MORE HW ANSWERS IN 3340, SPRING 2017

ALLEN KNUTSON

HW #8 due 3/30. 4.1 #2. The coefficient on x^n is not zero, and all later coefficients are arbitrary, so $(p-1)p^n$.

4.1#5.

#6. Every number but 0 is a root, by Cauchy's theorem.

#14. The inverse of such a matrix is $\begin{bmatrix} c & d \\ 2c & d \end{bmatrix}$ where $(c,d) = (a,-b)/(a^2-2b^2)$, i.e., it's another matrix in the same set. Note that we're not dividing by zero because $\sqrt{2}$ is irrational.

4.2 #8. $f = q_1g_1 + r_1$, $q_1 = q_2g_2 + r_2$, hence $f = (q_2g_2 + r_2)g_1 + r_1 = q_2g_1g_2 + (r_2g_1 + r_1)$. Note $\deg r_1 < \deg g_1$ and $\deg r_2 < \deg g_2$, hence

$$\begin{aligned} \deg(r_2g_1 + r_1) &\leq \max(\deg r_2g_1, \deg r_1) \\ &= \max(\deg r_2g_1, \deg r_1) \\ &< \max(\deg g_2 + \deg g_1, \deg g_1) \\ &\leq \deg g_2 + \deg g_1 = \deg(g_1g_2) \end{aligned}$$

so $r_2g_1 + r_1$ must be the remainder.

#9. The remainder has to be degree ≤ 1, so $bx + c$. Hence

$$\begin{aligned} f(x) &= (x-a)^2m + bx + c \\ f'(x) &= 2(x-a)m + (x-a)^2m' + b \\ f(a) &= ba + c \\ f'(a) &= 0 + 0 + b \end{aligned}$$

Together, $bx + c = b(x-a) + ab + c = f'(a)(x-a) + f(a)$.

#11. Let $\tau = \exp(2\pi i/6)$, so $x^6-1 = (x-1)(x+1)(x-\tau)(x-\tau^5)(x-\tau^2)(x-\tau^4)$. The last four come in complex conjugate pairs, so combine to give $(x-\tau)(x-\tau^5) = x^2-(\tau+\bar{\tau})x+|\tau|^2 = x^2-x+1$ and $(x-\tau^2)(x-\tau^4) = x^2-(\tau^2+\bar{\tau}^2)x+|\tau^2|^2 = x^2+x+1$.

HW #9 due 4/13. 5.1 #1. a,d. b isn't closed under +, c isn't closed under times.

#3. a, c, d, e

#9. It's actually $(Z_2)^I$ as a ring.

#11. First, $a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$ so $0 = ab+ba$. But $(1+1)^2 = 1+1$ says $0 = 2$, so these rings have characteristic 2, i.e. $ba = -ba$, which is ab.

Date: May 21, 2017.

5.2 #2. Let I be the kernel. If $I \neq 0$, then $I \ni a \neq 0$, hence for all $f \in F$, $I \ni a(a^{-1}f)$, but then $I = F$.

#3. By #2 the image is a copy of F, or $\{0_E\}$. But $1_F \mapsto 1_E$, and since E is a field, $1_E \neq 0_E$. Hence the image is not just 0_E. Hence the image, assumed to be E, is a copy of F.

#13. Each solution of $x^2 = x$ in $\mathbb{Z} \oplus \mathbb{Z}$, namely $(0,0), (1,0), (0,1), (1,1)$ must map to a solution of in $\mathbb{Z}$, namely $0, 1$. We know that $(0,0) \mapsto 0$ and $(1,1) \mapsto 1$. So either $(1,0) \mapsto 0$ and $(0,1) \mapsto 1$ or vice versa, i.e. $(a,b) \mapsto b$ or $(a,b) \mapsto a$ respectively.

5.3 #9. If I is a prime ideal but not maximal, then $(\mathbb{Z} \oplus \mathbb{Z})/I$ is a domain but not a field. Since $\mathbb{Z} \oplus \mathbb{Z}$ is not a field, I cannot be 0.

If I contains an element (a,b) then $I \geq \mathbb{Z}a \oplus \mathbb{Z}b$; if $a, b \neq 0$ then the quotient has size $\leq ab$, but any finite domain is a field. So I can't contain such elements.

If I contains only elements of the form $(a,0)$, then $I = n\mathbb{Z} \oplus 0$ for n the GCD of those $\{a\}$. Then the quotient is $\mathbb{Z}/n \oplus \mathbb{Z}$, which is a domain only if $n = 1$.

