Math 430 – Practice Final Solutions

April 28, 2016

1. (a)

   Solution. A *cyclic group* is a group G that is generated by a single element. Namely, there is some $g \in G$ with the property that, for every $h \in G$ there is an $m \in \mathbb{Z}$ with $h = g^m$.

   (b)

   Solution. Suppose that G has order p. Then every element of G has order dividing p by Lagrange's theorem. Since p is prime, the only divisors are 1 and p, and only the identity element has order 1. Thus there is some element g of order p. The powers of G

   $$1, g, g^2, \ldots, g^{p-1}$$

   are all distinct and there are p of them. Thus every element of G is a power of g, so G is cyclic.

2. Let

   $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$$

   (a)

   Solution.

   $$\begin{aligned} \sigma^{-1} &= \begin{pmatrix} 3 & 6 & 4 & 1 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix} \end{aligned}$$

   (b)

   Solution. $\sigma = (134)(26)$.

   (c)

   Solution. $\sigma = (14)(13)(26)$.

   (d)

   Solution. σ is odd, since it is the product of an odd number of transpositions.

   (e)

   Solution. The order of σ is the least common multiple of the lengths of the cycles in its disjoint cycle decomposition, namely $\operatorname{lcm}(2, 3) = 6$.

3.

Solution. Suppose H is a subgroup of S_3. Then H contains the identity ρ_0. If H contains ρ_1 then it contains $\rho_2 = \rho_1^2$ and vice versa. Each μ_i has order 2, so H could be just $\{\rho_0, \mu_i\}$ for some i.

By Lagrange's theorem, the number of elements in H is either $1, 2, 3$, or 6, so once H contains four elements it must be all of S_3. If H contains two μs then it contains their product, which is either ρ_1 or ρ_2. We must then have $H = S_3$. Similarly, if H contains all ρs and a μ then we must have $H = S_3$.

As usual, the trivial subgroup and the whole group are normal. Moreover, $\{\rho_0, \rho_1, \rho_2\}$ is normal since it has index 2. The subgroups of order 2 are not normal since $(12)(13)(12) = (23)$, $(23)(12)(23) = (13)$ and $(13)(23)(13) = (12)$, so in each case there is some $g \in S_3$ with $g\mu_i g^{-1} \notin \{\rho_0, \mu_i\}$.

In summary the subgroups are

$$\begin{aligned}
&\{\rho_0\} \text{ (normal)},\\
&\{\rho_0, \mu_1\} \text{ (not normal)},\\
&\{\rho_0, \mu_2\} \text{ (not normal)},\\
&\{\rho_0, \mu_3\} \text{ (not normal)},\\
&\{\rho_0, \rho_1, \rho_2\} \text{ (normal)},\\
&S_3 \text{ (normal)}.
\end{aligned}$$

4. (a)

   Solution. A *zero divisor* a in a ring R is a nonzero element of R so that there is some other nonzero element $b \in R$ with $ab = 0$.

   (b)

   Solution. A *unit* u in a ring R with unity is an element $u \in R$ so that there is some other element $v \in R$ with $uv = 1$.

   (c)

   Solution. Units: $1, 3, 7, 9$. Zero divisors: $2, 4, 5, 6, 8$. Note that 0 is not a zero divisor.

5. (a)

   Solution. $x^2 - 2$ is irreducible because $\sqrt{2}$ is not rational (or by Eisenstein's criterion for $p = 2$).

   (b)

   Solution. $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ so it is reducible. We can use the intermediate value theorem to prove this rigorously: $0^2 - 2 < 0$ and $2^2 - 2 > 0$ so there is a square root of 2 in $\mathbb{R}$.

   (c)

   Solution. Since $3^2 - 2 \equiv 0 \pmod 7$, it is reducible.

   (d)

   Solution. Let $f(x) = x^4 + x^2 + 1$. It has no roots since $x^4 \geq 0$ and $x^2 \geq 0$ for all $x \in \mathbb{R}$. Suppose

   $$f(x) = (x^2 + ax + b)(x^2 + cx + d).$$

   Then

   $$\begin{aligned}
   a + c &= 0,\\
   b + ac + d &= 1,\\
   ad + bc &= 0,\\
   bd &= 1.
   \end{aligned}$$

   So $c = -a$ and $d = 1/b$ from the first and last equations. The third equation then implies $a/b - ab = 0$ so $a = 0$ or $b = \pm 1$. If $a = 0$, the second equation implies $b + 1/b = 1$ so

$b^2 - b + 1 = 0$, which has no real roots. If $b = d = -1$, the second equation implies $-a^2 = 3$, which has no real roots. If $b = d = 1$, the second equation implies $-a^2 = -1$, so $a = \pm 1$. Thus

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$$

is reducible.

