group of order 12 which is generated by two elements s and t such that $s^6 = 1$ and $t^2 = s^3 = (st)^2$. Prove that such a group T exists by constructing it as a semidirect product of $\mathbb{Z}_3$ by $\mathbb{Z}_4$.

5. Find composition series for the following groups:

   (a) the quaternion group H_8;

   (b) the dihedral group D_6; and

   (c) $A_4 \times A_4$.

We say that a finite group is **solvable** if the group has a normal series for which each of the consecutive quotients is abelian.

6. Show that every subgroup and every quotient group of a solvable group is solvable.

Math 536 Homework 4
Spring 2016
Due: Friday, February 12

1. Let $\beta : B \to C$ be a surjective homomorphism of abelian groups. Show that if F is free abelian and $\alpha : F \to C$ is any homomorphism, then there exists a homomorphism $\gamma : F \to B$ making the diagram below commute, i.e. such that $\beta\gamma = \alpha$. (We say that F has the *projective property*.)

$$\begin{tikzcd} & F \arrow[d, "\alpha"] \arrow[dl, dotted, "\gamma"'] & \\ B \arrow[r, "\beta"'] & C \arrow[r] & 0 \end{tikzcd}$$

2. Use the previous exercise to deduce the following: If H is a subgroup of an abelian group G and G/H is free abelian, then H is a direct summand of G, that is there exists a subgroup K of G (with $K \cong G/H$) such that $G \cong H \oplus K$.

3. Suppose G is a finitely generated abelian group. Show that there exist finitely generated free abelian groups F_1, F_2 such that $G \cong F_1/F_2$.

4. Let G be the abelian group defined by generators x, y, and z and relations

$$\begin{aligned} 15x + 3y &= 0 \\ 3x + 7y + 4z &= 0 \\ 18x + 14y + 8z &= 0. \end{aligned}$$

Express G as a direct product of two cyclic groups.

5. Let G be the group $\mathbb{Q}/\mathbb{Z}$.

   (a) Prove that every finitely generated subgroup of G is cyclic.

   (b) Show that for every positive integer t, G has a unique cyclic subgroup of order t.

Math 536 Homework 5
Spring 2016
Due: Friday, February 26

1. Show that A_6 has no subgroup of order 72.

2. For which primes p and positive integers n is every p-Sylow subgroup of the symmetric group S_n commutative?

3. How many elements of order 7 must there be in a simple group of order 168?

4. Suppose that a finite group G has only one Sylow p-subgroup for each $p \mid |G|$. Show that G is a direct product of its Sylow p-subgroups.

5. Let H be a normal subgroup of a finite group G, and assume that $|H| = p$. Prove that H is contained in every p-Sylow subgroup of G.

Math 536 Homework 6
Spring 2016
Due: Friday, March 4

1. Count the number of prime ideals in the ring

$$\mathbb{Z}[x, y]/(6, (x-2)^2, y^6)$$

and give an explicit set of generators for each. Which of these contain the class of x? (The whole ring is not considered a prime ideal.)

2. Describe the maximal ideals $\mathfrak{m}$ of the polynomial ring $\mathbb{Z}[x]$ in one variable over the integers that contain the integer 30 and the polynomial x^2+1. Give explicitly two generators for each such maximal ideal $\mathfrak{m}$, and prove that the ideals that you found are maximal. How many such maximal ideals are there?

3. Let R be a commutative ring with 1, and let $I \subseteq R$ be an ideal.

   (a) The radical $\sqrt{I}$ of I is defined to be the set

   $$\sqrt{I} = \{a \in R : a^n \in I \text{ for some } n > 0 \text{ (depending on } a)\}$$

   Prove that $\sqrt{I}$ is an ideal and that $R/\sqrt{I}$ has no nonzero nilpotents. (An element $x \in R$ is nilpotent if there exists some positive integer m such that $x^m = 0$.)

   (b) Let $R = \mathbb{Z}$ and fix an integer $m \geq 2$. What is the radical $\sqrt{(m)}$ of the ideal generated by the integer m?

   (c) Let $R = \mathbb{Q}[x, y]$, the ring of polynomials in two variables with rational coefficients, and let $I = (x^2, y^5)$ be the ideal generated by x^2 and y^5. Find $\sqrt{I}$.

4. Assume that R is a domain, and let $\mathfrak{p}$ be a prime ideal of R. Let $S := R - \mathfrak{p}$. Show that S is a multiplicative subset of R. Let $R_{\mathfrak{p}} := S^{-1}R$. Show that the ring $R_{\mathfrak{p}}$ has a unique maximal ideal, consisting of all elements a/s with $a \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. (A ring R which is commutative and has a unique maximal ideal is called a *local ring*.)

