Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Solution Set 3

3.1 This problem is a review of the basic concepts from ring theory.

(a) Suppose R satisfies the definition of a ring, except that we drop the requirement that $+$ is commutative. Prove that $+$ must be commutative (so R is a ring, after all).

> Applying left and right distributivity separately to expand $(1+1)(a+b)$ yields
> $$a+b+a+b = (1+1)(a+b) = a+a+b+b$$
> and the claim instantly follows.

(b) Suppose S is a subring of the ring R. Prove that $S^\times \leq R^\times$. [*In applications of ring theory (e.g. to algebraic number theory) this is an extremely desirable property.*]

> It suffices to prove that $S^\times \leq R^\times$. Recall that to be a subring, the multiplicative identities of S and R must agree; let's call this identity 1. If $x \in S^\times$, then there exists $\overline{x} \in S^\times$ such that $x\overline{x} = 1$. But this implies that the same equality holds in R, whence $x \in R^\times$.

(c) Let $M_{2\times 2}(\mathbb{R})$ denote the ring consisting of all 2×2 matrices with real entries. Find a subset $S \subseteq M_{2\times 2}(\mathbb{R})$ such that S is a ring under the same addition and multiplication as $M_{2\times 2}(\mathbb{R})$, but isn't a subring of $M_{2\times 2}(\mathbb{R})$. Is $S^\times \leq M_{2\times 2}(\mathbb{R})^\times$ for your example?

> Let
> $$S := \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \right\}.$$
> This is easily checked to be a ring with multiplicative identity $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$. This disagrees with identity element of $M_{2\times 2}(\mathbb{R})$, which is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so S cannot be a subring. Moreover, we easily see that
> $$S^\times \not\leq M_{2\times 2}(\mathbb{R}),$$
> since for example the identity element $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ of S has determinant 0, hence cannot be a unit in $M_{2\times 2}(\mathbb{R})$.

(d) Prove that the only ring homomorphism from $\mathbb{Z}_6$ to itself is the identity map.

> Let $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_6$ be a ring homomorphism. Then $\varphi(0) = 0$ and $\varphi(1) = 1$, whence
> $$\varphi(n) = \varphi(\underbrace{1+1+\cdots+1}_{n\text{ times}}) = \underbrace{\varphi(1)+\varphi(1)+\cdots+\varphi(1)}_{n\text{ times}} = n.$$

(e) Find all $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_6$ which preserve addition and multiplication.

Note that any such φ must satisfy $\varphi(0) = 0$, since $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$. As in the previous part, since 1 generates $\mathbb{Z}_6$ additively, the map φ is completely determined by where it sends 1. Accordingly, any function $\mathbb{Z}_6 \to \mathbb{Z}_6$ that preserves addition must be one of $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_5$, where

$$\begin{aligned} \varphi_n : \mathbb{Z}_6 &\longrightarrow \mathbb{Z}_6 \\ a &\longmapsto an \pmod 6. \end{aligned}$$

If φ_n preserves multiplication, then

$$nab \equiv \varphi_n(ab) = \varphi_n(a)\varphi_n(b) \equiv n^2 ab,$$

whence $n \equiv n^2 \pmod 6$. This is easily seen to be satisfied iff $n = 0, 1, 3, 4$. Thus there are precisely four functions $\mathbb{Z}_6 \to \mathbb{Z}_6$ that preserve both addition and multiplication: φ_0, φ_1, φ_3, and φ_4. (Only one of these—φ_1—is a ring homomorphism though.)

(f) Suppose $\varphi : R \to S$ is a ring homomorphism. Prove that φ restricted to $R^\times$ is a *group* homomorphism from $R^\times \to S^\times$. Would this result still hold if we removed the requirement that $\varphi(1) = 1$ from the definition of ring homomorphism?