(e)

Solution. The factorization in part (d) holds in $\mathbb{Z}[x]$ and thus determines a factorization in $\mathbb{Z}_2[x]$ by reducing the coefficients modulo 2. So

$$x^4 + x^2 + 1 = (x^2 + x + 1)^2$$

is reducible.

(f)

Solution. Evaluating this polynomial at $x = 1$ yields $1 + 1 + 1 + 1 = 0$, so it is reducible.

6. (a)

Solution. Since $\sqrt{2} \in \mathbb{R}$, S is a subset of $\mathbb{R}$. The sum of two elements

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

is again an element of S, as is the product of two elements

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

and the negation of an element

$$-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}.$$

Finally, the inverse of an element is an element of S as well:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

(b)

Solution. We first show that $\langle x^2 - 2 \rangle \subseteq \mathcal{I}$. Suppose $f(x) = (x^2 - 2)g(x) \in \langle x^2 - 2 \rangle$. Then $f(\sqrt{2}) = ((\sqrt{2})^2 - 2)g(\sqrt{2}) = 0$, so $f \in \mathcal{I}$.
Now suppose that $f(x) \in \mathcal{I}$, so that $f(\sqrt{2}) = 0$. Since $\sqrt{2}$ is a root of f, we may factor $f(x) = (x - \sqrt{2})g_1(x)$ for some $g_1(x) \in S[x]$.
Consider the map $\sigma : S[x] \to S[x]$ which maps each coefficient $a + b\sqrt{2}$ to $a - b\sqrt{2}$. It is a ring homomorphism, and thus

$$\begin{aligned} \sigma(f) &= \sigma(x - \sqrt{2})\sigma(g_1) \\ f &= (x + \sqrt{2})\sigma(g_1), \end{aligned}$$

since $f \in \mathbb{Q}[x]$ and is thus fixed by σ. Therefore $f(-\sqrt{2}) = 0$, so $f(x)$ is divisible by $x + \sqrt{2}$. We can thus factor

$$f(x) = (x - \sqrt{2})g_1(x) = (x - \sqrt{2})(x + \sqrt{2})g_2(x) = (x^2 - 2)g_2(x).$$

Thus $\mathcal{I} \subseteq \langle x^2 - 2 \rangle$, so in fact the two ideals are equal.

(c) Define a map $\phi : \mathbb{Q}[x] \to S$ by

$$\phi(f) = f(\sqrt{2}).$$

By part (b), the kernel of ϕ is $\langle x^2 - 2\rangle$. Moreover, ϕ is surjective since $\phi(a + bx) = a + b\sqrt{2}$. So by the first isomorphism theorem, S is isomorphic to $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

7. (a)

Solution. A *principal ideal* in a commutative ring R with unity is an ideal I of the form $\langle a\rangle = \{ra : r \in R\}$ for some $a \in R$.

(b)

Solution. Suppose $I \subset \mathbb{Z}$ is an ideal. If $I = 0$ then $I = \langle 0\rangle$ is principal. Otherwise, there is some positive element of I since I is closed under negation; let a be the smallest positive element of I. I claim that $I = \langle a\rangle$.

Certainly $\langle a\rangle \subseteq I$: $na \in I$ for all $n\mathbb{Z}$ since I is an ideal and $a \in I$. Suppose that $b \in I$. Using the division algorithm, we may write $b = qa + r$ with $0 \le r < a$. Then $r = b - qa \in I$. But we chose a to be the smallest positive element of I, so we must have $r = 0$. Therefore $b = qa \in \langle a\rangle$ and $I \subseteq \langle a\rangle$.

8. (a)

Solution. A *greatest common divisor* of two elements a, b in an integral domain R is an element $d \in R$ so that $d \mid a$ and $d \mid b$, and if $e \in R$ is any other element with $e \mid a$ and $e \mid b$ then $e \mid d$.

(b)

Solution. Let $I = \langle a, b\rangle = \{ra + sb : r, s \in R\}$ be the ideal generated by a and b. Since R is a PID, there is some element $d \in R$ with $\langle a, b\rangle = \langle d\rangle$. I claim that d is a greatest common divisor of a and b.

Since $a \in \langle d\rangle$ we have $d \mid a$, and likewise for b. Now suppose $a = xe$ and $b = ye$. Since $\langle a, b\rangle = \langle d\rangle$, there are elements $r, s \in R$ with $d = ra + bs$. Then

$$d = ra + bs = (rx + sy)e,$$

so $e \mid d$.