Hence the only possibilities are $I = \mathbb{Z} \oplus 0$ and the reverse case, $0 \oplus \mathbb{Z}$.

#11. $x \in Ann(a) \iff xa = 0 \implies rxa = 0 \iff rx \in Ann(a)$ Not to mention $Ann(a)$ being closed under addition and subtraction.

#12a. If $a^n = 0$, then $(ra)^n = r^n a^n = r^n 0 = 0$. If $a^n = 0$ and $b^m = 0$, then $(a+b)^{m+n} = \sum_k \binom{m+n}{k} a^k b^{m+n-k}$, and for each k, either $k \geq m$ or $m + n - k \geq n$, i.e. each term on the RHS dies. Hence $a + b$ is also nilpotent.

b. Let $x \in R$, $\bar{x} := x + N \in R/N$. If $(\bar{x})^n = 0_{R/N}$, then $x^n \in N$, i.e. for some m we have $(x^n)^m = 0$. But then $x^{mn} = 0$, i.e. $x \in N$ also. Hence $\bar{x} = 0$.

c. If P is prime, then R/P is a domain, so has no zero divisors. Any nilpotent is a zero divisor, so any nilpotent in R/P must be 0. Upstairs, any nilpotent in R must be in P. Hence $P \supseteq N$.

HW #10 due 4/20. 4.3 #3. Using F's multiplication, $e_F^2 - e_F = 0$. Hence the same is true in E's multiplication. Take this equation and factor it in E: $e_F(e_F - e_E) = 0$. Since $e_F \neq 0$ in F, they're different in E, so we can multiply by the inverse of e_F, and learn $e_F - e_E = 0$.

#8. Use the evaluation homomorphism $x \mapsto \sqrt{2}i$.

#10. Embed the second ring in $\mathbb{C}$ as $\mathbb{Q}[i]$, taking $x \mapsto i$, for convenience. Call the two coset of the first $\bar{x}$, so $\bar{x}^2 = -2$ in the first ring.

Let ϕ be such an isomorphism. Then $0 = \phi(x^2 - 2) = \phi(x)^2 - 2$, i.e. $\phi(x) = \pm\sqrt{2}i$. But then the second ring has $\sqrt{2}i$ and i hence has $\sqrt{2}$, whereas its intersection with $\mathbb{R}$ is $\mathbb{Q}$ so cannot, contradiction.

#14. The first is the usual Pythagoras thing. If ϕ were such an isomorphism, then $0 = \phi(\sqrt{3}^2 - 3) = \phi(\sqrt{3})^2 - 3$ but by the first part there are no numbers doing that in the second field.

5.4 #4. This map is $1:1$, so an isomorphism with the image. If D is not a field, then the image can't be the whole $Q(D)$ since that is a field. Conversely, if D is a field, then the map is onto, so an isomorphism.

#6a. The homomorphism is given; one has to check that it's a homomorphism (which is straightforward) and well-defined (likewise).

b. The map $Q(D_1) \to Q(D_2)$ wouldn't be $1:1$, which is impossible since $Q(D_1)$ is a field.

#8. This is a subring of $\mathbb{Q}$, hence a domain. It contains $\mathbb{Z}$, so its fractions contain $\mathbb{Q}$, hence equal $\mathbb{Q}$.

#13. The question is whether this is well-defined – i.e. from $\frac{a}{b} = \frac{ac}{bc}$, does $\bar{\partial}(\frac{a}{b}) = \bar{\partial}(\frac{ac}{bc})$. Well,

$$\begin{aligned}
\bar{\partial}(\frac{ac}{bc}) &= (bc\partial(ac) - ac\partial(bc))/(bc)^2 \\
&= (b(\partial(a)c + a\partial(c)) - a(\partial(b)c + b\partial(c))/(b^2c) \\
&= (b(\partial(a)c) - a(\partial(b)c)/(b^2c) \\
&= (b(\partial(a)) - a(\partial(b))/b^2 \\
&= \bar{\partial}(\frac{a}{b})
\end{aligned}$$