It's clear that φ restricted to $S^\times$ is a group homomorphism $S^\times \to R$, so it suffices to prove that $\varphi(S^\times) \subseteq R^\times$. If $x \in S^\times$ then there exists $\overline{x} \in S^\times$ such that $x\overline{x} = 1$, whence $\varphi(x)\varphi(\overline{x}) = \varphi(1) = 1$; it instantly follows that $\varphi(x) \in R^\times$.

If we remove the condition that $\varphi(1) = 1$, this is very false. For example, the constant zero map $\varphi(n) = 0$ trivially satisfies all the properties of a ring homomorphism apart from sending 1 to 1, but the image of φ consists of 0, which isn't a unit in R.

(g) Suppose $\varphi : R \to S$ is a ring homomorphism, and that $\ker\varphi$ is a subring of R. What can you conclude about the ring S?

By definition of *subring*, we deduce that $1 \in \ker\varphi$, or in other words, that $\varphi(1) = 0$. On the other hand, by definition of *ring homomorphism*, we know $\varphi(1) = 1$. Thus $1 = 0$ in S, whence for any $n \in S$ we have $n = n \cdot 1 = n \cdot 0 = 0$. In other words, $S = \{0\}$, the zero ring!

(h) Is $\mathbb{Z}$ an ideal of $\mathbb{R}$ (viewed as a ring)? Is $\mathbb{Z}$ an ideal of $\mathbb{Q}$ (viewed as a ring)?

No to both, because multiplication isn't 'swallowed': $1 \cdot \frac{1}{2} \in \mathbb{Z}$.

(i) Consider the set $I := \{f \in \mathbb{Z}[t] : f(0) \text{ is even}\}$. Prove that I is an ideal of the ring $\mathbb{Z}[t]$, but not a principal ideal. Find a minimal set of generators of I.

Here's a generator: $(2, t)$. (Minimal because non-principal.)

3.2 Let K be a field.

(a) Prove that $0x = 0$ for all $x \in K$, and that $xy = 0$ implies $x = 0$ or $y = 0$.

Evaluate $(0+0)x$ in two different ways. 2nd Q: WLOG say $x \neq 0$. Then $y = x^{-1}0 = 0$

(b) Prove that char K must either be 0 or prime.

Given any $k \in \mathbb{Z}$, we define an element $\widehat{k} \in K$ by

$$\widehat{k} := \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}}$$

(NOTE: this notation wasn't introduced in class!) Observe that $\widehat{k\ell} = \hat{k}\hat{\ell}$ for any $k, \ell \in \mathbb{Z}$. Now suppose char $K = n > 0$; this implies $\hat{n} = 0$. Writing $n = ab$ with a, b positive integers, we find

$$0 = \hat{n} = \hat{a}\hat{b}$$

By part (a), this means one of $\hat{a}$ or $\hat{b}$ is zero. In particular, if both a and b are smaller than n this would contradict the minimality of the characteristic. Hence the only factorization of n must be the trivial one, i.e. n must be prime.

(c) Given two fields K and K', prove that if char $K \neq$ char K' then there's no embedding of K into K'.

WLOG say $n :=$ char $K >$ char K'. Suppose $\varphi : K \to K'$ is a homomorphism. Then prove that $\varphi(0) = 0$ and $\varphi(1) = 1$. But this implies that $\varphi(\hat{n}) = 0 = \varphi(0)$, whence φ cannot be injective.

(d) Give an example of two non-isomorphic fields that have the same characteristic.

char $\mathbb{Q}$ = char $\mathbb{R}$, but there's no bijection between $\mathbb{Q}$ and $\mathbb{R}$, hence no isomorphism either.

3.3 Given a field K, define P_K to be the intersection of all subfields of K.

(a) Prove that P_K is a field.

Straightforward verification.

(b) If char $K = 0$, then P_K is isomorphic to a familiar field. Which one? Prove it.

$\mathbb{Q}$

(c) If char $K = p$, then P_K is isomorphic to a familiar field. Which one? Prove it.

$\mathbb{Z}_p$ aka $\mathbb{F}_p$.