5. Let $f : A \to A'$ be a surjective homomorphism of rings (with identity), and assume that A is local, $A' \neq 0$. Show that A' is local.

Math 536 Homework 7
Spring 2016
Due: Friday, March 18

(*) ~~1~~. Let D be an integer ≥ 1 and let R be the set of all elements $a + b\sqrt{-D}$ with $a, b \in \mathbb{Z}$.

- ✓ (a) Show that R is a ring.
- ✓ (b) Let $N : R \to \mathbb{Z}$ be the norm map, i.e. the map given by

$$N(a + b\sqrt{-D}) = (a + b\sqrt{-D})(a - b\sqrt{-D}).$$

  Show that for $u, v \in R$ we have $N(uv) = N(u)N(v)$.
- ✓ (c) Show that $u \in R$ is a unit if and only if $N(u) = \pm 1$. ← Sould this be $N(u) = +1$?
- ✓ (d) Show that if $D \geq 2$, then the only units in R are ± 1.
- ✓ (e) Show that $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.
- ✓ (f) Use the above elements to prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
- ✓ (g) Are the elements $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ prime in the ring R?

2. Let R be the following subring of the complex numbers:

$$R = \{a + b\frac{(1 + \sqrt{-19})}{2} : a, b \in \mathbb{Z}\}.$$

Show that R is not a Euclidean domain. (*Hint:* First show that the only units of R are ± 1. Then, assuming by contradiction that R has a Euclidean function δ, let x be a nonzero nonunit of R minimizing δ and consider R/xR.)

(*) ~~3~~. Determine the irreducible elements of $\mathbb{Z}[i]$. In particular, determine which integers are irreducible in $\mathbb{Z}[i]$. (You may not use any results of Dummit and Foote, pages 289-291.)

(*) ~~4~~. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to the function $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.

Math 536 Homework 8
Spring 2016
Due: Friday, March 25

~~1.~~ ~~(a)~~ (Euclid's algorithm for finding the gcd.) Let a_1, a_2 be nonzero elements of a Euclidean domain R. Define a_i and q_i recursively by $a_1 = q_1 \cdot a_2 + a_3, a_i = q_i a_{i+1} + a_{i+2}$ where $\delta(a_{i+2}) < \delta(a_{i+1})$. Show that there exists an n such that $a_n \neq 0$ but $a_{n+1} = 0$, and that $\gcd(a_1, a_2) = a_n$. Also use the equations to obtain an expression for the gcd in the form $xa_1 + ya_2$.

~~(b)~~ Compute the gcd of the following two polynomials in $\mathbb{Q}[X]$:

$$f = X^3 + X^2 + X - 3\,, \quad g = X^6 - X^5 + 6X^2 - 13X + 7.$$

~~2.~~ Let R be a principal ideal domain, and let I, J be two nonzero ideals of R. Show that

$$IJ = I \cap J$$

if and only if $I + J = R$.

~~3.~~ Let $R = \mathbb{Z}[\sqrt{-5}]$. On Homework 7 we proved that R is not a UFD. Let $a = 6$, and $b = 2 + 2\sqrt{-5}$. Show that the greatest common divisor of a and b does not exist.

~~4.~~ (a) Is $X^6 + X^3 + 1$ irreducible in $\mathbb{Q}[X]$?

(b) Is $X^2 + Y^2 - 1$ irreducible in $\mathbb{Q}[X, Y]$?

~~5.~~ Prove that if R is a domain which is not a field, then $R[X]$ is not a PID.

~~6.~~ Let F be a field, and $f(x)$ an irreducible polynomial in $F[x]$. Show that $f(x)$ is irreducible in $F(t)[x]$, t an indeterminate. Here $F(t)$ is the quotient field of $F[t]$.

Thus, we ~~have~~

Thm.

R: integral domain.

Then $R[X]$: PID $\Leftrightarrow$ R: field.

Math 536 Homework 9
Spring 2016
Due: Friday, April 8

1. Suppose that R is a commutative ring with identity such that every submodule of every free R-module is free. Show that R is a PID.

2. Let $R := \mathbb{Z}[X]$. Give an example of a finitely generated R-module that does not decompose into a finite direct sum of cyclic R-modules.

3. Let M be the module generated over $\mathbb{Q}[x]$ by the generators a, b satisfying the relations

$$(x-1)a + (x-1)b = 0$$
$$(x^4-1)a + (x^4+x^3+x^2-x-2)b = 0$$

Decompose M as a direct sum of cyclic $\mathbb{Q}[x]$-modules.

4. Let $\mathbb{F}_2$ be the field with 2 elements and let $R = \mathbb{F}_2[X]$. List, up to isomorphism, all R-modules with 8 elements.