HW #11 due 5/4. 6.1 #1. They satisfy (a) x^2-2, (b) x^2-n, (c) $(x+\sqrt{3}+\sqrt{5})(x+\sqrt{3}-\sqrt{5})(x-\sqrt{3}+\sqrt{5})(x-\sqrt{3}-\sqrt{5}) = ((x+\sqrt{3})^2-5)((x-\sqrt{3})^2-5) = ((x^2+2x\sqrt{3}+3)-5)((x^2-2x\sqrt{3}+3)-5) = (x^2-2+2x\sqrt{3})(x^2+2-2x\sqrt{3}) = (x^2-2)^2-12x^2$, (d) $(x^2-2)^2-3$, (e) $(2x+1-\sqrt{3}i)(2x+1+\sqrt{3}i) = (2x+1)^2+3$, (f) $(x-\sqrt[3]{2}-\sqrt{2})(x-ct+\sqrt{2})(x-\sqrt[3]{2}\omega-\sqrt{2})(x-ct\omega+\sqrt{2})(x-\sqrt[3]{2}\omega^2-\sqrt{2})(x-ct\omega^2+\sqrt{2}) = ...$

#3. If $f(x) = \sum_{i=1}^{n} c_i x^i$, and $f(u) = 0$, then let $g(x) = f(x-a) = \sum_{i=1}^{n} c_i (x-a)^i$, and obtain $g(u+a) = 0$.

#7. Since $E \neq K$, there is some $e \in E \setminus K$, hence $e \in F = K(u)$ and can be written $p(u)/q(u)$ where p, q have coefficients in K. Therefore $p(x) - q(x)e$ is a polynomial equation that u satisfies, with coefficients in $K(e) \leq E$. That wouldn't be impressive if this were the zero polynomial, but it's not because $q(u) \neq 0$ and $e \notin K$.

6.2 #2(a) $2, \{1, \sqrt{3}\}$. (b) $2, \{1, \sqrt{3}\}$. (c) $1, \{1\}$.

#5. Consider the degrees of the extensions

$$\begin{array}{ccc} & F[x]/\langle f(x)\rangle & \\ F & & K[x]/\langle f(x)\rangle \\ & K & \end{array}$$

The degree $[F[x]/\langle f(x)\rangle : K]$ is divisible by $[F:K]$ and $[K[x]/\langle f(x)\rangle : K]$, which by assumption are relatively prime, hence is divisible by their product. But we can generate it using products of basis elements from the two, so it can't be larger: that degree must be equal to the product. Hence $[F[x]/\langle f(x)\rangle : F] = [K[x]/\langle f(x)\rangle : K] = \deg f$, and therefore $f(x)$ is irreducible in $F[x]$.

6.5 #5. These cubic polynomials would have a linear factor if they factored, hence a root in $\mathbb{F}_3$, but we check the three possibilities and don't find any roots.

Let's call the numbers in the quotients a and b, to avoid confusion, so $a^3 - a - 1 = b^3 - b + 1 = 0$. Then their powers are

$$1, a, a^2, a+1, a^2+a, a^2+a+1, a^2-a+1, -a^2-a+1, -a^2-1, a-1, a^2-a, -a^2+a+1, a^2-1$$

$$1, b, b^2, b-1, b^2-b, -b^2+b-1, b^2+b+1, b^2-b-1, -b^2-1, b+1, b^2+b, b^2+b-1, b^2-1,$$
$$-1, -b, -b^2, -b+1, -b^2+b, b^2-b+1, -b^2-b-1, -b^2+b+1, b^2+1, -b-1, -b^2-b, -b^2-b+1, -b^2+1, 1$$

i.e. a is order 13 in the multiplicative group, but b is order 26. Hence a will have to be b^2 raised to some power relatively prime to 13. The choices turn out to be $7, 8, 11$.

HW #12 due Tuesday 5/9. 6.4 #1. (a) $\mathbb{Q}[\sqrt{2}]$ (b) $\mathbb{Q}[\sqrt{3}i]$ (c) $\mathbb{Q}[\sqrt{2}i, \sqrt{3}]$ (d) $\mathbb{Q}[\sqrt[3]{5}, \exp(2\pi i/3)]$

#5. Just Z_p; every element is a root already.

#14a. It factors completely, and generates that field. (b) Ditto.

8.1 #2. Let's present it as $F_3[x]/\langle x^3 - x - 1\rangle$, so $1, x, x^2$ are a basis. The Galois group is of size 3, and is generated by the Frobenius $u \mapsto u^3$, i.e. the other nontrivial element is $u \mapsto u^9$.

#6. Its elements are given by $\sqrt{2} \mapsto \pm\sqrt{2}$, $i \mapsto \pm i$ (independent choices).

#7. Let $\sigma : E \to F$ be an isomorphism. Then $\rho \mapsto \sigma\rho\sigma^{-1}$ is an isomorphism of $Gal(E/K) \to Gal(F/K)$, with inverse $\tau \mapsto \sigma^{-1}\tau\sigma$.