MA 542: Modern Algebra II / Spring 2023
Homework assignment #6
Due Friday 4/14/23

Final version.

Edited 4/8/23 to fix typo in (4b).

Edited 4/10/23 to give an option of simplifying (15) .

(1) For each finite simple field extension $L = K(\alpha)$ over K below, find the minimial polynomial $m(x)$ of α over K and determine how $m(x)$ factors in $L[x]$. Use this factorization to find the number of automorphisms in $\mathrm{Aut}(L/K)$.

Can you determine the group structure of $\mathrm{Aut}(L/K)$?

(a) $K = \mathbb{Q}$, $\alpha = \sqrt[6]{108}$
(b) $K = \mathbb{F}_5$, α is a root of $y^2 + 2y + 3$ in $\mathbb{F}_5[y]$
(c) $K = \mathbb{F}_2$, α is a root of $y^3 + y + 1$ in $\mathbb{F}_2[y]$ (Problem (13) on HW #3 may be helpful.)
(d) $K = \mathbb{Q}(t)$, $\alpha = t^{1/4}$
(e) $K = \mathbb{Q}(i, t)$, $\alpha = t^{1/4}$
(f) $K = \mathbb{F}_5(t)$, $\alpha = t^{1/3}$
(g) $K = \mathbb{F}_7(t)$, $\alpha = t^{1/3}$

Refresher on finite groups: Write up solutions to *at least three* of the problems (2)–(6). You do not need to write up solutions to all five, but you're responsible for understanding this material; come ask me if you get stuck. A lot of this material appears in BB 3.5 and 3.6.

Recall (or learn) that a *subgroup diagram* for a finite group G is a visual representation of the lattice of subgroups of G, where G is at the top, the trivial subgroup is at the bottom, and we connect subgroups with lines to indicate containment. See BB Examples 3.5.1, 3.5.2, 3.6.4, 3.6.5.

(2) The *cyclic* group $\mathbb{Z}_n$ is the additive group of the ring $\mathbb{Z}_n$.

(a) Prove that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.
(b) Make a subgroup diagram for $\mathbb{Z}_6$ and $\mathbb{Z}_{18}$.

(3) The multiplicative groups $\mathbb{Z}_n^\times$ is a finite abelian group with $\phi(n)$ elements. If n is prime then $\mathbb{Z}_n^\times$ is always cyclic.

(a) Prove that $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ if and only if $\gcd(m, n) = 1$.
(b) Make a subgroup diagram for $\mathbb{Z}_{15}^\times$ and $\mathbb{Z}_{25}^\times$.
(c) **Optional challenge problem:** When is $\mathbb{Z}_n^\times$ cyclic? See problems (3) and (4) on `https://math.bu.edu/people/medved/Teach/541F2019/541F2019_Cyclicity.pdf`.

(4) The *symmetric group* S_n is the group of order $n!$ of permutations of the indices $\{1, 2, \ldots, n\}$. To keep track of elements of S_n, we typically use cycle notation, which is described in Theorem 2.3.5 and Examples 2.3.6 and 2.3.7.

(a) Make a subgroup diagram for S_3. (Use cycle notation.)
(b) Prove that $H := \{e, (1\,2)(3\,4), (1\,3)(2\,4), ~~(1\,4)(2\,4)~~ (1\,4)(2\,3)\}$ is a normal subgroup of S_4.

Describe the quotient group S_4/H.

(c) **Optional challenge problem:** Show that the group of rotational symmetries of a cube is isomorphic to S_4.

(*Hint:* Show that permuting the four diagonals of the cube gives an injective map $\mathrm{Rot}(\mathrm{Cube}) \hookrightarrow \mathrm{Symm}(\mathrm{diagonals}) \simeq S_4$.)

(5) For $n \geq 2$, the *alternating group* A_n is the index-2 subgroup of S_n of even permutations of the indices $\{1, 2, \ldots, n\}$.

A permutation $\sigma \in S_n$ is *even* if it can be expressed as a product of an even number of *transpositions* (permutations of the form $(a\,b)$ for indices $a \neq b$); otherwise it is *odd*. It is a theorem that the map $\mathrm{sgn} : S_n \to \{\pm 1\}$ mapping σ to $\mathrm{sgn}(\sigma) := (-1)^k$ if $\sigma = \tau_1 \ldots \tau_k$, where τ_i are transpositions, is well defined. See Proposition 2.3.10 and Theorem 2.3.11.

(a) Make a subgroup diagram for A_4.

(b) Show that H from (4b) is a normal subgroup of A_4. Give the three cosets of H in A_4. What is the structure of A_4/H?

(c) Show that the group of rotational symmetries of a regular tetrahedron is isomorphic to A_4. (*Hint:* Consider the action on the four vertices.)

For $n \geq 5$ one can show that A_n is *simple* (that is, has no nontrivial proper normal subgroups): see Theorem 7.7.4. As a corollary, the group S_n is not *solvable* (Definition 7.6.1) if $n \geq 5$.

(6) The *dihedral group* D_n is the group of symmetries of a regular n-gon in the plane. The group D_n has $2n$ elements consisting of an index-2 cyclic subgroup of rotations

$$\langle r \rangle = \{1, r, \cdots, r^{n-1}\},$$

where r is the rotation in the plane by $360°/n$ counterclockwise (to fix ideas); and n order-2 flips, about axes of symmetry connecting vertices of the n-gon to midpoints of opposite sides (if n is odd) or vertices to opposite vertices and midpoints of opposite sides to each other (if n is even). If f is any such flip, one can show that $D_n = \{1, r, \ldots, r^{n-1}, f, fr, \ldots, fr^{n-1}\}$.

See Example 3.6.1 for a detailed analysis of $D_4 \simeq \mathrm{Symm}({}^3_4\square^2_1) \subseteq S_4$; and Example 3.6.3 for D_n more generally (with a for a rotation by $360°/n$ and b for a flip).

(a) Construct an explicit isomorphism to show that $D_3 \simeq S_3$.

(b) BB 3.6.20

Added 7 April 2023

Read BB sections 6.4, 6.5, and 8.2.

(7) BB 6.4.1(b)(d), 6.4.2(a)(d)

(8) BB 6.4.7

(9) BB 6.4.11

(10) BB 6.4.15

(11) BB 6.5.5

(12) BB 6.5.8

(13) BB 6.5.9

(14) BB 6.5.11

(15) BB 8.2.1. The *Galois group* of the irreducible polynomial $p(x)$ of $K[x]$ is the group we've been denoting $\mathrm{Aut}(L/K)$ for L is a splitting field for $p(x)$. Feel free to assume that $K = \mathbb{F}_p$.

(16) BB 8.2.5

Additional problems: solve these, but no need to write up or turn in.

- BB 6.4.6
- BB 6.4.14
- BB 6.5.3
- BB 6.5.10
- BB 8.2.2
- BB 8.2.3
- BB 8.2.6
- BB 8.2.7
- BB 8.2.10