5. Show that for a noncommutative ring R, we can have $R^m \cong R^n$ for distinct integers m, n, so free modules over noncommutative need not have a well-defined rank. (Hint: Let k be a field and let V be the polynomial ring in one variable over k. Then V is an infinite-dimensional vector space over k. Let R be the endomorphism ring of V, $R = \mathrm{End}_k(V)$, and show that R has the desired property.)

Math 536 Homework 10
Spring 2016
Due: Friday, April 15

1. Let R be a domain containing a field k as a subring. Suppose that R is a finite dimensional vector space over k under the ring multiplication. Show that R is a field.

2. Construct a splitting field for $X^5 - 2$ over $\mathbb{Q}$. What is its degree over $\mathbb{Q}$?

3. (a) Let F be a finite field of characteristic p. Show that the cardinality of F, $|F|$, is a power of p, $|F| = q = p^m$ for some integer $m \geq 1$.

   (b) Show that F is a splitting field for $f(X) = X^q - X$.

   (c) Show that any other finite field with $q = p^m$ elements is isomorphic to F.

   Please do not use Dummit and Foote, pages 549-551, for this problem.

4. Let E be a splitting field of $x^{35} - 1$ over $\mathbb{F}_8$. Determine the cardinality of E and make a diagram showing all subfields of E and the inclusions between them.

5. Let $f(X)$ be an irreducible polynomial in $F[X]$, where F has characteristic $p > 0$. Show that $f(X)$ can be written as $f(X) = g(X^{p^e})$ where $g(X)$ is irreducible and separable. Deduce that every root of $f(X)$ has the same multiplicity p^e in any splitting field.

6. Let E, F be two finite extensions of a field k, contained in a larger field K. Show that

$$[EF : k] \leq [E : k][F : k].$$

   Here EF denotes the *compositum* of E and F in K, which is the smallest subfield of K containing both E and F.

Math 536 Homework 11
Spring 2016
Due: Friday, April 22

1. Give explicit generators for the subfields of $\mathbb{C}$ which are splitting fields of the following polynomials over $\mathbb{Q}$, and find the degree of each such splitting field.

   (a) $(X^3 - 2)(X^2 - 2)$

   (b) $X^2 + X + 1$

   (c) $X^6 - 1$

   (d) $X^6 - 8$

   (e) $X^8 + 16$

2. Let p be a prime number, let $q = p^n$, and let F be a splitting field of the polynomial $f(X) = X^q - X \in \mathbb{F}_p[X]$. Prove that F has exactly $q = p^n$ elements.

   (This shows that for each integer n, there exists a field F with p^n elements. On the last homework we already showed that such a field, if it exists, is unique up to isomorphism.)

3. Let ζ be a primitive 7-th root of unity, say $\zeta = e^{2\pi i/7}$. In this exercise we will analyze the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$.

   $\mathbb{Q}(\xi)$.

   (a) Show that the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$ is a Galois extension. What is $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$?

   (b) Show that the automorphism σ of E which sends ζ to ζ^3 generates $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$.

   (c) What is the subfield of $\mathbb{Q}[\zeta]$ that is fixed by the subgroup $\langle\sigma^2\rangle$ of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$?

4. Compute the Galois group of a splitting field for $X^5 - 2$ over $\mathbb{Q}$.

5. Let $K = \mathbb{Q}(\sqrt{a})$ where $a \in \mathbb{Z}$, $a < 0$. Show that K cannot be embedded in any extension L of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q})$ cyclic and of order divisible by 4.

Math 536 Homework 12
Spring 2016
Due: Friday, April 29

1. It is a fact that, if p is prime, then S_p is generated by a transposition and a p-cycle.

   (a) Show that if a polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible of prime degree p and has exactly $p-2$ real roots, then its Galois group is S_p. $\boxed{\text{Use Sylow}}$ (or Cauchy).

   (b) Find the Galois group G of $f(x) = x^5 - 6x + 3$ over $\mathbb{Q}$. (*Hints*: a) Find a transposition in the Galois group. b) Use calculus to analyze the graph of $f(x)$.)

2. What is the Galois group of the splitting field of each of the following polynomials?

   (a) $X^3 - X - 1$ over $\mathbb{Q}$.

   (b) $X^3 - 10$ over $\mathbb{Q}$. D_3

   (c) $X^3 - 10$ over $\mathbb{Q}(\sqrt{2})$. D_3

   (d) $X^3 - 10$ over $\mathbb{Q}(\sqrt{-3})$. C_3

   (e) $X^3 - X - 1$ over $\mathbb{Q}(\sqrt{-23})$.

