Study guide

- Read Saracino, §13, up to the end of p. 125. Pages 126 through 129 are optional.
- (We are skipping §14 and §15.)
- Read Saracino §16, at least up to the definitions on pages 153–155 (axioms of a ring and basic terminology).
- Know the definition of the *kernel* of a group homomorphism.
- A slogan: normal subgroups are the same as kernels. Why is this?
- Isomorphismsm of groups is an equivalence relation. How do you prove this?
- Know the *fundamental theorem of group homomorphisms*, including its proof (to be covered Tuesday 11/10) and some examples.
- Definitions: *ring*, *multiplicative identity*, *multiplicative inverse*, *field*.

1. Read and understand the statement of Theorem 12.6 in the textbook, on images and inverse images of subgroups. Prove parts (ii) and (iii) (which are left as exercises in the book).

2. Suppose that $\phi : G \to H$ is a surjective group homomorphism, and that both G and H are finite groups. Prove that $|H|$ divides $|G|$.

3. Let G be an abelian group and let D be the subset of $G \times G$ consisting of elements of the form (g, g). Prove that $D \trianglelefteq (G \times G)$, and that $(G \times G)/D \cong G$ (use the fundamental theorem 13.2).

4. Let G denote the set of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, with $a, c \neq 0$ (these are called "upper triangular" matrices). This is a subgroup of $\mathrm{GL}(2, \mathbb{R})$ (you can assume this without proof). Let H denote the subset of G consisting of all elements in which $a = c = 1$.

   (a) Prove that H is a subgroup of G.

   (b) Use the fundamental theorem (13.2) to prove that

   $$G/H \cong (\mathbb{R} - \{0\}, \cdot) \times (\mathbb{R} - \{0\}, \cdot).$$

5. Suppose that G is a group of odd order, and $n \geq 2$ is an integer. Let $\phi : S_n \to G$ be a group homomorphism (where S_n is the symmetric group of degree n).

   (a) Prove that any transposition (2-cycle) is in $\ker \phi$.

   (b) Prove that ϕ must be the trivial homomorphism (i.e. $\phi(x) = e_G$ for all $x \in S_n$).

6. Let $\mathrm{Aut}\, G$ denote the set of all automorphisms of a group G, and let $\circ$ denote composition of functions (recall that an automorphism is an isomorphism from a group to itself). Prove that $(\mathrm{Aut}\, G, \circ)$ is a group. This is called the *automorphism group* of the group G.

Note The remaining problems concern some basics of *rings* and *fields*, which we only briefly defined on Thursday 11/5. You do not need any of the theory of rings yet; just work these using the definitions directly. They are on this week's set so that you can practice a bit with the axioms and gain some facility with them.

7. Let R be a ring. We will denote the additive identity (that is, the identity in the additive group $(R,+)$) by 0_R, or simply 0. By definition, this means that $a+0_R = 0_R + a = a$ for all $a \in R$. A ring is *not required to have* a multiplicative identity, but *if it does have one* it will be denoted 1_R, and the ring is called a *ring with unity*. By definition, 1_R is a multiplicative identity if $a1_R = 1_R a = a$ for all $a \in R$.

   (a) Prove that for all $a \in R$, $a\ 0_R = 0_R\ a = 0_R$. (This is Theorem 16.1(i) in the book; try to prove it yourself before reading the proof, but read the book's proof if you are stuck.)

   (b) Prove that if R has a multiplicative identity 1_R, then it is unique. That is, if 1_R and $1'_R$ are both multiplicative identity elements, then $1_R = 1'_R$.

   (c) Prove that if R is a ring with unity 1_R, then $(-1_R)\cdot a = -a$ for all $a \in R$. (Here, $-a$ denotes the additive inverse of a, i.e. the inverse in the additive group $(R,+)$.)

   (d) Let $a \in R$. An element $b \in R$ is called a *multiplicative inverse* of a if $ab = ba = 1_R$. Prove that if a has a multiplicative inverse, then it is unique. (Therefore going forward, we will denote the unique multiplicative inverse of a by a^{-1}.)

8. Let K denote the set of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Prove that K forms a field, when equipped with the usual addition and multiplication from $\mathbb{R}$.

9. Call an element a of a ring R *idempotent* if $a^2 = a$ (in a ring, a^2 is shorthand for $a \cdot a$). Call a ring *Boolean* if every element is idempotent. Prove that if R is a Boolean ring, then

   (a) for all $a \in R$, $a + a = 0_R$, and

   (b) R is commutative.

   Hint for (a): consider the expression $(a+a)^2$.