3. Let p be an odd prime, and let ζ be a primitive p-th root of unity in $\mathbb{C}$ (for example, take $\zeta = e^{2\pi i/p}$). Let $E = \mathbb{Q}[\zeta]$, and let $G = \text{Gal}(E/\mathbb{Q})$. Show that $G = (\mathbb{Z}/p\mathbb{Z})^*$. Let H be the subgroup of index 2 in G. Put $\alpha := \sum_{i\in H} \zeta^i$ and $\beta := \sum_{i \in G-H} \zeta^i$. Show:

   $\boxed{H \text{ is unique since } (\mathbb{Z}/p\mathbb{Z})^* : \text{cyclic.}}$

   (a) α and β are fixed by H;

   (b) if $\sigma \in G - H$, then $\sigma\alpha = \beta, \sigma\beta = \alpha$.

   Use (a) and (b) to show that α and β are roots of the polynomial $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$. (?) Compute $\alpha\beta$ and show that the fixed field of H is $\mathbb{Q}[\sqrt{p}]$ when $p \equiv 1 \mod 4$ and $\mathbb{Q}[\sqrt{-p}]$ when $p \equiv 3 \mod 4$.

4. Let $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $E = M[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}]$ (subfields of $\mathbb{R}$).

   (a) Show that M is Galois over $\mathbb{Q}$ with Galois group the Klein 4-group $C_2 \times C_2$.

   (?) (b) Show that E is Galois over $\mathbb{Q}$ with Galois group the quaternion group.

$i + j = 0$, some $i \in H$, $j \in G - H$

$\iff -1$ is non-square mod p.

Math 536
Spring 2016
Practice Problems

1. Suppose that F is the splitting field of $f = x^4 - 11$ over $\mathbb{Q}$. Compute the Galois group G of F over $\mathbb{Q}$. D_4.

2. Let $K := \mathbb{Q}[\alpha]$ where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^6 + 3$.

   Prove that K is Galois over $\mathbb{Q}$ and determine its Galois group. Give explicit generators for all intermediate fields F with $\mathbb{Q} \subset F \subset K$.

   You may use the fact that $(1 \pm \sqrt{-3})/2$ are the primitive sixth roots of unity.

3. Let $f(x) = x^8 - 1$. Find the Galois group of $f(x)$ over each of the following fields:

   (a) The rational field $\mathbb{Q}$. $C_2 \times C_2$

   (b) The field $\mathbb{Q}(i)$. C_2

   (c) The field $\mathbb{F}_3$ of three elements. C_2.

4. Construct an extension field K of $\mathbb{Q}$ such that $K/\mathbb{Q}$ is Galois with Galois group the cyclic group of order 5.

5. Suppose that $\alpha \in \mathbb{C}$ with $\alpha^n = a \in \mathbb{Q}$ and such that $\mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ is Galois. Further suppose that F is the field containing $\mathbb{Q}$ generated by all the roots of unity in $\mathbb{Q}[\alpha]$. Show that $\mathrm{Gal}(\mathbb{Q}[\alpha] : F)$ is a cyclic group.

6. Let R denote the ring $\mathbb{Q}[x]$, and let N denote the R-module $R/(x^2+1)$. Further suppose that M and M' are finitely generated R-modules such that

$$M \oplus N \cong M' \oplus N.$$

   Prove that $M \cong M'$ as R-modules.

7. (a) Let K be a splitting field of $x^{48} - 1$ over $\mathbb{F}_9$, the field with 9 elements. Determine the cardinality of K and make a diagram showing all subfields of K and the inclusions between them. $|K| = 81$.

$$\begin{array}{c} K \\ \mid \; 2 \\ \mathbb{F}_9. \end{array}$$

   (b) How many roots does $(x^2-5)(x^3-7)$ have in K?

8. Let K be a field, and let L be an extension field of K. Let $u \in L$, and assume that the minimal polynomial of u over K is $x^n - a$ for some $a \in K$. Let $n = md$ for positive integers m, d.

   (a) Show that $[K(u^m) : K] = d$.

   (b) What is the minimal polynomial of u^m over K? $x^d - a$.

9. (a) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{F}_2[X]$ have and what are their degrees? 35, 1 of deg 1, 1 of deg 2, 3 of deg 4, 30 of deg 8.

   (b) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{Q}[X]$ have and what are their degrees? 8. $\leftarrow X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ irr over $\mathbb{Q}$.

   $\deg(\Phi_d(X)) = \phi(d)$.

$$\begin{array}{c} \mathbb{F}_{2^8} \\ \mid \\ \mathbb{F}_{2^4} \\ \mid \\ \mathbb{F}_{2^2} \\ \mid \\ \mathbb{F}_2, \end{array}$$